



A MITEL
PRODUCT
GUIDE

Unify OpenScape WLAN Phone WL4

Configuration Manual
08/2024

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. 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"), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively "Unify") or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

© Copyright 2024, Mitel Networks Corporation

All rights reserved

Contents

1 Introduction.....	8
1.1 Target Group.....	8
1.2 Prerequisites.....	8
1.3 General Recommendations.....	8
1.4 GDPR Considerations.....	9
2 Handset Deployment.....	10
2.1 Deployment Methods.....	10
2.2 Prerequisites to Handset Deployment.....	10
2.3 Deploy Handsets Using the WSG DM.....	11
2.4 Deploy Handsets Using WinPDM.....	12
2.5 Deploy Handsets Using the Admin Menu.....	13
2.6 Work with Templates.....	13
2.6.1 Create a Template.....	14
2.6.2 Create a Network Template in WinPDM.....	14
2.6.3 Apply a Template to a Handset without a Number.....	15
2.6.4 Apply a Template to a Handset with a Number.....	16
2.6.5 Save Handset Configuration as a Template.....	16
2.7 Create Numbers.....	17
2.8 Assign a Number to a Handset.....	17
2.9 Handset Configuration.....	18
2.10 Handset Synchronization.....	19
3 Parameter Configuration.....	20
3.1 Network Settings.....	20
3.1.1 Change the Active Network.....	20
3.1.2 Change the Network Name.....	20
3.1.3 Automatic Switch between the Networks.....	20
3.1.4 SSID.....	21
3.1.5 Handset IP Address Settings.....	21
3.1.5.1 DNS Server Settings.....	22
3.1.6 Security Settings.....	22
3.1.6.1 Open Authentication.....	22
3.1.6.2 WPA/WPA2-Personal and WPA3-Personal.....	22
3.1.6.3 WPA2-Enterprise and WPA3-Enterprise.....	23
3.1.6.4 Allow Outdated Security Protocols.....	24
3.1.6.5 WinPDM Authentication.....	24
3.1.7 Radio and Channel Selection.....	25
3.1.7.1 5 GHz Channels.....	25
3.1.7.2 2.4 GHz Channels.....	26
3.1.7.3 Advanced 802.11 Channels.....	27
3.1.7.4 802.11k Neighbor List.....	27
3.1.8 Configure Regulatory Domain.....	27
3.1.9 IP DSCP for Voice and Signaling.....	28
3.1.10 TSPEC Call Admission Control.....	28
3.1.11 Roaming Method.....	29
3.1.12 A-MPDU Packet Aggregation.....	29
3.1.13 Deauthenticate on Roam.....	29
3.2 Unite Module Settings.....	29
3.2.1 IP Address and Password to the Unite Module.....	29
3.2.2 Connection Mode.....	30

3.2.3 Server Certificate Validation.....	30
3.2.4 Websocket Authentication.....	31
3.2.5 Websocket Client Certificate.....	31
3.2.6 Contacts.....	31
3.2.6.1 Import Contacts.....	31
3.2.6.2 Company Phonebook.....	32
3.2.6.3 Central Phonebook.....	33
3.3 Handset Settings.....	33
3.3.1 Key Lock and Phone Lock Settings.....	33
3.3.1.1 Automatic Key Lock.....	33
3.3.1.2 Automatic Key Unlock.....	34
3.3.1.3 Phone Lock.....	34
3.3.1.4 Automatic Lock Time.....	35
3.3.2 Display.....	35
3.3.2.1 Hide Menu Items.....	35
3.3.2.2 User Display Text and Number.....	35
3.3.2.3 Rotate Display Text.....	36
3.3.2.4 Font Style.....	36
3.3.2.5 Backlight Timeout.....	36
3.3.2.6 Brightness.....	36
3.3.2.7 Screen Saver.....	36
3.3.3 Regional Settings.....	37
3.3.3.1 Set Time & Date.....	37
3.3.3.2 Select Default Language and Writing Language.....	38
3.3.3.3 Dialing Tone Pattern.....	38
3.3.4 Audio Settings.....	38
3.3.4.1 Prevent Handset from Being Muted.....	39
3.3.4.2 Hearing Aid.....	39
3.3.4.3 Ring Signal in Handset.....	39
3.3.4.4 Gain Offset Calibration.....	39
3.3.5 Headset Configuration.....	40
3.3.5.1 Headset Type.....	40
3.3.5.2 Headset User Model.....	40
3.3.5.3 Call with a Headset.....	40
3.3.6 Shared Phone.....	41
3.3.7 Shortcuts.....	41
3.3.7.1 Configure Hot and Navigation Keys.....	42
3.3.7.2 Shortcut Functions.....	43
3.3.7.3 Multifunction Button.....	43
3.3.8 Messaging Settings.....	44
3.3.8.1 Configure Message Alerts with Beep Codes.....	46
3.3.8.2 Examples of TTR and TTP Settings.....	48
3.3.8.3 Message Retransmit Limit.....	51
3.3.8.4 Message Templates.....	52
3.3.9 In Charger Actions and Behavior.....	53
3.3.9.1 Quick Answer.....	53
3.3.9.2 In Charger Action when Not in Call.....	53
3.3.9.3 Clear Lists in Charger.....	54
3.3.9.4 USB Behavior.....	54
3.3.9.5 Show and Indicate Messages in Charger.....	54
3.3.10 Handset and Battery Warnings.....	55
3.3.10.1 No Network Warning.....	55
3.3.10.2 No Access Warning.....	56
3.3.10.3 Dialog Window for No Network/No Access Warnings.....	56
3.3.10.4 Battery Warning.....	57
3.3.11 System Administration in the Handset.....	57

3.3.11.1 Block Access to the Admin Menu.....	58
3.3.11.2 Admin Menu Tree in the Handset.....	59
3.3.11.3 Quick Access to Admin Menu Functions and Device Information.....	60
3.3.11.4 Change Admin Access Code.....	60
3.3.11.5 Transfer Unlock File.....	61
3.4 Location.....	61
3.4.1 Enable BLE Location.....	62
3.4.2 Configure Handset for Cisco MSE or AiRISTA Flow RTLS.....	62
3.5 Telephony.....	63
3.5.1 VoIP.....	63
3.5.1.1 VoIP Protocol.....	63
3.5.1.2 Endpoint ID and Endpoint Number.....	66
3.5.1.3 Import Trust and Application Certificates.....	67
3.5.1.4 Replace Call Rejected with User Busy.....	67
3.5.1.5 ICE Negotiation.....	68
3.5.1.6 Codec Configuration.....	68
3.5.1.7 Offer Secure RTP.....	69
3.5.1.8 Internal Call Number Length.....	69
3.5.2 Call Waiting Behavior and Sound.....	69
3.5.3 Allow Blind Transfer.....	70
3.5.4 Soft Key Functions During Call.....	70
3.5.5 Dial Pause Time.....	71
3.5.6 Code for Call Completion.....	71
3.5.7 Code for Hiding Call ID.....	71
3.5.8 Calling Line Identification Restriction (CLIR).....	72
3.5.9 Hide Missed Call Window.....	72
3.5.10 Prevent Calls from Being Saved in the Call List.....	72
3.5.11 Voicemail Service.....	72
3.5.12 Emergency Call Numbers.....	73
3.5.13 OpenScape 4000 Busy Actions.....	73
3.5.14 Pickup Groups.....	74
3.6 Services.....	74
3.7 Alarm Settings.....	75
3.7.1 Common Alarm Settings.....	75
3.7.2 Push-button and Test Alarms.....	76
3.7.3 Man-down and No-movement Alarms.....	78
3.7.4 Emergency Call Alarm.....	79
3.7.5 Call Predefined Number without Sending Alarm.....	79
3.8 Push-to-Talk Group Call.....	79
3.8.1 Configure a PTT Call.....	79
3.8.2 PTT Call Disconnect Warning.....	80
3.9 Profiles.....	80
3.9.1 User Profiles.....	80
3.9.1.1 Configure Sound and Alerts.....	81
3.9.1.2 Configure Presence and Diversion.....	82
3.9.1.3 Configure Answering.....	83
3.9.1.4 Configure Alarm Settings.....	83
3.9.1.5 Configure Soft Keys.....	84
3.9.2 System Profiles.....	84
3.9.2.1 Configure Sounds and Alerts Groups (Sub-group).....	85
3.9.2.2 Configure Presence Groups (Sub-group).....	86
3.9.2.3 Configure Answering Groups (Sub-group).....	87
3.9.2.4 Configure Alarm Settings Group (Sub-group).....	87
3.9.2.5 Configure Soft Key Groups (Sub-group).....	88
3.9.2.6 Configure Idle Display Groups (Sub-group).....	89
3.9.2.7 Create System Profile Using Predefined Sub-Groups.....	89

3.9.2.8 Activate and Deactivate System Profile.....	90
4 System Deployment Planning.....	92
4.1 Show RSSI.....	92
4.2 Scan the Channels.....	93
4.3 Range Beep.....	94
4.4 Location Survey.....	94
4.5 BLE Beacon Scan.....	95
5 Maintenance.....	97
5.1 Handset Software Upgrade.....	97
5.1.1 Upgrade Software Using WinPDM.....	97
5.1.2 Upgrade Software using WSG DM.....	97
5.2 Upgrade Handset Functionality Using Licenses.....	98
5.2.1 Automatic License Upgrade.....	98
5.2.2 Upgrade License Using Import/Export.....	99
5.2.3 Manual License Upgrade.....	99
5.2.4 Move License.....	99
5.3 Perform a Factory Reset.....	101
5.4 Handset Replacement.....	101
5.4.1 Replace the Handset using WSG DM.....	102
5.4.2 Replace the Handset using WinPDM.....	103
5.4.3 Parameter Migration.....	104
5.5 Change the Number of a Handset.....	105
5.6 Change the WLAN Security Mode in Existing Installation.....	105
5.7 Create a Configuration Backup.....	106
6 Troubleshooting.....	107
6.1 Operational Problems.....	107
6.2 Warning Messages.....	109
6.3 Logging.....	115
6.3.1 Syslog.....	115
6.3.2 PCAP and Remote PCAP Capturing.....	116
6.3.3 Save Logs.....	116
6.3.4 Send Logs over SFTP.....	117
6.3.5 Trace Configuration.....	117
6.3.6 Low Level WLAN debug.....	118
6.3.7 SNMP.....	118
7 Related Documents.....	120
8 Document History.....	121
9 Configure Custom Sounds.....	123
9.1 Customize the Default Handset Beeps.....	125
10 Easy Deployment.....	127
10.1 Prerequisites for Easy Deployment.....	127
10.2 WLAN Discovery.....	128
10.3 Unite Module Discovery.....	129
10.3.1 Server Discovery Using the DHCP Option 43.....	129
10.3.2 Server Discovery Using the Ascom Service Discovery Protocol (ASDP).....	130
10.4 Easy Deployment and VLAN.....	130
10.5 Easy Deployment and Certificates.....	131
10.6 Parameter Download.....	132
10.7 DHCP Related.....	133
10.7.1 DHCP Vendor Options Explained.....	133
10.7.1.1 The Vendor 43 Option Field Explained According to the RFC.....	135

10.7.2 Configuration Example of a Linux Server Using DHCP Option 43.....	138
10.7.3 Configuration Example of an MS Windows 2003 Server.....	138
10.7.3.1 Define New Vendor Class to Support Multiple Types of Clients.....	141
10.7.3.2 Configure Sub-options for a Vendor Class in an MS Windows 2003 DHCP Server.....	142
10.7.3.3 Troubleshooting Easy Deployment in an MS 2003/2008 DHCP Server.....	143
10.7.4 Configure DHCP Options in a Cisco Device Running the Cisco IOS DHCP Server.....	143
11 SCEP.....	145
11.1 Configure SCEP Using WinPDM/WSG DM.....	146
11.2 Configure SCEP Using DHCP Option 43.....	146

1 Introduction

This document contains detailed information accompanied with easy-to-follow instructions on how to deploy, maintain, and configure Unify OpenScape WLAN Phone WL4 to function in a VoWiFi system. This document also provides guidelines on how to identify some of the most common problem areas and suggests approaches for troubleshooting.

This document describes how to configure the handset using the WinPDM/WSG DM . Configuration using the handset's menu is out of scope of this document and not described here except for the cases when configuration is performed using the Admin menu. For the details, please refer to *Unify OpenScape WLAN Phone WL4, User Manual, TD 93342EN* .

This version of the document provides configuration procedures for handsets running the latest released software (v3.0.0 or later). Some information in this version of the document might be not applicable to the earlier software releases, therefore it is recommended to use the latest software version to get up-to-date information from this document as well as the most from your handset.

This document provides guidelines on how to use and maintain the following models of the handset:

- 1) WL4
- 2) WL4 Messaging
- 3) WL4 Plus

Unify WL4 is referred to as the "handset" in this manual and can be specifically marked with "WL4 only" or "WL4 Messaging only", or "WL4 Plus only" whenever the functionality differs between the handset models.

1.1 Target Group

This manual is primarily intended for service technicians and system administrators who are responsible for commissioning and configuration of Unify WL4 handsets.

1.2 Prerequisites

It is recommended to have a basic knowledge of the Unify VoWiFi system and handset registration in the PBX.

1.3 General Recommendations

- Keep the handset software updated. Most new software releases will contain security patches.
- Some functions should only be enabled within a "secured network". Within the context of this document, "secured network" means a network that is protected by a firewall and cannot be accessed by untrusted parties.

1.4 GDPR Considerations

The handset provides data protection. To comply with the GDPR by default, the **Auto phone lock** and **Clear lists in charger** parameters must be enabled on the handset. This will protect personal data such as call lists and messages from unauthorized access. It will also prevent unauthorized persons from making calls or sending messages using the handset.

The phone lock PIN code (4-8 digits, default "0000") can be activated and changed by the user directly on the handset or by the system administrator using the WinPDM/WSG DM .

For more information, see User Manual, Unify OpenScape WLAN Phone WL4.

2 Handset Deployment

This chapter describes how to deploy Unify WL4 handsets to a VoWiFi system.

2.1 Deployment Methods

Handsets can be deployed in different ways depending on the size of the VoWiFi system.

Large VoWiFi system

Deployment can be performed Over-the-Air (OTA) using Easy Deployment together with WSG DM .

This method is feasible in large installations where you need to deploy, upgrade, and configure a large amount of handsets simultaneously without collecting them from the users. When Easy Deployment is used, the handset tries to associate with a predefined (staging) Wi-Fi network and the Unite module using a DHCP server or the Ascom Service Discovery Protocol (ASDP). Once the connection has been established, the handset synchronizes with the parameters stored in the WSG DM .

Deployment using WSG DM alone has certain limitations as it still requires physical access to handsets at the pre-deployment stage to manually set network parameters and configure settings to establish the connection with the Unite module.

For more information, refer to [Easy Deployment](#) on page 127 or [Deploy Handsets Using the WSG DM](#) on page 11.

Small VoWiFi system

Deployment can be performed either using WinPDM or the Admin menu on the handset.

These methods are feasible in small sites where a small number of handsets exist or can be used in cases when a quick change of parameter values is required, for example, in a lab environment, or in cases when a test installation should be run locally on one handset before OTA deployment. In case the WSG DM is not used at your site, WinPDM can be used instead. Using these methods you can deploy and configure only one handset at a time and the handsets need to be collected from users.

For more information, refer to [Deploy Handsets Using WinPDM](#) on page 12 or [Deploy Handsets Using the Admin Menu](#) on page 13.

2.2 Prerequisites to Handset Deployment

Deploying handsets to a VoWiFi system requires the following:

- 1) The handset batteries are charged.
- 2) DP1 Desktop Programmer is set up in case WinPDM is used.
- 3) A phone number plan is available for the handsets.
- 4) The IP address plan is set up to support the number of handsets to be deployed.

- 5) A VoWiFi system where some or all of the following components (depending on the system configuration) are available:
- **DHCP Server** allows devices to request and obtain IP addresses from the server that has a list of addresses available for assignment. If the WLAN does not have access to a DHCP server, it is necessary to have a list of static IP addresses.
 - **Staging WLAN system** in case Easy Deployment is used.
 - **WinPDM** helps to administrate and configure the handsets.
 - **Unite module** handles all communication between the WLAN and its built-in WSG DM . Before installing the handset, make sure the WSG DM address is available.
 - **NTP server** ensures network time synchronization.

Prerequisites for OTA Management

Handsets need to have a WLAN association that can be IP routed to WSG DM . With Easy Deployment, handsets can be installed using a (staging) WLAN with a predefined SSID and security profile as well as the IP address to the Unite module.

The connection to the WSG DM can be installed either in legacy mode or using the secure Websocket (recommended method). In case the WSG DM is upgraded to the latest version, it can be configured to support either one of these, or both modes. For the details, refer to [Connection Mode](#) on page 30.

If Easy Deployment is not used, the network parameters and settings to establish the connection with the Unite module must be set manually using the Admin menu on the handset or WinPDM. For the details, refer to [Deploy Handsets Using WinPDM](#) on page 12 or [Deploy Handsets Using the Admin Menu](#) on page 13.

Prerequisites for Local Management

There are no specific prerequisites to be met to deploy handsets using the Admin menu or WinPDM, except for the DP1 Desktop Programmer to be set up in case WinPDM is used. For this type of deployment, you can use newly delivered as well as factory reset handsets.

2.3 Deploy Handsets Using the WSG DM

To deploy handsets to the VoWiFi system, perform the following steps:

- 1) If Easy deployment has been used, the handset(s) should have automatically obtained the network parameters and the Unite module address, so no additional configuration is required and you can go directly to the step 2.

If Easy deployment has not been used, set the network parameters and configure settings to establish the connection with the Unite module manually either using WinPDM or the Admin menu. For the details, refer to the steps 4–6 in [Deploy Handsets Using WinPDM](#) on page 12 or [Deploy Handsets Using the Admin Menu](#) on page 13.

- 2) Open a web browser and enter the address of the WSG DM .
- 3) Open the WSG DM and log in (if necessary).

- 4) Create a number or a range of numbers for the handsets, refer to [Create Numbers](#) on page 17.
- 5) Assign the number to the handset, refer to [Assign a Number to a Handset](#) on page 17.
- 6) Manage the certificates as described in [Import Trust and Application Certificates](#) on page 67.

NOTICE:

If the WLAN system uses an 802.1X security protocol that requires certificates for authentication/encryption to the WLAN, this method is not the best option since the certificates must be manually installed for each handset before the first login. The Easy Deployment process overcomes this problem by using a staging WLAN, which does not use 802.1X.

Alternatively, if a SCEP server is available, this can be accomplished by following the steps in [SCEP](#) on page 145 to have the necessary certificates automatically generated and downloaded to the handset.

- 7) Optionally, create a template with the common handset settings applicable to all handsets of the same device type (exclude the parameters configured in the network template) and apply this template to the handset(s), refer to [Create a Template](#) on page 14 and [Apply a Template to a Handset with a Number](#) on page 16.

2.4 Deploy Handsets Using WinPDM

To deploy a handset using WinPDM, perform the following steps:

- 1) Open WinPDM.
- 2) Create a number or a range of numbers for the handsets, refer to [Create Numbers](#) on page 17.
- 3) Assign the number to the handset, refer to [Assign a Number to a Handset](#) on page 17.
- 4) Create a template (network template) that contains the required network parameters that can be applied to a number of handsets, refer to [Create a Network Template in WinPDM](#) on page 14.
- 5) Apply the network template to the handset(s), refer to [Apply a Template to a Handset with a Number](#) on page 16.
- 6) Manage the certificates as described in [Import Trust and Application Certificates](#) on page 67.

NOTICE:

If the WLAN system uses an 802.1X security protocol that requires certificates for authentication/encryption to the WLAN, this method is not the best option since the certificates must be manually installed for each handset before the first login. The Easy Deployment process

overcomes this problem by using a staging WLAN, which does not use 802.1X.

Alternatively, if a SCEP server is available, this can be accomplished by following the steps in [SCEP](#) on page 145 to have the necessary certificates automatically generated and downloaded to the handset.

- 7) Optionally, create a template with the common handset settings applicable to all handsets of the same device type (exclude the parameters configured in the network template) and apply this template to the handset(s), refer to [Create a Template](#) on page 14 and [Apply a Template to a Handset with a Number](#) on page 16.
- 8) Remove the handset from the DP1 Desktop Programmer when the synchronization is finished.

Repeat the steps 5–9 for every handset.

2.5 Deploy Handsets Using the Admin Menu

NOTICE:

Only a limited set of settings can be configured using the Admin menu.

To deploy a handset using the Admin menu, perform the following steps:

- 1) Enter the Admin access code while the handset is showing the `No network` message at start-up.

NOTICE:

40022 is the default Admin access code that can be changed in WinPDM/WSG DM . For more information, refer to [Change Admin Access Code](#) on page 60.

- 2) Set the following parameters:
 - a) In the **Network setup** menu, set all the required system settings for the WLAN. No certificates can be entered or referred to using the Admin menu.
 - b) In the **WSG** menu, set the IP address and password (if any) to the Unite module.

The handset will attempt to install the connection using the secure Websocket and the default credentials. If this fails, the handset will attempt to perform a legacy mode connection.
 - c) In the **VoIP** menu , set the required parameters to access the PBX and enable VoIP calls.

2.6 Work with Templates

This section describes how to work with templates, specifically how to create new templates and apply them to handsets with and without numbers.

2.6.1 Create a Template

Templates are a collection of user defined parameter values. These templates can be used to create common settings to be used on several handsets of a certain device type.

NOTICE:

The number of parameters in the template affects the time it takes to apply the template to the selected handset. In order to minimize the network traffic, it is recommended to set only those parameters that are planned to be used on the handset.

NOTICE:

When creating a template in both WinPDM and the WSG DM, the templates must be identical to avoid that the parameters override each other when synchronizing the handset.

NOTICE:

If a template has been already created in one Device Manager, for example WSG DM, it is possible to export and use the same template in WinPDM. For more information, refer to *Portable Device Manager for Windows (WinPDM), Installation and Operation Manual, TD 92712EN*.

To create a template, perform the following steps:

- 1) Open the **Templates** tab.
- 2) In the **Template** menu, select **New...** or press **CTRL + N**. The *New template* window opens.
- 3) In the **Device type** and **Parameter definition** drop-down lists, select the correct device type and parameter definition.
- 4) In the **Name** field, enter a descriptive name for the template.
- 5) Click **OK**. The *Edit template* window opens.
- 6) Set the required parameters, refer to [Parameter Configuration](#) on page 20.
- 7) Click **OK** to save the template.

For additional details on how to work and manage templates, refer to *Portable Device Manager for Windows (WinPDM), Installation and Operation Manual, TD 92712EN*.

2.6.2 Create a Network Template in WinPDM

This section describes how to create a template with the network parameters and settings to establish the connection with the Unite module. To create a network template, follow the steps below:

- 1) Open WinPDM.
- 2) Open the **Templates** tab.

- 3) In the **Template** menu, select **New...** or press **CTRL + N**. The *New template* window opens.
- 4) In the **Device type** and **Parameter definition** drop-down lists, select the correct device type and parameter definition.
- 5) In the **Name** field, enter a descriptive name for the template.
- 6) Click **OK**. The *Edit template* window opens.
- 7) Select **Network > Network X (A-D)** to configure the network settings, refer to [Network Settings](#) on page 20.

Configure the required parameters for the respective network, for example system and security settings for WLAN, and any certificates for 802.1X. Select the frequency band and set the required channels to be used on the handset. If using a security mode that requires certificates, use an NTP server as well to assure the correct time in the handset, as certificates are only valid within a certain time. For the details, refer to [Set Time & Date](#) on page 37.

- 8) Select **Device > wsg** to configure the settings to access the Unite module, refer to [Unite Module Settings](#) on page 29.

The connection to the WSG DM can be installed either in legacy mode or using the secure Websocket (recommended method).

NOTICE:

It is not recommended to use Automatic mode.

- If the connection should be installed using the legacy mode, the procedure is the following:
 - Select **Connection mode > Legacy**.
 - Enter the IP address and password (if any) to the Unite module, refer to [IP Address and Password to the Unite Module](#) on page 29.
 - If the connection should be installed using the secure Websocket, the procedure is the following:
 - Select **Connection mode > Secure Websocket**.
 - Enter the IP address and password (if any) to the Unite module, refer to [IP Address and Password to the Unite Module](#) on page 29.
 - Enter the username and password to the Unite Websocket interface, refer to [Websocket Authentication](#) on page 31.
 - Choose whether to validate the certificate provided by the WSG DM or not, refer to [Server Certificate Validation](#) on page 30.
 - If required, choose a client certificate to use for authenticating towards the WSG DM, refer to [Websocket Client Certificate](#) on page 31.
- 9) When done, click **OK**.

2.6.3 Apply a Template to a Handset without a Number

NOTICE:

Applying a template to a handset without a number is possible only in WinPDM.

- 1) Place the handset in the DP1 Desktop Programmer.

- 2) In the opened *Found Device Wizard* window, select **Apply template**.
- 3) Click **Next**. Only templates with a parameter version matching the selected handset are shown.
- 4) Select the template to apply and click **OK**.

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

2.6.4 Apply a Template to a Handset with a Number

To apply a template to a handset with a number, perform the following steps:

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

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

- 2) In the **Number** menu (or right-click the handset(s)), select **Apply template....**
- 3) Select the required template and click **OK**. The handset(s) might restart depending on the parameters that have been changed.

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

The **Last run template** column in the **Numbers** tab shows the name of the most recently applied template.

2.6.5 Save Handset Configuration as a Template

It is possible to save the settings of a handset as a template. The template will only contain configuration data, it does not include contacts, certificates, and other personal data. This template can be used as a backup if you want to restore the configuration of a handset at a later stage or as a template that can be applied to other handsets.

To save the handset configuration as a template, perform the following steps:

- 1) In the **Numbers** tab, select the handset which configuration you want to use as a template.
- 2) In the **Number** menu (or right-click the handset), select **Use as template...** and enter a descriptive name for it.
- 3) In the *Edit template* window, all handset parameters are selected by default. If one or more parameters are not required, clear the check box next to the parameter.

Some parameters are user-specific and if this type of template needs to be applied to several handsets, it is recommended to exclude the following parameters:

- **User display text** defines a text string displayed in Idle mode. The parameter is located in **Device > Settings**.
- **Phone lock PIN code** defines the security code used to unlock the keypad. The parameter is located in **Device > Settings > Locks**.
- **Endpoint ID** defines the identity/name of the user registered in the PBX. The parameter is located in **VoIP > General**.

- 4) Click **OK**.

2.7 Create Numbers

This section describes how to create a single or a range of numbers for the handset(s).



CAUTION: Do not assign numbers to handsets that are already configured and functional. When you assign numbers to handsets that already exist in the system, WinPDM/WSG DM will automatically overwrite the existing parameters in the handset, since these handsets are not saved in WinPDM/WSG DM.

- 1) Open the **Numbers** tab.
- 2) In the **Number** menu, select **New...** or press **CTRL + N**. The *New numbers* window opens.
- 3) In the **Device type** and **Parameter definition** drop-down lists, select the correct device type and parameter definition.
- 4) If you have a template you want to apply to the numbers, select it in the **Template** drop-down list.

NOTICE:

The parameter version of the template must be equal to or earlier than the selected parameter version.

- 5) In the **Prefix** field, enter the prefix (if needed) to be added to the number(s).
- 6) Select one of the following options:
 - a) Create a single number by selecting the **Single** option. Enter the number in the **Call number** field.
 - b) Create a range of numbers by selecting the **Range** option. Enter the start call number and the end call number in the corresponding fields.

NOTICE:

The maximum range that can be added at a time is 100 numbers.

- 7) Click **OK**.

2.8 Assign a Number to a Handset

There are different ways to associate the handset with the number you created earlier.

NOTICE:

Do not assign numbers to handsets that already have numbers.

Using the WinPDM/WSG DM

- 1) Open the **Numbers** tab and select the device to be associated with a number.
- 2) In the **Number** menu (or right-click the handset), select **Associate with device...**
- 3) In the opened window, select the handset that shall receive the selected number.
- 4) When done, click **OK**. The number is now assigned to the handset.

Using the WinPDM only

- 1) Place the handset into the DP1 Desktop Programmer.
- 2) In the opened *Found Device Wizard* window, select **Associate with number** and click **OK**.

NOTICE:

If the **Associate with number** option is disabled, it means that there is no number available for this device type.

- 3) In the opened window, select the number to associate with the handset and click **OK**. The number is now assigned to the handset.

2.9 Handset Configuration

If you want to configure a limited set of parameters for an individual handset, you can apply changes either using the WinPDM/WSG DM or the Admin menu directly on the handset. For more information, refer to [System Administration in the Handset](#) on page 57.

If you want to configure a wide range of handsets without collecting them from the users, it is recommended to use the WSG DM and apply a template created for a device type. Alternatively, you can use WinPDM but in this case the handsets need to be collected from users.

Configure a Single Handset

- 1) Open the **Numbers** tab, and select the handset that requires a change of parameters.
- 2) In the **Number** menu (or right-click the handset), select **Edit parameters**.
- 3) Set the required parameters and when done, click **OK**.

The handset automatically receives an update when it is connected to WinPDM/WSG DM and might restart (depends on the parameters that have been changed).

Configure a Range of Handset

- 1) Create a template and set the required parameters, refer to [Create a Template](#) on page 14 and [Parameter Configuration](#) on page 20.

NOTICE:

It is recommended to create a common template with shared parameters to apply to several handsets simultaneously.

- 2) Apply the template to the handsets, refer to [Apply a Template to a Handset with a Number](#) on page 16 or [Apply a Template to a Handset without a Number](#) on page 15.

2.10 Handset Synchronization

This section describes how synchronization works between the handset and the WinPDM/WSG DM .

- 1) If a parameter has been changed in the handset, it is transferred to the WinPDM/WSG DM , and vice versa.
- 2) If a parameter has been changed in the WinPDM/WSG DM while the handset was offline, the changes are applied once the handset is online.
- 3) If the same parameter has been changed both in the WinPDM/WSG DM and the handset, the value in the WinPDM/WSG DM overrides the value in the handset.

Changes made in the WSG DM are not stored in the WinPDM as there is no connection between the two systems. The database of the WinPDM synchronizes with the handset when the handset is placed in the DP1 Desktop Programmer.

NOTICE:

Since there is no connection between the WinPDM and WSG DM except via the handset, the WLAN and device manager settings can differ in two systems. Parameters can revert to old values when the handset is placed in the DP1 Desktop Programmer.

When the handset is removed from the DP1 Desktop Programmer, it synchronizes with the WSG DM .

3 Parameter Configuration

This section describes how to configure parameters for Unify WL4 handsets.

The parameters are defined in `.def` files that are delivered by Ascom (Sweden) AB and uploaded at [Ascom Partner Extranet](#) together with the released software.

NOTICE:

In some cases the handset can restart (depends on the changed settings) and the `Remotely updated` dialog window will appear on the handset after the update.

If you want to know more about some specific parameter, click the **Help** icon



and check the help text.

3.1 Network Settings

This section describes the parameters available when configuring the handset in a WLAN system.

3.1.1 Change the Active Network

The handset can switch between four different WLAN system configurations called **Network A**, **Network B**, **Network C**, and **Network D**. To change the active network, do as follows:

- 1) Select **Network > General**.
- 2) In the **Active network** drop-down list, select **Network X** (A-D).

3.1.2 Change the Network Name

The name of the used network can be changed in the following way:

- 1) Select **Network > Network X** (A-D).
- 2) In the **Network name** field, enter the new name of the network.

On the handset, the name of the used network is visible in the **Connections > Network** menu.

3.1.3 Automatic Switch between the Networks

The handset can be configured to automatically switch between the available networks¹ on site. For example, when connection with Network A is lost, the handset will automatically use the available Network B as a fallback.

- 1) Select **Network > General**.

¹ Network should be enabled and configured as well as included into the auto-switch network list.

- 2) In the **Auto-switch network** drop-down list, select **On**.
- 3) In the **Auto-switch network timeout** field, enter the time (in seconds) before the handset will try to connect to the other network.
- 4) For the networks that should be included in the auto-switch network list:
 - a) Select **Network > Network X (A-D)**.
 - b) In the **Include in auto-switch network** drop-down list, select **Yes** to enable the switch between the networks.

3.1.4 SSID

Service Set Identifier (SSID) is the name of the Wi-Fi network that the handset associates with. To set the SSID, do the following:

- 1) Select **Network > Network X (A-D)**.
- 2) In the **SSID** field, enter system SSID (case-sensitive).

NOTICE:

Not all special characters can be used when entering the SSID using the Admin menu on the handset. If some characters cannot be used on the handset, use the WinPDM/ WSG DM instead.

3.1.5 Handset IP Address Settings

This section describes how to configure the handset to receive an IP address automatically from a DHCP server as well as how to assign static IP address for each handset in case your network does not support DHCP.

Assign Automatic IP Address

To automatically assign an IP address to the handset, select **Network > Network X (A-D) > DHCP mode > On**.

No additional configuration is required. The phone IP address, subnet mask, and default gateway are automatically set up.

Assign Static IP Address

To manually assign an IP address to the handset, do as follows:

- 1) Select **Network > Network X (A-D) > DHCP mode > Off (static mode)**.
- 2) In the **Phone IP address** field, enter the unique IP address for the handset.
- 3) In the **Subnet mask** field, enter the subnet mask.
- 4) In the **Default gateway** field, enter the IP address for the default gateway.

If you need to specify the DNS server address, please refer to [DNS Server Settings](#) on page 22.

3.1.5.1 DNS Server Settings

It is possible to configure the DNS server for the handset to use. If the primary DNS server is available, it is always used. If not, the secondary DNS server is used instead.

- 1) Verify that **Network > Network X (A-D) > DHCP mode** is set to **Off (static mode)**.
- 2) In the **Primary DNS** field, enter the IP address for the primary DNS server.

To configure the secondary DNS server, enter the IP address in the **Secondary DNS** field.

3.1.6 Security Settings

WLAN can be configured to use various encryption and authentication schemes. The most frequently used encryption and authentication modes are found in **Network > Network X (A-D) > Security mode** and include the following:

- 1) **Open**
- 2) **WPA/WPA2-Personal**
- 3) **WPA3-Personal**
- 4) **WPA2-Enterprise**
- 5) **WPA3-Enterprise**

NOTICE:

The use of extensive authentication schemes without any fast roaming method can cause incidents of dropped speech during handover due to the time to process the authentication.

3.1.6.1 Open Authentication

Open authentication method means that no encryption or authentication is required because no exchange or verification of identity takes place. Using open authentication, any handset can authenticate with the AP, as long as the handset is aware of the SSID used on the network. If open authentication method should be used, select **Network > Network X (A-D) > Security mode > Open**.

3.1.6.2 WPA/WPA2-Personal and WPA3-Personal

WPA3 requires the use of 802.11w Protected Management Frames (PMF) standard. When WPA2 is used, PMF is not mandatory but will be used by the handset if enabled in the AP. Encrypting management frames such as Deauth will make WPA2 and WPA3 more robust and is therefore recommended to be always used unless prevented by interoperability issues.

To select **WPA/WPA2-Personal** or **WPA3-Personal** as the security mode, perform the following steps:

- 1) Select **Network > Network X (A-D)**.
- 2) In the **Security mode** drop-down list, select **WPA/WPA2-Personal** or **WPA3-Personal**.
- 3) In the **Passphrase** field, enter the password to be used for network access.

NOTICE:

Not all special characters can be used when entering the SSID using the Admin menu on the handset. If some characters cannot be used on the handset, use the WinPDM/WSG DM instead.

3.1.6.3 WPA2-Enterprise and WPA3-Enterprise

It is recommended to use either WPA2-Enterprise or WPA3-Enterprise as an authentication method to set a consistent baseline of security.

Compared to WPA/WPA2- and WPA3-Personal, WPA2- and WPA3-Enterprise use stronger encryption, authentication, and key management strategies for wireless data and system security. WPA3 requires the use of 802.11w PMF standard, while WPA2 does not mandate its use but will be used by the handset if enabled in the AP.

The authentication security can be improved using certificates. It is recommended to use trusted certificates to authenticate the WLAN, and it is required to use application certificates to present to the WLAN for client authentication. The handset performs validation of the server side certificate by default. It is important not to disable this functionality since the handset will not be protected against rogue AP's. Both EAP-TLS and PEAP-MSCHAPv2 use certificate-based authentication. EAP-TLS can be made more secure with the help of mutual certificate validation.

- 1) For server validation, import the trusted certificate by performing the following steps:
 - In the **Numbers** tab, right-click the handset's number and select **Manage certificates**.
 - In the **Trusted list** and the **Application certificates** tabs, click **Browse** and select the certificates to import. When done, click **Close**.

NOTICE:

Skip this step, if validation of server certificate is disabled (see step 9). Skip this step as well, if SCEP is used to automatically download trusted certificates to the handset, refer to [SCEP](#) on page 145.

- 2) Select **Network > Network X (A-D)**.
- 3) In the **Security mode** drop-down list, select **WPA2-Enterprise** or **WPA3-Enterprise**.
- 4) In the **EAP method** drop-down list, select **PEAP-MSCHAPv2** or **EAP-TLS** as the authentication method.
- 5) In the **EAP authentication identity** field, enter the user name for EAP authentication.

- 6) If **PEAP-MSCHAPv2** has been selected, enter the password for EAP authentication in the **EAP authentication password** field.
- 7) The use of **EAP anonymous identity** parameter is optional. This field is used for non-encrypted use with EAP types that support different tunnelled identity, such as EAP-PEAP/MSCHAPv2, in order to reveal the real identity only to the authentication server.
- 8) In the **EAP client certificate** drop-down list, select the application certificate or set it to **Automatic**.
- 9) The use of **EAP server certificate validation** parameter is optional. If you want to disable the validation of server certificate during authentication, select **No**.

NOTICE:

By disabling the validation, the server is not authenticated and may be a rouge one.

NOTICE:

The server must send its complete certificate chain.

3.1.6.4 Allow Outdated Security Protocols

The following supported protocols and algorithm versions are vulnerable to attacks, that is why the parameter **Device > General > Allow outdated security protocols** should be set to **No** to disable them unless they are required for compatibility with older equipment:

- TLS 1.0 and TLS 1.1
- SHA-1 (when used for signature verification)
- RSA, DSA or DH keys shorter than 2048 bits
- ECC keys shorter than 224 bits

This setting affects all encrypted traffic from the handset, including WPA2- and WPA3-Enterprise authentication and SIP over TLS.

3.1.6.5 WinPDM Authentication

WinPDM application allows full administration access to the handset.

In order to enable efficient deployment of new handsets, the USB interface of all new or factory reset handsets is configured to allow unauthenticated connections from the WinPDM application. As soon as the initial configuration is done, it is imperative to disable WinPDM access or add authentication.

This can be done either by changing the USB port to only allow charging or by entering the Admin access code before the use of WinPDM is allowed:

- 1) In the handset, select **Main menu > Settings > Admin menu > USB > Charge only**.
- 2) In the WinPDM/WSG DM , select **Device > General > USB behavior > Charge**.

- 3) In the WinPDM/WSG DM , select **Device > General > WinPDM authentication > On**.

The **USB behavior** parameter also allows the USB interface to be configured in MTP/file transfer mode. This allows the part of the handset file system that contains log files to be mounted and inspected from a PC. Although such log files are encrypted, it is recommended not to leave this function enabled when it is not used. For the details, refer to [USB Behavior](#) on page 54.

3.1.7 Radio and Channel Selection

The handset supports both 5 GHz radio and 2.4 GHz radio, but 5 GHz radio and 2.4 GHz radio cannot be used simultaneously. The radio defines the channels to use when scanning for APs but regulatory domain may further limit which channels that are used by the handset.

3.1.7.1 5 GHz Channels

This setting defines which 5 GHz channels shall be used on the handset. To select a 5 GHz channel, perform the following steps:

- 1) Select **Network > Network X (A-D)**.
- 2) In the **Frequency band** drop-down list, select **5 GHz**.
- 3) In the **5 GHz channels** drop-down list, select one of the following:
 - **All**
 - **Non DFS**
 - **UNII-1** (recommended to use)
 - **UNII-3**
 - **UNII-1, UNII-2**
 - **UNII-1, UNII-2, UNII-3**
 - **UNII-1, UNII-2 Extended**
 - **Advanced** (requires additional configuration, refer to [Advanced 802.11 Channels](#) on page 27)

IMPORTANT:

The amount of channels enabled on the handset should be minimized to the channels that are used in the WLAN system.

If **All** is selected, the handset will scan all channels for APs. The more channels the handset has to scan, the longer each scan round will take. This is especially true for DFS channels, where only time-consuming passive scanning can be performed. Longer scan times means bigger risk that voice quality is affected.

NOTICE:

In case **Regulatory domain** has been set to **World mode (802.11d)**, the handset will further limit which channels are allowed to be used. For the details, refer to [Configure Regulatory Domain](#) on page 27.

The table below lists bands and channels on the 5 GHz band:

Band	Frequency band	Channel	Type of channels
UNII-1	5.150–5.250 GHz	36,40,44,48	Non DFS
UNII-2	5.250–5.350 GHz	52,56,60,64	DFS
UNII-2 Extended	5.470–5.725 GHz	100,104,108,112,116,120,124,128,132,136,140,144 ^{2 3}	DFS
UNII-3	5.725–5.850 GHz	149, 153, 157, 161, 165	Non DFS, allowed in some countries

3.1.7.2 2.4 GHz Channels

This setting defines which 2.4 GHz channels shall be used on the handset. To select a 2.4 GHz channel, perform the following steps:

- 1) Select **Network > Network X (A-D)**.
- 2) In the **Frequency band** drop-down list, select **2.4 GHz**.
- 3) In the **2.4 GHz channels** drop-down list, select one of the following:
 - a) **All**
 - b) **1, 6, 11** (default, recommended to use)
 - c) **Advanced** (requires additional configuration, refer to [Advanced 802.11 Channels](#) on page 27)

NOTICE:

In case **Regulatory domain** has been set to **World mode (802.11d)**, the handset will further limit which channels are allowed to be used. For the details, refer to [Configure Regulatory Domain](#) on page 27.

IMPORTANT:

The amount of channels enabled on the handset should be minimized to the channels that are used in the WLAN system.

If **All** is selected, the handset will scan all channels for APs. The more channels the handset has to scan, the longer each scan round will take. Longer scan times means bigger risk that voice quality is affected.

The table below lists channels on the 2.4 GHz band:

² Channel 144 is slightly outside the specified band (5.710–5.730 GHz).

³ In some countries the following rules apply for the UNII-2e band:

- 1) Devices will not transmit on channels that overlap the 5600 - 5650 MHz band (Ch 120, 124 and 128).
- 2) For outdoor use any installation of either a master or a client device within 35 km of a Terminal Doppler Weather Radar (TDWR) location shall be separated by at least 30 MHz (center-to-center) from the TDWR operating frequency. Table of current TWDR can be found in the FCC document “443999 D01 Approval of DFS UNII Devices v01r04”.

Frequency band	Channel
2.421 - 2.484 GHz	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14

3.1.7.3 Advanced 802.11 Channels

This setting defines which 802.11 channels to use. It is only used if the parameter in **2.4 GHz channels** or **5 GHz channels** is set to **Advanced**.

NOTICE:

If **Advanced** is selected, it is indicated on the handset by having all options unchecked in the **Main menu > Settings > Admin menu > Network setup > 2.4 GHz channels**, or **5 GHz channels**. If any of these unchecked channels are selected using the Admin menu, the only way to reselect **Advanced**, is to reconfigure it in WinPDM/WSG DM.

To configure the channels to be scanned, perform the following steps:

- 1) Select **Network > Network X (A-D)**.
- 2) In the **Advanced 802.11 channels** field, enter the channels to scan in a comma-separated list, for example **1, 6, 11**. The order has no impact, that is, **11, 6, 1** gives the same result.

3.1.7.4 802.11k Neighbor List

Unify WL4 handsets have optional support for roaming based on 802.11k neighbor lists.

If **Network > Network X (A-D) > Use 802.11k neighbor list** is set to **Yes**, the handset will primarily scan only a subset of the enabled 2.4/5 GHz channels for a new AP candidate when roaming. To facilitate roaming, the handset uses the 802.11k neighbor lists received from the AP to choose which channels to scan during the roaming process. If this partial scan fails to find a roaming candidate, and the measured signal strength of the AP continues to drop, the handset will fall back to scanning channels selected in **Network > Network X (A-D) > 2.4 GHz channels** or **5 GHz channels**.

3.1.8 Configure Regulatory Domain

The wireless spectrum regulatory domain defines which region's rules the handset should comply to.

At start-up, the handset is passively listening for information about which regulatory domain is present before making any transmissions. To ensure that the local frequency rules are not violated, the recommendation is to use **World mode (802.11d)**. The 802.11d regulatory domain information is broadcast in beacons and contains information on which channels and power levels are allowed.

NOTICE:

802.11d is not allowed in the USA and Canada.

Based on the region, different actions should be taken to set regulatory domain:

- 1) If the handset is used in the USA or Canada, set regulatory domain as described below:

- a) Select **Network > Network X (A-D)**.
- b) In the **Regulatory domain** drop-down list, select **USA** or **Canada**.

- 2) If the handset is used in the rest of the world, set **World mode (802.11d)**.

If set to **World mode (802.11d)**, but 802.11d is not supported by the infrastructure, the handset will use safe default. As the result of this, not all allowed channels might be allowed for use.

3.1.9 IP DSCP for Voice and 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 WLAN. The settings in the handset must agree with the settings in the system, otherwise it results in bad voice quality.

- 1) Select **Network > Network X (A-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**

3.1.10 TSPEC Call Admission Control

This parameter defines if Call Admission Control via WMM TSPECs (Traffic Specifications) is to be used or not on the WLAN. To configure **TSPEC Call Admission Control**, perform the following steps:

- 1) Select **Network > Network X (A-D)**.
- 2) In the **TSPEC Call Admission Control** drop-down list, select one of the following:
 - **Off** to disable traffic streams allocation for each call.
 - **Automatic** to enable traffic streams allocation for each call if required by the system. Even if the system does not require admission control the call will be set up.
 - **Required** if the system must require admission control to set up a call.

3.1.11 Roaming Method

To select a roaming method, perform the following steps:

- 1) Select **Network > Network X (A-D)**.
- 2) In the **Roaming method** drop-down list, select one of the following:
 - a) **PMKSA Caching** for the systems that do not support FT or OKC. When this option is selected, OKC is automatically disabled.
 - b) **Fast BSS Transition (FT)** for the systems that support FT, otherwise use OKC (recommended method).
 - c) **OKC** (Opportunistic Key Caching) in the systems where OKC is used instead of FT on an AP that supports both.

3.1.12 A-MPDU Packet Aggregation

During interoperability testing there have been issues with the Aruba and Stellar controllers when the A-MPDU aggregation was enabled in the handset. Therefore, it is recommended to set **Network > Network X (A-D) > A-MPDU Packet Aggregation** parameter to **Off** when connecting to Aruba or Stellar Wi-Fi and **On** when connecting to other networks.

3.1.13 Deauthenticate on Roam

When enabled, the handset will upon roam leave the current AP by transmitting a deauthentication frame. When disabled (default), the handset will upon roam notify the current AP that it is going into power-save mode, and then perform the roam. This may help the Wi-Fi infrastructure to avoid deallocating resources for the client.

To enable the feature, select **Network > Network X (A-D) > Deauthenticate on roam > Yes**.

3.2 Unite Module Settings

This section describes the parameters that should be configured to establish connection to the Unite module.

3.2.1 IP Address and Password to the Unite Module

The Unite module handles all communication between the WLAN and its built-in Device Manager (WSG DM). Using the Unite module, it is possible to perform different actions, for example send messages from a web browser to a handset, handle messages to groups, perform parameter synchronisation and software upgrade, search for telephone numbers in a central database (on PC), provide absence handling, and etc.

To configure the IP address, do the following:

- 1) Select **Device > wsg**.
- 2) In the **IP address** field, enter the IP address of the Unite module. If empty, no messaging or alarm functions are available.

- 3) In the **Password** field, enter the password of the Unite module.

If Secure Websocket (WSS) is not used and the handset and WSG DM are not located on the same secured network, it is recommended to configure the handset with the IP address of the WSG DM . If no address is specified, DHCP and ASDP will be used to find an available server, and those protocols are both unencrypted and unauthenticated.

3.2.2 Connection Mode

This parameter defines how the handset should connect to Unite module and can be configured in the following way:

- 1) Select **Device** > **wsG** .
- 2) In the **Connection mode** drop-down list, select one of the following:
 - **Secure Websocket** (WSS) provides stronger encryption and authentication using TLS and certificates. If selected, additional parameters are available for configuration, refer to [Server Certificate Validation](#) on page 30, [Websocket Authentication](#) on page 31, and [Websocket Client Certificate](#) on page 31.

WSS requires at least v3.0.0 of handset software and v4.10.0 of WSG DM software.
 - **Legacy** mode can be used with older versions of the WSG DM that have no WSS support.
 - **Automatic** is the default setting that is intended to be used only during the handset deployment and must be changed to either **Secure Websocket** or **Legacy** when configuring the handset.

3.2.3 Server Certificate Validation

In WSS mode, the handset can be configured to perform validation of the server-side certificate. It is recommended to enable this functionality since the handset will otherwise not perform any authentication of the WSG DM .

NOTICE:

The certificate (public key) of the WSG DM has to be download to the **Trusted list** of the handset prior to enabling **Server certificate validation**. Since the handset will not establish the connect with the WSG DM if the validation process fails, it is recommended to verify that the configuration is correct on a single handset before deploying.

To enable validation of the Unite server certificate when connecting using secure Websocket, do the following:

- 1) Verify that the **Device** > **wsG** > **Unite IP connection mode** has been set to **Secure Websocket**.
- 2) In the **Server certificate validation** drop-down list, select **Yes**.

3.2.4 Websocket Authentication

The handset is delivered with a default username (`device`) and password (`changethis`) in order to enable easy deployment. These credentials must be changed when configuring the handset. To change the default username and password, do the following:

- 1) Verify that the **Device > wsg > Unite IP connection mode** has been set to **Secure Websocket**.
- 2) In the **Websocket authentication username** field, enter the user name for the HTTP Basic Authentication of the Unite Websocket interface.
- 3) In the **Websocket authentication password** field, enter the password for the HTTP Basic Authentication used for the Unite Websocket interface.

Use a strong password since it will be used to authenticate to the WSG DM . This is especially important if verification of the handset certificate is not configured in the WSG DM .

3.2.5 Websocket Client Certificate

This parameter defines the certificate the handset should present to the Unite server on connection.

If **Device > wsg > Client certificate** is set to **Automatic**, a certificate received from SCEP server (if exists) will be used.

If **Client certificate** is set to **None** or a client certificate is not available, the server will not be authenticated by the handset.

3.2.6 Contacts

This section describes how to create and import company and central phonebook numbers.

3.2.6.1 Import Contacts

A file containing contacts (local phonebook) can be imported to WinPDM/WSG DM and synchronized with a handset. The phonebook file is a tab-separated file (`.txt`, `.csv`, or `.skv`) that contains two items per row, number, and name.

NOTICE:

If a local phonebook file is imported to the handset where the local phonebook already exists, the old contacts will be overwritten by the contacts from the imported file.

To import contacts from a file, do the following:

- 1) In the **Numbers** tab, select the handset where you want to import the contacts to.
- 2) From the **Number** menu (or right-click the handset), select **Import contacts > From file...** or **From number...**
- 3) Select the file containing contacts and then click **Open**.

- 4) Verify that the contacts have been imported to the handset.

For more information, refer to *Portable Device Manager for Windows (WinPDM), Installation and Operation Manual, TD 92712EN*.

3.2.6.2 Company Phonebook

It is possible to create a phonebook that is administered centrally and uploaded to the handset from WinPDM/WSG DM. If this feature is used, the 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, refer to [Create a Company Phonebook File](#) on page 32.
- 2) In the **Devices** tab, select the handset where you want to upload the company phonebook to.

NOTICE:

It is possible to import contacts to several handsets at the same time, but the handsets have to be of the same device type.

- 3) From the **Devices** menu (or right-click the handset), select **Upload company phonebook...**
- 4) In the opened window, click **Import...** and select the company phonebook file to upload. When done, then click **Open**.
- 5) Click **OK**.
- 6) If a company phonebook already exists on the handset, the *Existing company phonebook will be replaced, Continue?* dialog window will appear. Click **Yes** to continue.
- 7) Verify that the company phonebook has been uploaded to the handset.

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 by the supplier.

The format of the rows in the phonebook file is as follows:

<Name><tab><phone number><carriage return>, followed by additional rows for each entry.

The following characters are accepted in the handset number field in the phonebook file, but are ignored when the phonebook file is created:

- 1) Left parenthesis: (
- 2) Right parenthesis:)
- 3) Hyphen: -
- 4) Space: " "

For more information, refer to *Portable Device Manager for Windows (WinPDM), Installation and Operation Manual, TD 92712EN*.

3.2.6.3 Central Phonebook

NOTICE: Applicable only if your system supports the function.

If the system 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 > WSG** .
- 2) In the **Central phonebook number** field, enter the number to the central phonebook.

The number to be used is set to 999999 by default. If the system is not equipped with a central phonebook, this menu option can be removed from the handset by entering an empty value.

3.3 Handset Settings

Parameters described in this section can be either changed directly on the handset or using the WinPDM/WSG DM to assist the user or set the initial values when the handset is deployed.

NOTICE:

Configuration using the handset's menu is out of scope of this document and not described here. For the details, please refer to *Unify OpenScape WLAN Phone WL4, User Manual, TD 93342EN* .

3.3.1 Key Lock and Phone Lock Settings

This section describes how to configure the handset in a way to protect it from an unauthorized use or from unintentional key presses.

3.3.1.1 Automatic Key Lock

Automatic key lock setting helps to avoid situations when keys are accidentally pressed.

NOTICE:

If configured, it is possible to dial any of up to five predefined emergency numbers when the keypad is locked, refer to [Emergency Call Numbers](#) on page 73 .

Other examples of exceptions that override the key lock is personal alarm, mute ALS, shortcut call, and cancel Man-down/No-movement alarms .

To configure the **Automatic key lock**, perform the following steps:

- 1) Select **Device > Settings**.

2) In the **Automatic key lock** drop-down list, select one of the following:

- **On** to enable the automatic key lock, also during an ongoing call.
- **On except for calls** to enable the automatic key lock in Idle mode, but not during an ongoing call.
- **Off** to disable automatic key lock.

If **Automatic key lock** has been enabled, the keypad will be automatically locked after a certain period of inactivity. To change the default time (20 seconds), refer to the [Automatic Lock Time](#) on page 35.

3.3.1.2 Automatic Key Unlock

This setting allows to automatically disable a key lock during an incoming call or message so user does not need to unlock handset to answer. To configure the **Automatic key unlock**, perform the followings steps:

1) Select **Device > Settings**.

2) In the **Automatic key unlock** drop-down list, select one of the following:

- **On** if you want the handset keypad to be unlocked automatically at incoming calls and messages.
- **Off** if you want to keep the handset keypad locked at incoming calls and messages.

3.3.1.3 Phone Lock

Phone lock is used to prevent unauthorized usage of the handset. A phone lock code is required to unlock the handset and access its functions.

NOTICE:

If configured, it is possible to dial any of up to five predefined emergency numbers when the keypad is locked, refer to [Emergency Call Numbers](#) on page 73. Another example of exception that overrides the phone lock is personal alarm.

NOTICE:

It is not recommended to use phone lock when using the shared phone feature, refer to [Shared Phone](#) on page 41.

To configure the **Phone lock**, perform the following steps:

1) Select **Device > Settings**.

2) In the **Phone lock** drop-down list, select one of the following:

- **On** to lock the handset after a specified time when it is not used. For more information, refer to [Automatic Lock Time](#) on page 35.
- **On in charger** to lock the handset when placed in charger.
- **Off** to keep the handset unlocked.

3) If **On in charger** or **On** has been selected, enter the password in the **Phone lock code** field.

3.3.1.4 Automatic Lock Time

When either **Automatic key lock** and/or **Phone lock** is set to **On** or **On except calls**⁴, the lock is activated after a specified period of time. It is possible to change the default time (20 seconds) by doing the following:

- 1) Select **Device > Settings**.
- 2) In the **Automatic lock time** drop-down list, select one of the following:
 - **5 seconds**
 - **10 seconds**
 - **20 seconds** (default)
 - **30 seconds**
 - **1 minute**
 - **3 minutes**

3.3.2 Display

This section describes how to configure or change the display settings for the handset.

3.3.2.1 Hide Menu Items

It is possible to configure the handset in a way to hide the whole menu or certain menu items. To configure **Visibility**, perform the following steps:

- 1) Select **Customization > Visibility**.
- 2) For the applicable menu items in the drop-down lists, select one of the following:
 - **Hide** to conceal the menu or menu items from the user.
 - **Show** to keep the menu or menu item visible on the handset (the user can apply changes).
 - **Read only** to keep the menu or menu item visible on the handset (the user cannot make any changes).

3.3.2.2 User Display Text and Number

User display text parameter defines the text to be displayed on the handset in Idle mode instead of the Endpoint ID. If nothing is entered in this text field, the Endpoint ID is used by default.

User display number defines the number to be displayed on the handset in Idle mode. If this parameter is empty, the Endpoint number is shown.

For additional details on Endpoint ID and number, please refer to [Endpoint ID and Endpoint Number](#) on page 66.

To configure **User display text** and/or **User display number**, do the following:

- 1) Select **Device > Settings**.

⁴ Applicable to **Automatic key lock** only

- 2) In the **User display text** and/or **User display number** field(s), enter the text/number to be displayed in Idle mode.

3.3.2.3 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. To enable this function, select **Device > Settings > Rotate display text > On**.

3.3.2.4 Font Style

The display font style can be changed to bold for improved readability by selecting **Device > Settings > Font style > Bold**.

3.3.2.5 Backlight Timeout

The **Backlight timeout** option defines how long (20 sec by default) the backlight shall be activated in Idle mode. To set the time that passes before the backlight is turned off, perform the following steps:

- 1) Select **Device > General**.
- 2) In the **Backlight timeout** field, enter the number of seconds (1–60 sec).

3.3.2.6 Brightness

To configure the brightness of the handset, perform the following steps:

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

3.3.2.7 Screen Saver

The handset can be configured to display some or no information when it is not in use and when it is placed in a charger. To configure the screen saver, perform the following steps:

- 1) Select **Device > Settings**.
- 2) In the **Screen saver** drop-down list, select one of the following:
 - **Information** to display battery status and identification information while the handset is not in use.
 - **Black** to have a black screen when the handset is not in use.
 - **Black also in call** to have a black screen when the handset is not in use and during the ongoing call.

NOTICE:

It is recommended to use the screen saver setting **Black also in call** to extend the battery life.

3.3.3 Regional Settings

This section describes how to configure date and time on the handset as well as how to set the default language and dialing tone pattern.

3.3.3.1 Set Time & Date

To set the time and date, perform the following steps:

- 1) Select **Device > General**.
- 2) In the **Time zone** drop-down list, select the applicable time zone.
- 3) If the time zone **Other** has been selected, a valid string must be entered in the **Time zone string** field to define the time zone.

NOTICE:

Only unquoted format is supported.

- For time zones and time zone formats, refer to <http://www.timeanddate.com> and <http://pubs.opengroup.org>.
 - For an example of use of time zone strings, refer to [Example of Time Zone String Use](#) on page 37.
 - For the details on how to use time zone strings to automatically update for daylight saving time, refer to [String to Update for Daylight Saving Time](#) on page 37.
- 4) In the **NTP server** field, enter the address of the time server. If it is not set, the IP PBX address is used.
 - 5) Select **Device > Settings**.
 - 6) In the **Time format** drop-down list, select the required time format.
 - 7) In the **Date format** drop-down list, select the required date format.

Example of Time Zone String Use

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). The daylight saving time for the year 2013 begins at two a clock, on a Sunday, the second week in March (M3.2.0/2). The daylight saving time 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>
```

String to Update for Daylight Saving Time

Enter the time zone string to automatically update for daylight saving time:

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

- **Std** is time zone (for example EST for Eastern Standard Time).
- **Offset** is time difference between the time zone and the UTC (Universal Time Coordinator).

- **Dst** defines daylight saving time zone (for example EDT for Eastern Daylight Time).
- **Second Offset** defines time difference between the daylight saving time and the UTC.
- **Date/ Time, Date/ Time** defines the beginning and end of daylight saving time.
 - **Date format** – Mm.n.d (d day of n week in the m month)
 - **Time format** – hh:mm:ss in 24-hour format

NOTICE:

A week always starts on a Sunday and the number for Sunday is 0.

3.3.3.2 Select Default Language and Writing Language

The **Language** option defines the default language of the handset. This setting can later be changed by the user.

The **Writing language** option defines the language used when writing in text fields.

- 1) Select **Device > Settings**.
- 2) In the **Language** and the **Writing Language** drop-down lists, select the languages to be used.

3.3.3.3 Dialing Tone Pattern

To define the tone pattern to use when calling from the handset, perform the following steps:

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

3.3.4 Audio Settings

To configure volume levels for different call modes, perform the following steps:

- 1) Select **Audio > Volume**.
- 2) Select the appropriate volume type from the drop-down lists:
 - **Handsfree volume** sets the volume for ongoing call in loudspeaking mode .
 - **Headset volume** sets the volume for ongoing call when a headset is connected.
 - **Speaker volume** sets the volume for ongoing call in speaker mode (normal call mode).
- 3) In the **Persistent volumes** drop-down list, select **Yes** to automatically store volume changes in the handset for future calls.

The parameter affects the **Handset**, **Headset**, and **Loudspeaking** mode.

NOTICE:

Changing volume parameters can result in lower sound quality and high sound level. Evaluate carefully before applying.

3.3.4.1 Prevent Handset from Being Muted

The handset can be configured to not allow the user to mute the handset or set the volume below a certain level. To prevent the user from muting the handset, select **Audio > General > Prevent silent > On**.

3.3.4.2 Hearing Aid

When **Hearing aid** is enabled, the volume is changed so that the magnetic signal fulfill the requirements for a hearing aid with telecoil.

To enable this parameter, select **Audio > General > Hearing aid > On**.

3.3.4.3 Ring Signal in Handset

To define if the ring signal should be available in both the headset and the loudspeaker or only in the loudspeaker, perform the following steps:

- 1) Select **Audio > General**.
- 2) In the **Ring signal in headset** drop-down list, select **Both headset and loudspeaker** or **Only loudspeaker**.

3.3.4.4 Gain Offset Calibration

To optimize audio quality, perform the following steps:

- 1) In the **Audio** folder, select what should be optimized:
 - **Handset**
 - **Headset**
 - **Loudspeaker**
 - **Bluetooth**
- 2) Change the values of the following if necessary:
 - **Microphone gain offset**
 - **Speaker gain offset**
 - **Microphone side-tone gain offset** (available for **Handset** and **Headset** modes only).

NOTICE:

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

3.3.5 Headset Configuration

This section describes how to configure a handset to dial the last called or predefined number using a wired or Bluetooth headset as well as how to apply settings in order to achieve optimal voice quality.

3.3.5.1 Headset Type

To achieve an optimal voice quality, it is recommended to select the applicable headset profile. To select the headset model, perform the following steps:

- 1) Select **Headset > General**.
- 2) Select the applicable item from the **Headset type** drop-down list:
 - **Mic on boom**
 - **Mic on cable**
 - **User model** (requires additional configuration, refer to [Headset User Model](#) on page 40).

If the preconfigured profile for a wired headset (**Mic on boom** or **Mic on cable**) does not match the headset in use or the audio performance is bad, a customized headset profile (**User model**) can be used instead. Once configured, a customized profile appears in the handset menu.

3.3.5.2 Headset User Model

The following 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 wired headset model to be used.
- 3) In the following drop-down lists, select the applicable values for the wired headset:
 - **Microphone gain** adjusts microphone gain when a headset is used.
 - **Speaker gain** adjusts the speaker gain when a headset is used.
 - **Side tone** adjusts the side tone attenuation when headset is connected.

NOTICE:

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

3.3.5.3 Call with a Headset

To configure the handset to make a call using a wired headset, perform the following steps:

- 1) Select **Headset > General**.

- 2) In the **Call with headset button** drop-down list, select one of the following:
 - a) **Not activated** allows to answer/end call.
 - b) **Last called number** allows to dial the last called number.
 - c) **Predefined number** allows to dial any predefined number. If selected, in the **Predefined number** field, enter the number to be dialed when the headset button is pressed.

Call Using a Bluetooth Headset

To configure the Bluetooth behavior on outgoing calls, perform the following steps:

- 1) Select **Bluetooth > General > Bluetooth enabled > Yes**.
- 2) In the **Call with bluetooth headset button** drop-down list, select **Last called number** or **Predefined number** to define what number to dial when the headset button is pressed when the handset is not in a call or not ringing.

If the **Predefined number** has been selected, type in the required number in the **Predefined number** field.
- 3) In the **Show audio transfer question on outgoing calls** drop-down list, select **Yes** to have the option to route the audio to the handset when starting a new outgoing call with a connected Bluetooth headset. In this case, the user is informed that the audio is routed through the headset and can choose to route it back to the handset. Otherwise, no dialog window is displayed.

3.3.6 Shared Phone

By default, the handset is used in **Personal** mode. It is possible to use the handset as a shared phone by selecting **Device > General > Phone mode > Shared**. When sharing a phone with multiple users, each user has their individual settings that are accessible using a personal user name and password (the password can be a common password for all users or the call number). To use the shared phone functionality, the handset needs to be connected to the Unite module.

NOTICE:

If a personal phone number is accidentally entered into the shared handset, the handset becomes personal and cannot be used as a shared phone any longer. The handset must be configured to be a shared phone again.

3.3.7 Shortcuts

One-click access to predefined functions can be configured for soft keys, hot keys, navigation keys, and the Multifunction button⁵. For example, a soft key can be configured to place a call or open a specific menu.

⁵ Applicable to WL4 and WL4 Messaging only.

Generally, shortcuts are not available when the handset is in a call mode. Although, a hot key configured to execute a service, for example **Send data** ⁶, is available during calls.

NOTICE:

It is recommended to use services (refer to [Services](#) on page 74) in combination with shortcuts, otherwise a user needs to enter the **Services** menu and trigger a service from the menu.

Shortcuts for hot keys, navigation keys, and the Multifunction button are configured in the **Shortcuts** folder and described in the current chapter.

Shortcuts for soft keys are configured in the **User Profiles** folder and described in [Configure Soft Keys](#) on page 84.

3.3.7.1 Configure Hot and Navigation Keys

This section describes how to configure and assign a specific action to perform when the configured hot and/or navigation key is pressed.

Configure a Hot Key

A hot key is activated by pressing a pre-programmed button **0**, **2–9** for more than 1 second in Idle mode. For example, the hot key function can be used to change the profile, send a message, or make a phone call to a specific number. To configure the hot key(s), do the following:

- 1) Select **Shortcuts > Hot key 0** (or 2–9).
- 2) In the **Function** drop-down list, select the action to be performed when the configured key is pressed. For the whole list of available functions, refer to [Shortcut Functions](#) on page 43.
- 3) In the **Value** field, enter the applicable value for a function, for example a phone number.

NOTICE:

Only certain functions require a value.

- 4) In the **Control question** drop-down list, select **Yes** to display the **Proceed?** dialog window every time the configured key is pressed. This setting prevents from the assigned action to be performed immediately in cases when a key has been pressed by mistake.
- 5) In the **Read only** drop-down list, select **True** to prevent the user from changing the shortcut.

Configure a Navigation Key

- 1) Select **Shortcuts > Navigation Key Up**, **Down**, **Left**, or **Right**.
- 2) Follow the steps 2–5 as described above in [Configure a Hot Key](#) on page 42.

⁶ Applicable to WL4 Messaging and WL4 Plus only.

3.3.7.2 Shortcut Functions

This section describes all available functions that can be assigned to soft keys, hot keys, navigation keys, and the Multifunction button. The list of all functions is found in the **Function** drop-down list and includes the following:

- **Not Used**
- **Phone Call**
- **Phone Call Loudspeaker**
- **Call List**
- **Contact List**
- **Central Phonebook** (system-dependent feature)
- **Message inbox** (applicable to WL4 Messaging and WL4 Plus only)
- **Send Message** (applicable to WL4 Messaging and WL4 Plus only)
- **Change Profile Normal**
- **Change Profile X (1–4)** (the selected profile must be first configured, refer to the [Profiles](#) on page 80)
- **Open Menu Main Menu**
- **Open Menu Calls**
- **Open Menu Call Services**
- **Open Menu Call Pickup Groups**
- **Open Menu Connections**
- **Open Menu Contacts**
- **Open Menu Messaging** (applicable to WL4 Messaging and WL4 Plus only)
- **Open Menu Profiles**
- **Open Menu Settings**
- **Executive Service X (1–10)** (applicable to WL4 Messaging and WL4 Plus only)
- **Logout** (applicable to **Share phone** feature only)
- **Call Diversions**
- **RSSI Measure**

3.3.7.3 Multifunction Button

This section describes how to assign different functions to the Multifunction button.

Configure the Multifunction Button as a Shortcut

NOTICE:

Applicable to WL4 and WL4 Messaging only.

The Multifunction button can be configured to perform various actions on a long and multi-press, for example to open a specific menu or to initiate a call. To assign functions for a long and multi-press, do the following:

- 1) Select **Shortcuts > Multi-function Button Longpress** or **Multi-function Button Multipress**.

- 2) In the **Function** drop-down list, select the action to be performed when the configured key is pressed. For the whole list of available functions, refer to [Shortcut Functions](#) on page 43.
- 3) In the **Value** field, enter the applicable value for a function, for example a phone number.

NOTICE:

Only certain functions require a value.

- 4) In the **Control question** drop-down list, select **Yes** to display the *Proceed?* dialog window every time the configured key is pressed. This setting prevents from the assigned action to be performed immediately in cases when a key has been pressed by mistake.
- 5) In the **Read only** drop-down list, select **True** to prevent the user from changing the shortcut.

Configure the Multifunction Button to be a PTT button

NOTICE:

Applicable to WL4 Messaging only.

By default, the Mute button is used as a Push-to-Talk (PTT) button. Although, for users who are required to wear gloves, it is more practical to configure the Multifunction button for the PTT function. To set the Multifunction button as a PTT button, select **Device > Call > Multi func button for PTT > On**.

3.3.8 Messaging Settings

NOTICE:

Applicable to WL4 Messaging and WL4 Plus only.

To configure the way incoming messages are indicated and displayed on handset, go into the **Device > Messaging** and configure the following parameters:

- 1) **Message list representation** can be represented by number/name or message text.
- 2) **Message text size** defines the text size used when displaying messages.
- 3) **Time to read (TTR)** defines if the user needs to close a message manually or if the message automatically closes when the TTR expires. Regardless of how a message is closed, it is removed from the message queue and stored in the Inbox. TTR starts when a message is displayed and continues to run when the message is placed in the messaging queue. If a user presses any key when a message is displayed, the TTR is reset. For examples, refer to [Examples of TTR and TTP Settings](#) on page 48.

If the messages needs to be closed manually, in the **Time to read (TTR)** drop-down list, select **Close manually**. Otherwise, select the required time from the list.

- 4) **Time to prioritize (TTP)** defines how long time messages keep their priority status. The TTP starts when a message is displayed. If a user presses any

key when a message is displayed, the TTP is reset. If receiving a message with higher priority than the displayed message, the message with lower priority is placed in queue and its TTP is paused. When the TTP elapses for a message, it is put last in the queue. For examples, refer to [Examples of TTR and TTP Settings](#) on page 48.

The following options can be selected:

- **No prioritization** means that the messages are displayed in chronological order without taking into account their priority.
 - **Prioritize 10/20/30 seconds** and **Prioritize 1/2/5/10 minutes** mean that messages are displayed in an order depending on their priority.
 - **Prioritize forever** means that a message with the highest priority is always displayed first and it is shown until the user closes it.
- 5) **Repeat message indication** enables/disables message indications. It sets whether a message indication is repeated until confirmed by the user or not. The repetition rate is 7 seconds. If the message itself contains a repetition, it overrides this setting.
 - 6) **Vibrator for message during call** defines if the handset vibrates or not when receiving messages during an ongoing call. It is possible to have vibration always activated or set it only for urgent messages.
 - 7) **Message alert during call** defines if a message alert should be played or not when receiving a message during a call. It is possible to have alert always activated or set it only for urgent messages.
 - 8) **IM option mode** is used for customer-specific applications and sets that three soft keys are placed automatically, that is on soft keys or in an option menu (list).
 - 9) **Call priority** defines whether call information shown on the display during an incoming, ongoing, and outgoing call is suppressed when viewing a message. It also defines whether an ongoing call is disconnected when receiving a PTT invitation with **Answer mode** set to **Automatically**. The following values can be set:
 - **0** call indication overrides all messages and the ongoing call is never disconnected.
 - **1–9** comparison with message priority; highest priority is shown, and a PTT invitation with higher priority causes disconnection of ongoing call.
 - **10** call indication on the display is always suppressed and the ongoing call is always disconnected by a PTT invitation.

The tables below show examples of priority settings and how they affect the handset's behavior.

Table 1: Call Priority vs PTT Priority

Call priority	PTT invitation (priority) ⁷	Disconnect an ongoing call?
0	1	No, since this call priority setting overrides all PTT invitations regardless of priority.
6	6	No, an ongoing call is not disconnected when the priority is equal.

⁷ PTT invitation received as incoming call has always priority 6, while PTT invitation received as message can have priority 1–9 depending on configuration.

Call priority	PTT invitation (priority) ⁷	Disconnect an ongoing call?
2	1	Yes, immediately since the PTT priority is set to 1 and is also higher than Call priority.
3	2	Yes, after 10 seconds since the PTT priority is higher than Call priority.
10	1	Yes, immediately since the PTT priority is set to 1 and also is higher than Call priority.
10	2	Yes, after 10 seconds since the PTT priority is higher than Call priority.

Table 2: Call Priority vs Message Priority

Call priority	Displayed message (priority)	Call information suppressed?
0	1	No, since this call priority setting overrides all messages regardless of priority.
7	6	Yes, since the priority of the displayed message is higher than the incoming call.
6	6	Yes, since the message is considered as most important when the priority is equal.
1	3	No, since the priority of the incoming call is higher than the displayed message.
10	1	Yes, the call information is always suppressed regardless of the message priority.

1) **Show and indicate messages in charger**, refer to [Show and Indicate Messages in Charger](#) on page 54.

3.3.8.1 Configure Message Alerts with Beep Codes

This section describes the use of beep codes for incoming messages.

Beeps according to beep code, **High beeps according to beep code**, **Enhanced beeps according to beep code**, and **Custom sounds according to beep code** parameters described in the current section can be enabled both for **User Profiles** and **System Profiles**. For the details, please refer to the [Configure Sound and Alerts](#) on page 81 or [Configure Sounds and Alerts Groups \(Sub-group\)](#) on page 85.

Beeps or High Beeps According to Beep Code

In case of regular beeps, the handset plays the original message alerts that are mapped to the beep codes. In case of high beep codes, the handset plays the

⁷ PTT invitation received as incoming call has always priority 6, while PTT invitation received as message can have priority 1–9 depending on configuration.

original message alerts that are mapped to the beep codes with a higher pitch than the regular beeps.

Beep code sent from a system or application	Corresponding sound from the handset
Beep code 0	No message alert is played
Beep codes 1–6	1–5, and 10 beeps, respectively
Beep code 7	Siren

Enhanced Beeps According to Beep Code

The handset plays the extended message alerts that are mapped to the beep codes, but in the form of melodies.

Beep code sent from a system or application	Corresponding sound from the handset
Beep code 0	No message alert is played
Beep codes 1–3	1–3 beeps, respectively
Beep code 4	3 tones chime
Beep code 5	10 beeps
Beep code 6	Alarm sweep
Beep code 7	Siren

Custom Sounds According to Beep Code

The handset can play customized message alerts that are mapped to beep codes. The message alerts must first be customized and then mapped to the beep codes.

NOTICE:

It is recommended to use this feature to create a message alert that sounds like the equipment (for example a respirator) that generates an alarm. You can also use custom sounds in cases when you want to customize any of the default handset beeps (Beeps and Enhanced beeps), refer to [Configure Custom Sounds](#) on page 123.

Beep code sent from a system or application	Corresponding sound from the handset
Beep code 0	No message alert is played
Beep codes 1–7	Corresponding customized sound

To create customized sounds, do the following:

- 1) Select **Audio > Custom sounds > Custom sound X (1–10)**.

2) Set the following parameters:

- **Label** is the name of the custom sound (required). The name is visible when mapping the custom sound to a beep code later on.
- **Melody** is the text string represents a non-polyphonic sound. Example of melodies are set by default for **Custom sound X** (1–10), refer to [Configure Custom Sounds](#) on page 123.
- **Beat** is the tempo in beats per minute to be used when playing the sound.
- **Style** is the ratio of note to rest period to be used when playing the sound.
- **Instrument** is the instrument to be used when playing the sound.

3.3.8.2 Examples of TTR and TTP Settings

Example 1

This example describes the message handling with the following message settings:

- 1) TTP – Prioritize forever
- 2) TTR – Close manually

NOTICE:

It is recommended to use these settings if messages with the highest priority are always displayed until the user closes the current message.

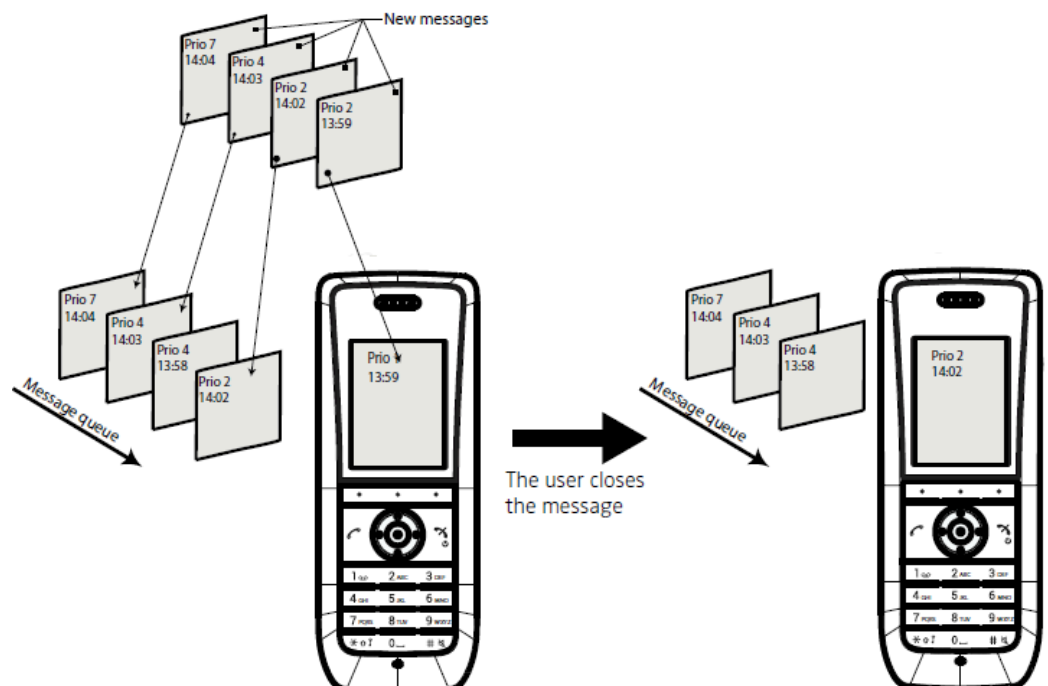


Figure 1: Queuing and Prioritizing for Messages with Equal Priorities

In [Figure 1: Queuing and Prioritizing for Messages with Equal Priorities](#) on page 48, a message with priority 2 is received at 13:59 and is displayed in the handset. Another message with equal priority is received at 14:02 and is placed in the queue. If no messages with higher priority are received, the user needs to close the currently displayed message to show the next message in the queue, in this case, the message received at 14:02. The closed message is indicated as a read message in the Inbox.

Example 2

This example describes the message handling with the following message settings:

- 1) TTP – 20 seconds
- 2) TTR – Close manually

NOTICE:

It is recommended to use these settings in case the user needs not to be interrupted for 20 seconds while reading a message, unless a message with a higher priority is received. After the user has read a message, its priority is no longer important, and the TTP expires.

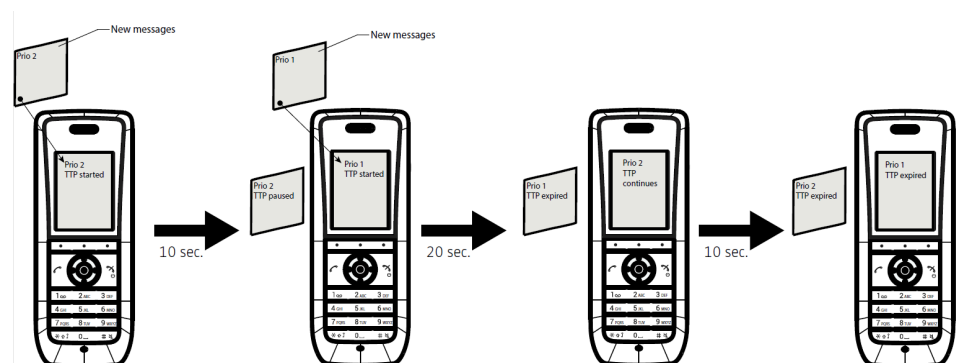


Figure 2: Queuing and Prioritizing for Messages with Different Priorities

In [Figure 2: Queuing and Prioritizing for Messages with Different Priorities](#) on page 49, a message with priority 2 is received and displayed in the handset, and the TTP for the message is started.

After 10 seconds, a second message with priority 1 is received and displayed while the message with priority 2 is put in the queue. TTP for the message with priority 2 is paused, and TTP for the message with priority 1 is started.

After 20 seconds, TTP expires for the message with prio 1 and the message is placed in the queue. The message with priority 2 is shown again and its TTP continues.

TTP expires after 10 seconds for the message with priority 2. In this case, all messages have been shown for 20 seconds each, and the oldest shown message with the highest priority is displayed, in this case, the message with priority 1. The handset does not indicate when it shows the message again, since it already has been shown and indicated once. The message with priority 2 is placed in the queue.

Example 3

This example describes the message handling with the following message settings:

- TTP – 20 seconds
- TTR – 2 minutes

NOTICE:

It is recommended to use these settings in case the user needs not to be interrupted for 20 seconds while reading a message, unless a message with a higher priority is received. After the user has read a message, its priority is no longer important, and the TTP expires.

In addition, if a message is not shown again within the TTR interval, it is considered as not important and is removed from the queue.

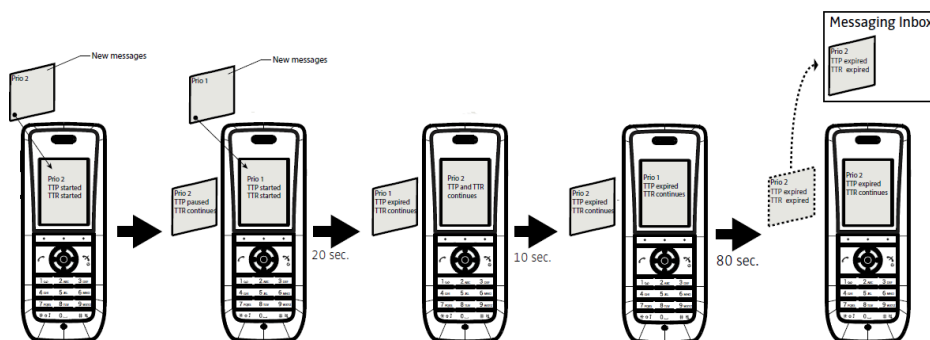


Figure 3: Message Handling without Manually Closing a Message

In [Figure 3: Message Handling without Manually Closing a Message](#) on page 50, a message with priority 2 is received and displayed in the handset. TTP and TTR for the message is started.

After 10 seconds, a second message with priority 1 is received and displayed while the message with priority 2 is put in the queue. TTP for the message with priority 2 is paused, but TTR continues. TTP and TTR for the message with priority 1 is started.

After 20 seconds, TTP expires but TTR continues for the message with prio 1 and the message is placed in the queue. The message with priority 2 is shown again and its TTP continues.

TTP expires after 10 seconds but TTR continues for the message with priority 2. In this case, all messages have been shown 20 seconds each, and the oldest shown message with the highest priority is displayed, in this case, the message with priority 1. The handset does not indicate when it shows the message again, since it already has been shown and indicated once. The message with priority 2 is placed in the queue.

After 80 seconds, the TTR expires for the message with priority 2, and it is removed from the queue and is indicated as an unread message in the Inbox. When TTR expires for the message with priority 1, it is also indicated as an unread message in the Inbox.

If no messages have been read/closed manually and TTP expires for each message, the New message(s): [number of messages]. View now? dialog window is displayed. All messages are indicated as unread messages in the Inbox.

Example 4

This example describes the message handling with the following message settings:

- TTP – No prioritization
- TTR – Close manually

NOTICE:

It is recommended to use these settings if messages regardless of priority are read in chronological order, that is, the newest message is displayed first.

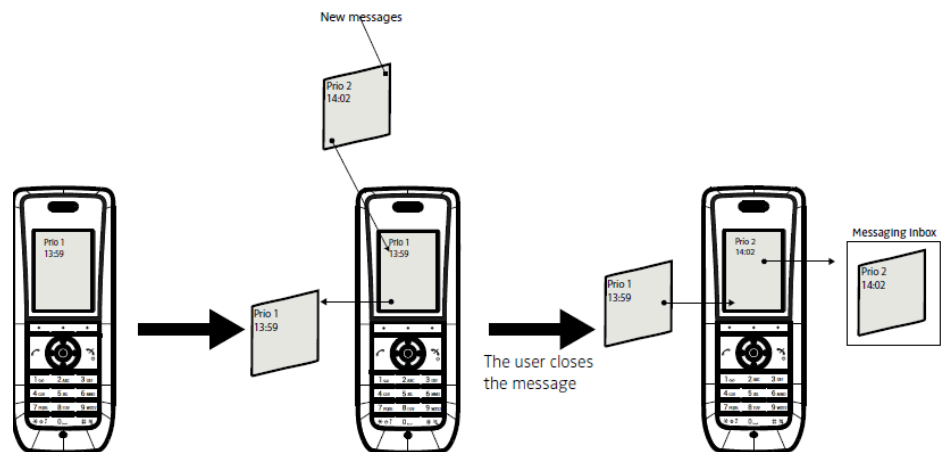


Figure 4: Messages Displayed in Chronological Order Regardless of Priority

In [Figure 4: Messages Displayed in Chronological Order Regardless of Priority](#) on page 51, a message with priority 1 is received at 13:59. Another message with priority 2 is received at 14:02 and is displayed. The message with priority 1 is put in the message queue. The user needs to close the current message with priority 2 to show the message with priority 1 in the queue. When closing the message with priority 2 it is indicated as a read message in the Inbox.

3.3.8.3 Message Retransmit Limit

This parameter defines the number of retransmissions before the transmission of the message is considered as failed. The retransmission procedure begins if a sent message is not acknowledged within 15 seconds.

- 1) Select **Device** > **wsg**.
- 2) In the **Message retransmit limit**, set the maximum number of retransmissions.

3.3.8.4 Message Templates

NOTICE:

Applicable to WL4 Messaging and WL4 Plus only.

Handsets can be configured with predefined messages using the message template function. A predefined message can be used in the following ways:

- 1) When the user wants to decline a call, but still would like to acknowledge it with a message (requires a parameter setting, refer to [Configure the Handset for Message Templates](#) on page 52).
- 2) When the user wants to send a fast response to the received message instead of writing an answer from scratch.
- 3) When the user want to write a new message using the predefined message.

For additional information about how the message template function is used, refer to *Unify OpenScape WLAN Phone WL4, User Manual, TD 93342EN*.

3.3.8.4.1 Configure the Handset for Message Templates

To activate the message template function in the handset so that a user can decline a call with a predefined message, perform the following steps:

- 1) Select **User Profiles > Normal or Profile X (1–4) > Answering**.
- 2) In the **Can reply with a message template when rejecting a call** drop-down list, select **Yes** to show the `Reply with a message template?` dialog window every time when a user rejects an incoming call.

NOTICE:

If no message templates are defined, the dialog window is not shown.

3.3.8.4.2 Create Message Templates

A handset can be configured with up to five predefined messages. A message cannot exceed 50 characters. To create a message, perform the following steps:

- 1) Select **Device > Messaging**.
- 2) Expand the **Messaging** menu and select **Message Template X (1–5)**.
- 3) In the **Message Text** field, write a message that you want to be used as predefined.

NOTICE:

If a system uses a character set other than UTF-8 for SMS, make sure that the characters entered into the message strings are compatible with the character set used by the system. Entering characters that cannot be encoded by the system may cause a type conversion error, the delivery failure accompanied with the `Message failed` dialog window.

3.3.9 In Charger Actions and Behavior

This section describes different types of actions that can be configured for the handset when it is placed in a charger.

3.3.9.1 Quick Answer

The handset can be configured to automatically answer an incoming call when removed from charger. To enable this function, select **Device > Call > Quick answer > Yes**.

3.3.9.2 In Charger Action when Not in Call

This setting defines an action to perform when handset is placed in charger. To configure the **In charger action** parameter, perform the following steps:

- 1) Select **Device > Settings**.
- 2) In the **In charger action** drop-down list, select one of the following:
 - **No action**
 - **Switch off** to turn the handset off when placed in charger. The handset is turned on again when removed from the charger .
 - **Sound off** to mute the handset when placed in charger .

NOTICE:

All incoming messages are affected by this setting including PTT invitations received as messages and all other messages regardless of priority (even messages with breakthrough such as high/alarm priority). To silence only messages without breakthrough (low/normal priority), select the **Sound off** parameter.

To mute all messages (regardless of priority), set the **Device > Messaging > Show and indicate messages in charger** to **Off**. For the details, refer to [Show and Indicate Messages in Charger](#) on page 54.

-
- **Change profile** to automatically change profile when placed in charger (applicable to WL4 Plus only) .

In the **Change profile in charger** drop-down list, select the profile to be used. For the details on how to configure the selected profile, please refer to [Profiles](#) on page 80.

- 3) In the **In charger Message absent** drop-down list, select one of the following:

NOTICE:

This function is applicable to WL4 Messaging and WL4 Plus only.

- **No** to save all incoming messages in the Inbox while the handset is placed in the charger (default).
- **Yes** to not receive any messages. If a message is sent from a system, it is notified that the handset is absent.

3.3.9.3 Clear Lists in Charger

This parameter defines if message and call lists are deleted when the handset is placed in the charger. To configure **Clear lists in charger**, perform the following steps:

- 1) Select **Device > General**.
- 2) In the **Clear lists in charger** drop-down list, select one of the following:
 - **Yes** to delete all records in message and call lists when the handset is placed in charger.
 - **No** to delete nothing.

3.3.9.4 USB Behavior

This setting defines the behavior of the handset when it is connected to a PC over USB. To configure **USB Behavior**, perform the following steps:

- 1) Select **Device > General**.
- 2) In the **USB Behavior** drop-down list, select one of the following:
 - **Ask** to manually chose the preferred mode (**WinPDM**, **MTP**, or **Charge**) each time the handset is connected to a PC over USB.
 - **WinPDM** allows the handset to communicate with the WinPDM application on a PC.
 - **MTP** shows the handset as a media device and allows to view and transfer log files from the handset.
 - **Charge** sets the handset to charge only mode.

If **Ask** or **WinPDM** is selected, it is possible to configure the **WinPDM authentication** parameter to restrict access to WinPDM. For more information, refer to [WinPDM Authentication](#) on page 24.

3.3.9.5 Show and Indicate Messages in Charger

NOTICE:

Applicable to WL4 Messaging and WL4 Plus only.

It defines how incoming messages are displayed or indicated while the handset is placed in charger.

NOTICE:

All incoming messages are affected by this setting including PTT invitations received as messages and all other messages regardless of priority (even messages with breakthrough such as high/alarm priority). To silence only messages without breakthrough (low/normal priority), enable the **Sound off** parameter in **Device > Settings > In charger action**.

- 1) Select **Device > Messaging**.
- 2) In the **Show and indicate messages in charger** drop-down list, select one of the following:
 - **On** to show and indicate (by beep) any incoming message while the handset is in charger (default).
 - **Off** to mute any alert for incoming messages. If selected, the **New message** icon is still displayed on the handset and all incoming messages are stored as unread in the Inbox.

3.3.10 Handset and Battery Warnings

This section includes information about how to configure indications for **No network** and **No access** warning messages as well as how to set warning indication when battery charge level is low.

3.3.10.1 No Network Warning

If the handset has no coverage, it shows the **No network** warning message on the handset in Idle mode. It is also accompanied with a vibrating alert (if enabled), a beep signal (if enabled), and displays a dialog window (if enabled).

To configure the **No network warning** indication, perform the following steps:

- 1) Select **Device > General**.
- 2) In the **No network warning** drop-down list, select one of the following:
 - **Indicate repeatedly** defines that a short beep signal is on (if enabled), **No network** warning message is displayed in Idle mode, the vibrating alert is on (if enabled), a dialog window is shown (if enabled). This simultaneous indication is repeated every minute for 30 minutes. This is the default setting.
 - **Indicate once** defines that a short beep signal is on (if enabled), **No network** warning message is displayed in Idle mode, the vibrating alert is on (if enabled), a dialog window is shown (if enabled). This simultaneous indication is made only once.
 - **Indication off** defines that a short beep signal is off (even if enabled), **No network** warning message is displayed in Idle mode, the vibrating alert is off (even if enabled), a dialog window is either shown or not (depends on the parameter settings).

NOTICE:

Even if **Indication off** is selected, a dialog window still appears when **Device > General > Dialog window for no network/no access warnings** is set to **Yes**.

3.3.10.2 No Access Warning

If the handset has no access, has lost messaging and/or voice connection, it shows the **No access**, **Messaging only**, or **Voice only** warning message on the handset in Idle mode. It is also accompanied with a vibrating alert (if enabled), a beep signal (if enabled), and a dialog window (if enabled).

No access message means that there is neither voice nor messaging connection.

To configure the **No access warning**, perform the following steps:

- 1) Select **Device > General**.
- 2) In the **No access warning** drop-down list, select one of the following:
 - **Indicate repeatedly** defines that a short beep signal is on, **No access/Voice only/Messaging only** warning message is displayed in Idle mode, the vibrating alert is on (if enabled), a dialog window is shown (if enabled). This simultaneous indication is repeated every minute for 30 minutes.
 - **Indicate once** defines that a short beep signal is on, **No access** warning message is displayed in Idle mode, the vibrating alert is on (if enabled), a dialog window is shown (if enabled). This simultaneous indication is made only once.
 - **Indication off** defines that a short beep signal is off, **No access** warning message is displayed in Idle mode, the vibrating alert is off (if enabled), a dialog window is either shown or not (depends on the parameter settings). This is the default setting.

NOTICE:

Even if **Indication off** is selected, a dialog window still appears when **Device > General > Dialog window for no network/no access warnings** is set to **Yes**.

3.3.10.3 Dialog Window for No Network/No Access Warnings

This parameter defines if the **No network**, **No access**, **Voice only**, and **Messaging only** dialog window is visible or not on the handset.

- 1) Select **Device > General**.

- 2) In the **Dialog window for no network/no access warnings** drop-down list, select one of the following:

- a) **Yes** to show the dialog window on the handset (default).

NOTICE:

When set to **Yes**, it overrides the **Indication off** setting in **Device > General > No network warning** or **No access warning**, so the dialog window is still shown.

- b) **No** to hide the dialog window but still show the warning message on the handset in Idle mode.

3.3.10.4 Battery Warning

When the battery is low, the warning indication can be set to different modes.

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

3.3.11 System Administration in the Handset

The handset has a hidden Admin menu for system administrators that can be used to perform quick changes directly on the handset.

To access the **Admin menu** on the handset, select **Main Menu > Settings** and enter the Admin access code (default 40022). 40022 is the default access code used for all handsets and it is therefore important to change it before the handset is deployed. For the details on how to change the PIN code, please refer to [Change Admin Access Code](#) on page 60.

IMPORTANT: It is important not to lose the new Admin access code. If neither the WinPDM/WSG DM connection nor the Admin access code is available, there will be no way to reconfigure or factory reset the handset.

NOTICE:

If the handset has been factory reset or not configured, enter the Admin access code while the handset is showing the **No network** message at start-up.

The Admin menu contains the following information:

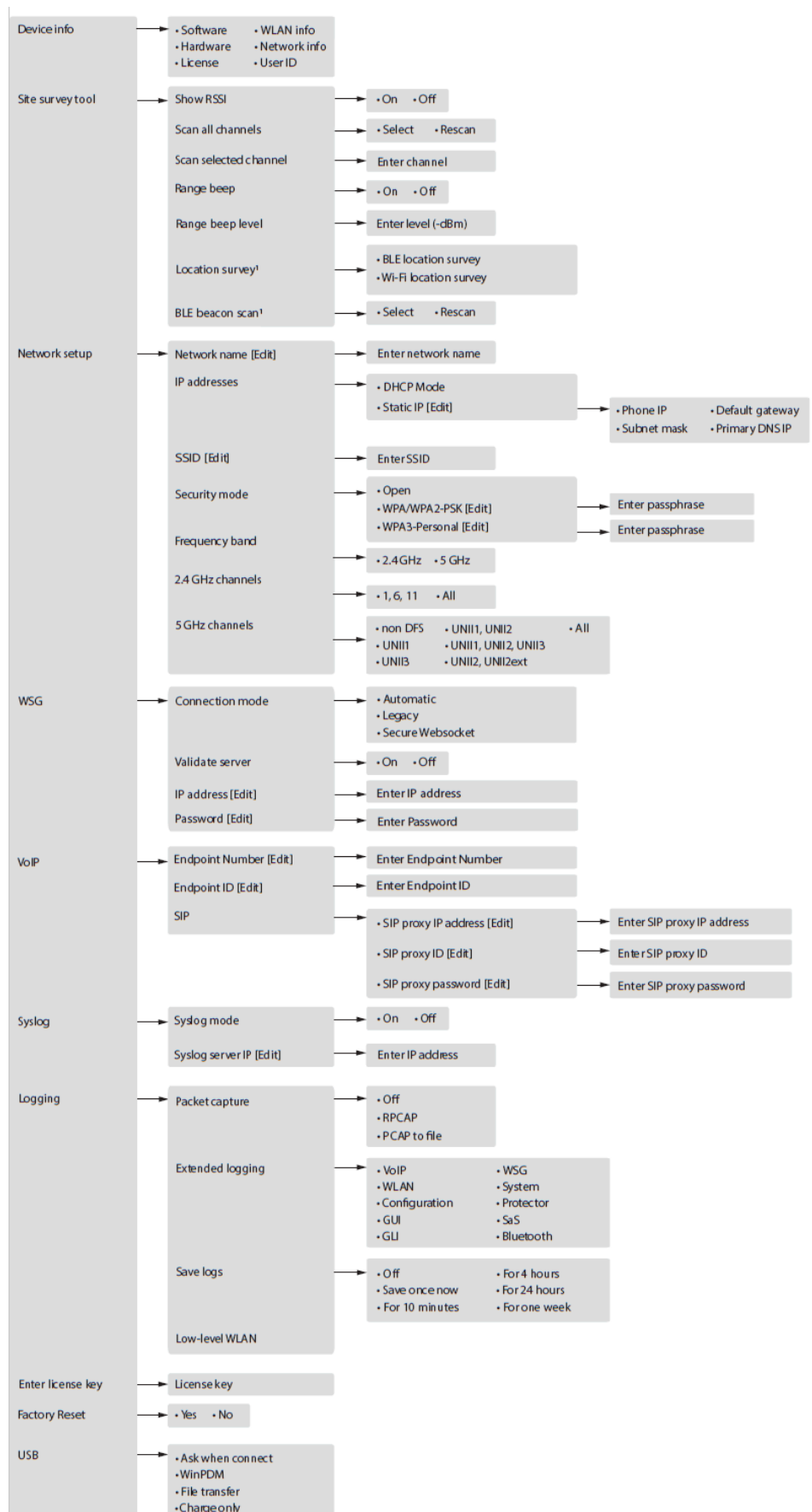
- Device information including the following:
 - Software
 - Hardware
 - License
 - WLAN info
 - Network info
 - User ID
- Site survey tool
- Network setup menu
- WSG menu
- VoIP menu
- Syslog
- Logging options
- Entering license key
- Factory reset option
- USB behavior

3.3.11.1 Block Access to the Admin Menu

By default, it is possible to access the Admin menu from the handset. To prevent users from accessing the Admin menu, perform the following steps:

- 1) Select **Device > General**.
- 2) In the **Admin menu access** drop-down list, select **Off**.

3.3.11.2 Admin Menu Tree in the Handset



To get the detailed information about the whole Main menu structure, refer to *OpenScape WLAN Phone WL4, User Guide*

3.3.11.3 Quick Access to Admin Menu Functions and Device Information

For quick access to device information and certain functions, the following codes can be used in Idle mode.

Code	Information
*#34#	To access Device info in the Admin menu. Select either of the following menus: 1) Software 2) Hardware 3) License 4) WLAN info 5) Network info 6) User ID
*#35#	To access Enter license key in the Admin menu.
*#76#	To view RSSI information. NOTE: RSSI information is displayed in Picture-in-Picture (PIP) mode and might be disturbing when using the handset. To hide the RSSI window, enter *#76# one more time in Idle mode.
*#77#	To access Site survey tool in the Admin menu. Select either of the following menus: 1) Show RSSI 2) Scan all channels 3) Scan selected channels 4) Range beep 5) Range beep level 6) Location survey (applicable to WL4 Plus only) 7) BLE beacon scan (applicable to WL4 Plus only)

3.3.11.4 Change Admin Access Code

In case the Admin access code has been forgotten, it is possible to reset it by performing the following steps:

- 1) Select **Device** > **General**.**
- 2) In the **Admin access code** field, enter a new password.**

3.3.11.5 Transfer Unlock File

Transfer unlock file parameter is used for debugging purposes. Due to security reasons, the handset needs to be factory-reset after debugging is finished.

NOTICE:

Unlock file is generated and delivered by Ascom (Sweden) AB.

- 1) Select **Device > General**.
- 2) Open the unlock file in any preferable editor and copy the whole string value that is delivered in base64 format.

NOTICE:

The name of the file corresponds to the serial number of the handset used for debugging.

- 3) Paste the copied text into the **Transfer Unlock File** field and press **Enter**.
- 4) Save changes in the WinPDM/WSG DM .
- 5) Restart the handset.

3.4 Location

The following location systems are supported by the handset:

- 1) Cisco MSE that uses APs to measure the client signal strength for received data packets and forward those measurements to the Cisco MSE, refer to [Configure Handset for Cisco MSE or AiRISTA Flow RTLS](#) on page 62 (applicable to WL4 Plus only).
- 2) AiRISTA Flow RTLS that enables the handset to collect information about the APs and their measured radio field strength and forward this information to the AiRISTA Flow Positioning Engine, which calculates the location of the handset, refer to [Configure Handset for Cisco MSE or AiRISTA Flow RTLS](#) on page 62 (applicable to WL4 Plus only).
- 3) BLE location enables location tracking via BLE beacons, refer to [Enable BLE Location](#) on page 62 (applicable to WL4 Plus only).

Special Location

A special location is a valid location received from a location device that triggers the handset to automatically send the location information list to the system. A special location is marked with an asterisk (*) next to location ID in the location survey list. To prevent the system from being overloaded, a special location that has already been received in the last three seconds will not be sent to the system again.

To allow the handset to send location information when entering the range of BLE location device (which is defined as a special location), select **Location > Common > Special location > On**.

3.4.1 Enable BLE Location

NOTICE:

Applicable to WL4 Plus only.

Bluetooth Low Energy (BLE) is a form of wireless communication designed specifically for short-range communication. The BLE technology uses BLE beacons that are strategically mounted throughout locations, to broadcast BLE signals in a given range. BLE infrastructure works indoors and outdoors. When this parameter is enabled the identification of the four latest detected BLE Locators is included in an alarm or location request.

To configure **BLE location**, perform the following steps:

- 1) Select **BLE location** > **On** to enable the location service.
- 2) Configure the following parameters:
 - a) **BLE idle duration** defines the idle time (in seconds) between BLE scans. If the idle duration is zero, the handset scans continuously.
 - b) **BLE scan duration** defines (in seconds) for how long the handset should scan.
 - c) **BLE RSSI offset** defines (in dBm) the BLE location RSSI offset. A higher value makes the BLE location less sensitive by increasing the perceived RSSI value of the current location.
 - d) **BLE RSSI threshold** defines (in dBm) the RSSI threshold for a BLE location. The handset filters out any BLE location below the set RSSI.
 - e) **BLE UUID filter** defines the UUID that the handset should scan for.

3.4.2 Configure Handset for Cisco MSE or AiRISTA Flow RTLS

NOTICE:

Applicable to WL4 Plus only.

The handset is compatible with both Cisco MSE and AiRISTA Flow RTLS, which give a more accurate location than AP Location. To configure the handset to use these location services, follow the steps below:

- 1) Select **Location** > **Common** > **WLAN location scanning** > **On**.
- 2) In the **WLAN scanning interval** field, set the time between the scanning periods.

- 3) In the **WLAN scans per scanning period** drop-down list, select how many scans should be performed during each scanning period.

NOTICE:

Close scanning periods and frequent scans per period shorten the battery time.

NOTICE:

You can additionally configure the handset so location scanning is performed at shorter intervals (1s), which can be useful when performing site survey in RTLS deployments. On the handset, go to the Admin menu and select **Site survey tool > Location survey > Wi-Fi location survey > On**.

- 4) If AiRISTA Flow RTLS solution is used, select **Location > AiRISTA Flow > AiRISTA Flow Location Scanning > Yes** and configure the following parameters:
- a) **IP address** defines the IP address of the AiRISTA Flow RTLS server. The handset will send locations to this server.
 - b) **Listening port** defines the port the AiRISTA Flow RTLS server is listening to.

3.5 Telephony

3.5.1 VoIP

This section includes information about the parameters that should be configured in the first place to enable SIP calls.

3.5.1.1 VoIP Protocol

A protocol is a set of standard rules for data traffic required to send information over a communication channel. The supported VoIP protocol is Session Initiation Protocol (SIP). To configure SIP, go into the **VoIP > SIP**.

The following SIP parameters are available:

SIP Transport	Defines the protocol (UDP, TCP, or TLS) to be used for SIP signaling.
----------------------	--

SIP TLS client certificate	- If SIP transport is set to TLS, select a client certificate to be used for authentication with the SIP proxy. You can use either self-signed (automatically generated) or imported application certificates. Refer to Import Trust and Application Certificates on page 67 to get the details on how to import certificates to the handset. - If SIP transport is set to Automatic, a certificate is chosen in the following order: 1) Certificate received from SCEP server is used (if exists). 2) Built-in certificate is used (only available for certain handset versions). 3) Self-signed certificate is used.
Validate server certificate	Controls if the handset will require SIP proxy authentication when SIP transport is set to TLS. 1) If set to Yes, the certificate corresponding to the key used to sign the certificate of the SIP proxy (i.e. the "root certificate") must be imported as a trusted certificate. For a self-signed certificate this is the certificate itself. Refer to Import Trust and Application Certificates on page 67 to get the details on how to import certificates to the handset. 2) If set to No, encrypted connections can be set up without loading any trusted certificates into the handset.
Outbound proxy mode	Allows to send all outgoing SIP messages to the outbound proxy which then forwards them to the SIP proxy identified by SIP proxy ID 1) Select Yes to connect the handset to the SIP proxy through an outbound proxy. 2) Set to No to connect the handset directly to the SIP proxy (Primary SIP proxy and/or Secondary SIP proxy).

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. If the handset fails to register with the primary SIP proxy, it can register with the optional secondary SIP proxy. Examples of valid formats are: 192.168.1.1 or proxy1.mydomain.com, or 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. NOTE: This parameter is only visible if Outbound proxy mode is set to No. NOTE: Only a plain IP address is shown in the Admin menu under the VoIP > SIP > SIP proxy IP address.
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 <i>Primary SIP proxy</i> above. When the handset has connected to the Secondary SIP proxy, it continuously tries to reconnect to the Primary SIP proxy. NOTE: This parameter is only visible if Outbound proxy mode is set to No.
Outbound proxy	Defines the primary outbound proxy by a domain name, an IP address, or an IP address with a port number.
Listening port	Defines 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 assigned IP addresses.
SIP proxy password	Defines the password to be used when the handset registers at the SIP proxy.
Send DTMF using RFC 2833 or SIP INFO	Defines the path the DTMF signaling should take. 1) If set to RFC 2833, the DTMF signaling is sent in the RTP stream (from handset to handset). 2) If set to SIP INFO, the DTMF signaling is sent using SIP signaling (through the PBX).

Hold type	Defines the type of hold that is sent 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 handset shall use Endpoint number , Endpoint ID , or MAC address to register with the SIP proxy.
Authentication identity	Defines if the handset shall use Endpoint number , Endpoint ID , or MAC address to authenticate with the SIP proxy.
MOH locally (Music on Hold)	Allows the handset to play music when a call is placed on hold. If PBX does not support MOH, tone is played instead.
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 <code>USE_PROXY</code> message.
SIP Register Expiration	Defines the number of seconds for register expiration to the PBX.
Far-End NAT Traversal	Allows phone communications to traverse a NAT device that is farthest away from the SIP server and near the handsets. The parameter is used when the SIP server is not local and the phones are behind a NAT.
Register with SIP instance-id	When set to Yes, the MAC address is send in SIP REGISTER message according to RFC 5626. When an emergency call is established, the SIP server authenticates the handset through the MAC Address of REGISTER message and forwards it to the system so that the handset's location is clearly identified. NOTE: This is a solution that Avaya PBX supports.

3.5.1.2 Endpoint ID and Endpoint Number

The **Endpoint ID** and **Endpoint number** are automatically received when registering the handset in the PBX system.

Endpoint ID

The **Endpoint ID** is the identity (name or number) that is registered for the user in the system and displayed on the handset in Idle mode. To change the identity, select **VoIP > General** and enter a new ID in the **Endpoint ID** field.

User display text (for example a name) can be used instead of the Endpoint ID, for the details refer to [User Display Text and Number](#) on page 35.

Endpoint Number

The **Endpoint number** can be changed only on the handset through **Main menu > Settings > Admin menu > VoIP**.

If required, shorten the **Endpoint number** by doing the following:

- 1) Select **Device > Settings**.
- 2) In the **Endpoint number display length text** field, select the total number of digits to be displayed. To show the whole number, select **Show all**.

3.5.1.3 Import Trust and Application Certificates

This section describes how to import trust and application certificates. For additional details on certificates, refer to *Portable Device Manager for Windows (WinPDM), Installation and Operation Manual, TD 92712EN*.

Import Trust Certificates

- 1) Upload at least one **Self-signed certificate** and up to seven **Intermediate certificates**, which are used to establish the trust chain of the server certificate. The commonly understood name of these certificate types is **Trusted certificate**.
- 2) Open the **Numbers** tab and select the handset to manage the certificates.
- 3) In the **Number** menu (or right-click the handset), select **Manage certificates**. The *Manage certificates* window opens.
- 4) In the **Trust list** tab, click **Browse** and select the certificates to import. Click **Close**.

Import Application Certificates

- 1) Upload an application certificate (also known as a device or client certificate). The uploaded file must be a PKCS #12 (.p12) file containing the private key and associated certificate.
- 2) Open the **Numbers** tab and select the handset to manage the certificates.
- 3) In the **Number** menu (or right-click the handset), select **Manage certificates**. The *Manage certificates* window opens.
- 4) In **Application certificates** tab, click **Browse** and select the certificate to import. Click **Close**.

3.5.1.4 Replace Call Rejected with User Busy

This parameter allows the handset to send **User Busy** instead of **Call rejected** cause code if an incoming call is rejected. If the parameter is set, the calling party will not know if the called party is currently talking or actively rejecting the call.

NOTICE:

It is recommended to set this parameter if the PBX (or another system) can not interpret the **Call rejected** cause code.

To enable the setting, select **VoIP > General > Replace Call Rejected with User Busy > Yes**.

3.5.1.5 ICE Negotiation

ICE negotiation can be used during call setup to enable NAT traversal and WebRTC interoperability. NAT traversal allows data traffic to get to a specified destination when a device does not have a public IP address. The handset supports the ICE, STUN and TURN protocols for NAT traversal.

- 1) Go to **VoIP > General**.
- 2) In the **ICE Negotiation** drop-down list, select **Yes**.
- 3) Set the **STUN** and **TURN** parameters depending on the used protocol.
 - **STUN server address** defines the STUN server to use for NAT traversal. Up to two STUN servers can be configured which should be queried in parallel. The STUN server addresses to the different servers should be separated by a semi-colon (;).

The server address must be entered in one of the following formats:

- A single DNS name and an optional port, for example
`stun.example.com:1234`
- A comma-separated list of one or two IP addresses and optional ports, for example `172.16.13.1:1234, 172.16.13.2`

- **TURN server address** defines the TURN server to use for NAT traversal.

A TURN server can be configured and the server address must be entered in one of the following formats:

- A single DNS name and an optional port, for example
`turn.example.com:1234`
- A comma-separated list of one or two IP addresses and optional ports, for example `172.16.13.1:1234, 172.16.13.2`

A TURN server configuration can optionally be followed by a protocol specification such as `turn.company.tld?protocol=prot`, where **prot** can be either `tcp` or `udp`.

- **TURN server user name** defines the user name for accessing the TURN server.
- **TURN server password** defines the password for accessing the TURN server.

3.5.1.6 Codec Configuration

A codec encodes a stream or signal for transmission, which is often used in streaming media applications. This setting defines how to packetize and compress the sound in a voice call. To define which codec to use for speech (default G.711 A-law), do the following:

- 1) Select **VoIP > General**.
- 2) In the **Codec configuration** drop-down list, select the applicable codec.
 - a) **G.711 A-law** (EU, and also more common in the rest of the world)
 - b) **G.711 u-law** (US, especially North America, and Japan)
 - c) **G.729**
 - d) **G.729A**
 - e) **G.722**
 - f) **OPUS Wide band**

- 3) In the **Codec packetization time configuration** drop-down list, select the packetization time to use for speech (value 20–60 ms).

3.5.1.7 Offer Secure RTP

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

TLS and SRTP must be enabled for the SIP connection in order to protect the confidentiality of the phone calls. The SRTP encryption algorithm defaults to AES_CM_128_HMAC_SHA1_80.

The handset will perform validation of the server side certificate by default. It is important not to disable this functionality since the handset will then have no protection against rogue SIP servers. This is especially true when DNS requests over an untrusted IP connection is used to locate the SIP proxy IP address.

SIP Protocol

- 1) Go to **VoIP > SIP**.
- 2) In the **SIP Transport** drop-down list, select **TLS**.
- 3) Go to **VoIP > General**
- 4) In the **Offer Secure RTP** drop-down list, select **Yes**.
- 5) In the **Secure RTP Crypto** drop-down list, select the preferred SRTP encryption.

A **Secure call** icon  that appears in a call window is used to indicate a secure call voice connection. **Non-secure call** icon  is used in cases when voice connection is not secure.

NOTICE:

Secure call and **Non-secure call** icons only appear if both **TLS** (encrypted signalling) and **Offer Secure RTP > Yes** are selected.

3.5.1.8 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.

3.5.2 Call Waiting Behavior and Sound

The default behavior is to indicate with the `Incoming call` dialog window and call waiting sound that a second call is waiting for 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. The call waiting sound can also

changed and be either set to a short two-beep tone or a loud melody, if the user is located in a noisy environment.

Configure Call Waiting Behavior

- 1) Select **Device > Call**.
- 2) In the **Call waiting behavior** drop-down list, select one of the following:
 - a) **Call waiting indication** to receive second call indicated by sound and the **Incoming call** dialog window.
 - b) **Reject call** to automatically decline the second call (no sound or dialog window occurs).

Configure Call Waiting Sound

NOTICE:

Applicable to WL4 Messaging and WL4 Plus only.

- 1) Select **Device > Call**.
- 2) In the **Call waiting sound** drop-down list, select one of the following:
 - a) **Beep** to indicate the second call with a short two-beep tone.
 - b) **Melody** to indicate the second call with a melody suitable for noisy environments.



WARNING: Changing to the parameter **Melody** may result in a high sound level as the **Call waiting sound** follows the volume of the active call and can cause hearing damage.

3.5.3 Allow Blind Transfer

The handset is configured in a way to allow the call to be transferred to another number using the **In call menu > Transf. to new**.

To disable this setting, select **Device > Call > Allow blind transfer > No**.

3.5.4 Soft Key Functions During Call

It is possible to configure the In Call functions that are accessed by pressing the left or right soft key during a call. To configure the soft key functions, perform the following steps:

- 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:

- **Conference**
- **Contacts**
- **Messaging** (applicable to WL4 Messaging and WL4 Plus only)
- **No action**
- **End call**
- **Hold**
- **Loudspeaker**
- **New call (put active on hold)**
- **Retrieve**
- **Switch**
- **Transfer (to held call)**
- **Transfer to new call (blind transfer)**

In case **No action** is selected, soft keys are hidden during a call. Instead, the default soft keys **Loudspeaker** and **End call** are displayed.

3.5.5 Dial Pause Time

By adding a **P** to a phone number, a pause is added and is activated when dialing. To configure the duration of the pause, do the following:

- 1) Select **Device > Call**.
- 2) In the **Dial pause time** field, enter a pause time in the interval 1–3 s.

3.5.6 Code for Call Completion

When a call is made to a busy handset or when the called party cannot answer, it is possible to configure the handset in a way to send notification when the user is available again.

- 1) Select **Device > Call**.
- 2) Configure the required parameters:
 - a) Code for call completion busy subscriber is used to order call completion on busy subscriber. Enter the code, for example *1.
 - b) **Code for call completion no reply** is used to order call completion on no reply. Enter the code, for example *2.
 - c) **Code for cancel all call completions** is used to cancel any active call completions for this handset. Enter the code, for example *3.

If the field is left empty, the feature is disabled.

3.5.7 Code for Hiding Call ID

It is possible to configure the handset to hide the calling ID.

To do this, select **Device > Call > Code for hide calling ID (CLIR)** and enter the required code, for example *4. If left empty, this feature is disabled.

3.5.8 Calling Line Identification Restriction (CLIR)

The handset can be configured to hide the number and name of the calling party from the called party.

NOTICE:

Even if CLIR is enabled, there is an override function available to authorities, such as the police. In this case the identity of the caller is seen.

To hide the caller's number and name, select **Device > Call > CLIR (Calling Line Identification Restriction) > On**.

3.5.9 Hide Missed Call Window

By default, the dialog window showing the total number of missed calls is displayed on the handset after each 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` dialog window is not displayed on the handset.

To hide the dialog window, select **Device > Call > Show missed calls dialog window > No**.

3.5.10 Prevent Calls from Being Saved in the Call List

It is possible to disable storing outgoing and incoming calls in the Call list, which can be useful to prevent unauthorized access to the Call list. To prevent all calls from being saved, select **Device > Call > Enable call list > Off**.

3.5.11 Voicemail Service

The handset can be configured to use voicemail service to leave voice messages in case a called party is busy or unavailable. Below is the list of voicemail parameters available for configuration.

Message Centre Number

Defines the number to the Message Centre endpoint. If specified, the handset will interrogate with the Message Centre for voicemail Message Waiting Indication (MWI) after registering with the SIP Proxy.

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

Voice Mail Number

Defines the user's voicemail number in the Message Centre (required in some systems).

- 1) Select **Device > Message center**.

- 2) In the **Voicemail number** field, enter the number to the handset's voicemail Inbox.

Voice Mail Call Clears MWI

This parameter can be enabled to deactivate voicemail message waiting indications in the Message Centre when calling the defined voicemail number.

To enable the setting, select **Device > Message center > Voicemail call clears MWI > Yes**.

3.5.12 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.

NOTICE:

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, the use of 5421 and 1256 is allowed.

To configure the emergency call number, do the following:

- 1) Select **Device > Emergency call Numbers**.
- 2) In the **Emergency call Number** field(s), enter the desired emergency number(s).

Emergency Ring Signal

A separate ring signal for incoming emergency callbacks can be configured to distinguish the emergency ring signal from other handset ring signals. When an emergency call is made from the handset, it first goes to an emergency center that switches the call to the appropriate emergency service. This local emergency service then calls back the handset user who can identify the incoming call by this specific callback emergency ring signal.

- 1) Select **Audio > General**.
- 2) In the **Emergency ring signal** field, choose the ring signal for incoming emergency callback calls.

It is possible to configure the handset to sent an alarm when an emergency number is dialed. For more information, refer to [Emergency Call Alarm](#) on page 79.

3.5.13 OpenScape 4000 Busy Actions

If supported by the PBX, it is possible to configure up to four prioritized options to be shown to the calling party when an outgoing call is rejected because the called party is busy. To make it available, the SIP server must signal support for the feature and both the function and a valid feature code must be set:

- 1) Select **Unify busy actions** > **1–4**.
- 2) In the **Function** drop-down list, select one of the following parameters:
 - **None**
 - **Call completion** allows you to book a callback as soon as the called party is available again.
 - **Busy override** allows you to join a call in progress.
 - **Emergency disconnect** allows you to terminate a call in progress and get a one to one call.
 - **Emergency intrusion** allows you to get through to the called party and get a one to one call.
- 3) In the **FAC** field, enter a code to be used.

3.5.14 Pickup Groups

Pickup groups make it possible to answer other users' incoming calls when they are not available. To configure pickup groups, perform the following steps:

- 1) Select **Pickup groups** > **1–10**.
- 2) In the **Pickup group name** field, enter a descriptive name that identifies this call pickup group in the handset menu.
- 3) In the **Pickup group URI** field, enter the URI that identifies this call pickup group in the PBX.
- 4) Set **Pickup group status** > **On** to enable this call pickup group.

3.6 Services

NOTICE:

Applicable to WL4 Plus only.

It is possible to configure up to ten frequently used functions that can be accessed from the handset's **Services** menu.

NOTICE:

It is recommended to use services in combination with shortcuts (refer to [Shortcuts](#) on page 41), otherwise a user needs to enter the **Services** menu and trigger a service from the menu.

- Select **Services** > **1–10**.
- In the **Service name** field, enter the name of the service to be displayed on the handset.

- 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**.

NOTICE:

This field is only applicable for PTT. If the PTT is not configured, continue with [Push-to-Talk Group Call](#) on page 79.

- Under **Service function**, select the service to be used:
 - 1) **Phone call** to dial a predefined number.
 - 2) **Send data** to send predefined data and/or prompt for the data.
 - 3) **Send message** to write a message and send it to a predefined number
 - 4) **Push To Talk** to start a PTT session.
 - 5) **Edit alarm data** to add the data that will be sent with an alarm at transmission.
- In the **Service user data** field, enter the data to be used for the selected service function (not applicable for PTT).
- In the **Service prefix for user data** field, enter the prefix for the service user data (if needed).

3.7 Alarm Settings

NOTICE: Applicable to WL4 Plus only.

This section describes how to configure the handset to send push-button and test alarms when the handset's top button⁸ is pressed as well as how to program man-down and no-movement alarms to provide personal safety monitoring .

This section also describes how to configure the handset to send the emergency call alarm when a user calls an external or internal number specified in the system as the emergency number.

3.7.1 Common Alarm Settings

To configure the common alarm settings, perform the following steps:

- 1) Select **Alarm > Common**.
- 2) In the **Stored alarm data** field, enter the data to be sent together with an alarm, for example some predefined text.

⁸ In case of WL4 Plus, the button is used as a push-button alarm.

- 3) In the **Indicate triggered alarm with vibrator** and/or **Indicate triggered alarm with beep signal** drop-list(s), select if sent alarms are indicated by vibration and/or by a beep signal.

NOTICE:

If you set **Alarm > Alarm on long press** and/or **Alarm on multiple press** to **Silent alarm**, there will be no indication of an alarm being sent (no beep, vibrating alert, or dialog window).

- 4) In the **Password protect ALS** drop-down list, select if a phone lock password must be entered to turn off the Acoustic Location Signal (ALS).
- 5) In the **Number for automatic call after alarm** field, enter the phone number to dial automatically once the alarm has been triggered. This number can also be dialed without sending an alarm, refer to [Call Predefined Number without Sending Alarm](#) on page 79.

3.7.2 Push-button and Test Alarms

The handset's alarm button can be configured to send two different types of alarm. An alarm can either be a push-button alarm with a personal alarm functionality or a test alarm that is used to test the personal alarm. It is also possible to configure how push-button and test alarms are handled in a system.

Configure Push-button and Test Alarms

To configure the behavior of push-button and test alarms, perform the following steps:

- 1) Select **Alarm > Alarm on long press** or **Alarm on multiple press**.

NOTICE:

Parameters for long press and multiple press are the same, except for the parameter **Duration for long press** that is replaced with **Define multiple press**.

- 2) In the **Alarm type for long press** and/or **Alarm type for multiple press** drop-down list(s), select what type of alarm is sent when the alarm button is pressed and hold (long press) or pressed multiple times. The following options are available:
- **Test alarm**
 - **Push-button Alarm 1**
 - **Push-button Alarm 2**
 - **Not used**

NOTICE:

If **Not used** is selected, a predefined number can still be called automatically when pressing the alarm button. For more information, refer to [Call Predefined Number without Sending Alarm](#) on page 79.

- 3) In the **Text indication for alarm on long press** and/or **Text indication for alarm on multiple press** field(s), enter the text to be displayed on the handset once the alarm has been triggered.

NOTICE:

If this field is empty, **Test alarm** (default text for long press) or **Personal alarm** (default text for multiple press) is shown.

- 4) In the **Duration for long press** drop-down list, select how long (0.5 sec - 5.0 sec) the alarm button should be pressed and hold until it is recognized as a long press (long press parameter only).

In the **Define multiple press** drop-down list, select how many times in one sequence (2, 3, or 4 times) the alarm button should be pressed to be recognized as a multi-press (multiple press parameter only).

NOTICE:

If the **Duration for long press** is set to 0 seconds, multiple press alarm cannot be used.

- 5) In the **Silent alarm** drop-down list, select **Yes** if you want to have no indication of an alarm being sent or received (no sound signal, vibrating alert, dialog window, Acoustic Location Signal (ALS), or notification light on the display).
- 6) In the **ALS** drop-down list, select if high-pitched sound should be used to locate the person triggering the alarm.
-

NOTICE:

If both parameters **ALS** and **Silent alarm** are set, ALS will not be used.

NOTICE:

The ALS is not triggered if **Mode for automatic call after alarm** is set to other than **Off**.

- 7) In the **Mode for automatic call after alarm** drop-down list, select the way to establish the call once the alarm has been sent. The following modes are available:

- **Off**
- **Normal** places an ordinary call.
- **Loudspeaker** places a call with turned on loudspeaker.
- **Monitoring** places a one-way call where the called party can only listen to a conversation.

- 8) Select **Alarm > Common > Number for automatic call after alarm**. Enter the number to be called once the alarm button has been pressed (optional).

The handset can be also configured in way so information about the handset's location is sent along with an alarm. For more information, refer to [Location](#) on page 61.

3.7.3 Man-down and No-movement Alarms

The handset can also be programmed to send man-down and no-movement alarms to provide personal safety monitoring. These alarms are suitable for workplaces where maximum security and accessibility is required. If an accident occur, colleagues and management are informed within seconds and the person in need can be located immediately.

The man-down alarm is triggered if the handset is tilted (default 45°) from the vertical plane for a predefined period of time (default 7 s). The no-movement alarm is triggered if no movement is detected during a predefined period of time (default 30 s). When a man-down or no-movement has been detected, the handset enters a warning phase (usually seven seconds long).

Configure Man-down and No-movement Alarms

- 1) Select **Alarm > Man-down and No-movement alarm**.
- 2) In the **Man-down detection time** and/or **No-movement detection time** field(s), enter the delay in seconds between the detection of man-down/no-movement and the warning phase.
- 3) In the **Man-down warning angle** drop-down list, select the deflection angle of the handset for man-down detection (low 45 degrees and high 60 degrees). The angle is 0 degrees when the handset is in upright position and 90 degrees when the handset lies down.
- 4) In the **Warning phase duration** field, enter the time in seconds how long the warning phase is active.
- 5) In the **NM-MD extra delay used** drop-down list, select if the user shall have the possibility to delay the detection of the man-down and no-movement alarms. When enabled, the user can extend the detection time for man-down and no-movement alarms by pressing the **Mute** button and then pressing **Yes** to confirm the *Delay MD/NM detection?* message. The corresponding display icon flashes until the alarm is active again.
- 6) In the **NM-MD extra delay time** field, enter the time in minutes for how long the detection of the man-down and no-movement alarms is delayed.
- 7) In the **ALS** drop-down list, select if high-pitched sound should be used to locate the person triggering the alarm.

NOTICE:

The ALS is not triggered if **Mode for automatic call after alarm** is set to other than **Off**.

- 8) In the **Mode for automatic call after alarm** drop-down list, select the way to establish the call once the alarm has been sent.
- 9) In the **Turn off NM-MD during in-call or outgoing-call state** drop-down list, select if the man-down and no-movement alarms can be triggered during a phone call.
- 10) In the **Reset man-down warning automatically** drop-down list, select if the user shall be able to cancel the warning phase by changing the position of the handset.
- 11) In the **Volume for warning phase alert** drop-down list, select the loudness of alert in the warning phase.
- 12) In the **Sound for warning phase alert** drop-down list, select the sound for alert in the warning phase. It is recommended to use **Siren tones** in noisy environments.

3.7.4 Emergency Call Alarm

This section describes how to enable **Emergency call alarm** function on the handset. To configure the handset to send an alarm when the user calls an emergency number, do the following:

- 1) Select **Alarm > Emergency call**.
- 2) In the **Emergency call alarm** drop-down list, select **On**.
- 3) In the **Alarm type text** field, write the text to be shown on the handset when an emergency call alarm is triggered. If this field is left empty, the default `Emergency call alarm` dialog window is shown.

For the details on how to configure the emergency call numbers, please refer to [Emergency Call Numbers](#) on page 73.

3.7.5 Call Predefined Number without Sending Alarm

It is possible to use the alarm button to automatically dial a predefined number without sending an alarm. The following example shows how to configure the handset to dial a number when the button is pressed and hold (long press).

- 1) Select **Alarm > Common**.
- 2) In the **Number for automatic call after alarm** field, enter the number to be dialed.
- 3) Select **Alarm > Alarm on long press > Alarm type for long press > Not used**.
- 4) In the **Mode for automatic call after alarm** drop-down list, select the way the call is established after the alarm has been sent.

3.8 Push-to-Talk Group Call

NOTICE:

Applicable to WL4 Plus only.

To be able to configure a PTT session, the following information is required:

- 1) The group number of the PTT group.
- 2) The phone number to the conference bridge.

NOTICE:

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.

3.8.1 Configure a PTT Call

To configure a PTT group call, perform the following steps:

- 1) Select **Push-To-Talk X** (1–10).

2) The following parameters can be configured:

- **Session name** defines the name of the PTT session.
- **Group number** defines the group number to which the call setup for this PTT session is sent.
- **Display text** defines the text shown on the display during the PTT session.
- **PTT session signal** defines how the PTT session is indicated.
- **Conference number** defines the call number to the conference bridge. The call number is sent when a PTT session is initiated from or accepted by the handset.
- **Answer mode** defines which answer mode the handset has for the PTT session. Select **Manual** if the user must accept the session. Select **Auto** to set up the session automatically.
- **Speaker mode** defines which speaker mode the handset has for the PTT session. Select **Normal** to start session with the speaker turned on. Select **Loud** to start the session with the loudspeaker turned on.

Additional parameters can be configured for PTT group calls:

- Automatic key lock can be enabled during an ongoing call. For more information, refer to [Automatic Key Lock](#) on page 33 and [Automatic Lock Time](#) on page 35.
- A service can be configured to access the PTT session from the handset. If not configured, continue with [Services](#) on page 74.

3.8.2 PTT Call Disconnect Warning

To enable a warning sound if the PTT session is terminated for any other reason than the user ending the call, select **Device > Call > PTT Call disconnect warning > Yes**.

3.9 Profiles

There are two types of profiles that can be configured for the handset:

- 1) User profiles, refer to the [User Profiles](#) on page 80
- 2) System profiles, refer to the [System Profiles](#) on page 84

3.9.1 User Profiles

User profiles are used to set up customized profiles for incoming calls, message alerts, message volume, vibrating alerts, key sound, and so on.

This can be useful when more users use the same handset, who want different sound profiles. It can also be used for temporary settings, for example, while in a meeting, incoming calls can be set to silent.

To create a user profile, perform the following steps:

- 1) Select **User Profiles > Normal** or **Profile X** (1-4).
- 2) In the **Profile name** field, enter the name of the profile.

3) Configure the following parameters:

- **Sound and Alerts** contains sound and alert settings for calls and messages, refer to [Configure Sound and Alerts](#) on page 81.
- **Presence and diversion** contains settings for message absent and call diversion, refer to [Configure Presence and Diversion](#) on page 82.
- **Answering** contains settings for how incoming calls are answered, refer to [Configure Answering](#) on page 83.
- **Alarm settings** contains settings for which alarm type is used (applicable to WL4 Plus only) , refer to [Configure Alarm Settings](#) on page 83.
- **Soft keys** contains shortcut settings to predefined functions, refer to [Configure Soft Keys](#) on page 84.

4) If required, select the profile to be active, by selecting **User Profiles** and change the default **Active Profile** to the desired profile.

It is also possible to configure profiles directly on the handset, refer to *Unify OpenScape WLAN Phone WL4, User Manual, TD 93342EN* .

3.9.1.1 Configure Sound and Alerts

This section describes how to configure or change audio and vibration signals on the handset.

- 1) Select **User Profiles > Normal or Profile X (1-4) > Sound and Alerts**.
- 2) In the **Internal ring signal**, **External ring signal** , **Call pickup group ring signal** , and **Callback ring signal** drop-down lists, select one of the following signals:
 - a) **Ring signal X** defines one of the 15 different predefined melodies.
 - b) **Beep X** defines one of the 7 beeps.
 - c) **Custom sound X** (8–10) defines one of the 3 proprietary melodies made by coding with the help of a specific code table.
- 3) In the **Ring volume** drop-down list, select one of the following:
 - **Silent** disables any ring signal.
 - **Volume X** (1–8) defines different ring signal volumes from lowest (1) to highest (8).
- 4) In the **Vibrator** drop-down list, select one of the following:
 - **On** enables the vibrating alert for incoming calls and messages.
 - **On if silent** enables the vibrating alert for incoming calls and messages only if the handset is muted or the volume is set to **Silent**.
 - **Off** disables the vibrating alert.
- 5) In the **Key sound** drop-down list, select one of the following:
 - **Click** enables click sound when a key is pressed on the handset.
 - **Tone** enables tone signal heard when a key is pressed on the handset.
 - **Silent** mutes all keys.
- 6) In the **Message alert** drop-down list, select one of the following:

NOTICE:

The message sound for incoming messages can be either a melody or a single beep. Only the parameter **Custom sounds according to beep code** can be customized. For

more information, refer to [Customize the Default Handset Beeps](#) on page 125.

- **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 the system. For the details, refer to [Configure Message Alerts with Beep Codes](#) on page 46
 - **High beeps according to beep code** is the same type as **Beeps according to beep code**, but with a higher pitch. For the details, refer to [Configure Message Alerts with Beep Codes](#) on page 46
 - **Enhanced beeps according to beep code** is the same type as **Beeps according to beep code**, but in the form of a melody. For the details, refer to [Enhanced Beeps According to Beep Code](#) on page 47
 - **Custom sounds according to beep code** uses the customized melody. For the details, refer to [Custom Sounds According to Beep Code](#) on page 47
- 7) In the **Message volume** drop-down list, select one of the following:
- a) **Silent** disables any audible message indication for incoming messages.
 - b) **Volume X** (1–8) defines different message indication volumes from lowest (1) to highest (8).
 - c) **Follow ring volume** enables the message indication volume followed by the ring volume (default).

3.9.1.2 Configure Presence and Diversion

To configure message absent and call diversion parameters, perform the following steps:

- 1) Select **User Profiles > Normal** or **Profile X (1-4) > Presence and diversion**.
- 2) In the **Message absent** drop-down list, select one of the following:

NOTICE:

Applicable to WL4 Plus only.

- **On** to show that the handset is absent when the message is received. The message can be redirected to another destination.
 - **Off** to disable message absence.
- 3) In the **Default diversion number** field, enter the default number that will be used in case when no diversion number is set for any of specific diversions described below.
 - 4) In the **Diversion no answer number of seconds** field, enter the number of seconds to pass before a call is diverted to another number. Applicable only if **Diversion on no answer** parameter is enabled.

- 5) In the **Diversion for all calls (external)** drop-down list, select **On** to divert all incoming external calls to another number. Specify a number in the **All calls diversion number (external)** field.

To divert all internal calls, select **Diversion for all calls (internal)** > **On** and specify a number in the **All calls diversion number (internal)** field.

- 6) In the **Diversion on user busy (external)** drop-down list, select **On** to divert all incoming external calls to another number in case the called party is busy. Specify a number in **On busy diversion number (external)** field.

To divert the internal calls when the called party is busy, select **Diversion on user busy (internal)** > **On** and specify a number in the **On busy diversion number (internal)** field.

- 7) In the **Diversion on no answer (external)** drop-down list, select or **On** to divert all incoming external calls to another number in case the called party cannot answer. Specify a number in **No answer diversion number (external)** field.

To divert the internal calls, select **Diversion on no answer (internal)** > **Yes** and specify a number in the **No answer diversion number (internal)** field.

3.9.1.3 Configure Answering

This section describes how to configure the answering behavior for the handset.

- 1) Select **User Profiles** > **Normal** or **Profile X (1-4)** > **Answering**.
- 2) In the **Answering key** drop-down list, choose between:
 - a) **Call key** to answer an incoming call by pressing the **Call** key.
 - b) **Any key** to answer an incoming call by pressing any key.
- 3) In the **Answer mode** drop-down list, select one of the following:
 - a) **Normal** to answer the call by pressing the **Call** key.
 - b) **Automatically** to answer the call automatically after 1 second.
 - c) **Loudspeaking** to answer the call in loudspeaking mode once the **Call** key is pressed .
 - d) **Automatically loudspeaking** to answer the call automatically in loudspeaking mode after 1 second .
- 4) In the **Can reply with a message template when rejecting a call** drop-down list, select **Yes** to show the *Reply with a message template?* dialog window every time when a user rejects an incoming call (applicable to WL4 Messaging and WL4 Plus only).

NOTICE:

If no message templates are defined, the dialog window is not shown. For more information, please refer to [Message Templates](#) on page 52.

3.9.1.4 Configure Alarm Settings

NOTICE:

Applicable only to WL4 Plus.

To configure alarm settings for the different profiles, perform the following steps:

- 1) Select **User Profiles** > **Normal** or **Profile X (1-4)** > **Alarm settings**.
- 2) In the **Man-down alarm** and **No-movement alarm** drop-down lists, select **On** to enable alarms.

3.9.1.5 Configure Soft Keys

When configuring soft keys, both name and function must be set.

- 1) Select **User Profiles** > **Normal** or **Profile X (1-4)** > **Soft keys**.
- 2) Expand the **Soft keys** folder and select **Soft key Left**, **Soft key Middle**, or **Soft key Right**.
- 3) In the **Soft key name** field, enter the text (6 characters max.) that will be shown on the handset above the soft key.
- 4) In the **Function** drop-down list, select the action to be performed when the configured key is pressed. For the whole list of available functions, refer to [Shortcut Functions](#) on page 43.
- 5) In the **Value** field, enter the applicable value for a function, for example a phone number.

NOTICE:

Only certain functions require a value.

- 6) In the **Control question** drop-down list, select **Yes** to display the *Proceed?* dialog window every time the configured key is pressed. This setting prevents from the assigned action to be performed immediately in cases when a key has been pressed by mistake.

3.9.2 System Profiles

NOTICE:

Applicable to WL4 Messaging and WL4 Plus only.

A system profile can be used when there are certain settings in a handset that the user is not allowed to change.

NOTICE:

A system profile overrides all **Normal** or **Profile X (1-4)** settings.

To create a system profile, perform the following steps:

- 1) Configure **System Profiles Sub Group**. The following sub-groups are available:
 - **Presence groups** contains settings for message absent, refer to [Configure Presence Groups \(Sub-group\)](#) on page 86.
 - **Answering groups** contains settings for how incoming calls are answered, refer to [Configure Answering Groups \(Sub-group\)](#) on page 87.
 - **Sound and alerts groups** contains sound and alert settings for calls and messages, refer to [Configure Sounds and Alerts Groups \(Sub-group\)](#) on page 85.
 - **Soft key groups** contains shortcut settings to predefined functions using soft keys, refer to [Configure Soft Key Groups \(Sub-group\)](#) on page 88.
 - **Alarm settings groups**⁹ contains settings for which alarm type is used and how, refer to [Configure Alarm Settings Group \(Sub-group\)](#) on page 87.
 - **Idle display groups** contains settings to show the system profile name in Idle mode.

For additional details, refer to [Create System Profile Using Predefined Sub-Groups](#) on page 89.

- 2) Connect the system profile to the created sub-group(s).

Once a system profile has been created, it can be used whenever desired and can be turned off and on again. For more information, refer to [Activate and Deactivate System Profile](#) on page 90.

3.9.2.1 Configure Sounds and Alerts Groups (Sub-group)

To configure sounds and alerts groups, perform the following steps:

- 1) Select **System Profiles > System Profiles Sub Groups > Sound and alerts groups > Sound and alerts group X (1–5)**.
- 2) In the **Name of group** field, enter a descriptive name.
- 3) In the **Ring volume** drop-down list, select one of the following:
 - **Silent** disables any ring signal.
 - **Volume X (1–8)** defines different ring signal volumes from lowest (1) to highest (8).
- 4) In the **Vibrator** drop-down list, select one of the following:
 - **On** enables the vibrating alert for incoming calls and messages.
 - **On if silent** enables the vibrating alert for incoming calls and messages only if the handset is muted or the volume is set to **Silent**.
 - **Off** disables the vibrating alert.
- 5) In the **Internal ring signal**, **External ring signal**, **Call pickup group ring signal**, and **Callback ring signal** drop-down lists, select one of the following signals:
 - **Ring signal X** defines one of the 15 different predefined melodies.
 - **Beep X** defines one of the 7 beeps.
 - **Custom sound X (8–10)** defines one of the 3 proprietary melodies made by coding with the help of a specific code table.

⁹ Applicable to WL4 Plus only.

- 6) In the **Key sound** drop-down list, select one of the following:
- **Click** enables click sound when a key is pressed on the handset.
 - **Tone** enables tone signal heard when a key is pressed on the handset.
 - **Silent** mutes all keys.
- 7) In the **Message alert** drop-down list, select one of the following:

NOTICE:

The message sound for incoming messages can be either a melody or a single beep. Only the parameter **Custom sounds according to beep code** can be customized. For more information, refer to [Customize the Default Handset Beeps](#) on page 125.

- **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 the system. For the details, refer to [Beeps or High Beeps According to Beep Code](#) on page 46
 - **High beeps according to beep code** is the same type as **Beeps according to beep code**, but with a higher pitch. For the details, refer to [Beeps or High Beeps According to Beep Code](#) on page 46
 - **Enhanced beeps according to beep code** is the same type as **Beeps according to beep code**, but in the form of a melody. For the details, refer to [Enhanced Beeps According to Beep Code](#) on page 47
 - **Custom sounds according to beep code** uses the customized melody. For the details, refer to [Custom Sounds According to Beep Code](#) on page 47
- 8) In the **Message volume** drop-down list, select one of the following:
- **Silent** disables any audible message indication for incoming messages.
 - **Volume X** (1–8) defines different message indication volumes from lowest (1) to highest (8).
 - **Follow ring volume** enables the message indication volume followed by the ring volume (default).

3.9.2.2 Configure Presence Groups (Sub-group)

To configure presence groups, perform the following steps:

- 1) Select **System Profiles > System Profiles Sub Groups > Presence groups > Presence group X** (1–2).
- 2) In the **Name of group** field, enter a descriptive name.

- 3) In the **Message absent** drop-down list, select one of the following:

NOTICE:

Applicable to WL4 Plus only.

- a) **On** to show that the handset is absent when the message is received.
The message can be redirected to another destination.
- b) **Off** to disable message absence.

3.9.2.3 Configure Answering Groups (Sub-group)

To configure answering groups, perform the following steps:

- 1) Select **System Profiles > System Profiles Sub Groups > Answering groups > Answering group X (1–4)**.
- 2) In the **Name of group** field, enter a descriptive name.
- 3) In the **Answer mode** drop-down list, select one of the following:
 - a) **Normal** to answer the call by pressing the **Call** key.
 - b) **Automatically** to answer the call automatically after 1 second.
 - c) **Loudspeaking** to answer the call in loudspeaking mode once the **Call** key is pressed.
 - d) **Automatically loudspeaking** to answer the call automatically in loudspeaking mode after 1 second.

3.9.2.4 Configure Alarm Settings Group (Sub-group)

NOTICE:

Applicable to WL4 Plus only.

To configure alarm settings groups, perform the following steps:

- 1) Select **System Profiles > System Profiles Sub Groups > Alarm settings groups > Alarm settings group X (1–5)**.
- 2) In the **Name of group** field, enter a descriptive name.
- 3) Expand the **Alarm settings group X (1–5)** folder to see additional settings:
 - a) **Common**
 - In the **Stored alarm data** field, enter the data to be sent together with an alarm, for example some predefined text.
 - In the **Indicate triggered alarm with vibrator** and/or **Indicate triggered alarm with beep signal** drop-down list(s), select if sent alarms are indicated by vibration and/or by a beep signal.
 - b) **Alarm on long press** and **Alarm on multiple press**
 - In the **Alarm type for long press** and/or **Alarm type for multiple press** drop-down list(s), select what type of alarm is sent when the alarm button is pressed and hold (long press) or pressed multiple times. The following options are available:
 - **Test alarm**

- **Push-button Alarm 1**
- **Push-button Alarm 2**
- **Not used**

NOTICE:

If **Not used** is selected, a predefined number can still be called automatically when pressing the alarm button. For more information, refer to [Call Predefined Number without Sending Alarm](#) on page 79.

- In the **ALS** drop-down list, select if high-pitched sound should be used to locate the person triggering the alarm.

NOTICE:

If both parameters **ALS** and **Alarm > Alarm on long press** or **Alarm on multiple press > Silent alarm** are set, ALS will not be used.

NOTICE:

The ALS is not triggered if **Alarm > Alarm on long press** or **Alarm on multiple press > Mode for automatic call after alarm** is set to other than **Off**.

c) No-movement and Man-down

- To enable **Man-down alarm** and **No-movement alarm**, select **On**.
- In the **Man-down detection time** and/or **No-movement detection time** field(s), enter the delay in seconds between the detection of man-down/no-movement and the warning phase.
- In the **Warning phase duration** field, enter the time in seconds how long the warning phase is active.
- In the **ALS** drop-down list, select if high-pitched sound should be used to locate the person triggering the alarm.

3.9.2.5 Configure Soft Key Groups (Sub-group)

To configure soft key groups, perform the following steps:

- 1) Select **System Profiles > System Profiles Sub Groups > Soft key groups > Soft key group X (1-5)**.
- 2) In the **Name of group** field, enter a descriptive name.
- 3) Expand the **Soft key group X (1-5)** folder and select **Soft key left**, **Soft key middle**, or **Soft key right**.
- 4) In the **Soft key name** field, enter the text that will be shown on the handset above the soft key.
- 5) In the **Function** drop-down list, select the action to be performed when the configured key is pressed. For the whole list of available functions, refer to [Shortcut Functions](#) on page 43.

- 6) In the **Value** field, enter the applicable value for a function, for example a phone number.

NOTICE:

Only certain functions require a value.

- 7) In the **Control question** drop-down list, select **Yes** to display the *Proceed?* dialog window every time the configured key is pressed. This setting prevents from the assigned action to be performed immediately in cases when a key has been pressed by mistake.

3.9.2.6 Configure Idle Display Groups (Sub-group)

To configure the Idle display groups, perform the following:

- 1) Select **System Profiles > System Profiles Sub Groups > Idle display groups > Idle display group X (1–2)**.
- 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:
 - a) **Yes** to show the system profile name when the handset is in Idle mode.
 - b) **No** to hide the system profile name.

3.9.2.7 Create System Profile Using Predefined Sub-Groups

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

NOTICE:

If **Not Used** is selected, user profile settings are used if set.

Select **System Profiles > Profile X (1–5)** and configure the required parameters:

- 1) In the **Profile name** field, enter a descriptive name to identify this system profile.
- 2) **Activation and deactivation sound** defines the sound that is heard when the profile is activated or deactivated. Custom sounds are configured through **Audio > Custom sounds > Custom sound X (1–10)**.
- 3) **Presence group** defines which predefined presence group (sub-group) is used in this system profile.
- 4) **Sound and alerts group** defines which predefined sound and alerts group (sub-group) is used in this system profile.
- 5) **Soft keys group** defines which predefined soft key group (sub-group) is used in this system profile.
- 6) **Answering group** defines which predefined answering group (sub-group) is used in this system profile.

- 7) **Alarm settings group** ¹⁰ defines which predefined alarm settings group (sub-group) is used in this system profile.
- 8) **Idle display group** defines which predefined idle display group (sub-group) is used in this system profile.

3.9.2.8 Activate and Deactivate System Profile

Once a system profile has been created, you can activate it through **System profiles > Active system profile > System profile X (1-5)**.

There are certain rules that should be taken into account when using system profiles:

- A system profile overrides all **User Profile X (1-4)** and **Normal** settings.

The image below shows that the user profile (Profile1) is configured in a way that all three soft keys have shortcuts to three different menus (Main menu, Calls menu, and Messaging inbox). The system profile (System1) has shortcuts to open the Messaging inbox and make a call to the administrator Maria. When activating the system profile (System1), it overrides the complete group of the soft key parameters used in the user profile (Profile1) with its own values.

NOTICE:

The way parameter groups are arranged is seen under **System Profiles > System Profiles Sub Groups**.

- The system profile can be used in combination with the user profile, but if there is a conflict between the settings in the system profile and the settings in the user profile, the settings in the system profile will be used by default.
- If a user changes a setting in the handset menu that is determined by a system profile, the changes will be not applied. The image below shows that a system profile has been activated under the name "System1" and soft key functions are determined by the system profile settings. If a user attempts to change, for example, the name of these functions using the handset menu, the changes will not be applied. Changes will be applied only in case if the system profile is deactivated.

¹⁰ Applicable to WL4 Plus only.

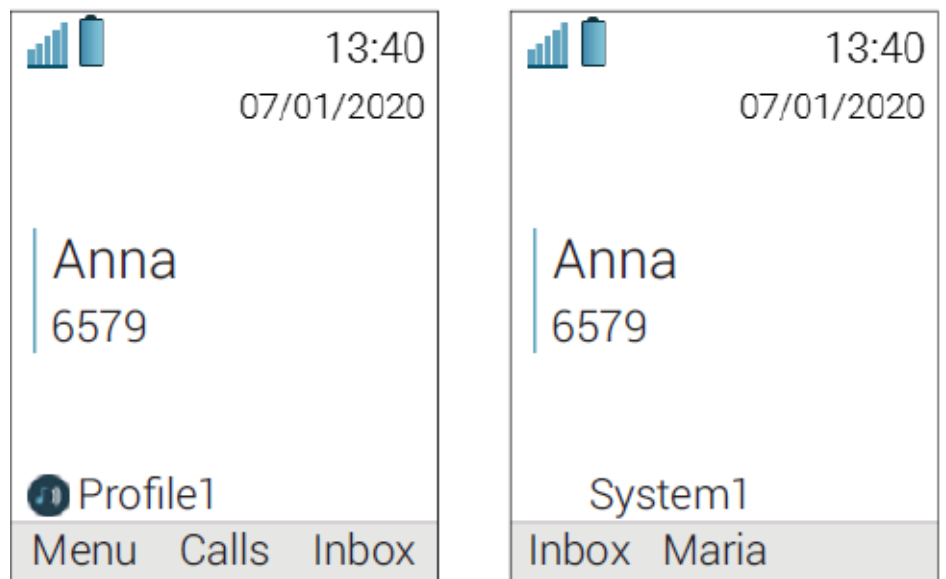


Figure 5: Example of user profile X (left) and system profile (right) configuration

4 System Deployment Planning

This section includes information about built-in **Site survey tool** that can be used to check information about the site that the handset operates in and possible RF problems caused by the layout of the site. The handset is the recommended tool for performing a site survey to verify the VoWiFi system deployment.

It is possible to access the **Site survey tool** through the Admin menu or entering the quick access code in Idle mode (refer to [Quick Access to Admin Menu Functions and Device Information](#) on page 60).

4.1 Show RSSI

The handset has an integrated site survey feature that can be used as a tool to track information about the received signal strength, channel, bandwidth, and BSSID of the current and previously associated APs, refer to [Figure 6: RSSI information](#) on page 93. The built-in tool 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.

To view the RSSI information, go into the Admin menu and select **Site survey tool > Show RSSI > On** or enter the quick access code *#76# in Idle mode.

NOTICE:

RSSI information is displayed in Picture-in-Picture (PIP) mode and might be disturbing during normal handset operation. It is recommended to use the tool only while checking the state of the Wi-Fi network.

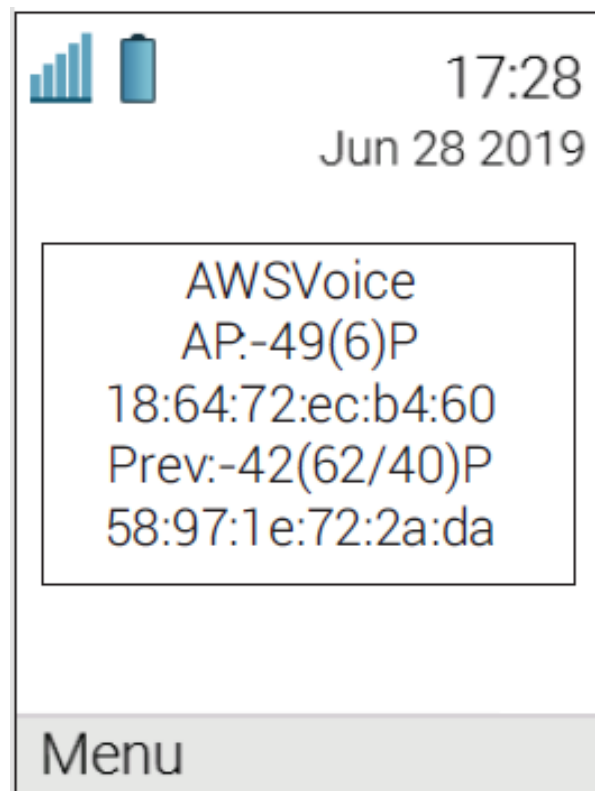


Figure 6: RSSI information

4.2 Scan the Channels

The default configuration for the handset is to use channels 1, 6, and 11 on the 2.4 GHz frequency band. To perform a site survey, it is important to configure the handset to use the frequency band and channels on which the site survey will be performed. For example, it is possible to scan all 2.4 GHz or 5 GHz channels by setting the frequency band parameter accordingly and then setting parameter **2.4 GHz channels** or **5 GHz channels** to **All**, respectively.

It is important to remember to revert back to the original settings after the site survey is finished.

The regulatory domain also affects the channels that can be used. For instance, channels 12 and 13 are only possible to scan if the handset is configured to operate in **World mode (802.11d)**.

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

For 2.4 GHz channels, it is strongly recommended to set back the handset to **1,6,11** before normal use. For 5 GHz channels, it is strongly recommended to set back the handset to **UNII-1** before normal use.

Scan All Channels

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

- 1) In the Admin menu of the handset, select **Site survey tool > Scan all channels**.
- 2) Select the SSID to display the associated AP.
- 3) Select an AP to display information on SSID, Channel, and MAC address.

Scan a Specific Channel

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

- 1) In the Admin menu of the handset, select **Site survey tool > Scan selected channel**.
- 2) Enter the channel to be scanned.
- 3) Select an AP to display information on SSID, Channel, and MAC address.

4.3 Range Beep

The range beep function enables a beep to be played whenever the handset experiences a filtered field strength of below the configured value (default -70 dBm) from the currently associated AP.

Sudden drops in field strength caused by the environment are delayed because the value of field strength is filtered, for example when walking through a door into a room. Therefore 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 by default. In the site survey menu it is possible to change the RSSI threshold. This is useful if a specific area is designed to have a coverage level other than -70 dBm.

- 1) In the Admin menu of the handset, select **Site survey tool > Range beep level**.
- 2) Enter the new RSSI threshold and press **OK**.

Range Beep on a Configured RSSI Threshold

By enabling **Range beep**, the handset gives a beep sound when the signal goes below the selected threshold. To enable this parameter, in the Admin menu of the handset, select **Site survey tool > Range beep > On**.

4.4 Location Survey

This section describes how to perform location survey on the handset. For additional details on supported location systems, refer to [Location](#) on page 61.

To configure the handset to provide the location data, perform the following procedure:

- 1) In the Admin menu of the handset, select **Site survey tool > Location survey**.

2) Select one of the following:

- **BLE location survey** (applicable to WL4 Plus only) to display BLE location information. **RSSI** defines a signal strength of the detected BLE beacon.
- **Wi-Fi location survey** causes WLAN location scanning to be performed at shorter intervals (1s), which can be useful when performing site survey in RTLS deployments.

For the **Wi-Fi location survey** feature to function, the parameter **Location > Common > WLAN location scanning** must be first set to **On**.

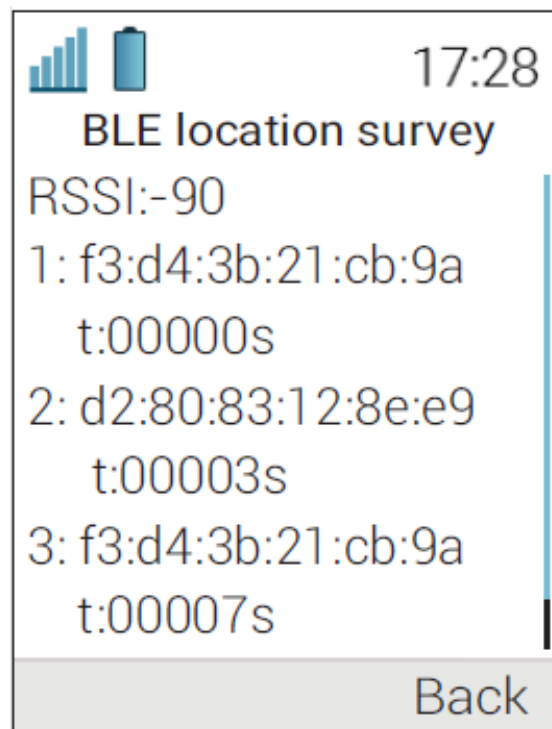


Figure 7: Example of BLE location information

4.5 BLE Beacon Scan

NOTICE:

Applicable to WL4 Plus only.

When BLE beacon scan is performed, the four latest detected BLE beacon locators are displayed on the handset as shown in [Figure 8: Example of BLE beacon scan screen \(left\) with additional details \(right\)](#) on page 96.

In the Admin menu of the handset, select **Site survey tool > BLE beacon scan**.

- Press **Select** to view the beacon details, such as RSSI and UUID.
- Press **Rescan** to repeat scanning.

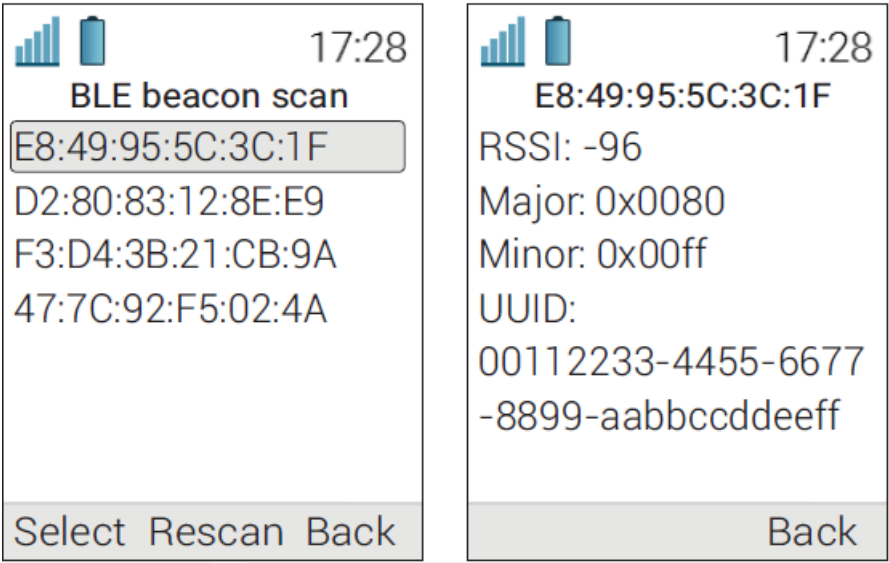


Figure 8: Example of BLE beacon scan screen (left) with additional details (right)

5 Maintenance

This chapter describes how maintain Unify WL4 handsets in a VoWiFi system, with a focus on how to change handset functionality through the license upgrade and update handset software as well as how to perform handset replacement and factory reset. This chapter also describes how to change the security mode of the Wi-Fi infrastructure for already deployed handsets.

5.1 Handset Software Upgrade

NOTICE:

Read the Release Notes before applying any changes in order to get up-to-date information about the software release.

The handset software can be upgraded using one of the following:

- 1) WinPDM, refer to [Upgrade Software Using WinPDM](#) on page 97.
- 2) WSG DM , refer to [Upgrade Software using WSG DM](#) on page 97.

5.1.1 Upgrade Software Using WinPDM

Software upgrade using WinPDM is performed in small VoWiFi systems or when WSG DM is not available. The handsets need to be collected by the administrator because the software is upgraded using the DP1 Desktop Programmer connected to WinPDM.

To upgrade software, do the following:

Open the WinPDM.

Place the handset in the DP1 Desktop Programmer.

In the **Devices** tab, select the handset to be upgraded.

From the **Device** menu (or right-click the handset), select **Upgrade software....**

In the **Available files** drop-down list, select the desired software file (.bin).

If required, click **Import** to add the software file to the list. Locate the software file (.bin or .pkg) and click **Open**.

Click **OK**. The Shutting down dialog window followed by the Remotely updated message is shown on the handset.

5.1.2 Upgrade Software using WSG DM

To upgrade the handset software, follow the steps below:

- 1) In the **Devices** tab, select the handset to be upgraded.
- 2) From the **Device** menu (or right-click the handset), select **Upgrade software...**
- 3) In the **Available files** drop-down list, select the desired software file (.bin).

If required, click **Import** to add the software file to the list. Locate the software file (.bin or .pkg) and click **Open**.

- 4) In the **Upgrade** and **Activate new software** sections, select when the software is upgraded and activated on the handset, respectively.
- 5) Click **OK**. The *Shutting down followed by the Remotely updated* dialog window is shown on the handset.

5.2 Upgrade Handset Functionality Using Licenses

The handset functionality can be upgraded in one of the following ways:

- 1) Automatic upgrade, refer to [Automatic License Upgrade](#) on page 98.
- 2) License upgrade using import or export, refer to [Upgrade License Using Import/Export](#) on page 99.
- 3) Manual upgrade, refer to [Manual License Upgrade](#) on page 99.

NOTICE:

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

The following license upgrade is available:

- 1) Upgrade license from WL4 to WL4 Messaging

For additional details, refer to *Portable Device Manager for Windows (WinPDM), Installation and Operation Manual, TD 92712EN*.

5.2.1 Automatic License Upgrade

Use this option if the WinPDM/WSG DM is connected to the Internet.

Automatic license upgrade is a way of upgrading automatically to the correct license for a handset. The first time a handset logs in to the WinPDM/WSG DM it asks the license server for the latest license. When the handset logs in at a later time, there is no automatic check for licenses, so if a new license has been purchased from the license web, you need to use the **Refresh** function (refer to [Refresh Function](#) on page 98) to synchronize the license information in WinPDM/WSG DM with the information in the license server.

In order to get a purchased license for a handset, a connection with the license server is made. The WinPDM/WSG DM automatically receives the serial number from the handset, sends it to the license server which returns a license key that the WinPDM/WSG DM sends to the handset. The handset upgrades and the correct license information (device type) is shown both in the WinPDM/WSG DM and on the handset.

Refresh Function

- 1) If WinPDM is used, place the handset into the DP1 Desktop Programmer.
- 2) In the **Licenses** tab, select the handset to be synchronized.
- 3) From the **License** menu (or right-click the handset), select **Refresh**. The handset's license information in the WinPDM/WSG DM is synchronized with the information in the license server and transferred to the handset.
- 4) The handset restarts.
- 5) Verify that the handset has been upgraded according to the license option.

5.2.2 Upgrade License Using Import/Export

Use this option if WinPDM/WSG DM has no connection to the Internet.

NOTICE:

In this scenario, a license upgrade file must be purchased online. For this purpose, use a PC with the Internet connection to access the License Web page and download the licensing file.

To upgrade the license, perform the following steps:

- 1) Export licensing information from the WinPDM/WSG DM to a file (.xml):
 - In the **Licenses** tab, select the handset that shall be exported.
 - From the **License** menu (or right-click the handset), select **Export**.
 - Enter a name for the file (.xml) and then click **Save**.
- 2) Purchase the license upgrade file from the [License Web page](#) using the exported in the first step file. When done, a license file containing the license keys for the handset is generated.
- 3) Import the purchased license file to the WinPDM/WSG DM:
 - If WinPDM is used, place the licensed handset in the DP1 Desktop Programmer.
 - From the **File** menu, select **Import > Licenses**.
 - Select the license file to be imported (.xml) and then click **Open**.
- 4) When the file is imported, the license key is downloaded to the handset and the handset restarts.
- 5) Verify that the handset has been upgraded according to the license option.

5.2.3 Manual License Upgrade

Use this option if the handset's serial number cannot be exported to a file because WinPDM/WSG DM is not used.

To manually upgrade the license, perform the following steps:

- 1) Enter the handset's serial number at the [License Web page](#) to get the corresponding license key for the handset.
- 2) In the Admin menu of the handset, select **Enter license key**.
- 3) Enter the license key without blanks.
- 4) Press **OK**. If the license key is valid, the `License key accepted` dialog window is shown. The handset restarts.
- 5) Verify that the handset has been upgraded according to the license option.

5.2.4 Move License

It is possible to move a product license to an unlicensed handset. For example, a WL4 Messaging license can be moved from an old handset to a spare unlicensed handset (WL4).

This procedure requires the use of WinPDM/WSG DM that supports the move license feature and the Internet connection to access the license server.

Move a License Using the WinPDM

- 1) Place the licensed handset in the DP1 Desktop Programmer.
- 2) In the **Licenses** tab, select the licensed handset (must be online).
- 3) From the **License** menu (or right-click the handset), select **Move license....**
- 4) In the opened *Move license* window, select the handset that shall receive the license and click **OK**. The licensed handset in the DP1 Desktop Programmer restarts and becomes unlicensed.

NOTICE:

If there is no handset shown in the *Move license* window, factory reset the unlicensed handset and place it into the DP1 Desktop Programmer before performing this step. For the details on factory reset, refer to [Factory Reset using the Handset](#) on page 101.

- 5) Place the unlicensed handset in the DP1 Desktop Programmer. The license is transferred and the handset restarts.
- 6) Verify that the spare handset has received the old handset's license.

NOTICE:

If the device type of the handset remained unchanged in WinPDM and/or the handset did not restart automatically, do the following:

- In the **Licenses** tab, select the handset (must be online).
- From the **License** menu (or right-click the handset), select **Refresh**.

Move a License Using the WSG DM

- 1) Verify that the unlicensed handset is configured with the basic network settings. If not, do as follows:
 - Enter the Admin access code while the handset is showing the `No network` message at start-up. Otherwise, go into the **Main menu > Settings** and enter the Admin access code there.
 - In the **Network setup** menu, set all the required system settings for the WLAN. No certificates can be entered or referred to using the Admin menu.
 - In the **WSG** menu, set the IP address and password (if any) to the Unite module.

The handset will attempt to install the connection using the secure Websocket and the default credentials. If this fails, the handset will attempt to perform a legacy mode connection.
- 2) In the **Licenses** tab, select the licensed handset (must be online).
- 3) From the **License** menu (or right-click the handset), select **Move license....**
- 4) In the opened *Move license* window, select the unlicensed handset and click **OK**. The license is transferred and both handsets restart.

- 5) Verify that the spare handset has received the old handset's license.

NOTICE:

If the device type of the handset(s) remained unchanged in WSG DM and/or the handset(s) did not restart automatically, do the following:

- In the **Licenses** tab, select the handset (must be online).
 - From the **License** menu (or right-click the handset), select **Refresh**.
-

5.3 Perform a Factory Reset

The factory reset of a handset can be performed using WinPDM/WSG DM or the handset. A factory reset restores all configuration settings to their default values. For example, PBX subscriptions, contacts, certificates are removed. The software and licenses are left intact.

Factory Reset using WinPDM/WSG DM

To perform a factory reset, do the following:

- 1) In the **Devices** tab, select the handset to be factory reset (the handset must be online).
- 2) From the **Device** menu (or right-click the handset), select **Factory reset**.
- 3) In the opened *Reset devices* window, click **Yes**. The handset restarts.

Factory Reset using the Handset

To perform a factory reset using the handset, do the following:

- 1) In the Admin menu, select **Factory Reset**.
- 2) In the opened *Reset portable?* dialog window, press **Yes**. The handset restarts.

5.4 Handset Replacement

It is possible to replace an old/broken handset with a new or spare handset. Handsets registered in WinPDM/WSG DM are associated with a device type, device ID, and number. During the replacement procedure, the broken/old handset's device type and number are associated with the new/spare handset's device ID.

Handsets can be replaced using the:

- 1) WSG DM, refer to [Replace the Handset using WSG DM](#) on page 102.

NOTICE:

If a spare handset has been factory reset or does not have configured network settings, it must be first configured in WinPDM. For the details, refer to the [Deploy Handsets Using WinPDM](#) on page 12.

- 2) WinPDM, refer to [Replace the Handset using WinPDM](#) on page 103.

NOTICE:

If the spare handset has been previously used, perform a factory reset. For more information, refer to [Perform a Factory Reset](#) on page 101.

The table below show what type of data can/cannot be replaced during the procedure:

Data replaced	Data not replaced
User parameters	Certificates
Contacts	Call list
	Messages
	Company phone book
	Licenses
	NOTE: Handset's license(s) can be moved to an unlicensed handset, refer to Replace the Handset and Move the License using WinPDM on page 104 or Replace the Handset and Move the License using WSG DM on page 103.

5.4.1 Replace the Handset using WSG DM

If a handset should be replaced with a new one, it is possible to transfer the old handset number to a spare handset. The spare handset must be of the same device type as the old one.

To replace the handset, perform the following steps:

- 1) Make sure that the old handset is saved in the WSG DM . If not, do as follows:
 - a) In the **Numbers** tab, select the handset to be synchronized and saved.
 - b) From the **Number** menu (or right-click the handset), select **Save**.
- 2) If the old handset is online in the WSG DM , switch it off. The handset is shown as offline after a while.

- 3) Take the spare handset and verify that it is configured with the basic network settings. If not, do as follows:

- a) Enter the Admin access code while the handset is showing the `No network` message at start-up. Otherwise, go into the **Main menu > Settings** and enter the Admin access code there.
- b) In the **Network setup** menu, set all the required system settings for the WLAN. No certificates can be entered or referred to using the Admin menu.
- c) In the **WSG** menu, set the IP address and password (if any) to the Unite module.

The handset will attempt to install the connection using the secure Websocket and the default credentials. If this fails, the handset will attempt to perform a legacy mode connection.

- 4) Factory reset the spare handset.
- 5) In the opened *Login* window, enter the old's handset number and leave the password blank. When done, press **Login**.

The spare handset connects to the WSG DM using earlier configured basic network settings to receive an update from the system. The handset might restart.

- 6) Verify that the last stored settings for the old handset have been transferred to the spare handset.

Replace the Handset and Move the License using WSG DM

If you need to perform handset replacement together with license migration, the procedure is the following:

- 1) Replace the old handset with the spare one as described above in the [Replace the Handset using WSG DM](#) on page 102.
- 2) Switch the spare handset off and turn the old handset on.
- 3) In the **Licenses** tab of the WSG DM, select the old handset (must be online).
- 4) From the **License** menu (or right-click the handset), select **Move license....**
- 5) In the opened *Move license* window, select the spare handset and click **OK**.
The old handset restarts and the license is transferred to the spare handset.
- 6) Switch the old handset off and switch the spare handset on.
- 7) Verify that the spare handset has received the old's handset license.

NOTICE:

If the device type of the handset remained unchanged in WSG DM ?>, do the following:

- a) In the **Licenses** tab, select the handset (must be online).
 - b) From the **License** menu (or right-click the handset), select **Refresh**.
-

5.4.2 Replace the Handset using WinPDM

If a handset should be replaced with a new one, it is possible to transfer the old handset number to a spare handset. The spare handset must be of the same device type as the old one.

To replace the handset, perform the following steps:

- 1) Place the old handset into the DP1 Desktop Programmer. Make sure that the handset is saved in the WinPDM. If not, do as follows:
 - a) In the **Numbers** tab, select the handset to be synchronized and saved.
 - b) From the **Number** menu (or right-click the handset), select **Save**.
- 2) Remove the old handset from the DP1 Desktop Programmer and place the spare handset instead.
- 3) In the **Numbers** tab, select the spare handset.
- 4) From the **Number** menu (or right-click the handset), select **Associate with device**.
- 5) In the opened list, select the old handset to be replaced with the spare handset and click **OK**.
- 6) Verify that the spare handset has received the old's handset number.

Replace the Handset and Move the License using WinPDM

If you need to perform handset replacement together with license migration, the procedure is the following:

- 1) Move the license from the old handset to the spare handset as described in [Move a License Using the WinPDM](#) on page 100.
- 2) Replace the handset as described above starting from the step 3.

5.4.3 Parameter Migration

The parameter migration feature allows parameters of a certain handset variant to be applied to any compatible handset, for example, WL3 template can be used for WL4 handsets. When migrating, the parameters must be first saved in a template.

The same template can be also used for different handset variants, for example for WL4 and WL4 Plus.

NOTICE:

WL4 Plus specific parameters are ignored by the WL4.

NOTICE:

Though the same template can be also used for different handset variants, for example for WL4 and WL4 Plus, there is no guarantee that all parameters will be configured as expected. That is why, it is recommended to use a template specifically for each device type. Otherwise, you need to check the handset after parameter migration and make sure that the configuration is correct.

The example below shows how to migrate parameters from WL3 to WL4 handset:

- 1) If WinPDM is used, place WL4 handset into the DP1 Desktop Programmer.
- 2) In the **Templates** tab, select the template used for WL3 handset that you want to use for parameter migration.
- 3) In the **Template** menu (or right-click the template), select **Apply to....**

- 4) In the opened window, select the WL4 handset that shall receive new parameters and click **OK**.
- 5) The handset receives the template and might restart.
- 6) To verify that the handset has received the template with the new parameters, in the **Numbers** tab, check the **Last run template** column.

For additional details on parameter migration, please refer to *Unify WL4 VoWiFi System, Migration Guide, TD 93455EN*.

5.5 Change the Number of a Handset

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

- 1) Open the **Numbers** tab, and select the handset to be updated with a new number.
- 2) In the **Number** menu (or right-click the handset), select **Rename...**
- 3) In the **New prefix** field, enter the new prefix (if needed).
- 4) In the **New number** field, enter the new number.

NOTICE:

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 WinPDM/WSG DM.

- 5) Click **OK**.

The new number is synchronized with the handset when it is connected to WinPDM/WSG DM.

5.6 Change the WLAN Security Mode in Existing Installation

IMPORTANT: The synchronization of new settings to the handset settings cannot be performed if the settings in the AP is changed before the settings in the handset. Change settings in the handset before change settings in the AP.

It is recommended to leave one AP 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. To change the WLAN password/authentication, perform the following steps:

- 1) Create a new template with the new security settings, refer to [Security Settings](#) on page 22.
- 2) Apply the new template to the handsets. The handsets will start an automatic update and restart.

NOTICE: During the update and restart, the handsets have no access to the WLAN system.

Maintenance

Create a Configuration Backup

- 3) Change the security settings for the APs. The handsets are now able to access the WLAN.

5.7 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 for Windows (WinPDM), Installation and Operation Manual, TD 92712EN*.

6 Troubleshooting

This chapter offers possible solutions for common operational errors. The following section covers common system and hardware-related problems that might be encountered when using the handset, together with suggestions on how to troubleshoot them. This chapter also includes information about some recommended internal troubleshooting tools for monitoring and analyzing data along with a list of common issues with suggested troubleshooting steps.

NOTICE:

If other users experience similar issues, there may be a system error.

6.1 Operational Problems

Fault	Probable cause	Action or comment
It is not possible to mute the handset by long-pressing the Sound off key/Mute button. It is not possible to set the ring volume to Silent .	A handset restriction prevents the user to silence the handset.	Change the parameter Prevent silent in Audio > General .
Connected call but no sound or one way sound.	- IP addressing fault. - The handset is muted. - The handset has bad speaker/microphone.	- Make a note of 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. - Check if the handsets are muted. - Use a headset to eliminate bad speakers/microphone.
There are no entries in the Call list.	A handset restriction prevents calls from being saved in the call list.	Change the parameter Enable call list to Yes in Device > Call .

Fault	Probable cause	Action or comment
Voice quality is bad.	Increased traffic load or interference.	• Check if QoS is working in both directions. Voice traffic should be prioritized on both the LAN and the WLAN. • Connect to other phones (wired, analogue or external) to define if it is the other end that may cause bad quality. • Do a site survey and check for areas with too low or too high coverage and other interfering 802.11 systems. • Do a network performance test to ensure the wired LAN/backbone has adequate capacity. • Use a spectrum analyzer and look for non-802.11 interference.
Battery life is short.	• DTIM might not be set correctly. • Cisco MSE , AiRISTA Flow, or BLE location client settings need to be changed.	• Check the Beacon interval and DTIM settings in the AP. • Verify the coverage, since low signal strength will make the handset to constantly search for other APs and thereby consuming more power. • Use a sniffer and check the amount of broadcast traffic that is transmitted on the WLAN. • Check if correct models of the chargers are used. • Verify with another battery. • If using Cisco MSE, AiRISTA Flow, or BLE location client, change the settings, for example, decrease the scanning interval.

Fault	Probable cause	Action or comment
The handset does not start up correctly after a software upgrade.	The new software does not work as intended for the parameter settings in this handset.	The handset stores two software versions, which makes it possible to revert back to the earlier software. Restore the earlier version of the software by performing the following steps: • Switch off the handset. • Press and hold keys 7 and 8, and press On/Off at the same time. The handset loads the earlier software and keeps it until the handset is restarted.

6.2 Warning Messages

The following table contains errors that are shown on the handset display.

No access	
Probable cause	Action

The handset has found and associated to the WLAN (a wireless network with the configured SSID and correct security settings), but cannot connect to the SIP proxy or the Unite module.	— Check if the handset is connected to the correct SSID by entering the WLAN info screen (non-configured handset might connect to an open or staging network instead of the required one). If the handset is not connected to the correct SSID, configure the WLAN parameters in the handset. — Check if the handset has the correct network settings, for example, IP address (either static or received by the DHCP) by entering the Network info screen. If not, correct the handset network parameters and/or the DHCP server configuration. — Check if it is possible to ping the handset, Unite module, and SIP proxy from another PC. — Check the VoIP settings in the handset and SIP proxy well as check the WSG settings in the handset (under the Admin menu) and Unite module. — Make sure that the connection mode matches between the handset and the Unite module. If Secure Websocket is used, make sure that certificate validation, Websocket interface credentials (username and password) are used correctly. — Restart the handset.
---	---

No network	
Probable cause	Action
The handset has lost WLAN connection or out of coverage.	Try to move to another part of the room/building or wait until the connection is restored. NOTE: When re-entering the coverage area it can take a couple of minutes before the handset is automatically registered into the system. NOTE: When leaving a bad state for another bad state, the dialog window reopens and the beep sounds again (if enabled).

The handset cannot find the wireless infrastructure with settings matching those configured in the handset.	— Check the SSID. The SSID configured in the handset must be identical to the SSID configured in the system infrastructure. — Check the security settings. The security settings, that is, authentication and encryption must match the settings in the system infrastructure. — Check for 802.11d multi-regulatory domain settings. The handset must be able to detect in which country it is located to use the correct channel and transmit power settings. — Check which channels are used. By default, the handset uses channels 1, 6, and 11 in the 2.4 GHz range and all channels in the 5 GHz range. If the infrastructure is configured to use any other channel, change it to use only 1, 6, and 11 or all channels as these are the recommended settings. — Check that the correct Network (A, B, C or D) setting is selected.
The handset is faulty.	Send the handset for service.

Voice only

Probable cause	Action
The handset is configured to use both SIP proxy and the Unite module, but has lost contact with the Unite module.	— Check the Unite module address. Try to ping the Unite module from another PC. — Remove the handset from the DP1 Desktop Programmer. When connected to the WinPDM through USB on the DP1 Desktop Programmer, the handset cannot connect to the Unite module and may show <i>Voice only</i>. — If messaging is not used in the system, verify that the Unite module address is configured to 0.0.0.0.

Limited mode

Probable cause	Action
The PBX is in Server mode backup .	No action needed. Wait for the PBX backup to be complete.

Messaging only

Probable cause	Action
The handset is configured to use both a SIP proxy and the Unite module but has lost contact with the SIP proxy.	— Check the SIP proxy address. Try to ping the SIP proxy from another PC. — Try to send a message. The idle connection check interval to the Unite module is much longer than to the SIP proxy. Sometimes when network connection is lost, the handset shows <code>Messaging only</code> for quite some time, because it discovers it has lost connection to the SIP proxy much faster than it discovers the loss of connection to the Unite module. In this case the handset will eventually change to <code>No access</code>. — If the handset is supposed to use SIP proxy discovery, verify that the configured SIP proxy IP address is 0.0.0.0. — Check the Endpoint number and the Endpoint ID. If both are configured, they must match with the Endpoint ID and Endpoint number registered in the IP PBX. Clear the Endpoint ID.

SCEP renewal failed. Contact handset admin for help	
Probable cause	Action
SCEP renewal procedure has failed. SCEP renewal failed. Contact handset admin for help is shown when the existing certificate is due to expire in more than 24 hours or has already expired.	Install a new SCEP certificate.
A new SCEP certificate cannot be installed because the certificate has a validity period shorter than one hour.	Change the SCEP server configuration.
The SCEP server returned the already installed certificate when the handset tried to renew the threshold.	Increase the Renew threshold period on the handset or update the SCEP server configuration.

SCEP server validation has failed.	Disable SCEP server validation and install the correct certificate in the Trust list or delete all installed certificates from the Trust list in order to set the handset to Trust On First Use (TOFU) mode.
The handset was unable to connect to the SCEP server.	Check that the SCEP URL can be reached from the network the handset is connected to.
Incorrect SCEP parameters received from the DHCP server or incorrect SCEP parameters set using WinPDM/WSG DM .	Check that the handset's date and time is set correctly, preferably using NTP. If the time or date on the handset differs from the current time or date, the certificate might consider the connection invalid. This is the most common in cases when the certificate expires earlier than the time or date set on the handset.
The handset got an error back from the SCEP server.	Check the SCEP server logs.

SCEP certificate expires soon. Contact handset admin

Probable cause	Action
SCEP renewal procedure has failed. SCEP certificate expires soon. Contact handset admin is shown when the existing certificate is due to expire in 24 hours or less.	Install a new SCEP certificate.

SERVICE NEEDED ^{11 12}

Probable cause	Action
The handset is faulty.	— Select the Reboot option on the left soft key. — If the problem persists, try one of the following: 1) Power off the handset using the Off soft key in the middle and send the handset for service. 2) Perform a factory reset by selecting the Factory soft key on the right.

¹¹ This message is shown only in English.

¹² An additional message is also displayed describing the cause of the error.

Enter PIN code	
Probable cause	Action
Phone lock is activated.	Enter the required PIN code. If the PIN code has been lost, change it using WinPDM/WSG DM or do a factory reset.

Battery low, charge now	
Probable cause	Action
The battery level is low.	Charge the handset, or replace or charge the battery.

Phone book is not available at the moment.	
Probable cause	Action
The phone book is not activated or does not respond.	Try again later or if the fault persists, do a factory reset using the Admin menu or WinPDM/WSG DM. NOTE: It may take several minutes for the phone book to be available if there are many entries in the Contacts list and/or the company phone book.

Voice mail number not defined.	
Probable cause	Action
There is no voice mail number defined in the handset.	Define a voice mail number using WinPDM/WSG DM.

Remotely updated	
Probable cause	Action
The handset starts up after a parameter update.	No action needed. Wait for the handset to start up.

Updating handset...	
Probable cause	Action
The handset has retrieved new software, which is now upgrading the handset.	No action needed. Handset might restart depending on the parameter setting. The new software becomes active after the next handset restarts.

Handset is updated	
Probable cause	Action

The handset starts up after a software upgrade.	No action needed. Wait for the handset to start up.
---	---

Dev functions	
Probable cause	Action
Dev functions text is displayed instead of the current date in the Idle mode. The handset has been unlocked, for example, in order to run unofficial software builds, refer to Transfer Unlock File on page 61.	Factory reset the handset.

6.3 Logging

There are different types of logging that can be used, depending on the area to be investigated. The support engineer, in the first place, should investigate and rule out relatively easy to identify causes, such as incorrectly configured parameters. If no relevant information can be collected and the problem is persistent, logs should be collected.

6.3.1 Syslog

With Syslog you can monitor the status of the handset, for example, the status of the system, WLAN, calls, battery, etc. and upload this information to a specified server. The log is additionally stored in the handsets internal memory, from where it also may be extracted.

The data in the Syslog is limited to a short status update and do not include the descriptive information, so in situations where serious problems occur the additional tools should be used to capture the detailed logs.

The handset is able to transfer some logs to a remote syslog server. Since Syslog is both unauthenticated and unencrypted, Syslog is disabled by default and should only be enabled when used over a secured network.

In order to receive the syslog messages from a handset, the syslog functionality must be enabled and the syslog server must be specified. To enable the Syslog, do the following:

- 1) Select **Device > Log**.
- 2) In the **Syslog** drop-down list, select **On** to enable logging.
- 3) Select **Syslog server IP address** and specify the IP address of the server to receive system logs.

Stop the logging by selecting **Off** in the **Syslog** drop-down list.

6.3.2 PCAP and Remote PCAP Capturing

The Packet Capture (PCAP) logs play a critical role in troubleshooting network-related issues.

With Packet Capture (PCAP), you can sniff the network traffic on site, and uplink the captured packets to a PC, where the captured packets can be processed, analyzed and archived. The PCAP feature stores the network traffic sent and received by the handset. PCAP logs are stored in the handset's internal storage and can be opened, for example in Wireshark.

When the RPCAP server is activated on the handset, a client (for instance Wireshark) can connect and retrieve all IP protocol traffic to and from the handset.

The following procedure describes how to collect PCAP and RPCAP logs:

- 1) Select **Device > Log**.
- 2) In the **PCAP Capturing** drop-down list, choose between:
 - **PCAP to file**

NOTICE:

When running PCAP to file, the RTP data packets are not saved because they take up too much space.

- **RPCAP** to send logs to a remote server.

When the necessary logs have been collected, stop PCAP logging by selecting **PCAP Capturing > Off**. The created PCAP file becomes available only when you turn off PCAP capturing.

NOTICE:

Only run PCAP or RPCAP when needed, and shut it off when not used because it gives additional load to the handset, as well as the system (with mirroring copies) when using RPCAP.

PCAP files are not encrypted and can be retrieved using USB or SFTP. If logs should be sent to a remote server SFTP, additional configuration is required. For the details, refer to [Send Logs over SFTP](#) on page 117.

6.3.3 Save Logs

The handset continuously generates encrypted logs that can be sent to Ascom support for analysis. Logs are normally stored in volatile memory for a short period before they are deleted.

When **Save Logs** function is enabled, the logs are also saved in a persistent storage, until the specified time interval ends. All logs can be either collected during the specified time interval (from 10 minutes up to 1 week) or right after a problem has occurred by selecting the **Save once now** option.

If the persistent storage becomes full, the oldest logs are overwritten by newer ones.

NOTICE:

Depending on the nature of the issue, it may be required to change the default log levels as described in [Trace Configuration](#) on page 117. This controls which logs are generated and must be set before the problem occurs.

The following procedure explains how to collect and save logs:

- 1) Select **Device > Log**.
- 2) In the **Save logs** drop-down list, select one of the following:
 - **Save once now** to collect logs only once.
 - **Save for X time** to continuously save logs. Choose among 10 minutes, 4 hours, 24 hours, and 1 week.

The logs can be retrieved using USB or SFTP. If logs should be sent to a remote server SFTP, additional configuration is required. For the details, refer to [Send Logs over SFTP](#) on page 117.

6.3.4 Send Logs over SFTP

The handset can be configured to transfer encrypted log files to a remote SFTP server. Only password authentication is supported, so care must be taken when configuring the remote server so that other actions than uploading log files are not permitted.

Continuously transferring logs over SFTP makes it possible to have logging enabled for a long period of time without the risk of running out of storage space on the handset. There is a delay before a file is transferred from the handset.

To enable sending saved logs to the remote server over SFTP, perform the following steps:

- 1) Select **Device > Log**.
- 2) In the **Enable Sending Logs over SFTP** drop-down list, select **On**.
- 3) Once enabled, the following SFTP parameters can be configured:
 - a) **SFTP server IP address** defines the IP address of the remote server, which the handset sends logs to over SFTP.
 - b) **SFTP server authentication identity** defines the user name used to log in to the SFTP server.
 - c) **SFTP remote server authentication password** defines the password is used when the SFTP remote server requires a password.

6.3.5 Trace Configuration

- 1) In normal operation, all extended trace levels should be set to **Normal** since excessive logging can affect handset performance. When any trace is above the **Normal** level, it is indicated by the `Trace active` message in Idle mode.
- 2) Select **Device > Log**.

3) The trace level can be set on the following parameters:

- **Set WLAN Trace**
- **Set Configuration Trace Level**
- **Set GUI Trace Level**
- **Set GLI Trace**
- **Set Unite Trace**
- **Set VoIP Trace**
- **Set System Trace**
- **Set Protector Trace** (applicable to WL4 Plus only)
- **Set SaS Trace**
- **Set Bluetooth Trace**

4) Select one of the following logging levels:

- **Normal**
- **Verbose**

These settings only affect the encrypted internal handset logs, not the remote Syslog functionality.

NOTICE:

Restore the handset to **Normal** logging after logs are captured, since extra logging can affect handset performance.

6.3.6 Low Level WLAN debug

This parameter can be used to enable even more verbose WLAN debug information. It must be enabled only when requested by a support contact.

- 1) Select **Device > Log**.
- 2) In the **Low Level WLAN debug** field, enter the required string.

6.3.7 SNMP

The handset can be configured to provide a Simple Network Management Protocol (SNMPv2) interface where some diagnostic information can be retrieved by a SNMP agent, or sent from the handset using so called SNMP traps.

Since it is not possible to alter the handset configuration in any way over this interface, it is not critical from a security standpoint. Do however note that the login and data transfer is done unencrypted so it is recommended to only use SNMP within a secured network

To enable SNMP, perform the following steps:

- 1) Select **Device > Log**.
- 2) In the **SNMP** drop-down list, select **On**.
- 3) The standard SNMP community name **public**, can be changed to a specific name to enhance the security of the device. Enter the new name in the **SNMP community name** field.

SNMP Traps

The handset can send the following SNMP traps:

SNMP Trap	Description
In service	When the handset is started up and logged in to the SIP server.
Out of service	When the handset is switched off.
SIP online	When logged in to the SIP server again after the SIP connection had been lost.
SIP offline	When the SIP connection is lost, but the handset still has WLAN connection.
WLAN back	When handset's WLAN connection is back, after being disconnected.

To configure SNMP traps, perform the following steps:

- 1) Select **Device > Log**.
- 2) In the **SNMP traps** drop-down list, select **On**.
- 3) In the opened **SNMP manager IP address** field, enter the IP address of the SNMP manager.
- 4) In the opened **Port number for SNMP traps** field, enter the port number of the SNMP manager.

7 Related Documents

Unify OpenScape WLAN Phone WL4, Data Sheet, TD 93315EN

Unify OpenScape WLAN Phone WL4, User Manual, TD 93342EN

Unify WL4 VoWiFi System, Migration Guide, TD 93455EN

Portable Device Manager for Windows (WinPDM), Data Sheet, TD 92635EN

Portable Device Manager for Windows (WinPDM), Installation and Operation Manual, TD 92712EN

OpenStage Wireless Service Gateway (WSG), Installation and Operation Manual, TD 92442EN

8 Document History

Version	Date	Description
D	20 May 2021	General: Made editorial changes (restructured sections, updated parameter descriptions, added new parameter descriptions). New: Create a Network Template in WinPDM on page 14. Assign a Number to a Handset on page 17. Allow Outdated Security Protocols on page 24. Import Trust and Application Certificates on page 67. 802.11k Neighbor List on page 27. Unite Module Settings on page 29. Deauthenticate on Roam on page 29. Updated: Added a note into Import Contacts on page 31. Updated Deploy Handsets Using the WSG DM on page 11, Deploy Handsets Using WinPDM on page 12, and Deploy Handsets Using the Admin Menu on page 13 with the requirements to connect to the Unite module. Recommendations added into the WPA/WPA2-Personal and WPA3-Personal on page 22. WinPDM Authentication on page 24 SCEP failure warning message has been added in Warning Messages on page 109. Updated description for troubleshooting tools for the whole Logging on page 115 section and its subsections. Included “SIP TLS client certificate and “Validate server certificate” in VoIP Protocol on page 63. Included new parameters in Configure SCEP Using WinPDM/WSG DM on page 146.
C	29 June 2020	Update: 1.1 GDPR Considerations, page 1 5.2 Handset Replacement, page 70 New 5.2.1 Parameter Migration, page 71

Document History

Version	Date	Description
B	April 2020	General: Made editorial changes (restructured sections, updated parameter descriptions, added new parameter descriptions) Update: 2 Handset Deployment, page 2 3 Parameter Configuration, page 10 4 System Deployment Planning, page 64 New: 3.3.7 Roaming Method, page 16 3.4.21 Change Admin Access Code, page 30 5.8 Logging, page 77 C.5 SCEP, page 97 3.4.22 Block Access to the Admin Menu, page 30
A	January 2020	First version

9 Configure Custom Sounds

Before configuring custom sounds, it is recommended to have a basic knowledge on notes.

Custom sounds are configured in **Audio > Custom sounds > Melody**. The **Melody** parameter is represented by a text string consisting of several elements. For the details, refer to the table below:

Table 3: Elements, Melody strings, and parameters for melodies

Element		Sub-element	Values
Note	>	Octave-prefix	*0 (A=55 Hz) *1 (A=110 Hz) *2 *3 *4 (default) *5 *6 *7 *8 (A=14080 Hz) NOTE: 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

Table 4: Elements, Melody strings, and parameters for melodies

Element		Sub-element	Values
Note	>	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	r
		Duration	1 to 5 (1 = long pause, 5= short pause)
		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 9: Example of a Melody string on page 124 and Table 5: Explanation of the Melody string example on page 124 illustrate how to program a melody.



Figure 9: Example of a Melody string

Table 5: Explanation of the Melody string example

1	Octave-prefix
---	---------------

2	Vibration is turned on. The handset vibrates continuously.
3	Basic note with 1/8 duration
4	Iss 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

9.1 Customize the Default Handset Beeps

If it is required to create a custom sound out of any of the default handset beeps (Beep 1–10 and Enhanced beeps 1–7), the default definition of each beep can be used as a starting point for further customizing the sound.

The default definitions are described below.

Table 6: Definitions of Beeps

Custom sound	Beeps	Definition (default)
Custom sound 1	1 beep	*6e2r2
Custom sound 2	2 beeps	*6e3r3e3r3
Custom sound 3	3 beeps	*6e4r4e4r4e4r4
Custom sound 4	3 tone chime	*6c2r5:d2r5:e2r5
Custom sound 5	10 beeps	*6e4r4e4r4e4r3.e4r4e4r2e4r4e4r4e4r3.e4r4e4r4
Custom sound 6	Alarm sweep	(*5#f3g3#g3a3#a3b3*6c3#c3d3#d3e3r3@9)
Custom sound 7	Alarm siren	(*6c4e4@52)
Custom sound 8	Not predefined	Not predefined
Custom sound 9	Not predefined	Not predefined
Custom sound 10	Not predefined	Not predefined

Table 7: Definitions of Enhanced Beeps

Enhanced beeps	Beeps (default)	Definition
Enhanced beep 1	1 beep	*6e2r2
Enhanced beep 2	2 beeps	*6e3r3e3r3
Enhanced beep 3	3 beeps	*6e4r4e4r4e4r4

Configure Custom Sounds

Enhanced beep 4	3 tone chime	*6c2r5:d2r5:e2r5
Enhanced beep 5	10 beeps	*6e4r4e4r4e4r3.e4r4e4r2e4r4e4r4e4r3.e4r4e4r4
Enhanced beep 6	Alarm sweep	(*5#f3g3#g3a3#a3b3*6c3#c3d3#d3e3r3@9)
Enhanced beep 7	Alarm siren	(*6c4e4@52)

10 Easy Deployment

Easy deployment is done using a (staging) WLAN with a predefined SSID with a security profile and the Unite module.

Easy Deployment is done in the following three steps:

- 1) WLAN discovery, refer to [WLAN Discovery](#) on page 128.
- 2) Unite module discovery, refer to [Unite Module Discovery](#) on page 129.
- 3) Parameter download, refer to [Parameter Download](#) on page 132.

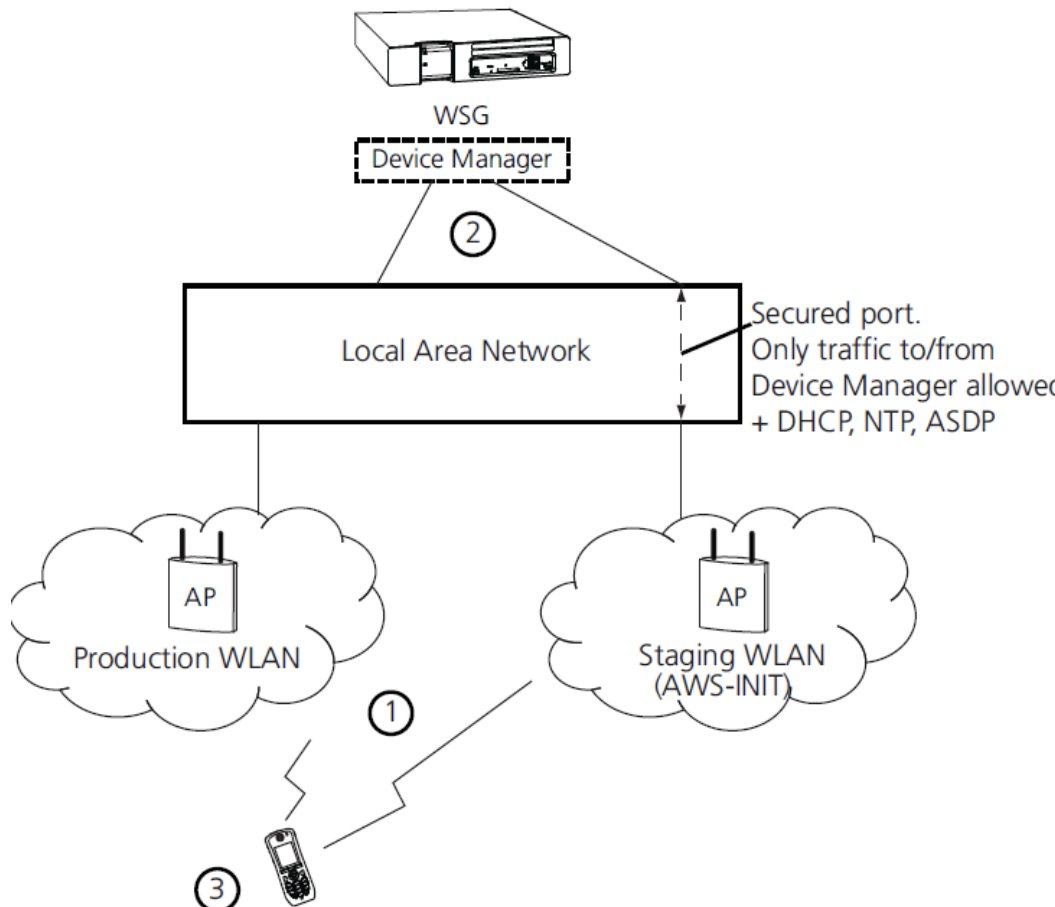


Figure 10: Easy Deployment

10.1 Prerequisites for Easy Deployment

Handsets are automatically installed by Easy Deployment, if the following is fulfilled:

- 1) The WLAN network needs at least one AP that allows access to the Unite module. The following default configuration is used, which cannot be changed:

SSID	AWS-INIT
Security mode	WPA/WPA2-Personal

Passphrase	AWS-INIT
------------	----------

On the handset, all other network parameters must be at their default settings, for example, the following:

DHCP mode	On
802.11 protocol	2.4 GHz or 5 GHz
2.4 GHz channels	1, 6, 11
5 GHz channels	All
World mode regulatory domain	World mode (802.11d)

- 2) No **SSID** for any of the **Networks X** (A-D) is configured on the handset.
- 3) The port to the Unite module must be open and not blocked.
- 4) The WSG DM must be configured to allow legacy connections or it must allow secure Websocket connections (recommended method) using the default credentials. For the details, refer to [Websocket Authentication](#) on page 31.
- 5) 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 the certificate validations).
- 6) The Call ID (endpoint number/phone number) is configured.

NOTICE:

The number to be used by a handset is entered directly on the handset, after a first successful access to the Unite module.

10.2 WLAN Discovery

The WLAN discovery starts when the new handset starts up. An already configured handset uses an entry stored in **Network > Networks X** (A-D), and tries to associate with that SSID.

If there is no WLAN network (SSID) configured in the handset, the handset tries to associate with a predefined default WLAN with SSID **AWS-INIT**, alternately on the 2.4 GHz frequency band and on the 5 GHz frequency band.

If the **AWS-INIT** is not connected on any frequency band within some seconds, the handset tries to connect to an open network. If it also fails, the alternatives are tried again, until succeeded. During this connection process, the **No network** warning message is displayed on the handset.



CAUTION:

Due to security reasons, it is not recommended to use an open network for staging.

The staging network **AWS-INIT** should be set up to only allow traffic to/from the WSG DM , and services for Easy Deployment (like DHCP, NTP, ASDP). It prevents unauthorized access to the network.

NOTICE:

The WLAN discovery process stops if any SSID for **Networks X** (A-D) is manually filled in, either by using the handset's Admin menu or WinPDM/WSG DM .

SSID (network name) can be viewed in the Admin menu on the handset in **Device info > WLAN info**. The **SSID** field shows currently used SSID.

INFO:

If the wireless network connection bars (see the upper-left corner of the display) come and go alternately, the pre-shared key (PSK) on the AP is probably wrongly configured, and the handset cannot connect to the AP. After a timeout, the `No network` warning message is shown on the handset.

10.3 Unite Module Discovery

Once the handset has a WLAN connection, the second step is to automatically get the IP address to the Unite module, which runs the WSG DM .

There are two ways to get the IP address automatically:

- 1) Using the vendor option functionality, Option 43 of a DHCP server. For more information, refer to [Server Discovery Using the DHCP Option 43](#) on page 129.
- 2) Using the Ascom Service Discovery Protocol (ASDP) implemented in the handset. For more information, refer to [Server Discovery Using the Ascom Service Discovery Protocol \(ASDP\)](#) on page 130.

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

10.3.1 Server Discovery Using the DHCP Option 43

A DHCP server can be configured to return the Unite module IP address, as part of the DHCP response to the handset, with other needed DHCP parameters. The Unite module 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 `OpenScapeWL4` is the Object Identifier (OID) for the handset.

In this way, a DHCP server can be configured to return the Unite module IP address only to those clients that expect it. Option 60 also allows different clients to use different settings in Option 43, if there are multiple clients in the network.

After the handset receives the IP address to the Unite module, it tries to log in to the WSG DM . The DHCP Option 43 is ignored once the Unite module IP address is configured in the handset.

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 server, is found in [Configuration Example of a Linux Server Using DHCP Option 43](#) on page 138 and [Configuration Example of an MS Windows 2003 Server](#) on page 138, respectively.

10.3.2 Server Discovery Using the Ascom Service Discovery Protocol (ASDP)

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

the Unite module that is 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 Unite module to support different client services. If there are multiple Unite 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 respond fastest.

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

Configure the Unite Module to Support WLAN Service Discovery Clients

For each module, the ASDP must be configured to support WLAN clients.

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

10.4 Easy Deployment and VLAN

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

Although, a mapping rule can 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, make sure that the handset can also associate with the production SSID after it has received its full configuration from the WSG DM used for Easy Deployment.

NOTICE:

When getting the production WLAN SSID, it may be mapped to another VLAN. In this case, the IP address is changed. The DHCP server options are also served by another scope or eventually another DHCP server.

If using a deployment VLAN, it may be required to have two WSG DM or it is possible to set up a restrictive routing between VLANs.

A direct configuration of Option 60 and Option 43 may also be used on a scope-by-scope basis if the system allows the separation of DHCP client devices to use independent scope ranges.

10.5 Easy Deployment and Certificates

NOTICE:

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

Application Certificate

If the production network is using individual application certificates, which, for example, are required for using EAP-TLS, first associate the certificates with the predefined number in the WSG DM used for Easy Deployment, and then select the required application certificate. Perform the steps, as described below in this section.

INFO:

If there is no application certificate in the WSG DM used for Easy Deployment, the handset is disconnected from the WLAN. To recover from this, first do a factory reset, and make sure that the application certificates are associated with the correct Number. You can also use the WinPDM to install the correct application certificate. Then try again.

Trusted Certificate

- 1) Upload at least one **Self-signed certificate** and up to seven **Intermediate certificates**, which are used to establish the trust chain of the server certificate. The commonly understood name of these certificate types is **Trusted certificate**.
- 2) Open the **Numbers** tab and select the handset to manage the certificates.
- 3) In the **Number** menu (or right-click the handset), select **Manage certificates**. The *Manage certificates* window opens.
- 4) In the **Trust list** tab and **Application certificates** tab, click **Browse** and select the certificates to import. When done, click **Close**.

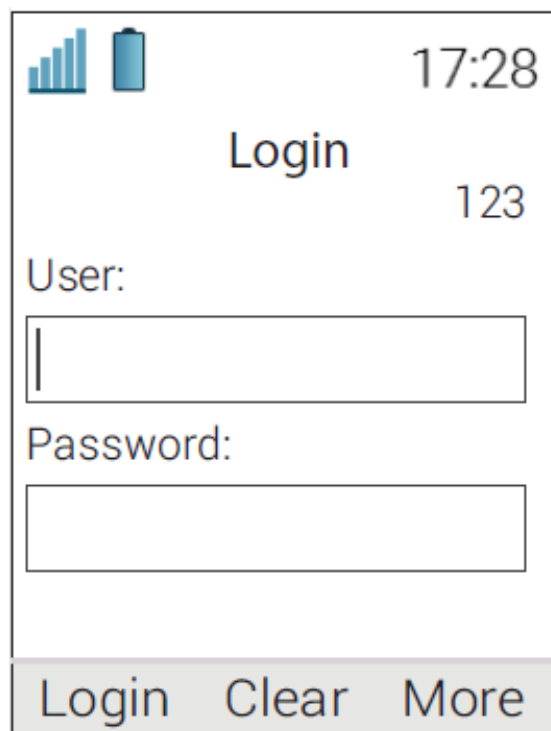
- 5) In the **Number** menu (or right-click the handset), select **Edit parameters**.
- 6) Select **Network > Network X (A-D)**.
- 7) In the **Security mode** drop-down list, select **WPA2–Enterprise** or **WPA3–Enterprise**.
- 8) In the **EAP** drop-down list, select **EAP-TLS**.
- 9) In the **EAP client certificate** drop-down list, select the application certificate to be used. When done, click **OK**.

For more information on certificates, refer to *Portable Device Manager for Windows (WinPDM), Installation and Operation Manual, TD 92712EN*.

10.6 Parameter Download

After successfully receiving the Unite module IP address, the handset tries to log in to the Unite system.

The handset has, at this stage, no number stored internally, and does not know its identity in the Unite system. When the `Login` screen is displayed on the handset, enter the intended endpoint number (that is, preferably the phone number of the handset) that the handset uses to log in to the Unite system.



The screenshot shows a handset's login interface. At the top left, there are icons for signal strength and battery. The time 17:28 is displayed in the top right. The word 'Login' is centered in a large font. Below it, the number '123' is displayed. There are two input fields: 'User:' and 'Password:'. At the bottom, there are three buttons: 'Login', 'Clear', and 'More'.

Figure 11: Login screen

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

After a successful login, the handset is synchronized with the parameters stored in the WSG DM.

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. If using a WLAN security protocol that uses certificates, make sure that the certificates (server/client) are saved to

each handset number in the WSG DM . If the WLAN parameters are wrong, the handset cannot associate with neither the staging nor the production WLAN again.

INFO:

If the wrong number is entered when the `Login` screen is displayed, make a factory reset and start again. For more information, refer to [Perform a Factory Reset](#) on page 101.

If there are no numbers configured in the WSG DM before the handset logs in for the first time, perform the following steps:

- 1) Create a number, refer to [Create Numbers](#) on page 17.
- 2) In the **Numbers** tab, select the created number.
- 3) In the **Number** menu (or right-click the number), select **Edit parameters**.
- 4) Select **Device > wsg > IP address** and check that the IP address for the Unite system is correct.
- 5) Enter the number in the handset's `Login` screen. Then the handset can log in to the same WSG DM .

INFO:

The WSG DM 's IP address can also be checked using the Admin menu of the handset through the **Device Info > Network info > Device manager**.

10.7 DHCP Related

10.7.1 DHCP Vendor Options Explained

The 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.

The DHCP options described in the RFC 2132, can also, besides a DHCP server, be used by a client.

An example of how a handset sends a DHCP Discover message to a DHCP server during the boot process, is shown in [Figure 12: Example of a DHCP Discover Message \(Omnipeek Trace\)](#) on page 134. In this image, the numbered points illustrate the following:

- 1) The amount of options requested.
- 2) Vendor options requested by the handset.
- 3) A specific set of Vendor options requested by the handset, by sending a Vendor Class Identifier (VCI).

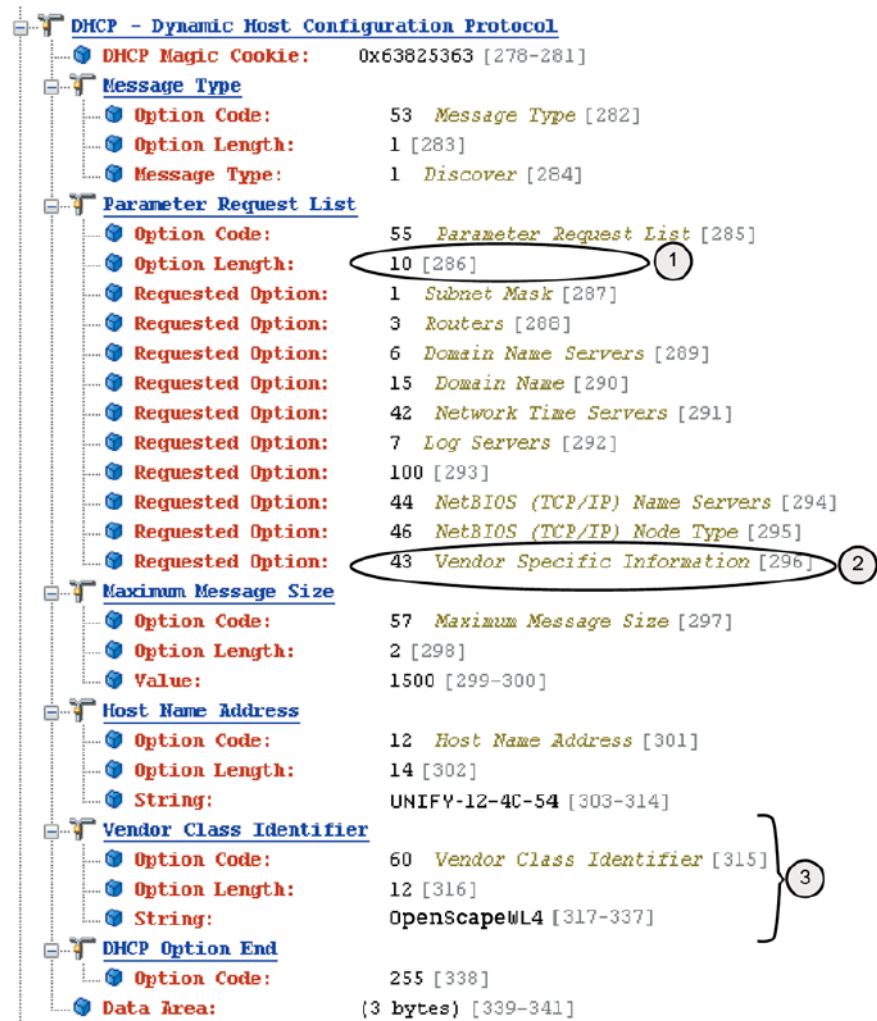


Figure 12: Example of a DHCP Discover Message (Omnipeek Trace)

In [Figure 13: Example of a DHCP Acknowledge \(Omnipeek Trace\)](#) on page 135, the DHCP server sends a DHCP ACK that confirms the settings the handset agreed to use, like the **43 Vendor Specific Information**.

When comparing the acknowledged options with the handset Requested Options in the trace in [Figure 12: Example of a DHCP Discover Message \(Omnipeek Trace\)](#) on page 134, it shows that not all requests were agreed on by the DHCP server. For example, the DHCP server does not acknowledge the options **42 Network Time Servers**, **7 Log servers**, and – by Omnipeek unknown – option **100**. Some options are also added by the DHCP server (without being asked for by the handset), for example, options 58, 59, 51, and 54, which are compulsory.



Figure 13: Example of a DHCP Acknowledge (Omnipeek Trace)

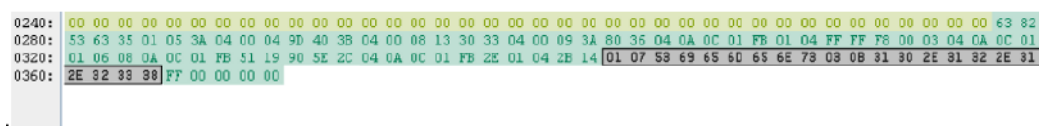


Figure 14: Example of a DHCP ACK in Hex (Omnipeek Trace)

10.7.1.1 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. The options are entered either in the IP address scope or for all scopes.

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 that 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.

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

To avoid having to send all Option 43 codes with useless tags to all clients, the use of Option 60 creates 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. Option 60 is called Vendor Class Identifier (VCI), and is defined by the manufacturer and programmed into the DHCP client of their devices.

[Table 8: Option 60 String Values](#) on page 136 lists some examples of Option 60 string values.

Table 8: Option 60 String Values

Vendor	Device	String	Option 43 returned value
Unify/Siemens	OpenScape WLAN Phone WL4	OpenScapeWL4	WSG IP address and vendor name
Aruba	Aruba AP	ArubaAP	Loopback address of the Aruba master controller
Cisco	Cisco AP	Cisco AP c1250	IP address of the WLAN controller

10.7.1.1.1 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.

Table 9: Option 43

Code	Length	Vendor-specific information element	Vendor-specific information element	Vendor-specific information element
43 (2b)	n	i1	i2	i3,...

The code for the option is 43, and its minimum length is 1. The numbers i1, i2, i3..., and so on, refer to information bytes. The length value n refers to the amount of information bytes in the field.

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

10.7.1.1.2 Option 43 with Encapsulated Vendor-specific Information

Normally a vendor needs to use multiple parameters for the 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 a format described in the table below:

Table 10: Information bytes format when using encapsulated vendor-specific extensions

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 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 and the total length are omitted.

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

Table 11: Option 43 Sub-fields

Code (Vendor name)	Length of vendor name string	Data items	Code (Unit module IP address)	Length of IP address	Data items	Code (optional)
01	7	Siemens	03	7–15	IPv4 address to the WSG DM (dot-decimal)	255

The code 255 is used as an optional marker of the end of the vendor field. SCEP parameters can also be sent in option 43. For more information, refer to [SCEP](#) on page 145.

When entering this information in a DHCP server, observe that the field length of the IP address can vary, depending on the amount of digits used. If, for example, using the address 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 of Sent Data with Option 43

To deploy a handset with the WSG DM with IP address 10.12.1.238, data is sent as Option 43 as follows:

NOTICE:

Search the internet for a tool that can assist in creating this string in hexadecimal format.

Table 12:

Hexadecimal	01:07:53:69:65:6D:65:6E:73:03:0B:31:30:2E:31:32:2E:31:2E:32:33:38
Printable text	\x01\x05Siemens\x03\x0B10.12.1.238

10.7.2 Configuration Example of a Linux Server Using DHCP Option 43

The code example below is taken from a Ubuntu Linux server. Enter the information in the `/etc/ltsp/dhcpd.conf` file.

Code Example

```
# Defining the option 43 with the proprietary sub-opcodes.
option space easy;
option easy.oem code 1 = string;
option easy.wsg code 3 = string;
class "vendors" {
match option vendor-class-identifier;
vendor-option-space easy;
}
subclass "vendors" " OpenScapeWL4 " {
option easy.oem " Siemens ";
option easy.wsg "10.12.1.238";
}
```

There are two options configured as code 1 and code 3, and both are defined as strings.

The server maps the string " OpenScapeWL4 " that was received from the handset using Option 60, as defined in the subclass paragraph.

There is no need to describe the length of the fields.

10.7.3 Configuration Example of an MS Windows 2003 Server

Adding Option 60 and 43 to the standard set of DHCP, at least in a lab environment, is a simple and fast solution, but has its drawbacks.

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.

NOTICE:

By configuring Option 43 directly 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. Therefore, there is no need to enter Option 60 values directly on a scope by creating a new option.

NOTICE:

There are several documents on the Internet that get this process wrong.

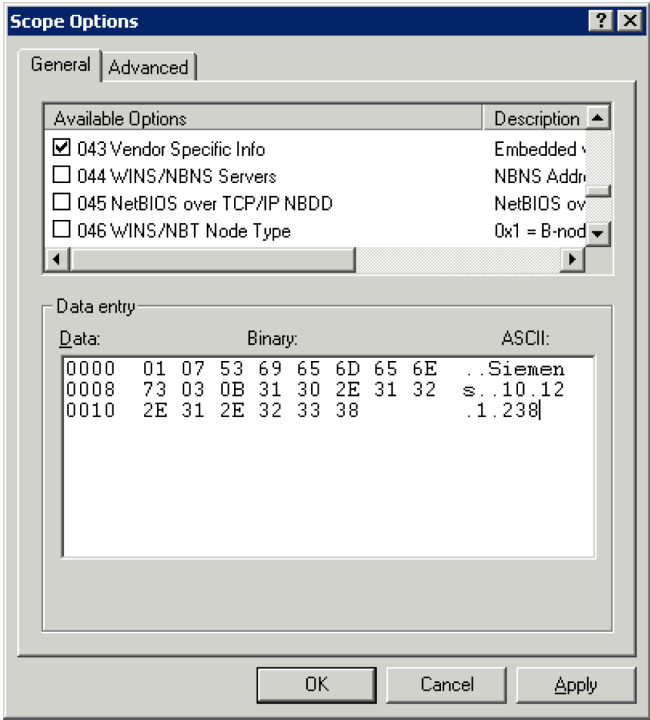
If set, option 43 is also offered to client computers.

Configure Option 43

This example illustrates how to set a vendor 43 option on the standard DHCP class, which is feasible if only vendor Option 43 is needed.

- 1) On the DHCP server, click the scope that the handsets should use, then right-click on **Scope Options** and select **Configure Options**.
- 2) In the **General tab** (the default Standard DHCP class), scroll down and select **043 Vendor Specific Info**.
- 3) In the data entry field, click to the left in the box to enter the string in binary or to the right to enter the string in ASCII. It is possible to switch between binary and ASCII.

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



NOTICE:

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 ("Siemens") 03 (10.12.1.238)
```

- 5) Click **OK** and save the new Option 43.
- 6) 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.

NOTICE:

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.

- 7) Test the configuration. If 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, but 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 a 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 03 .

NOTICE:

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 to the beginning of the string.

NOTICE:

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, which creates an Option 43 on the fly.

10.7.3.1 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, select **Define Vendor Classes**, and click **Add**.
- 2) In the *New Class* dialog box, enter a descriptive name for the Vendor class.
 - a) For example, in the **Display name** field, enter `Unify OpenScape WLAN Phone WL4`.
 - b) In the **Description** field, enter `Option 43 for Easy Deployment`. These fields are only used for displaying information for the administrator.
 - c) In the **ID** field, enter the vendor class identifier string (`OpenScapeWL4`). For the details refer to [Table 8: Option 60 String Values](#) on page 136.

NOTICE:

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

- 3) When done, click **OK**.

NOTICE:

The vendor class identifier 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).

10.7.3.2 Configure Sub-options for a Vendor Class in an MS Windows 2003 DHCP Server

The current sub-option string for the handset contains two codes (which in some documentation from vendors are referred to as tags). To build these two codes, one has to be defined with the value of Unify and one with the IP-address of the WSG DM .

- 1) Right-click on the DHCP server and select **Set Predefined Options**.
- 2) In **Option class**, select the vendor class that was created in section [Define New Vendor Class to Support Multiple Types of Clients](#) on page 141 and click **Add**. The *Option type* window opens.
- 3) In the **Name:** field, enter a descriptive name for the first sub-option, for example `VoWiFi Vendor`.
- 4) In the **Description:** field, enter, for example `Vendor Magic ID`.
- 5) In the **Data type:** field, select **Binary** to allow entering more than one byte.
- 6) In the **Code:** field, enter `001`, then click **OK**.

NOTICE:

A predefined value (by selecting **Edit Array**) is not needed to be entered here. It can be preferred to be set per scope instead (explained below).

- 7) For the second sub-option, repeat steps 1 – 2 described earlier in this section.
- 8) In the **Name:** field, enter a descriptive name for the second sub-option, for example `IP-address`, and copy it to the **Description:** field.
- 9) In the **Data type:** field, select **Binary** to allow entering more than one byte.
- 10) In the **Code:** field, enter `003` and click **OK**.
- 11) Add two sub-options to a scope and assign the required values. To do this, right-click on your scope and select **Scope Options > Configure Options**.
- 12) Select the **Advanced** tab.
- 13) 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](#) on page 141. Check the two sub-options that appear (**001 VoWiFi Vendor** and **003 Unite module IP address**).

NOTICE:

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

- 14) Select the first sub-option **001 VoWiFi Vendor** and enter the Vendor magic ID (Unify or in Binary/Hex: 53:69:65:6D:65:6E:73). Click to the left of the box for binary and to the right for ASCII code.

NOTICE:

Remove 00 that is displayed by default.

NOTICE:

A length value (in the **Data:** field) is not needed to be entered here (as normally done, when entering a TLV record). Click **OK**.

- 15) Select the second sub-option **003 IP address** and enter the Unite module IP address in binary/hexadecimal or ASCII. Click **OK**.
- 16) Test the configuration by factory-resetting a handset. If the configuration does not work, do a trace with a sniffer to see why.

NOTICE:

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

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

If a predefined DHCP option has been created by mistake and it needs to be deleted, the server might deny the operation (even if you have created the DHCP option). This is indicated by a grey **Delete** button. In this 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.

10.7.4 Configure 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.

To configure DHCP Option 43 for VoWiFi handsets, perform the following steps:

- 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 "OpenScapeWL4"
```

NOTICE:

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. Besides, every DHCP client receives the Option 43 values in a DHCP Offer, whether the values are relevant to the device or not.

- 4) Add the Option 43 line with the following syntax:

```
option 43 hex <hexadecimal string>
```

This hexadecimal string is assembled as a sequence of the type-length-value (TLV) values for the Option 43 sub-option, as described in [Configure Sub-options for a Vendor Class in an MS Windows 2003 DHCP Server](#) on page 142.

11 SCEP

Simple Certificate Enrollment Protocol (SCEP) is used for handling certificates in large VoWiFi systems and dispatching them without the need to manually approve each certificate. The SCEP protocol is also designed to make the renewal process of digital certificates as scalable as possible so new certificates are retrieved automatically when the old certificates are due to expire. SCEP issued certificates can be used to establish secure connections by enabling mutual authentication of the parties when connecting, for example, to a SIP Proxy or a Wi-Fi network.

SCEP can be configured using WinPDM/WSG DM or DHCP.

Device certificate (used by the handset when authenticating) and trusted certificates (used by the handset when authenticating other entities) can either be uploaded to the handset using WinPDM/WSG DM or by using SCEP.

Connecting to a SCEP server is the easiest way to set the handset up for TLS with mutual certificate verification. The handset can be configured with SCEP server login information either through DHCP or through user parameters. For the details, refer to [Configure SCEP Using WinPDM/WSG DM](#) on page 146 and [Configure SCEP Using DHCP Option 43](#) on page 146.

As is the case with Wi-Fi and TLS, server side certificate validation is enabled by default and must not be disabled. However, during the easy deployment process the handset will not have access to the server side certificate of the SCEP server upon its first connection. In this scenario, i.e. when no certificates are installed on the handset, it will connect to the SCEP server without certificate validation, so called trust on first use. It is for this reason highly recommended to perform this deployment operation on a secured network.

Since the certificate of the SCEP server will be stored on the handset during the first connection, and subsequent connections, for instance in order to perform certificate renewal, will include verification of the SCEP server identity.

NOTICE:

When installing a new SCEP certificate in a system, the validity period of the installed SCEP certificate must be at least one hour.

NOTICE:

The handset implements the client-side SCEP functionality. A third-party SCEP server is required to get a working SCEP solution. An example of a SCEP server is Microsoft Network Device Enrollment Service (NDES).

Since the handset may lose its network connection if it fails to renew the certificate before the expiration date, it is recommended to enable syslog and monitor the logs for SCEP procedure failures when SCEP is deployed. For the details, refer to [Syslog](#) on page 115.

If the certificate renewal fails, a warning message will be shown to the user informing about the upcoming expiration time of the existing certificate. For the details, refer to [Warning Messages](#) on page 109.

11.1 Configure SCEP Using WinPDM/WSG DM

To configure SCEP, perform the following steps:

- 1) Select **Device > SCEP**.
- 2) The following parameters are available for configuration:
 - a) **SCEP CA URL** defines URL to the SCEP server, for example `http://myscepserver.example.com/certsrv/mscep/mscep.dll`.
If left empty the handset uses SCEP configuration from the DHCP server instead (if available). For more information, refer to [Configure SCEP Using DHCP Option 43](#) on page 146.
 - b) **Password** defines the password used to authenticate the handset towards the SCEP server.
 - c) **Country (C)** (optional) defines two-letter ISO country code to be used in the generated certificate. It must be followed by the country code listed in https://www.ssl.com/csrs/country_codes/.
 - d) **Organization name (O)** (optional) defines organization name to be used in the generated certificate.
 - e) **Unit name (OU)** (optional) defines the name of your organizational unit (section or division) to be used in the generated certificate.
 - f) **State name (ST)** (optional) defines the name of the state or province to be used in the generated certificate.
 - g) **Common name (CN)** (optional) defines a descriptive common name to be used in the generated certificate. Different formats are allowed. MAC address in XYYZZAABBCC format or IPv4 address in abc.abc.abc.abc format, or string of printable characters. If left empty, the handset MAC address is used.
 - h) **Subject alternative name (SAN)** (optional) defines subject alternative name extension to be used in the generated certificate.
 - i) **Key length** defines the key length of the generated key pair.
 - j) **Validate server certificate** enables or disables the validation of the SCEP CA certificate during authentication.

NOTICE:

By disabling the validation, the server is not authenticated and may be a rouge one.

- k) **Renew threshold** defines the certificate lifetime (in percentage) that remains before the handset requests renewal of the certificate. A SCEP renewal is triggered when less then threshold of certificate total validity time is left. For example, if you select **20%**, the renewal of the certificate will be attempted when the certificate is 80% expired. Renewal attempts continue until the renewal is successful. The minimum allowed lifetime value that can be set is **10%** and the maximum is **50%**.

11.2 Configure SCEP Using DHCP Option 43

A DHCP server can be configured to return a SCEP URL, a password, and CSR customization options, as part of the DHCP response to the handset, with other needed DHCP parameters. The SCEP configuration 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 OpenScapeWL4 is the Object Identifier (OID) for the handset.

This way, a DHCP server can be configured to return SCEP options only to those clients that accept 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 SCEP configuration, it tries to request a certificate from the supplied URL using the supplied configuration. The configuration is stored in the handset and a new SCEP request will be made if a new DHCP response with a different SCEP configuration is received.

The following sub-options are used with Option 43:

- Sub-option 70: SCEP URL

For example: `http://myscepserver.example.com/certsrv/mscep/mscep.dll`

- Sub-option 71: Challenge password (optional)

For example: `MYCHALLENGEPASSWORD`

- Sub-option 72: CSR customization (optional)

For example:

```
K:2048;C:SE;ST:State;O:Organization;OU:Unit;CN:AABBCCDDEEFF;SAN:127.0.0.1;
```

CSR Custom format: `<key>:<value>;`

Table 13: Possible Key Value Pairs

Key	Value	Description
K	1024/2048 (4 characters)	Key length of the generated key pair.
C	2 characters	Country name to be used in the generated certificate. It must be followed by the country code listed in https://www.ssl.com/csrs/country_codes/
O	String (max 16 characters)	Organization name to be used in the generated certificate.
OU	String (max 16 characters)	Unit name to be used in the generated certificate.
ST	String (max 16 characters)	State or province name to be used in the generated certificate.
CN	String (max 32 characters)	Common name to be used in the generated certificate. Different formats are allowed. MAC address in XXYZZAABBCC format, or IPv4 address in abc.abc.abc.abc format, or a string of printable characters. If left empty, the handset MAC address is used.
SAN	String (max 32 characters)	Subject alternative name extension to be used in the generated certificate.

For examples on how to configure and troubleshoot Option 43 on a Linux and Microsoft Windows 2003/2008 server, see [Configuration Example of a Linux](#)

[Server Using DHCP Option 43](#) on page 138 and [Configuration Example of an MS Windows 2003 Server](#) on page 138, respectively.

