CONFIGURATION GUIDE

# Mitel 5634 VoWi-Fi Handset

Mitel®

Powering connections

**About this Document**

This document describes how to configure, maintain, and troubleshoot the Mitel 5634 VoWi-Fi Handset.

# Abbreviations and Glossary

**Abbreviations and Glossary**

| | |
|---|---|
| ALS | Acoustic Location Signal<br>A loud audio signal used for localizing the handset. |
| AP | Access Point |
| DHCP | Dynamic Host Configuration Protocol<br>A protocol for automating the configuration of computers and handsets that use TCP/IP. |
| DM | Device Manager |
| DNS | Domain Name Server |
| DSCP | Differentiated Services Code Point<br>QoS on the Internet Layer used both for WLANs and LANs. |
| DTIM | Delivery Traffic Indication Message |
| EAP | Extensible Authentication Protocol |
| EAP-TLS | EAP-Transport Layer Security |
| ELISE | Embedded Linux Server<br>A hardware platform used for WSM3/CPDM3. |
| GDPR | General Data Protection Regulation |
| GUI | Graphical User Interface<br>The interface between a user and a computer application. |
| ICE | Interactive Connectivity Establishment |
| IM | Interactive Messaging<br>Makes it possible to access information from an application and control the information by selecting an option received in a message. |
| IP | Internet Protocol<br>Global standard that specifies the format of datagrams and the addressing scheme. This is the principal communications protocol in the Internet Protocol suite. |
| LAN | Local Area Network |
| License | Authorization to upgrade the handset to another variant. |
| MAC | Medium Access Control<br>In IEEE 802 LAN/MAN standards, the MAC sublayer is the layer that controls the hardware responsible for interaction with the wired, optical, or wireless transmission medium. |
| NAT | Network Address Translator |
| NTP | Network Time Protocol |

| | |
|---|---|
| OTA | Over-the-Air |
| Parameter | A handset setting that can be configured using WinPDM/WSM3/CPDM3 DM. |
| PBX | Private Branch Exchange<br>A telephone system within an enterprise that switches calls between local lines and allows all users to share a certain number of external lines.<br>Also referred to as Unified communication server. |
| PEAP | Protected Extensible Authentication Protocol<br>A protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel, correcting deficiencies in EAP. |
| PEAP-MSCHAPv2 | PEAPv0/EAP-MSCHAPv2<br>The most common form of PEAP in use, and often referred to as only “PEAP”. It allows authentication to databases that support the MS-CHAPv2 format, including Microsoft NT and Microsoft Active Directory. |
| Production System | It includes the applications, systems, and protocols the handset uses after deployment, for example, WSM3/CPDM3, PBX, and WiFi. |
| PTT | Push-To-Talk |
| QoS | Quality of Service<br>Defines to what extent transmission rates, error rates, and so on are guaranteed in advance. |
| RSSI | Received Signal Strength Indication |
| RTLS | Real Time Locating System |
| Services | Predefined functions such as Phone Call, Send Data, Send Message, and so on, that are accessible from the Service menu. |
| SIP | Session Initiation Protocol<br>SIP is a signaling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video, and messaging applications. SIP is used for applications of Internet telephony for voice and video calls, in private IP telephone systems, in instant messaging over IP networks, and in mobile phones calling over LTE, Voice over LTE (VoLTE). |
| SSID | Service Set Identifier |
| STUN | Session Traversal Utilities for NAT |
| TURN | Traversal Using Relay NAT |
| VoIP | Voice over IP |
| VoWiFi | Voice over WiFi<br>It is a system running VoIP over WLAN. |

| | |
|---|---|
| WiFi | A family of radio technologies that is commonly used for implemeting a WLAN.<br>Used generically when referring to any type of IEEE 802.11 network. |
| WinPDM | Portable Device Manager (Windows version)<br>Used for managing devices, such as editing parameters and upgrading devices. WinPDM is a stand-alone application installed on a computer. It is used for small sites as it requires physical access to the handsets. |
| WLAN | Wireless Local Area Network<br>A type of LAN in which data is sent and received via high-frequency radio waves rather than cables or wires. The most common radio technology used for a WLAN is WiFi, implementing the IEEE 802.11 standards. |
| WPA/WPA2 | WPA/WPA2 mixed mode |
| WSM3/CPDM3 | Wireless Service Messaging gateway / Central Portable Device Manager<br>WSM3/CPDM3 is a gateway handling communication interfaces for DECT and VoWiFi systems and other basic messaging services, such as web messaging and messaging handset to handset (SMS). The WSM3/CPDM3 is installed on a reliable solid-state hardware. |

## Contents

# 1 Introduction

This document provides guidelines for deploying, configuring, maintaining, and troubleshooting the Mitel 5634 VoWiFi Handset.

The VoWiFi system provides wireless IP telephony, messaging, and alarm functions. Using third-party WLAN products, hardware, and software developed in-house, the system enables data and voice transmission together with seamless roaming.

The document is targeted at the following personnel:

- System administrators
- Service technicians

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

## 1.1 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 in the handset. For more information, see *Mitel 5634 VoWi-Fi Handset User Guide*.

These settings can also be configured by applying the provided GDPR template.

# 2 Handset Deployment

This section describes how to deploy handsets to a VoWiFi system.

## 2.1 Prerequisites

Deploying handsets to a VoWiFi system requires the following prerequisites:

- The handset batteries are charged.
- Chargers are set up in case WinPDM is used.
- A phone number plan is available for the handsets.
- The IP address plan is set up to support the number of handsets to be deployed.
- A VoWiFi system where some or all of the following components (depending on the system configuration) are available:
    - DHCP Server – It 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.
    - WinPDM – It is a stand-alone device management system used for administering and configuring handsets. All settings and updates are performed using the Mitel 5634 Desktop Programmer cradle connected over USB.
    - WSM3/CPDM3 – It handles all communication between the WLAN and its built-in WSM3/CPDM3 DM. Before installing the handset, make sure the WSM3/CPDM3 DM address is available.
    - NTP server – It ensures network time synchronization.

## 2.2 Handset Deployment into the VoWiFi System

The Mitel 5634 VoWiFi Handset can be deployed to a VoWiFi system in the following ways:

- **Over the Air (OTA) using the Wireless Service Messaging Device Manager (WSM3/CPDM3 DM)** — This is the recommended option to deploy handsets in a large VoWiFi system. The WSM3/CPDM3 DM can install, upgrade, and configure a large amount of handsets simultaneously without collecting them from the users.
  For more information, see 2.2.1 Deploy the Handset Using the WSM3/CPDM3 DM, page 2 and 2.2.1.1 Configure the Handset Using Easy Deployment, page 4.
- **Using Portable Device Manager (WinPDM)** — WinPDM can configure only one handset at a time, which is feasible in small VoWiFi systems. The handsets need to be collected from the users.
  For more information, see 2.2.2 Deploy the Handset Using WinPDM, page 6.
- **Using the Admin menu of the handset** — This option can be used in case only a quick change of a parameter value is needed, for example, in a lab environment or in a test installation.
  For more information, see 2.2.3 Deploy the Handset Using the Admin Menu, page 7.

When deploying handsets using WinPDM/WSM3/CPDM3 DM, it is recommended to create templates to be able to apply the same configuration to several handsets simultaneously. For more information, see 2.2.1.2 Create a Template in WinPDM/WSM3/CPDM3 DM, page 4, 2.2.1.4 Apply a Template to a Handset without a Number, page 5, and 2.2.1.5 Apply a Template to a Handset with a Number, page 6.

### 2.2.1 Deploy the Handset Using the WSM3/CPDM3 DM

For OTA device management, the handset needs to have a WLAN association that can be IP routed to WSM3/CPDM3 DM.

It is recommended to use Easy Deployment, where the handset first obtains the Unite IP address using a DHCP server or the Ascom Service Discovery Protocol (ASDP), then the WLAN parameters and the device manager information is distributed automatically to the handset from the WSM3/CPDM3.

If Easy Deployment is not used, the WLAN and WSM3/CPDM3 DM parameters can be set manually using the Admin menu in the handset or WinPDM.

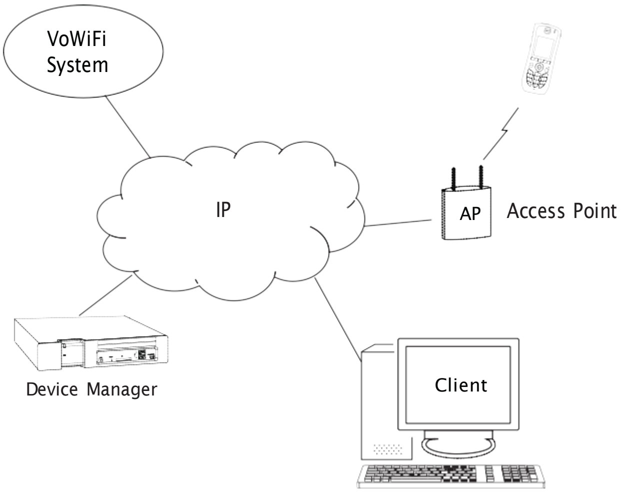
Then the handset logs into the WSM3/CPDM3 DM, and downloads the intended handset profile, which contains all other needed parameters for a site.

For more information, see 2.3.2 Configure the Handset Using the Admin Menu, page 8 and Appendix C Easy Deployment, page 93.

If the WLAN system uses an 802.1X security protocol that requires certificates for authentication/ encryption to the WLAN, the certificates must be prepared and stored individually in the WSM3/CPDM3 DM for each number before starting the Easy Deployment process. Alternatively, if a SCEP server is available, this can be accomplished by following the steps in C.5 SCEP, page 96 to have the necessary certificates automatically generated and downloaded to the handset.

If the handset must use a certificate to access a WLAN, follow the instructions in 2.2.2 Deploy the Handset Using WinPDM, page 6.

*Figure 1. Configuration of Handsets Over-the-Air (OTA)*



To deploy handsets to the VoWiFi system using the WSM3/CPDM3 DM, perform the following steps:

This section includes only the main steps of the deployment procedure. For details, see the corresponding sections.

1. Open a web browser and enter the address of the WSM3/CPDM3.
2. Open the WSM3/CPDM3 DM and log in if necessary.
3. Create a template with the following network parameters:
   - Network settings in **Network → General**:
     Under the respective network (**Network A**, **Network B**, **Network C**, or **Network D**), set the required parameters, for example, system settings for WLAN, such as **SSID**, **Security mode**, and any certificates for 802.1X. If using a security mode that requires certificates, also use an NTP server to assure the correct time in the handset, as certificates are only valid within a certain time.
   - VoIP settings in the **VoIP** menu:

Configure, for example, VoIP information, SIP proxy ID and address.

- Syslog settings in **Device → Log**:
  To be able to set the **Syslog server IP address**, the parameter **Syslog** must be enabled by selecting **On**.
- Unite settings in **Device → Unite**:
  Enter the IP address and password (if any) to the WSM3/CPDM3.

For details, see 2.2.1.2 Create a Template in WinPDM/WSM3/CPDM3 DM, page 4.
Include only non-default parameters to minimize network traffic when applying the template.

If using Easy Deployment, the IP address of the WSM3/CPDM3 DM in the template can either be set or it can be left blank in which case the server discovery process is used at every startup. For more information, see C.3 WSM3/CPDM3 Discovery, page 95.

4. Create numbers for the handsets.
   For details, see 2.2.1.3 Create Numbers in WinPDM/WSM3/CPDM3 DM, page 5.
5. Apply the network template to the handsets.
   For details, see 2.2.1.5 Apply a Template to a Handset with a Number, page 6 and 2.2.1.1 Configure the Handset Using Easy Deployment, page 4.

For more information, see the User Manual, Device Manager in WSM3/CPDM3.

### 2.2.1.1 Configure the Handset Using Easy Deployment

With the Easy Deployment procedure, handsets can be installed using a (staging) WLAN with a predefined SSID and security profile and a WSM3/CPDM3 with WSM3/CPDM3 DM.

The handsets are automatically installed if the following requirements are met:

- The LAN and VoWiFi system is configured for Easy Deployment.
- No network (SSID) is configured in the handset.
- The Call ID (endpoint number), that is, the phone number of the handset is configured.

When using Easy Deployment, make sure that the phone number plan and the parameters are correct. Inaccurate configuration can only be corrected in the WSM3/CPDM3 DM.

For further details, see Appendix C Easy Deployment, page 93.

### 2.2.1.2 Create a Template in WinPDM/WSM3/CPDM3 DM

Select only the modified parameters. If all parameters are selected, the system performance decreases.

To create a template, perform the following steps:

1. In WinPDM/WSM3/CPDM3 DM, select the **Templates** tab and click **Template → New...** or **CTRL + N**. The New template window is opened.
2. In the **Device type** and **Parameter definition** drop-down lists, select the corresponding device type and parameter definition to use.
3. In the **Name** field, enter a descriptive name for the template.
4. Click **OK**. The Edit template window is opened.
5. Set the required parameters.
6. Click **OK** to save the template.

For more information, see A.2 Manage Templates using WinPDM and WSM3/CPDM3 DM, page 88.

#### 2.2.1.3 Create Numbers in WinPDM/WSM3/CPDM3 DM

Create a range of numbers and apply the templates previously created in WinPDM/WSM3/CPDM3 DM.

**Important**

**When adding numbers to handsets that already exist in the system, WinPDM/WSM3/CPDM3 DM overwrites the existing parameters in the handset, since these handsets are not saved in WinPDM/WSM3/CPDM3 DM.**

Do not add numbers to handsets that are already configured and functional.

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

1. Open WinPDM/WSM3/CPDM3 DM.
2. Select the **Numbers** tab and click **Number → New...** or **CTRL + N**. The New numbers window is opened.
3. In the **Device type** and **Parameter definition** drop-down lists, select the corresponding device type and parameter definition to use.
4. In the **Prefix** field, enter the numbers' prefix (if needed).
5. Create a range of numbers by selecting the **Range** option. Enter the start call number and the end call number in the fields. Click **OK**.

   The maximum range that can be added at a time is 100 numbers.
6. Apply the network settings template to the selected handsets. See 2.2.1.5 Apply a Template to a Handset with a Number, page 6.
7. Apply the common settings template to the selected handsets. See 2.2.1.5 Apply a Template to a Handset with a Number, page 6.

   If the 802.1X security protocol with EAP-TLS or EAP-PEAP/MSCHAPv2 is used, also include the trusted CA certificate(s) and select the required application certificate.

   Application certificates cannot be distributed using a template, as they are individual. The application certificates must be installed first by editing each number. See D.3 Easy Deployment and Certificates, page 109.

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

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

1. Place the handset in the Mitel 5634 Desktop Programmer cradle.
2. In the **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.

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

To apply a template to a handset with a number in WinPDM/WSM3/CPDM3 DM, perform the following steps:

1. Open WinPDM/WSM3/CPDM3 DM.
2. In the **Numbers** tab, select the handset(s) you want to apply the template to.

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

3. Right-click and select **Apply template**.
   Only templates with a parameters version matching the selected handsets 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 handsets.

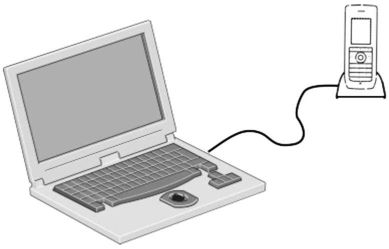
When looking at a handset on the Numbers tab, the column **Last run template** shows the name of the most recently applied template.

### 2.2.2 Deploy the Handset Using WinPDM

Using WinPDM only one handset can be deployed at a time. After configuring the WLAN parameters, it is possible to log in to the WSM3/CPDM3 DM for future OTA management.

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

*Figure 2. Connecting Handsets to the computer*



1. Open WinPDM.
2. Create numbers for the handsets.
   For details, see 2.2.1.3 Create Numbers in WinPDM/WSM3/CPDM3 DM, page 5.
3. Create a template with the following network parameters:
   - Network settings in **Network → General**:
     Under the respective network (**Network A**, **Network B**, **Network C**, or **Network D**), set the required parameters, for example, system settings for WLAN, such as **SSID**, **Security mode**, and any certificates for 802.1X. If using a security mode that requires certificates, also use an NTP server to assure the correct time in the handset, as certificates are only valid within a certain time.
   - VoIP settings in the **VoIP** menu:
     Configure, for example, VoIP information, SIP proxy ID and address.
   - Syslog settings in **Device → Log**:
     To be able to set the **Syslog server IP address**, the parameter **Syslog** must be enabled by selecting **On**.
   - Unite settings in **Device → Unite**:
     Enter the IP address and password (if any) to the WSM3/CPDM3.

   For details, see 2.2.1.2 Create a Template in WinPDM/WSM3/CPDM3 DM, page 4.

If the production system is using 802.1X security, this method is not the best option since the certificates must be manually installed in the handset before the first login. The Easy Deployment process overcomes this problem by using a staging WLAN, which does not use 802.1X.

If a network template has already been created in WSM3/CPDM3 DM, it can be exported and imported to WinPDM. For more information, see A.2 Manage Templates using WinPDM and WSM3/CPDM3 DM, page 88.

4. Place the handset into the Mitel 5634 Desktop Programmer cradle via a USB port. In the dialog window that appears after connecting the handset, select **WinPDM**. For more information, see 3.4.8.4 USB Behavior, page 21.
5. In the Device Wizard window, select **Associate with number** and press **OK**.
6. Select the handset to associate with and press **OK**.
   The number and parameter settings saved in the WinPDM are now synchronized with the handset. In addition, the handset's Device ID is also synchronized with the number in the WinPDM.
   If certificates must be used to access a VoWiFi system, also perform Item 8., page 7–Item 13., page 7.
7. Apply the network settings template to the handset. See 2.2.1.5 Apply a Template to a Handset with a Number, page 6.
8. In the **Numbers** tab, right-click the handset's number and select **Manage certificates**. A manage certificate window opens.
9. In the **Trust list** tab and **Application certificates** tab, click **Browse** and select the certificates to import. Click **Close**.
10. In the **Numbers** tab, right-click the handset's number and select **Edit parameters**.
11. Select the active network (**Network A**, **Network B**, **Network C**, or **Network D**).
12. In the **Security mode** drop-down list, select **EAP-TLS** or **PEAP-MSCHAPv2**.
13. In the **EAP application certificate** drop-down list, select the application certificate to be used. Click **OK**.
14. Remove the handset when the synchronization is finished.

Repeat Item 4., page 7–Item 14., page 7 for every handset.

### 2.2.3 Deploy the Handset Using the Admin Menu

It is possible to configure a handset using the Admin menu. This can be useful when neither WinPDM nor WSM3/CPDM3 DM is available and only a few handsets need to be configured.

Only a limited set of settings can be configured using the Admin menu. WPA2 Enterprise authentication, for example, cannot be configured.

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

1. Enter the Admin access code `40022` while the handset displays `No network`.

   `40022` is the default Admin access code that can be configured in WinPDM/WSM3/CPDM3 DM. In case none of them is available, contact the system administrator. For more information, see
   3.4.22 Change Admin Access Code, page 30.
2. Set the following parameters:
   - In the **Network setup** menu, set all the required system settings for the WLAN, for example **SSID** and **Security mode**. No certificates can be entered or referred to using the Admin menu.
   - In the **Unite** menu, set the IP address and password (if any) to the WSM3/CPDM3.
   - In the **VoIP** menu, set **VoIP protocol** and **SIP proxy IP address** to access the PBX.

- In the **Syslog** menu, the parameter **Syslog mode** must be enabled by selecting **On** to be able to set the **Syslog server IP**.

## 2.3 Handset Configuration

Handsets can be configured in the following ways:

- **Using WinPDM/WSM3/CPDM3 DM**
  For more information, see 2.3.1 Configure Handsets Using WinPDM/WSM3/CPDM3 DM, page 8.
- **Using the Admin menu of the handset**
  For more information, see 2.3.2 Configure the Handset Using the Admin Menu, page 8.

### 2.3.1 Configure Handsets Using WinPDM/WSM3/CPDM3 DM

This requires that handsets have been deployed to the VoWiFi system with access to WinPDM/WSM3/CPDM3 DM. For more information, see 2.2 Handset Deployment into the VoWiFi System, page 2. The recommended procedure for configuring handsets is to create a template to be able to apply the same configuration to several handsets simultaneously.

To configure handsets, perform the following steps:

1. Open the WinPDM/WSM3/CPDM3 DM.
2. Create a template with the required settings.
   For details, see 2.2.1.2 Create a Template in WinPDM/WSM3/CPDM3 DM, page 4.
3. Apply the template to the handsets.
   For details, see 2.2.1.5 Apply a Template to a Handset with a Number, page 6 or 2.2.1.4 Apply a Template to a Handset without a Number, page 5.

### 2.3.2 Configure the Handset Using the Admin Menu

The Admin menu of the handset can be used to perform quick changes in the handset.

For more information, see 3.4.21 System Administration in the Handset, page 28.

## 2.4 Handset Synchronization

Handset synchronization transfers parameter changes between the handset and the WinPDM/WSM3/CPDM3 DM and vice versa as follows:

- The handset synchronizes with the WSM3/CPDM3 DM at startup and immediately after every handset parameter change. (The change is done either by using the handset keypad or by editing parameters in the WSM3/CPDM3 DM.)
  If a parameter has been changed in the handset, it is transferred to the WinPDM/WSM3/CPDM3 DM.
- If a parameter has been changed in the WinPDM/WSM3/CPDM3 DM while the handset was offline, the changes are transferred when the handset is online.
- If a parameter has been changed in the WinPDM/WSM3/CPDM3 DM, it is transferred to the handset.
- If the same parameter has been changed in both the WinPDM/WSM3/CPDM3 DM and the handset, the value in the WinPDM/WSM3/CPDM3 DM overrides the value in the handset.

- Changes made in the WSM3/CPDM3 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 Mitel 5634 Desktop Programmer cradle via USB.

Since there is no connection between the WinPDM and WSM3/CPDM3 DM except over the handset, the WLAN and device manager settings can differ in the WinPDM and WSM3/CPDM3 DM. Parameters can revert to old values when the WinPDM synchronization process runs, that is, when the handset is placed in the Mitel 5634 Desktop Programmer cradle.

When the handset is removed from the Mitel 5634 Desktop Programmer cradle, the handset goes online with the Messaging system, and the synchronization process with the WSM3/CPDM3 DM starts. The solution for this is to avoid storing handset numbers in the WinPDM.

# 3 Parameter Configuration

This section describes how to configure handset parameters using WinPDM/WSM3/CPDM3 DM.

The parameters are defined in `.def` files that are regularly updated. For example, parameters are added or removed, or their values are changed.

Parameter configuration can restart the handset. The text `Remotely updated` is shown in the handset display when the handset restarts after the update.

For more information, see the help text that is accessible for each parameter by clicking the Help icon in the **Edit parameters** view.

## 3.1 Networks

The handset can switch between four different WLAN system configurations called **Network A**, **Network B**, **Network C**, and **Network D**. The name can be changed (using the Admin menu in the handset or the WinPDM/WSM3/CPDM3 DM) and is visible in the handset. For more information, see 3.1.2 Change Name of Network, page 10.

A handset can be configured for up to four different WLANs but only for one WSM3/CPDM3 and one VoIP System.

**Network A** is the default system that is used throughout this manual.

### 3.1.1 Change Active Network

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

### 3.1.2 Change Name of Network

The name is shown when selecting network in the handset.

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

### 3.1.3 Enable Switch Between Networks

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

1. Select **Network → General**.
2. In the **Auto-switch network** drop-down list, select **On**.
   The parameter **Auto-switch network timeout** appears, which defines the time before the handset tries to connect with the next included network.
3. Enter a value in seconds for **Auto-switch network timeout**.
4. For the networks that should be included in the auto-switch network:
   Select **Network → Network A Network B**, **Network C**, or **Network D**. In the **Include in auto-switch network** drop-down list, select **Yes** to enable the switch to **Network A → Network B → Network C → Network D**.

## 3.2 Handset IP Address Settings

The handset IP address settings can be configured in two ways:

- The handset can be configured to receive an IP address automatically from a DHCP server, see 3.2.1 Automatic IP Address Settings, page 11.
- If no DHCP server is used, a unique IP address must be entered manually for each handset, see 3.2.2 Static IP Address (Manual) Settings, page 11.

### 3.2.1 Automatic IP Address Settings

1. Select **Network → Network A Network B**, **Network C**, or **Network D**.
2. In the **DHCP mode** drop-down list, select one of the following:
   – **Off (static mode)**
   – **Use any DHCP**

   The phone IP address, subnet mask, and default gateway are automatically set up.

### 3.2.2 Static IP Address (Manual) Settings

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

#### 3.2.2.1 DNS Server Settings

It is possible to configure the DNS server that the handset uses. If the primary DNS server is available, it is always used. Otherwise, the secondary DNS server is used.

**Primary DNS Server**

1. Select **Network → Network A Network B**, **Network C**, or **Network D**.
2. In the **Primary DNS** field, enter the IP address for the primary DNS server.

**Secondary DNS Server**

1. Select **Network → Network A Network B**, **Network C**, or **Network D**.
2. In the **Secondary DNS** field, enter the IP address for the secondary DNS server.

## 3.3 Network Settings

### 3.3.1 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 that can be used.

**5 GHz Channels**

It defines which 5 GHz channels to use. It is recommended to use the value **UNII-1**.

Select **Advanced** only if the channels are to be set in the **802.11 channels** parameter, see Advanced: 802.11 Channels, page 13.

To select a 5 GHz channel in the WinPDM/WSM3/CPDM3 DM, perform the following steps:

1. Select **Network → Network A Network B**, **Network C**, or **Network 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**
   - **UNII-3**
   - **UNII-1, UNII-2**
   - **UNII-1, UNII-2, UNII-3**
   - **UNII-1, UNII-2 Extended**
   - **Advanced**
   - **802.11k**

   5634 VoWiFi Handset has optional support for roaming based on 802.11k neighbor lists. To enable it, set this parameter to **802.11k**. If 802.11k is enabled, only a subset of the 2.4/5 GHz channels that are enabled are scanned for a new AP candidate when roaming. It is decided by a 802.11k neighbor list which channels to scan, which must be sent by the current AP. If this partial scan fails to find a roaming candidate, a full scan of all channels is performed as if the parameter had been set to **All**.

   The selected World Mode Regulatory Domain defines which channels to use. For more information, see the table below.

**Table 1 Bands and Channels Used by WiFi A-radio**

| **Channel denomination** | **Frequency band** | **Channels** |
|---|---|---|
| Non DFS | 5.150–5.250 GHz, 5.725–5.845 GHz | 36, 40, 44, 48 149, 153, 157, 161, 165 |
| UNII-1 | 5.150–5.250 GHz | 36, 40, 44, 48 |
| UNII-2 | 5.250–5.350 GHz | 52, 56, 60, 64 |
| UNII-2 Extended | 5.470–5.725 GHz | 100, 104, 108, 112,116, 120, 124, 128, 132, 126, 140 |
| UNII-3 | 5.725–5.850 GHz | 149, 153, 157, 161, 165 |

### 2.4 GHz Channels

It defines which 2.4 GHz channels to use. It is recommended to use the default value **1, 6, 11**.

If set to **All**, all channels are scanned for APs, which decreases WLAN performance. Select **Advanced** only if the channels are to be set in the parameter **802.11 channels**. For more information, see Advanced: 802.11 Channels, page 13.

To select a 2,4 GHz channel in WinPDM/WSM3/CPDM3 DM, perform the following steps:

1. Select **Network → Network A Network B**, **Network C**, or **Network 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:
   - **All**

- **1, 6, 11**
- **Advanced**

**Advanced: 802.11 Channels**

It 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**.

To configure the channels to be scanned in WinPDM/WSM3/CPDM3 DM, perform the following steps:

1. Select **Network → Network A Network B**, **Network C**, or **Network D**.
2. Enter 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.

   ℹ It is not possible to scan channels in 2.4 GHz and 5 GHz simultaneously.

   ℹ If **Advanced** is selected in WinPDM/WSM3/CPDM3 DM, it is indicated in the handset display by having all options unchecked in the Admin menu in **Network setup → 2.4 GHz channels**, or **5 GHz channels**. If any of these unchecked channels are selected using the handset's Admin menu, the only way to reselect **Advanced**, is to reconfigure it in WinPDM/WSM3/CPDM3 DM.

ℹ Channels can also be configured in the Admin menu of the handset. For more information, see 3.4.21 System Administration in the Handset, page 28 and 3.4.21.1 Admin Menu Tree in the Handset, page 29.

### 3.3.2 SSID

Service Set Identifier (SSID) is the name of the network that the handset associates with.

1. Select **Network → Network A Network B**, **Network C**, or **Network D**.
2. In the **SSID** field, enter system SSID.

   ℹ SSID is case-sensitive.

### 3.3.3 Security Settings

The WLAN can be configured in WinPDM/WSM3/CPDM3 DM to use various encryption and authentication schemes. The most frequently used encryption and authentication modes are directly available in the **Security mode** drop-down list of **Network → Network A Network B**, **Network C**, or **Network D**.

ℹ 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.

#### 3.3.3.1 Open

If no encryption or authentication is required, perform the following steps:

1. Select **Network → Network A Network B**, **Network C**, or **Network D**.
2. In the **Security mode** drop-down list, select **Open**.

#### 3.3.3.2 WPA/WPA2-PSK

To select WPA/WPA2-PSK as the security mode, perform the following steps:

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

#### 3.3.3.3 PEAP-MSCHAPv2

PEAP-MSCHAPv2 (PEAPv0/EAP-MSCHAPv2) recommends the use of trusted certificates for authentication of the WLAN.

To select PEAP-MSCHAPv2 as the authentication method, perform the following steps:

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 **Trust list** tab of the Manage Certificates window, click **Browse** and select the trusted certificates to import. Click **Close**.
     This is not needed if validation is disabled in Item 7., page 14.

   Skip this step, if SCEP is used to automatically download trusted certificates to the handset. For more information, see C.5 SCEP, page 96.

2. Select **Network → Network A Network B**, **Network C**, or **Network D**.
3. In the **Security mode** drop-down list, select **PEAP-MSCHAPv2**.
4. In the **EAP authentication identity** field, enter the user name for EAP authentication.
5. In the **EAP authentication password** field, enter the password for EAP authentication.
6. The **EAP anonymous identity** is an optional parameter. This field is used for unencrypted 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.
7. In the **Validate server certificate** field, select **No** to disable the validation of server certificate during authentication.

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

The server must send its complete certificate chain.

#### 3.3.3.4 EAP-TLS

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.

To select EAP-TLS as the authentication method, perform the following steps:

1. For server validation, import the trusted certificate:
   - In the **Numbers** tab, right-click the handset's number and select **Manage certificates**.
   - In the **Trusted list** and the **Application certificates** tabs of the Manage Certificates window, click **Browse** and select the certificates to import. Click **Close**.
     This is not needed if validation is disabled in Item 7., page 15.
2. Select **Network → Network A Network B**, **Network C**, or **Network D**.
3. In the **Security mode** drop-down list, select **EAP-TLS**.

4. In the **EAP authentication identity** field, enter the user name for EAP authentication.
5. **EAP anonymous identity** is an optional parameter. This field is used for unencrypted 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.
6. In the **EAP client certificate** drop-down list, select the application certificate (in PKCS#12 format).
7. In the **Validate server certificate** field, select **No** to disable the validation of server certificate during authentication.

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

The server must send its complete certificate chain.

#### 3.3.3.5 WinPDM Authentication

When this parameter is enabled, it is required to enter the Admin access code to the handset before connecting to WinPDM.

This parameter is only visible if **USB behavior** is set to **Ask** or **WinPDM** in **Device → General**.

To enable **WinPDM authentication**, perform the following steps:

1. Select **Device → General**.
2. In the **WinPDM authentication** drop-down list, select **On**.

### 3.3.4 World Mode Regulatory Domain

There is a set of regional rules for the world mode settings and the a-band that the handset complies with. The preferred setting is **World mode (802.11d)**. The handset gets its regulatory settings from the AP. If it is not supported by the AP, perform the following steps:

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

### 3.3.5 IP DSCP for Voice/Signaling

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

1. Select **Network → Network A Network B**, **Network C**, or **Network 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**

### 3.3.6 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 A Network B**, **Network C**, or **Network 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.

### 3.3.7 Roaming Method

To select a roaming method, perform the following steps:

1. Select **Network → Network A Network B**, **Network C**, or **Network D**.
2. In the **Roaming method** drop-down list, select one of the following:
   - **PMKSA Caching** — Use it in systems that do not support FT or OKC.
   - **Fast BSS Transition (FT)** — Use FT if supported by the system, otherwise OKC.
   - **OKC** — Select this option to use Opportunistic Key Caching instead of FT on an AP that supports both.

### 3.3.8 IP Connectivity after Roaming

If the **Check IP connectivity after roaming** is set to **Yes**, it sends ICMP pings to the default gateway after each roam to verify that the local IP address is still valid.

### 3.3.9 A-MPDU Packet Aggregation

During interoperability testing there has been issues with the Aruba controllers when the A-MPDU aggregation was enabled in the handset. Therefore, it is recommended to set this parameter to **Off** when connecting to Aruba WiFi and **On** when connecting to other networks.

## 3.4 Handset Settings

Parameters described in this section can be changed using the handset and/or the WinPDM/WSM3/CPDM3 DM to assist the user or set the initial value when the handset is deployed.

For more information, see the Mitel 5634 VoWi-Fi Handset User Guide.

When the handset is placed in the charger, some settings for audio adjustments, messaging settings, and actions cannot be changed using the keypad.

### 3.4.1 Automatic Key Lock

Automatic key lock is used to avoid unintentional key presses. It can also be configured using the handset.

If configured, it is possible to dial any of up to five predefined emergency numbers when the keypad is locked, see 3.6.8 Emergency Call Numbers, page 42.

Other examples of exceptions that override the key lock is personal alarm, shortcut call, and mute ALS.

To activate or deactivate **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** – Activates the automatic key lock, also during an ongoing call.
   - **Off** – Deactivates automatic key lock.

### 3.4.2 Automatic Key Unlock

To enable or disable 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** – The handset keypad is unlocked automatically at incoming calls and messages.
   - **Off** – The handset is not unlocked automatically.

### 3.4.3 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.

If configured, it is possible to dial any of up to five predefined emergency numbers when the handset is locked. For more information, see 3.6.8 Emergency Call Numbers, page 42.

Another example of exception that overrides the phone lock is personal alarm.

It is not recommended to use phone lock when using the shared phone feature. For more information, see 3.4.16 Shared Phone, page 24.

To activate or deactivate **Phone lock**, perform the following steps:

1. Select **Device** → **Settings**.
2. In the **Phone lock** drop-down list, select one of the following:
   - **On** – The handset is locked after a specified time when it is not used. For more information, see 3.4.4 Automatic Lock Time, page 18.
   - **On in charger** – The handset is locked when placed in a charger.
   - **Off** – The handset is not locked.

When **Phone lock** is activated, define a password in the **Phone lock code** field.

### 3.4.4 Automatic Lock Time

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

To change the **Automatic lock time**, perform the following steps:

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

### 3.4.5 Multifunction Button

**Configure the Multifunction Button as a Shortcut**

ℹ Applicable to 5634 and 5634 Services only.

The Multifunction button can be defined for different functions on long press and multi press by performing the following steps:

1. Select **Shortcuts → Multifunction Button Long press** (or **Multi press**).
2. Continue with 3.4.17.4 Shortcut Settings, page 25.

**Configure the Multifunction Button to be a PTT button**

ℹ Applicable to 5634 Services 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, perform the following steps:

1. Select **Device → Call**.
2. In the **Multi func button for PTT** drop-down list, select **On**.

### 3.4.6 Audio Settings

To set the volumes for the different audio signals of the handset, perform the following steps:

1. Select **Audio → Volume**.
2. Select the appropriate volume type from the drop-down lists:
   - **Handsfree volume** — Sets the volume used in an active call in loudspeaking mode.
   - **Headset volume** — Sets the volume used in an active call when a headset is connected.
   - **Speaker volume** — Sets the volume used in an active call in speaker mode (normal call mode).

3. In the **Persistent volumes** drop-down list, select **Enable** to automatically store volume changes in the handset for future calls.
   The parameter affects the **Normal**, **Headset**, and **Loudspeaking** mode.

For selection of headset, see 3.4.7.1 Headset Type, page 19.

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

#### 3.4.6.1 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, perform the following steps:

1. Select **Audio → General**.
2. In the **Hearing aid** drop-down list, select **On** to enable it.

#### 3.4.6.2 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**.

#### 3.4.6.3 Gain Offset Calibration

To optimize audio quality, perform the following steps:

1. Select **Audio → Handset**, **Audio → Headset**, **Audio → Loudspeaker** (Applicable to 5634 Services only.), and/or **Audio → Bluetooth** (Applicable to 5634 Services only.).
2. Change the values of the following as necessary:
   - **Michrophone gain offset**
   - **Speaker gain offset**
   - **Microphone side-tone gain offset**

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

### 3.4.7 Headset Configuration

#### 3.4.7.1 Headset Type

To select the headset model that is used, perform the following:

1. Select **Headset → General**.
2. Select the applicable item from the **Headset type** drop-down list:
   - **Mic on boom**
   - **Mic on cable**
   - **User model**

If none of the headsets above are selected, this option can be used to configure an own headset profile.
If selected, additional configuration is required, see 3.4.7.2 Headset User Model, page 20.

#### 3.4.7.2 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 headset model to be used.
3. In the following drop-down lists, select the applicable values for the headset:
   - **Microphone gain**
   - **Speaker gain**
   - **Side tone**

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

#### 3.4.7.3 Call with Headset

To make a call using a wired or Bluetooth headset, perform the following:

1. Select **Headset → General**.
2. In the **Call with headset** drop-down list, select one of the following:
   - **Not activated** – It is only possible to answer/end a call.
   - **Last called number** – The last called number is dialed.
   - **Predefined number** – A predefined number is called. If selected, in the **Predefined number** field, enter the number to be dialed when the headset button is pressed.

### 3.4.8 Actions when the Handset is Placed in the Charger

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

#### 3.4.8.1 In charger Call Behavior

To configure **In charger call behavior**, perform the following steps:

1. Select **Device → Call**.
2. In the **In charger call behavior** drop-down list, select one of the following:
   - **No action**
   - **End** – The handset ends an ongoing call when placed in a charger.
   - **Put on Loudspeaker** – The handset turns on the loudspeaker when placed in a charger during a call.

#### 3.4.8.2 In Charger Action when Not in Call

To configure the **In charger action when not in call** 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** – No action is performed when handset is placed in the charger.
   - **Switch off** – The handset is switched off when placed in the charger.

- **Sound off** – The handset is muted when placed in the charger (except for messages with set **Break through** parameter, for example, **Prio 1** messages).
  To mute all messages (regardless of priority), set the **Device → Messaging → Show and indicate messages in charger** to **Off**.
- **Change profile** – The handset changes profile when placed in the charger.
  - In the **Change profile in charger** drop-down list, select the profile to be used.
  - If needed, configure the selected profile, see 3.5 Profiles, page 30.

3. In the **In charger Message absent** drop-down list, select one of the following:
   - **No** – Messages are saved in the handset's messaging inbox while the handset is placed in the charger (default).
   - **Yes** – If a message is sent from a system it is notified that the handset is absent. Messages are not sent to the handset.

   This function is applicable to 5634 Services and 5634 Alarm only.

#### 3.4.8.3 Clear Lists in Charger

If **Clear lists in charger** is set to **Yes**, message and call lists are deleted when the handset is placed in the charger. To configure this parameter, perform the following steps:

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

#### 3.4.8.4 USB Behavior

When set to **Ask**, a dialog window is displayed every time the phone is connected to a PC over USB. Otherwise, it behaves as defined.

1. Select **Device → General**.
2. In the **USB Behavior** drop-down list, select one of the following:
   - **Ask** — A dialog window is displayed every time the handset is connected to a PC over USB where one of the below modes may be chosen.
   - **WinPDM** — This mode allows the handset to communicate to the application WinPDM on a PC.
   - **MTP** — This mode shows the handset as a media device and allows transferring and viewing log files from the handset.
   - **Charge** — This option 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, see 3.3.3.5 WinPDM Authentication, page 15.

#### 3.4.8.5 Show and Indicate Messages in Charger

This function is applicable to 5634 Services and 5634 Alarm only.

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

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 instead 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** – Messages are shown and indicated (by beep) while the handset is in the charger (default).
   - **Off** – The message alert (if any) is muted and only the New message icon is displayed. The messages are still stored as unread messages in the Message inbox.

#### 3.4.8.6 Receive Messages in Charger

This function is applicable to 5634 Services and 5634 Alarm only.

It defines if received messages are saved or discarded while the handset is in the charger.

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

### 3.4.9 Transfer Unlock File

1. Select **Device → General**.
2. In the **Transfer Unlock File** drop-down list, enter the unlock file as a string.

Unlocking is performed for debugging purposes. Due to security reasons, the handset needs to be factory-reset after debugging is finished.

### 3.4.10 Hide Missed Call Window

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

To hide the Missed call window, perform the following steps:

1. Select **Device → Call**.
2. In the **Show missed calls dialog window** drop-down list, select **No**.

### 3.4.11 Prevent the Handset to Switch off

It is possible to prevent the user from switching off the handset when holding down the End key ⏻. When **Block switch off** is activated and the End key is held down, the `Switch off?` dialog window does not appear in the handset.

1. Select **Device → General**.
2. In the **Block switch off** drop-down list, select one of the following:

- **No** – The user can switch off the handset.
- **Yes** – The user cannot switch off the handset.

### 3.4.12 Disable Mute Function

To prevent the user from muting the handset, perform the following steps:

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

### 3.4.13 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, perform the following steps:

1. Select **Device → Call**.
2. In the **Enable call list** drop-down list, select **Off**.

### 3.4.14 Battery Warning

The warning when the battery is low 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**

### 3.4.15 No Network and No Access Warning

#### 3.4.15.1 No Network Warning

If the handset has no coverage, it shows `No network` in the handset display in idle mode. It also gives a vibrating alert (if enabled), a beep signal (if enabled), and displays a dialog window (if enabled by the system administrator).

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

1. Select **Device → General**.
2. In the **No network warning** drop-down list, select one of the following:
   - **Indicate repeatedly** – The beep is on (if enabled), `No network` is displayed in idle mode, the vibrating alert is on (if enabled), the dialog window is on (if enabled). This simultaneous indication is repeated every minute for 30 minutes.
   - **Indicate once** – The beep is on (if enabled), `No network` is displayed in idle mode, the vibrating alert is on (if enabled), the dialog window is on (if enabled). This simultaneous indication is made only once.
   - **Indication off** – The beep is off (even if enabled), `No network` is displayed in idle mode, the vibrating alert is off (even if enabled), the dialog window is either on or off, depending on the parameter settings.

Even if **Indication off** is set, the dialog window still appears when **Dialog window for no network and no access warnings** (in **Device → General**) is set to **Yes**.

### 3.4.15.2 No Access Warning

If the handset has no access, has lost messaging and/or voice connection, it shows `No access`, `Voice only`, or `Messaging only` in the handset display in idle mode. It also gives a vibrating alert (if enabled), a beep signal (if enabled), and a dialog window (if enabled by the system administrator).

`No access` 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** – This is the default and recommended setting for any handset used with medical devices. The beep is on, `No access`/`Voice only`/`Messaging only` is displayed in idle mode, the vibrating alert is on (if enabled). This simultaneous indication is repeated every minute for 30 minutes.
   - **Indicate once** – The beep is on, `No access` is displayed in idle mode, the vibrating alert is on (if enabled). This simultaneous indication is made only once.
   - **Indication off** – The beep is off, `No access` is displayed in idle mode, the vibrating alert is off (if enabled) depending on the parameter settings.

   Even if **Indication off** is set, the dialog window still appears when **Dialog window for no network and no access warnings** (in **Device → General**) is set to **Yes**.

### 3.4.15.3 Dialog Window for No Network/No Access Warnings

This parameter defines if the dialog windows `No network`, `No access`, `Voice only`, and `Messaging only` are visible or not on the handset display.

1. Select **Device → General**.
2. In the **Dialog window for no network/no access warnings** drop-down list, select one of the following:
   - **Yes** – The dialog window `No network`/`No access`/`Voice only`/`Messaging only` appears on the handset display.

     When set to **Yes** (default), it overrides the **Indication off** setting (in **Device → General → No network warning** or **No access warning**), that is, the dialog window is still shown.
   - **No** – The dialog window `No network`/`No access`/`Voice only`/`Messaging only` does not appear on the handset display.

## 3.4.16 Shared Phone

It is possible to use the handset as a shared phone. 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 following is required:

- A handset without certificates
- A WSM3/CPDM3

It is possible to set the same password on multiple personal handsets.

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.

By default, the handset is in **Personal** mode. To set it to **Shared**, perform the following steps in WinPDM/ WSM3/CPDM3 DM:

1. Select **Device** → **General**.
2. In the **Phone mode** drop-down list, select one of the following:
   - **Personal**
   - **Shared**

### 3.4.17 Shortcuts

One-click access to predefined functions can be configured for soft keys, hot keys, navigation keys, and the Multifunction button. For example, a soft key can be configured to make a call. Generally, shortcuts are only available when not in a call and in idle mode. Although, a hot key configured to Services with, for example, **Send data**, is available during calls in case of 5634 Services.

Shortcuts can be configured in **Shortcuts** in WinPDM/WSM3/CPDM3 DM, except for soft keys that can be configured in the **User Profiles** folder.

#### 3.4.17.1 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.

1. Select **Shortcuts** → **Hot keys 0** (or 2–9).
2. Continue with 3.4.17.4 Shortcut Settings, page 25.

#### 3.4.17.2 Configure a Soft Key

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

1. Select **User Profiles** → **Normal/Profile X** → **Soft keys** → **Soft key left**, **Soft key middle**, or **Soft key right**.
2. In the **Soft key name** field, enter the name of the soft key shortcut to be displayed in the handset.
3. Continue with 3.4.17.4 Shortcut Settings, page 25.

#### 3.4.17.3 Configure a Navigation Key

1. Select **Shortcuts** → **Navigation Key Up** (or **Down**, **Left**, or **Right**).
2. Continue with 3.4.17.4 Shortcut Settings, page 25.

#### 3.4.17.4 Shortcut Settings

1. In the **Function** drop-down list, select the required function:
   - **Not used**
   - **Phone call**

- **Phone call loudspeaker**
- **Call list**
- **Contact list**
- **Central phone book** (system-dependent feature)
- **Message inbox**
- **Send message**
- **Change profile normal**
- **Change profile 1–4** (If selecting profile 1–4, the profile must first be configured, see 3.5 Profiles, page 30.)
- **Open menu** (**Main menu**, **Calls**, **Call services**, **Connections**, **Contacts**, **Messaging**, **Services**, **Profiles**, **Settings**.)
- **Executive service X** (1–10)
- **Logout**[1]
- **Call diversions**
- **RSSI measure**
- **Execute call service X** (1–16)

2. In the **Value** field, enter the applicable value. This is mandatory when using the **Phone call** function.
3. In the **Control question** drop-down list, select **Yes** to display the `Proceed?` window after the key is pressed. This is used to prevent a function from being accessed by mistake.

#### 3.4.17.5 Soft Key Functions During Call

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

To configure the soft key functions, perform the following steps:

1. Select **Device → Call**.
2. In the **Right in call soft key name** field, enter the name of the soft key to be displayed during a call.
3. In the **Right in call soft key action** drop-down list, select one of the following functions:
   - **Conference**
   - **Contacts**
   - **Messaging**
   - **No action**
   - **End call**
   - **Hold**
   - **Loudspeaker**
   - **New call** (Put active on hold)
   - **Retrieve**
   - **Switch**
   - **Transfer** (To held call)
   - **Transfer to new call** (Blind transfer)

[1] Applicable to **Share phone** feature only.

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

### 3.4.18 Import Contacts

Phone book files (local phone book) can be imported to the handset using WinPDM/WSM3/CPDM3 DM. The phone book file is a tab-separated `.txt` file that contains two items per row, number and name.

For more information, see the WinPDM Installation and Operation Manual or the WSM3/CPDM3 User Manual.

### 3.4.19 Company Phone Book

It is possible to create a phone book that is administered centrally and uploaded to the handset from WinPDM/WSM3/CPDM3 DM. If this feature is used, the entries from **Contacts** and **Company Phone Book** are merged. The **Company Phone Book** entries are locked and cannot be edited in the handset.

Perform the following steps:

1. Create a Company phone book file. For more information, see Create a Company Phone Book File, page 27.
2. Import the Company phone book file to the WinPDM/WSM3/CPDM3 DM. For more information, see WinPDM Installation and Operation Manual or the WSM3/CPDM3 User Manual.
3. Upload the Company phone book file to the handset(s), see the Installation and Operation Manual, Portable Device Manager for Windows (WinPDM) or the User Manual, Device Manager in WSM3/CPDM3.

#### Create a Company Phone Book File

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

The format of the rows in the phone book 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 phone book file, but are ignored when the phone book file is created:

- Left parenthesis: (
- Right parenthesis: )
- Hyphen: –
- Space: “”

### 3.4.20 Central Phone Book

Applicable only if your system supports the function.

If the system is equipped with a messaging server with a phone book service, the Central phone book on that server can be accessed from the handset.

1. Select **Device → Unite**.

2. In the **Central phone book number** field, enter the number to the Central phone book.
   The number to be used is set to 999999 by default. If the system is not equipped with a Central phone book, this menu option can be removed from the handset by entering an empty value.

### 3.4.21 System Administration in the Handset

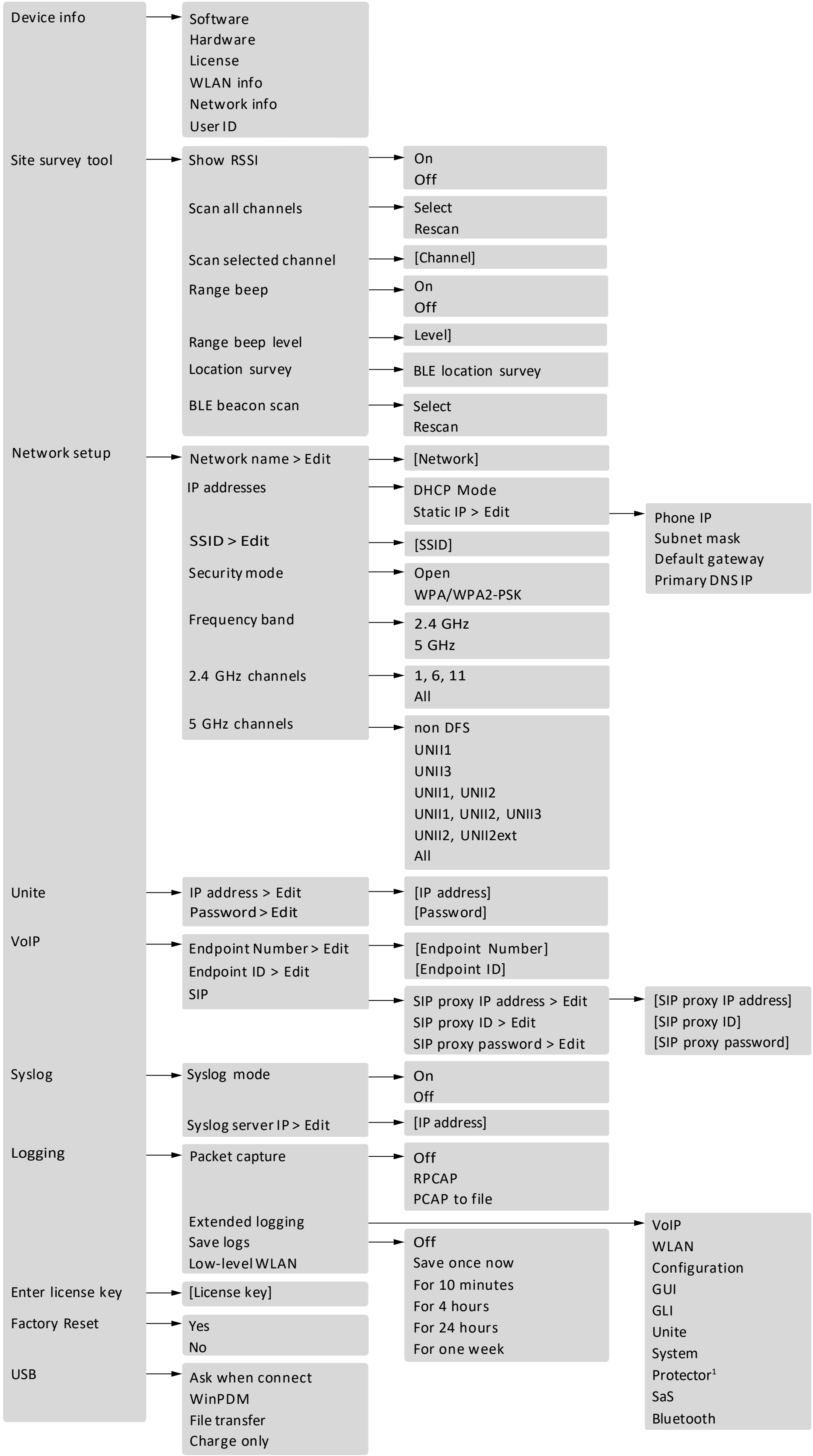
The handset has a hidden menu for system administrators that contains the following information:

- Device information including software, hardware, WLAN, network, and license information
- Site survey tool
- Network setup menus
- IP address and endpoint number options for Unite, VoIP, SIP, and Syslog server
- Logging options
- Entering license key
- Factory reset option
- USB behavior

To access the **Admin menu**, select **Menu → Settings**, and enter the Admin access code. The default code is `40022`, which is configurable in WinPDM/WSM3/CPDM3 DM.

If the handset has been factory reset or not been configured, in the `Connecting`/`No network` screen at start-up enter the Admin access code.

### 3.4.21.1 Admin Menu Tree in the Handset



[1] Applicable to 5634 Alarm only.

Other menus are described in the Mitel 5634 VoWi-Fi Handset User Guide.

#### 3.4.21.2 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.<br>Select either of the following menus: **Software**, **Hardware**, **License**, **WLAN info**, **Network info**, **User ID**, **TFTP info**. |
| *#35# | To access **Enter license key** in the Admin menu. |
| *#76# | To view RSSI information. |
| *#77# | To access **Site survey tool** in the Admin menu.<br>Select either of the following menus: **Show RSSI**, **Scan all channels**, **Scan selected channels**, **Range beep**, **Range beep level**, **Location survey**, **BLE beacon scan**. |

### 3.4.22 Change Admin Access Code

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

1. Open WinPDM/WSM3/CPDM3 DM.
2. Select **Device → General**.
3. In the **Admin access code** field, enter a new password.

### 3.4.23 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. Open WinPDM/WSM3/CPDM3 DM.
2. Select **Device → General**.
3. In the **Admin menu access** drop-down list, select **Off**.

## 3.5 Profiles

### 3.5.1 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** (where X represents **Profile 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. See 3.5.1.1 Configure Sound and Alerts, page 31.
   - **Presence and diversion** — Contains settings for message absent and call diversion. See 3.5.1.2 Configure Presence and Diversion, page 32.
   - **Answering** — Contains settings for how incoming calls are answered. See 3.5.1.3 Configure Answering, page 32.
   - **Soft keys** — Contains shortcut settings to predefined functions using key press. See 3.5.1.4 Configure Soft Keys, page 33.
   - **Call service** — Enables call services. See 3.5.1.5 Configure Call Service, page 33.
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 possible to configure profiles through the handset menu as well. See the Mitel 5634 VoWi-Fi Handset User Guide.

To exclude a parameter from **Profile X**, use the option **Not used**.

#### 3.5.1.1 Configure Sound and Alerts

To configure sounds and alerts, perform the following steps:

1. Select **User Profiles → Profile X → Sound and Alerts**.
2. In the **Internal ring signal**, **External 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** (Custom sound 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 mode** drop-down list, select one of the following:
   - **Silent** – There is no ring signal.
   - **Volume X (1–8)** – Different ring signal volumes from lowest (1) to highest (8).
4. In the **Vibrator** drop-down list, select one of the following:
   - **On** – The vibrating alert is active for incoming calls and messages.
   - **On if silent** – The vibrating alert is active for incoming calls and messages only if the handset is muted or the volume is set to **Silent**.
   - **Off** – The vibrating alert is off.
5. In the **Key sound** drop-down list, select one of the following:
   - **Click** – A click is heard when a key is pressed on the handset.
   - **Tone** – A tone is heard when a key is pressed on the handset.
   - **Silent** – There is no sound when a key is pressed on the handset.

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

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

   Only the parameter **Custom sounds according to beep code** can be customized. For more information, see Customize the Default Handset Beeps, page 92.

   - **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.
   - **High beeps according to beep code** – The same type as **Beeps according to beep code**, but with a higher pitch.
   - **Enhanced beeps according to beep code** – The same type as **Beeps according to beep code**, but in the form of a melody.
   - **Custom sounds according to beep code** – Melody coming from defined custom sounds.
7. In the **Message volume** drop-down list, select one of the following:
   - **Silent** – There is no audible message indication for incoming messages.
   - **Volume X** (1–8) – Different message indication volumes from lowest (1) to highest (8).
   - **Follow ring volume** – The message indication volume follows the ring volume.

### 3.5.1.2 Configure Presence and Diversion

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

1. Select **User Profiles → Profile X → Presence and diversion**.
2. In the **Message absent** drop-down list, select one of the following:
   - **On** – When a handset receives a message, it indicates that it is absent. The message can be redirected to another destination.
   - **Off** – Message absence is disabled.
3. In the **Diversion for all calls** drop-down list, select **Off** or **On**. When enabled, all calls are diverted to the number specified by the **All calls diversion number** parameter.
4. In the **Diversion on user busy** drop-down list, select **Off** or **On**. When enabled, calls are diverted to the number specified by the **On busy diversion number** parameter if the user is busy.
5. In the **No answer diversion** drop-down list, select **Off** or **On**. When enabled, calls are diverted to the number specified by the **No answer diversion number** parameter if the user does not answer an incoming call.

### 3.5.1.3 Configure Answering

To configure how to answer incoming calls, perform the following steps:

1. Select **User Profiles → Profile X → Answering**.
2. In the **Answering key** drop-down list, select one of the following:
   - **Call key** — Incoming calls are answered by pressing the Call key.
   - **Any key** — Incoming calls are answered by pressing any key.
3. In the **Answer mode** drop-down list, select one of the following:
   - **Normal** – The Call key needs to be pressed to answer the call.
   - **Automatically** – The call is automatically answered after 1 second.
   - **Loudspeaking** – The call is answered in loudspeaking mode by pressing the Call key.

   - **Automatically loudspeaking** – The call is automatically answered in loudspeaking mode after 1 second.

4. In the **Can reply with a message template when rejecting a call** drop-down list, select **Yes**. The dialog window `Reply with a message template?` appears when rejecting an incoming call.

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

   For more information, see 3.8 Message Templates, page 53.

#### 3.5.1.4 Configure Soft Keys

To configure soft key functions, perform the following steps:

1. Select **User Profiles → Profile X → Soft keys → Soft Key X** (where X represents the left, middle, or right soft key).
2. The following parameters can be configured:
   **Soft key name** – Defines the text that is shown in the handset display above the soft key.

   A maximum number of 6 characters fits in the soft key name.

   **Function** – Defines the function to be connected to the soft key. For the list of functions, see 3.4.17.4 Shortcut Settings, page 25.
   **Value** – Defines a value (for example, a phone number) for a function.

   Only certain functions require a value.

   **Control Question** – Defines if a `Proceed?` dialog window appears when pressing a soft key.

#### 3.5.1.5 Configure Call Service

To configure call services, perform the following steps:

1. Select **User Profiles → Profile X → Call service**.

   The Call service must first be configured in Device → Call services.

2. The following parameters can be configured:
   - **When activated** — Select the Call service to be used when this profile is activated.
   - **When deactivated** — Select the Call service to be used when this profile is deactivated.

Call service is not available for **Normal** profile.

### 3.5.2 System Profiles

Applicable to 5634 Services and 5634 Alarm only.

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

A system profile overrides all profile **Normal** or **Profile 1**–**Profile 4** settings, on all parameters in the group, for example, soft keys.

To create a system profile, perform the following steps:

1. Create a **System Profiles Sub-Group**.

   The following sub-groups are available:

   - **Presence groups** — Contains settings for message absent and call diversion. See 3.5.2.1 Configure Presence Groups (Sub-group), page 34.
   - **Answering groups** — Contains settings for how incoming calls are answered. See 3.5.2.2 Configure Answering Groups (Sub-group), page 34.
   - **Sound and alerts groups** — Contains sound and alert settings for calls and messages. See 3.5.2.3 Configure Sounds and Alerts Groups (Sub-group), page 35.
   - **Soft key groups** — Contains shortcut settings to predefined functions using soft keys. See 3.5.2.4 Configure Soft Key Groups (Sub-group), page 36.
   - **Alarm settings groups** — Contains settings for which alarm type is used and how. See 3.5.2.5 Configure Alarm Settings Group (Sub-group), page 36.
   - **Idle display groups** — Contains settings to show the system profile name during idle mode.

   For more information, see 3.5.2.7 Create System Profile Using Predefined Sub-Groups, page 37.

2. Connect the system profile to the created sub-group(s).
   Once a system profile is created, it can be used whenever desired and can be turned off and on again. For more information, see 3.5.2.8 Activate and Deactivate System Profile, page 37.

### 3.5.2.1 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**.
2. In the **Name of group** field, enter a descriptive name.
3. In the **Message absent** drop-down list, select one of the following:
   - **On** – When a handset receives a message, it indicates that it is absent. The message can be redirected to another destination.
   - **Off** – Message absence is disabled.

### 3.5.2.2 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**.
2. In the **Name of group** field, enter a descriptive name.
3. In the **Answer mode** drop-down list, select one of the following:
   - **Normal** – The Call key needs to be pressed to answer the call.
   - **Automatically** – The call is automatically answered after 1 second.
   - **Loudspeaking** – The call is answered in loudspeaking mode by pressing the Call key.
   - **Automatically loudspeaking** – The call is automatically answered in loudspeaking mode after 1 second.

#### 3.5.2.3 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**.
2. In the **Name of group** field, enter a descriptive name.
3. In the **Ring volume mode** drop-down list, select one of the following:
   - **Silent** – There is no ring signal.
   - **Volume X (1–8)** – Different ring signal volumes from lowest (1) to highest (8).
4. In the **Vibrator** drop-down list, select one of the following:
   - **On** – The vibrating alert is active for incoming calls and messages.
   - **On if silent** – The vibrating alert is active for incoming calls and messages only if the handset is muted or the volume is set to **Silent**.
   - **Off** – The vibrating alert is off.
5. In the **Internal ring signal**, **External 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** (Custom sound 8–10) – Defines one of the 3 proprietary melodies made by coding with the help of a specific code table.
6. In the **Key sound** drop-down list, select one of the following:
   - **Click** – A click is heard when a key is pressed on the handset.
   - **Tone** – A tone is heard when a key is pressed on the handset.
   - **Silent** – There is no sound when a key is pressed on the handset.
7. In the **Message alert** drop-down list, select one of the following:

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

   Only the parameter **Custom sounds according to beep code** can be customized. For more information, see Customize the Default Handset Beeps, page 92.

   - **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.
   - **High beeps according to beep code** – The same type as **Beeps according to beep code**, but with a higher pitch.
   - **Enhanced beeps according to beep code** – The same type as **Beeps according to beep code**, but in the form of a melody.
   - **Custom sounds according to beep code** – Melody coming from defined custom sounds.
8. In the **Message volume** drop-down list, select one of the following:
   - **Silent** – There is no audible message indication for incoming messages.
   - **Volume X** (1–8) – Different message indication volumes from lowest (1) to highest (8).
   - **Follow ring volume** – The message indication volume follows the ring volume.

#### 3.5.2.4 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**.
2. In the **Name of group** field, enter a descriptive name.
3. Select **Soft key group X → Soft key X** (left/middle/right), and edit the required settings.
   - **Soft key name** – Defines the text that is shown in the handset display above the soft key.

     A maximum number of 6 characters fits in the soft key name.

   - **Function** – Defines the function to be connected to the soft key. For the list of functions, see 3.4.17.4 Shortcut Settings, page 25.
   - **Value** – Defines a value (for example, a phone number) for a function.

     Only certain functions require a value.

   **Control Question** – Defines if a `Proceed?` dialog window appears when pressing a soft key.

#### 3.5.2.5 Configure Alarm Settings Group (Sub-group)

Applicable to 5634 Alarm 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**.
2. In the **Name of group** field, enter a descriptive name.
3. In the **Common** menu, the following parameters can be configured:
   - **Stored alarm data** – Predefined information that is sent with the alarm (for example a room number)
   - **Indicate triggered alarm with beep signal**
   - **Indicate triggered alarm with vibrator**

   If **Silent alarm** enabled, the handset does not show that an alarm has been triggered, that is, there is no sound signal, vibrating alert, dialog window, ALS, or notification light on the display.

4. In the **Alarm on long press** menu, the following parameters can be configured:
   - **Alarm type for long press** – Defines the type of alarm that is sent by a long press (press and hold) on the Alarm button. If **Not used** is selected, a predefined number can still be called automatically after an alarm without sending an alarm. For more information, see 3.9.5 Call Predefined Number without Sending Alarm, page 56.
   - **ALS** – Enables or disables the ramped-up ALS after the alarm has been sent.

     The ALS is paused if the automatic call after alarm is active. For more information, see 3.9.5 Call Predefined Number without Sending Alarm, page 56.

5. In the **Alarm on multiple press** menu, the following parameters can be configured:
   - **Alarm type for multiple press** – Defines the type of alarm that is sent when pressing the Alarm button twice or more. If **Not used** is selected, a predefined number can still be called automatically

after an alarm without sending an alarm. For more information, see 3.9.5 Call Predefined Number without Sending Alarm, page 56.

- **ALS** – Enables or disables the ramped up ALS after the alarm has been sent.

The ALS is paused if the automatic call after alarm is active. For more information, see 3.9.5 Call Predefined Number without Sending Alarm, page 56.

### 3.5.2.6 Configure Idle Display Groups (Sub-group)

By default, the system profile name is displayed in the handset. In case it is not needed to show the system profile name, perform the following steps:

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

### 3.5.2.7 Create System Profile Using Predefined Sub-Groups

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

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

To create a system profile using predefined sub-groups, perform the following steps:

1. Select **System Profiles → System Profile X**.
2. Configure the required parameters:
   - In the **Profile name** field, enter a descriptive name to identify this system profile.
   - **Activation and deactivation sound** — Defines the sound that is heard when the profile is activated or deactivated.
   - **Presence group** – Defines which predefined presence group (sub-group) is used in this system profile.
   - **Sound and alerts group** – Defines which predefined sound and alerts group (sub-group) is used in this system profile.
   - **Soft keys group** – Defines which predefined soft key group (sub-group) is used in this system profile.
   - **Answering group** – Defines which predefined answering group (sub-group) is used in this system profile.
   - **Alarm settings group** – Defines which predefined alarm settings group (sub-group) is used in this system profile.
   - **Idle display group** – Defines which predefined idle display group (sub-group) is used in this system profile.

### 3.5.2.8 Activate and Deactivate System Profile

When a system profile is created, it can be activated using WSM3/CPDM3 DM or a WSM3/CPDM3 application. For example, the application could be triggered by a positioning beacon.

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

To activate a system profile, perform the following steps:

1. Select **System profiles**.
2. In the **Active system profile** drop-down list, select one of the following:
   - **Normal** – No system profile is used.
   - **System profile 1–System profile 5**

A system profile overrides all **User Profile X** and **Normal** (profile) settings on all parameters in the group, see the following two examples.

**Example 1**

*Figure 3. User Profile X/Normal — Soft Key Settings*

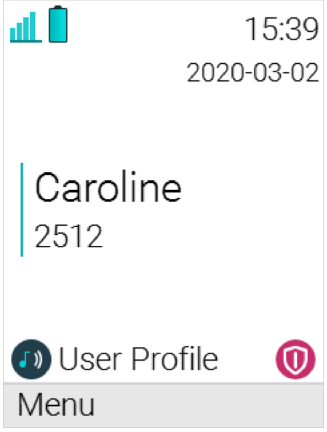
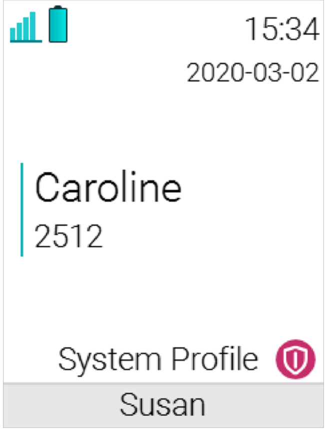

15:39
2020-03-02
Caroline
2512
User Profile
Menu

*Figure 4. System Profile — Soft Key Settings*


15:34
2020-03-02
Caroline
2512
System Profile
Susan

In Figure 3. *User Profile X/Normal — Soft Key Settings*, page 38, the **User Profile X** (or the profile **Normal**) is configured with a shortcut to open the menu on the left soft key.

In Figure 4. *System Profile — Soft Key Settings*, page 38, a system profile shortcut to make a call to the administrator Susan, is configured for the free middle soft key (2). When activating the system profile **Susan**, the left soft key **Menu** disappears, because the system profile overrides the complete group of the soft key parameters.

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

**Example 2**

If any settings are changed that are specified in the system profile, the settings are not applied. In this case, the alarm settings have been configured in the system profile **Alarm**. Then the user cannot change any alarm settings using the handset, although the **Alarm** menu is still visible.

## 3.6 Telephony

### 3.6.1 Endpoint ID and Endpoint Number

The **Endpoint ID** and **Endpoint number** are automatically received when registering the handset in the VoWiFi system. The **Endpoint ID** is normally the user's name registered in the PBX and it is displayed in the handset in idle mode. To change the displayed name, see 3.11.2 User Display Text, page 58.

The **Endpoint number** can only be changed in the Admin menu of the handset. For more information, see 3.4.21.1 Admin Menu Tree in the Handset, page 29.

To change the **Endpoint ID**, go to WinPDM/WSM3/CPDM3 DM, select **VoIP → General,** and enter a new ID in the
**Endpoint ID** field.

The **Endpoint ID** can also be configured in the Admin menu of the handset. For more information, see 3.4.21.1 Admin Menu Tree in the Handset, page 29.

If required, shorten the **Endpoint number**. For more information, see 3.6.2 Endpoint Number Display Length, page 39.

### 3.6.2 Endpoint Number Display Length

It defines the total number of digits to be displayed on the handset display in idle mode when the Endpoint number is shown. From 1 up to 6 digits (starting from the end of the number), or all, can be displayed.

1. Select **Device → Settings**.
2. In the **Endpoint number display length text** field, enter the number length to be displayed.

### 3.6.3 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 parameters, perform the following steps:

1. Select **VoIP → SIP**.
2. The following SIP parameters are available:
   - **SIP Transport** – Defines the protocol (**UDP**, **TCP** or **TLS**) to be used for SIP signaling. The TLS setting requires the Root certificate of the PBX certificate (The server must send its complete certificate chain.) to be uploaded as a trusted certificate. It is also possible to turn off the validation of the server certificate by setting **Validate server certificate** to **No**. In the **SIP TLS client certificate** drop-down list, select a certificate to be used for TLS applications, for example. secured VoIP signaling.

– **Outbound proxy mode** – Select **Yes** if the handsets are to connect with the SIP proxy through an outbound proxy. Set to **No** if the handsets are to connect directly with the SIP proxy (there may be two).

– **Primary SIP proxy** – Defines the primary SIP proxy by either an IP address, a domain name, or an IP address together with a port number.

Examples of valid formats are the following:

```
- 192.168.1.1
– proxy1.mydomain.com
- 192.168.1.1:5060
```

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

Only a plain IP address is shown in the handset's Admin menu (under **VoIP → SIP → SIP proxy IP address**).

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

The parameter is only visible if **Outbound Proxy mode** is set to **No**.

– **Secondary SIP proxy** – Defines the optional secondary SIP proxy, which is used if the handset fails to register with the primary SIP proxy. See definition examples in Primary SIP proxy above.
When the handset has connected to the Secondary SIP proxy, it continuously tries to reconnect to the Primary SIP proxy.

– **Outbound proxy** – Defines the primary outbound proxy by a domain name, an IP address, or an IP address with a port number.

The parameter is only visible if **Outbound Proxy mode** is set to **Yes**.

– **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.

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. If set to **RFC 2833**, the DTMF signaling is sent in the RTP stream, that is, from handset to handset. If set to **SIP INFO**, the DTMF signaling is sent using SIP signaling, that is, through the PBX.

– **Hold type** – Defines 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 endpoint uses its number, ID, or MAC address for the registration with the SIP proxy.

- **Authentication identity** – Defines if the endpoint uses its number, ID, or MAC address for the authentication with the SIP proxy.
- **Call forward locally** – When enabled, the call forwarding is handled locally by the handset instead of updating the PBX.

  The handset must be switched on and must have coverage to handle the **Call forward locally** functionality.
- **MOH locally** (Music on Hold) – If supported by the PBX, the handset plays music when a call is on hold. If the PBX does not support MOH, the handset plays a tone when the call is on hold.
- **Hold on transfer** – Puts a second call on hold before transfer, which is required by some SIP proxy servers.
- **Direct signaling** – Defines whether calls originating from other sources than the configured SIP Proxy should be accepted or redirected using `USE PROXY` message.
- **SIP Register Expiration** – Defines the number of seconds for register expiration to the PBX.
- **Far-End NAT Traversal** — Used when the SIP server is not local and the phones are behind a NAT. Enabling it allows phone communications to traverse a NAT device that is farthest away from the SIP server and near the handsets.

### 3.6.4 Codec

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.

1. Select **VoIP → General**.
2. In the **Codec configuration** drop-down list, select the applicable codec.
   - **Opus Wideband**
   - **G.711 A-law (EU)**
   - **G.711 u-law (US)**
   - **G.722**
   - **G.729**
   - **G.729A**
3. In the **Codec packetization time configuration** drop-down list, select the packetization time to use for speech (value 20–60 ms).

### 3.6.5 Offer Secure RTP

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

**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. Select the preferred SRTP encryption by assigning a value to **VoIP → General → Secure RTP Crypto**, which appears when enabling **Offer Secure RTP**.

### 3.6.6 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.

### 3.6.7 ICE Negotation

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 protocol used.

   The following parameters are available when ICE negotiation is enabled:

   – **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.

### 3.6.8 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.

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

1. Select **Device → Emergency call numbers**.
2. In the **Emergency call numbers** field, enter the desired emergency number(s).

For more information, see 3.9.4 Emergency Call Alarm, page 56.

### 3.6.9 Voice Mail Number

In some systems it is needed to assign the handset number of the voice mail service.

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

### 3.6.10 Message Center Number

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

1. Select **Device → Message center**.
2. In the **Message Center number** field, enter the number for the server.

### 3.6.11 Voice Mail Call Clears MWI

If enabled, the handset deactivates voice mail message waiting indications in the **Message Center** when calling the defined voice mail number.

To enable **Voice mail call clears MWI**, perform the following steps:

1. Select **Device → Message center**
2. In the **Voice mail call clears MWI** drop-down list, select **Yes**.

### 3.6.12 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, perform the following steps:

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

### 3.6.13 Quick Answer

The handset automatically answers a call (quick answer) when removed from the charger.

To enable **Quick answer**, perform the following steps:

1. Select **Device → Call**.
2. In the **Quick answer** drop-down list, select **Yes**.

### 3.6.14 Replace Call Rejected with User Busy

It is used if the system does not support call rejected.

To configure this function, perform the following steps:

1. Select **VoIP → General**.
2. In the **Replace Call Rejected with User Busy** drop-down list, select **Yes** or **No**.

### 3.6.15 Call Waiting Behavior

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

To configure **Call waiting behavior**, perform the following steps:

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

### 3.6.16 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, perform the following steps:

1. Select **Device → Call**.
2. In the **PTT Call disconnect warning** drop-down list, select **Yes**.

### 3.6.17 Configure In Call Functions

It is possible to define 10 extra system specific call services by codes. The codes can be configured using any character. Use `\U` to make the handset prompt for user input with numerical characters.

1. Select **Device → In call functionality → General purpose <number>**.
2. In the **Name** field, enter the name to be displayed in the **In call** menu.
3. In the **Data** field, enter the access code to be used for the function.
4. In the **Send as** field, select one of the following:
   - **New call** to send data as a new call.
   - **DTMF** to send data in the current call.
   - **Transfer** to send data as a call transfer.
5. In the **Auto disconnect** field, select **Yes** to automatically disconnect when the PBX has received the command.

Ask the PBX supplier for example templates to configure the relevant menu of the PBX.

### 3.6.18 Allow Blind Transfer

1. Select **Device → Call**.
2. In the **Allow blind transfer** drop-down list, select **No** to disable the option to do a blind transfer. By default, it is set to **Yes**.

Allowing blind transfer enables **New call** in the **In-call** menu.

### 3.6.19 Call Services

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

Up to 16 call services can be configured in WinPDM/WSM3/CPDM3 DM.

1. Select **Device → Call Services**.
2. Select a **General service** in the range of 1–16.
3. In the **Name** field, enter a name to be displayed in the **Call services menu**.
4. In the **Data** field, enter a PBX-specific code for the command.
5. In the **Auto disconnect** field, select **Yes** to automatically disconnect when the PBX has received the command. Otherwise, select **No**.

The access codes are PBX-dependent.

Ask the PBX supplier for example templates to configure the relevant menu of the PBX.

## 3.7 Messaging Settings

Applicable to 5634 Services and 5634 Alarm only.

It is possible to configure how incoming messages are indicated and displayed in the handset.

1. In **User Profiles → Normal, Profile X → Sound and alerts**, the following parameters can be configured:
   - **Vibrator** — Defines if the handset vibrates when receiving incoming calls and messages. For more information, see 3.5.1.1 Configure Sound and Alerts, page 31.
   - **Message alert** — Defines the message sound for incoming messages. For more information, see 3.5.1.1 Configure Sound and Alerts, page 31.
   - **Message volume** — Defines the message volume for incoming messages. By default, the message volume follows the ring volume, but a different message volume can be set with this parameter. For more information, see 3.5.1.1 Configure Sound and Alerts, page 31.
2. In **Device → Messaging**, the following parameters can be configured:
   - **Message list representation** — Can be set to number/name or message text.
   - **Message text size** — Defines the text size used when displaying messages.
   - **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 Messaging 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. See also 3.7.3 Examples of TTR and TTP Settings, page 50.

     The following options can be selected:

     - **Close manually**
     - **10/20/30 seconds**
     - **1/2/5/10 minutes**

- **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. See also 3.7.3 Examples of TTR and TTP Settings, page 50.

  The following options can be selected:

  - **No prioritization**
  - **Prioritize 10/20/30 seconds**
  - **Prioritize 1/2/5/10 minutes**
  - **Prioritize forever**
- **Repeat message indication** — This parameter 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.
- **Vibrator for message during call** — Defines if the handset vibrates when receiving messages during an ongoing call. The following options are available:
  - **Never activated**
  - **Only for urgent messages**
  - **Always activated**
- **Message alert during call** — Defines if a message alert should be played when receiving a message during a call. The following options are available:
  - **Never activated**
  - **Only for urgent messages**
  - **Always activated**
- **IM option mode** — This parameter 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).
- **Call priority**
  This parameter defines the following:
  - Whether call information presented on the display during an incoming, ongoing, and outgoing call is suppressed when viewing a message.
  - Whether an ongoing call is disconnected when receiving a PTT invitation with **Answer mode** set to **Automatically**.

  **0** – Call indication overrides all messages and the ongoing call is never disconnected (default).
  **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 2 Call Priority vs PTT Priority**

| **Call priority** | **PTT invitation (priority)[1]** | **Disconnection of 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. |
| 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. |

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

**Table 3 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. |

– **Show and indicate messages in charger** — Defines how incoming messages are displayed/indicated when the handset is placed in the charger.

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 instead in **Device → Settings → In charger action**.

To silence only messages without breakthrough (low/normal priority), enable the **Sound off** parameter instead in **Device → Settings → In charger action**.

- **Receive messages in charger** — Defines if received messages are saved or discarded when the handset is placed in the charger.

For more information, see 3.11.4 Rotate Display Text, page 59.

### 3.7.1 Configure Message Alerts with Beep Codes

The handset can map beep codes sent from a system/an application to different message alerts. There are several ways to treat the beep codes.

Message alerts can be configured in WinPDM/WSM3/CPDM3 DM in **User Profiles → Normal/Profile X → Sound and Alerts → Message alert**.

Only the parameter **Custom sounds according to beep code** can be customized. For more information, see Customize the Default Handset Beeps, page 92.

#### 3.7.1.1 Configure Beeps or High Beeps According to Beep Code

| 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 |

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

To configure **Beeps** or **High beeps**, perform the following steps:

1. Select **User profiles → Normal/Profile X → Sound and alerts**.
2. In the **Message alert** drop-down list, select **Beeps according to beep code** or **High beeps according to beep code**.

#### 3.7.1.2 Enhanced Beeps According to Beep Code

| 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 sent from a system or application | Corresponding sound from the handset |
|---|---|
| Beep code 6 | Alarm sweep |
| Beep code 7 | Siren |

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

1. Select **User profiles → Normal/Profile X → Sound and alerts**.
2. In the **Message alert** drop-down list, select **Enhanced beeps according to beep code**.

#### 3.7.1.3 Custom Sounds According to Beep Code

| 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 |

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.

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. Also use custom sound, if it is desired to customize any of the default handset beeps (Beeps and Enhanced beeps), see Appendix B Configure Custom Sounds, page 90.

### Create Customized Sound

1. Select **Audio → Custom sounds → Custom sound X** (where X represent 1–10).
2. Set the following parameters:
   - **Label** – The name of the custom sound (required). The name is visible when mapping the custom sound to a beep code later on.
   - **Melody** – The text string represents a non-polyphonic sound. By default, example of melodies, which are based on Enhanced beeps, are set for Custom Sound 1–7, see Appendix B Configure Custom Sounds, page 90.
   - **Beat** – The tempo in beats per minute to be used when playing the sound.
   - **Style** – The ratio of note to rest period to be used when playing the sound.
   - **Instrument** – The instrument to be used when playing the sound.

### Map Beep Codes to Customized Sounds

1. Select **Audio → Custom message alert**.
2. In the **Beep code** drop-down lists, select the customized sounds (8–10 available) to be used for respective beep codes.

**Enable Customized Sound**

1. Select **User profiles → Profile X → Sound and alerts**.
2. In the **Message alert** drop-down list, select **Custom sounds according to beep code**.

### 3.7.2 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 → Unite**.
2. In the **Message Retransmit Limit**, set the maximum number of retransmissions.

### 3.7.3 Examples of TTR and TTP Settings

**Example 1**

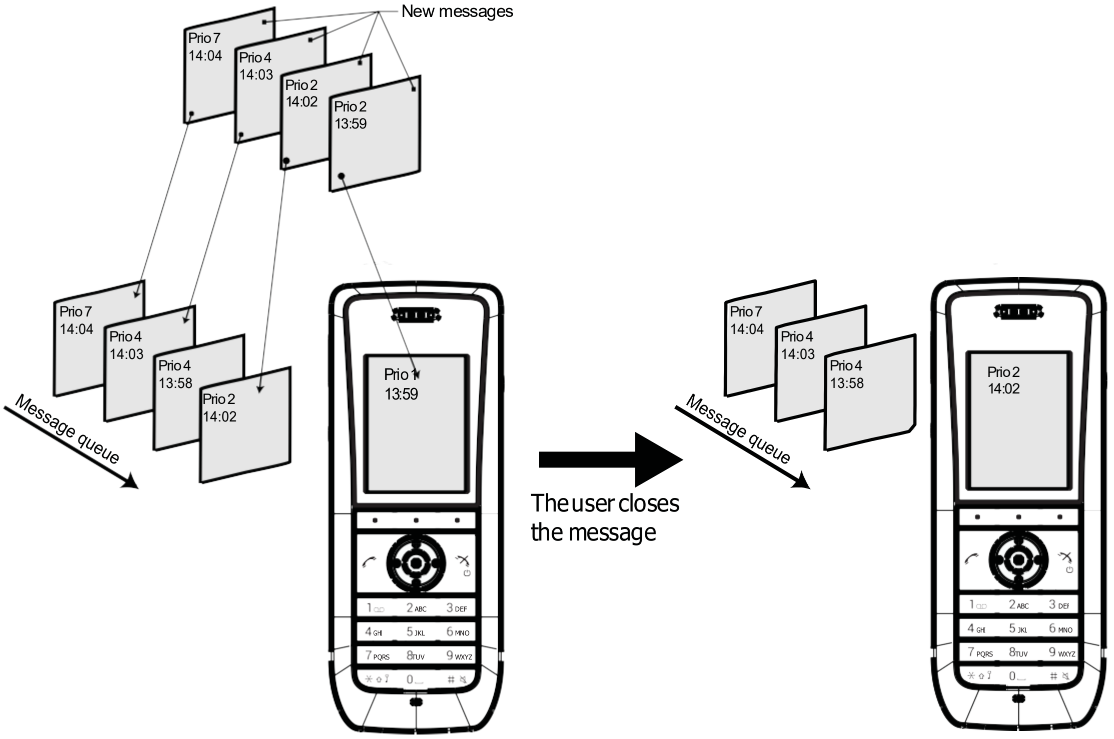
This example describes the message handling with the following message settings:

TTP – Prioritize forever

TTR – Close manually

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

*Figure 5. Queuing and Prioritizing for Messages with Equal Priorities*



In Figure 5. *Queuing and Prioritizing for Messages with Equal Priorities*, page 50, 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 Messaging inbox.

### Example 2

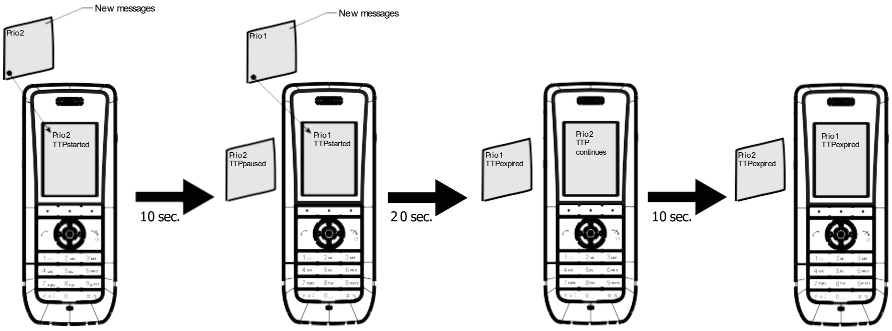
This example describes the message handling with the following message settings:

TTP – 20 seconds

TTR – Close manually

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 6. Queuing and Prioritizing for Messages with Different Priorities*



In Figure 6. *Queuing and Prioritizing for Messages with Different Priorities*, page 51, 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:

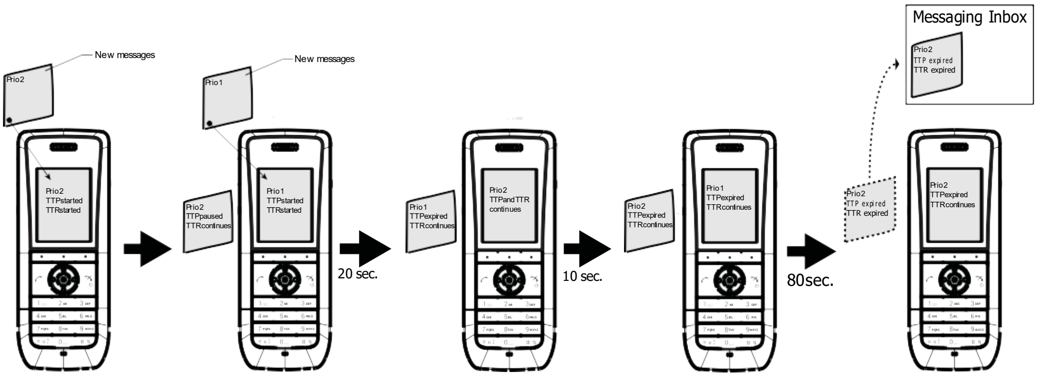
TTP – 20 seconds

TTR – 2 minutes

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 7. Message Handling without Manually Closing a Message*



In Figure 7. *Message Handling without Manually Closing a Message*, page 52, 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 Messaging inbox. When TTR expires for the message with priority 1, it is also indicated as an unread message in the Messaging inbox.

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

### Example 4

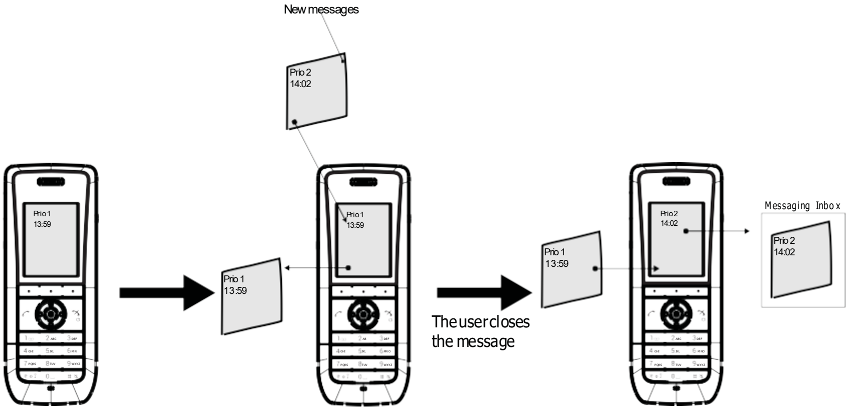
This example describes the message handling with the following message settings:

TTP – No prioritization

TTR – Close manually

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 8. Messages Displayed in Chronological Order Regardless of Priority*



In Figure 8. *Messages Displayed in Chronological Order Regardless of Priority*, page 53, 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 Messaging inbox.

## 3.8 Message Templates

Handsets can be configured with predefined messages using the message template function.

A predefined message can be used in the following ways:

- The user can decline the call but still acknowledge the receipt of the call by selecting a predefined message and sending it to the caller (requires a parameter setting, see 3.8.1 Configure the Handset for Message Templates, page 53 below).
- The user replies to an incoming text message by selecting a predefined message and sending it to the message sender (works by default).
- The user can construct a text message from a predefined message (works by default).

For additional information about how the message template function is used, see the Mitel 5634 VoWi-Fi Handset User Guide.

### 3.8.1 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 using WinPDM/WSM3/CPDM3 DM:

1. Select **User Profiles** → **Profile X** → **Answering**.
2. In the **Can reply with a message template when rejecting a call** drop-down list, select **Yes**. The dialog window `Reply with a message template?` appears when rejecting an incoming call.

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

### 3.8.2 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 in WinPDM/WSM3/CPDM3 DM:

1. Select **Device → Messaging → Message Template X** (where X is 1–5).
2. In the **Message text** field, write a message, then click **OK**.

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 failure of the message to arrive at the intended recipient, and a `Message failed` dialog window appears in the sender handset.

## 3.9 Alarm Settings

Applicable to 5634 Alarm only.

### 3.9.1 Common Alarm Settings

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

1. Select **Alarm → Common**.
2. Set any of the following parameters:
   - **Stored alarm data** — Information that is sent together with an alarm (for example a room number).
   - **Indicate triggered alarm with vibrator**
   - **Indicate triggered alarm with beep signal**

     If the parameter **Silent alarm** is set, no indication will be shown that an alarm has been sent or received, that is, there is no beep, vibrating alert, or dialog window.
   - **Password protect ALS** — Defines if a password is required to turn off the Acoustic Location Signal (ALS).
   - **Number for automatic call after alarm** — Defines which number the handset automatically calls after an alarm is sent. This number can also be dialed without sending an alarm, see 3.9.5 Call Predefined Number without Sending Alarm, page 56.

   See also 3.9.2 Push-Button Alarm, page 54– for additional parameter settings.

### 3.9.2 Push-Button Alarm

It is possible to configure how push-button alarms are handled in a system.

A push-button alarm can be activated by a user in two different ways:

- By a single long press
- By multiple presses

The following alarm types can be set:

- Push-button alarm
- Test alarm

To configure how the push-button alarm behave, perform the following steps:

1. Select one of the following:
   - **Alarm → Alarm on long press**
   - **Alarm → Alarm on multiple press**

2. Set any of the following parameters:

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

   - **Alarm type for long press** (or **Alarm type for multiple press**) — Defines which type of alarm is sent by a long press (or multiple press) on the Alarm button.
     **Test alarm**, **Push-button Alarm 1**, **Push-button Alarm 2**, or **Not used**.

     If **Not used** is selected, a predefined number can still be called automatically when pressing the Alarm button. For more information, see 3.9.5 Call Predefined Number without Sending Alarm, page 56.

   - **Text indication for alarm on long press** (or **Text indication for alarm on multiple press**).
     Enter a text to be displayed on the handset display when the alarm is triggered and sent.

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

   - **Duration for long press** (long press parameter only) — Defines how long the Alarm button should be pressed.
   - **Define multiple press** (multiple press parameter only) — Defines how many times the user must press the Alarm button to get a multiple press.
   - **Silent alarm** — If enabled, the handset does not show that an alarm has been triggered, that is, there is no sound signal, vibrating alert, dialog window, ALS, or notification light on the display.
   - **ALS** — It is a high-pitched sound used to locate the person triggering the alarm.

     If both parameters **ALS** and **Silent alarm** are set, ALS is not triggered.

     The ALS is paused if the automatic call after alarm is active. For more information, see 3.9.5 Call Predefined Number without Sending Alarm, page 56.

   - **Mode for automatic call after alarm** — The call can be established in the following ways:
     - **Off** – No call is established after alarm.
     - **Normal** – The call is established as an ordinary call.
     - **Loudspeaking** – The loudspeaker is turned on.
     - **Monitoring** – A one-way speech channel is established, that is, the called part can only listen to a conversation.

   For more information, see 3.9.1 Common Alarm Settings, page 54.
   Information about the handset’s location is sent along with an alarm. For more information, see 3.14 Location, page 61.

### 3.9.3 Test Alarm

To test if an alarm is working properly, perform the following steps:

1. In the **Alarm** menu, select **Alarm on long press** or **Alarm on multiple press**.
2. In the **Alarm type for long press** drop-down list (or **Alarm type for multiple press** drop-down list), select **Test alarm**.
3. In the **Text indication for alarm on multiple press** field (or **Text indication for alarm on long press)**, write the text to be shown in the handset display when the Alarm button is pressed.

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

4. Enter duration for the long press (between 0 to 5 s) or define the multiple press, that is, if a user must press 2, 3 or 4 times in a sequence on the Alarm button.

   If the duration for long press is 0 seconds, multiple press alarm cannot be used.

5. In the **ALS** drop-down list, select **Yes** to enable ALS.
6. In the **Mode for automatic call after alarm** drop-down list, select one of the following:
   - **Off** — The loudspeaker is turned off
   - **Normal** – The call is established as an ordinary call.
   - **Loudspeaker** – The loudspeaker is turned on.
   - **Monitoring** – The loudspeaker is muted and the microphone is on.
7. Select **Alarm → Common → Number for automatic call after alarm**. Enter the number to be called after the Alarm button is pressed (optional).
   The alarm can now be tested.

### 3.9.4 Emergency Call Alarm

1. Select **Alarm → Emergency call**
2. In the **Emergency call alarm** drop-down list, select one of the following:
   - **On** – An alarm is sent when the user calls an emergency number.
   - **Off** – No alarm is sent when the user calls an emergency number.
3. In the **Alarm type text** field, write the text to be shown in the handset display when an emergency call alarm is triggered. If this field is empty, the default text `Emergency call alarm` is shown.

For more information, see 3.6.8 Emergency Call Numbers, page 42.

### 3.9.5 Call Predefined Number without Sending Alarm

It is possible to use the push-button to automatically dial a predefined number without sending an alarm, that is, using the Alarm button only to call a predefined number. The following example describes how to configure the push-button (alarm on long press). The corresponding settings can also be configured for the push-button when it is pressed twice or more (alarm on multiple 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**.
4. In the **Alarm type for long press** drop-down list, select **Not used**.
5. In the **Mode for automatic call after alarm** drop-down list, select one of the following:
   - **Off** – No call is established after alarm.
   - **Normal** – The call is established as an ordinary call.
   - **Loudspeaking** – The loudspeaker is turned on.
   - **Monitoring** – A one-way speech channel is established, that is, the called part can only listen to a conversation.

Information about the handset's location is sent using an alarm (if available). For details, see 3.14 Location, page 61.

## 3.10 Regional Settings

### 3.10.1 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** is selected, a string must be entered in the **Time zone string** field to define the time zone.
   For time zones, see `http://www.timeanddate.com`.

   Only unquoted format is supported.

   Enter the time zone string to automatically update for daylight saving time: `<String = StdOffset [Dst[Offset], Date/Time, Date/Time]>`

   – **Std** – Time zone (for example EST for Eastern Standard Time).

   – **Offset** – Time difference between the time zone and the UTC (Universal Time Coordinator).

   – **Dst** – Daylight saving time zone (for example EDT for Eastern Daylight Time).

   – **Second Offset** – Time difference between the daylight saving time and the UTC.

   – **Date/Time, Date/Time** – 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

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

   Example:
   North Carolina is located in the Eastern Time Zone. Eastern Standard Time (EST) is 5 hours behind UTC (StdOffset = EST5), the Eastern Daylight Time (EDT) is 4 hours behind UTC (DstOffset = EDT4). 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>`
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 one of the following time formats.

   – 12:00 (AM/PM)

   – 24:00
7. In the **Date format** drop-down list, select the required date format.

### 3.10.2 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.

### 3.10.3 Dialing Tone Pattern

To define the tone pattern to use when dialing, perform the following steps:

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

## 3.11 Display

### 3.11.1 Hide Menu Items

It is possible to hide certain menu items in the handset.

To configure **Visibility**, perform the following steps:

1. Select **Customization → Visibility**.
2. Select **Hide**, **Show**, or **Read only** for the applicable menu items in the drop-down lists. If **Read only** is selected, the menu item is visible in the handset, but cannot be edited by the user.

   Several menu items of the following categories can be hidden:

   - **Connections**
   - **Calls**
   - **Contacts**
   - **Shortcuts**
   - **Messaging** (Applicable to 5634 and 5634 Services only.)
   - **Services**
   - **Profiles**
   - **Settings**

### 3.11.2 User Display Text

It defines the text to be shown on the display in idle mode. If nothing is entered in this text field, the endpoint ID is displayed.

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

### 3.11.3 User Display Number

It defines the number to be shown on the display in idle mode. If this parameter is empty, the Endpoint number is shown.

1. Select **Device → Settings**.
2. In the **User display number** field, enter the number to be displayed.

### 3.11.4 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. It can also be configured in the handset menu.

1. Select **Device → Settings**.
2. In the **Rotate display text** list, select **Off** or **On**.

### 3.11.5 Font Style

The display font style can be changed to bold for improved readability. It can also be configured in the handset menu.

1. Select **Device → Settings**.
2. In the **Font style** list, select **Normal** or **Bold**.

### 3.11.6 Backlight Timeout

The **Backlight timeout** option defines the number of seconds before the backlight of the handset is turned off 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 s).

### 3.11.7 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** – Maximum backlight is used.
   - **Power save** – Reduced backlight is used.

### 3.11.8 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** – Time and status, for example message indication, is shown on the screen saver.
   - **Black** – No information is shown on the screen saver.
   - **Black also in call** – The **Black** screen saver (with no information) is shown also during phone calls.

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

The screen saver can also be configured in the handset menu.

## 3.12 Services

Applicable to 5634 Services and 5634 Alarm only.

It is possible to configure up to 10 services that can be accessed from the handset's **Services** menu.

1. Select **Services**.
2. Select in the range of 1–10.
3. In the **Service name** field, enter the name of the service to be displayed in the handset's **Services** menu.
4. Under **Service function**, select the service to be used:
   - **Phone Call**
   - **Send data** (predefined data and/or prompt for the data)
   - **Send a message** (prompt for the message text)
   - **Push-to-Talk**
   - **Edit alarm data**
5. In the **Service user data** field, enter the data to be sent/dialed when using the service.

   This field is not applicable for PTT.
6. In the **Service prefix for user data** field, enter the prefix for the service user data (if needed).
7. In the **Service index** field, enter the corresponding index used for PTT. For example, if PTT group 1 is configured (located under **Push-To-Talk → 1**), the service index must be set to **1**.

   This field is only applicable for PTT.

   If the PTT is not configured, continue, with 3.13 Push-to-Talk Group Call, page 60.

It is also possible to configure soft keys to reach services quickly, see 3.4.17 Shortcuts, page 25.

## 3.13 Push-to-Talk Group Call

Applicable to 5634 Services and 5634 Alarm only.

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

- The group number of the PTT group defined in WinPDM/WSM3/CPDM3 DM
- The phone number to the conference bridge

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.

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

1. Select **Push-To-Talk → X** (where X represents 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.
3. If it is desired to have the automatic key lock on during an ongoing call, select **Device → Settings**. In the **Automatic key lock** drop-down list, change the automatic key lock setting to **On**. For more information, see 3.4.1 Automatic Key Lock, page 17 and 3.4.4 Automatic Lock Time, page 18.
4. A Service can be configured to access the PTT session from the handset. If not configured, continue with 3.12 Services, page 60.

The **In call** menu can be hidden for PTT calls.

## 3.14 Location

Applicable to 5634 Services and 5634 Alarm only.

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

The following RTLS solutions are supported:

- Cisco MSE — The handset must be configured to use this option.
- AiRISTA Flow RTLS — The handset must be configured to use this option.

The following can be configured in the **Location** menu of the WinPDM/WSM3/CPDM3 DM:

- **BLE location**— For more information, see 3.14.1 Enable BLE Location, page 61.

To allow sending location information when entering the range of an IR, LF, or BLE location device, which is defined as a special location, select **On** in the **Special location** drop-down list.

### 3.14.1 Enable BLE Location

Applicable to 5634 Services and 5634 Alarm only.

When this parameter is enabled the identification of the four latest detected BLE Locators is included in an alarm or location request.

To enable BLE location, perform the following steps:

1. In the **BLE location** drop-down list, select **On**.

2. Configure the following parameters:
   - **BLE idle duration** — Defines the idle time (in seconds) between BLE scans. If the idle duration is zero, the handset scans continuously.
   - **BLE scan duration** — Defines (in seconds) for how long the handset should scan.
   - **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.
   - **BLE RSSI threshold** — Defines (in dBm) the RSSI threshold for a BLE location. The handset filters out any BLE location below the set RSSI.
   - **BLE UUID filter** — Defines the UUID that the handset should scan for.

### 3.14.2 Configure Handset for Cisco MSE or AiRISTA Flow RTLS Solution

Applicable to 5634 Services and 5634 Alarm only.

1. Select **Location → Common**.
2. In the **WLAN location scanning** drop-down list, select **On**.
3. In the **WLAN scanning interval** field, set the time between the scanning periods.
   Close scanning periods and frequent scans per period shorten the battery time.
4. In the **WLAN scans per scanning period** drop-down list, select how many scans should be performed during each scanning period.
   Close scanning periods and frequent scans per period shorten the battery time.
   If the AiRISTA Flow RTLS solution is used, also perform the following step.
5. Select **Location → AiRISTA Flow**, and configure the following parameters:
   - **AiRISTA Flow Location Scanning** — If enabled, location information is sent to the specified AiRISTA Flow RTLS.
   - **IP address** — Defines the IP address of the AiRISTA Flow RTLS server, to which the handset reports locations.
   - **Listening port** — Defines the port the AiRISTA Flow RTLS server is listening to.

# 4 System Deployment Planning

## 4.1 Site Survey Tool

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

The built-in tools provide 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.

## 4.2 Scan the Channels

To be able to use the site survey functions in the handset, configure the site survey functions correctly.

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 instance, 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**.

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.

There are two ways of scanning channels:

- Scan all channels
  See 4.2.1 Scan All Channels, page 63.
- Scan a specific channel
  See 4.2.2 Scan a Specific Channel, page 63.

### 4.2.1 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.

### 4.2.2 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.

### 4.3.1 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**.

### 4.3.2 Range Beep on a Configurable RSSI Threshold

By enabling **Range beep**, the handset gives a beep sound when the signal goes below the selected threshold. To configure this parameter, perform the following steps:

1. Go to the **Site Survey Tool** menu using one of the followings ways:
   - If the handset has been factory-reset or not configured, enter the Admin access code and select **Site survey tool** in idle mode.
   - If the handset has been configured, in the handset menu, select **Settings** and enter the Admin access code.
2. Select **Range beep**.
3. Select one of the following:
   - **On** – Activates the range beeps.
   - **Off** – Deactivates the range beeps.

For more information, see 2.2.3 Deploy the Handset Using the Admin Menu, page 7.

## 4.4 Location Survey

The location survey function makes it possible to use Site survey mode for AiRISTA Flow that causes location scanning to be performed at intervals of 1 s.

## 4.5 BLE Location survey

1. In the Admin menu of the handset, select **Site survey tool → Location survey**.
2. Select the following:
   - **BLE location survey** — Applicable to 5634 Services and 5634 Alarm only.

For more information, see 3.4.21 System Administration in the Handset, page 28.

## 4.6 BLE Beacon Scan

1. In the Admin menu of the handset, select **Site survey tool → BLE beacon scan**.
2. It is possible to repeat the scan by selecting **Rescan**.

For more information, see 3.4.21 System Administration in the Handset, page 28.

# 5 Maintenance

## 5.1 Maintaining the Handset

In an existing VoWiFi system, it is important to be able to replace handsets, install new handsets, and replace faulty handsets. The recommended procedure is to use a template with basic network settings created in the WinPDM/WSM3/CPDM3 DM, and then import the rest of the settings that were created by the templates.

It is also important to be able to upgrade system parameters and security settings in the handsets. These upgrades are preferably done in WSM3/CPDM3 DM, if available.

If WinPDM/WSM3/CPDM3 DM is used, perform one of the following:

- To install a new handset, see 2.3.2 Configure the Handset Using the Admin Menu, page 8.
- To create spare handsets to be used when broken handsets need to be replaced later on, see 5.1.1 Configure Spare Handsets without a Number in Large Systems, page 66.

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

- To install a new handset, see 2.2.2 Deploy the Handset Using WinPDM, page 6.
- To replace a broken handset, see 5.2.4 Replace the Handset using WinPDM, page 73.

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

In VoWiFi systems where WinPDM/WSM3/CPDM3 DM is used, it is recommended to configure a few spare handsets without a number to be able to quickly replace a broken handset later on.

For more information, see and 2.2.1.4 Apply a Template to a Handset without a Number, page 5.

### 5.1.2 Handset Software Upgrade

Read the software release notes before changing the software.

The handset software can be upgraded using WinPDM/WSM3/CPDM3 DM.

#### 5.1.2.1 Upgrade Software using WSM3/CPDM3 DM

The handset software can be upgraded using WSM3/CPDM3 DM. Perform the following steps:

1. Open the **Devices** tab and select the handsets to be upgraded.
2. Right-click and click **Upgrade software...**.
3. In the **Available software** drop-down list, select the desired software file (`.bin`).
   If needed, import the software file to be used by clicking **Import**. Locate the software file (`.bin` or `.pkg`) and click **Open**.
4. In the **Upgrade** section and **Activate new software** section, select when the software is upgraded and activated on the handset, respectively.
5. Click **OK**. The dialog window `Shutting down` followed by `Remotely updated` is shown in the handset display.

It is also possible to upgrade several handsets of the same device type simultaneously using the Baseline function in the WSM3/CPDM3 DM.

### 5.1.3 Upgrade Handset Functionality Using Licenses

Users can upgrade a handset by downloading a license.

The following licenses are available:

- Mitel 5634 Services License
- Mitel 5634 Services to Alarm Upgrade License

There are three alternatives to upgrade a handset:

- Automatic upgrade, see 5.1.3.1 Automatic License Upgrade, page 67.
- License upgrade using import/export, see 5.1.3.2 Upgrade License Using Import/Export, page 67.
- Manual upgrade, see 5.1.3.3 Manual License Upgrade, page 68.

A license move from one handset to another requires internet access from either the PC (using WinPDM) or the WSM3/CPDM3.

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

#### 5.1.3.1 Automatic License Upgrade

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

1. Open the WinPDM.
2. Place the handset in the Mitel 5634 Desktop Programmer cradle.
   The first time the handset logs on the WinPDM, the license key is automatically downloaded to the handset, go to Item 4., page 67.
3. If the handset is logged on to the WinPDM after the first time, no automatic check for licenses is done. Synchronize the WinPDM and license server as follows:
   - Select the **Licences** tab.
   - Right-click the handset in the list.
   - Select **Refresh**.

   The license key is downloaded to the handset.
4. The handset restarts. See also 5.1.3 Upgrade Handset Functionality Using Licenses, page 67 to view the handset’s license option(s).
   If the handset is updated to a new device type (to 5634 or 5634 Services), both the new device and the old device is displayed in WinPDM. The old device has to be manually removed.

#### 5.1.3.2 Upgrade License Using Import/Export

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

To upgrade the license, perform the following steps:

1. Place the handset in the Mitel 5634 Desktop Programmer cradle.
2. Open the WinPDM.
   - Select the **Licences** tab.
   - Right-click the handset(s) in the list.
   - Select **Export**.

- Save the file on a computer with an internet connection to access the License Web later on.

3. In a web browser, enter the following address: `https://www.ascom-ws.com`

   The License Web is used for the following:

   - Importing the product information file
   - Viewing/purchasing the license(s) for the handset(s)
   - Downloading the license file containing the license key(s) for the handset(s)

   For more information on how to use the License Web, see the online help on the License Web or the *IP-DECT System (Global) and WiFi System (EMEA) Wireless Handset Advanced Capability Licensing Guide*.

4. When the license file (`.xml`) containing the license key(s) is downloaded from the License Web, select **File → Import → Licences** in the WinPDM to import the file.

5. When the file is imported, the license key(s) is downloaded to the handset(s) and the handset restarts. For more information, see 5.1.3 Upgrade Handset Functionality Using Licenses, page 67 to view the handset's license option(s).
   If the handset is updated to a new device type (to 5634 or 5634 Services), both the new device and the old device is displayed in WinPDM. The old device has to be manually removed.

#### 5.1.3.3 Manual License Upgrade

Use this option if the serial numbers of the handset cannot be exported to a file because WinPDM is not in use. The serial number(s) must be manually entered in the License Web to get the corresponding license key for the handset. The license key must also be manually entered in the handset. For more information on how to use the License Web, see the online help on the License Web or the *IP-DECT System (Global) and WiFi System (EMEA) Wireless Handset Advanced Capability Licensing Guide*.

If several handsets are upgraded, it is recommended to use 5.1.3.2 Upgrade License Using Import/Export, page 67.

The license key is added using the Admin menu in the handset. For more information, see 3.4.21 System Administration in the Handset, page 28.

To manually upgrade the license, perform the following steps:

1. In the handset menu, select **Settings**.
2. Enter the Admin menu using the Admin access code.
3. Select **Enter license key**.
4. Enter license key without blanks.
5. Press **OK**.

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

If the handset is updated to a new device type (to 5634 or 5634 Services), both the new device and the old device is displayed in WinPDM. The old device has to be manually removed.

#### 5.1.3.4 Move License

It is possible to move a product license (5634 Alarm or 5634 Services) to an unlicensed handset. Any optional licenses follow. For example, a 5634 Alarm license can be moved from a handset with a broken display to an unlicensed handset. The broken handset can then be sent for repairs.

It is required to have WinPDM/WSM3/CPDM3 DM that supports the license move function and to have connection to the license server.

### Move a License Using the WinPDM

1. Place the licensed handset in the Mitel 5634 Desktop Programmer.
2. On the **Licenses** tab, select the handset online.
3. On the **License** menu, click **Move license…**.
4. In the **Move license** dialog, select the unlicensed handset and click **OK**.
   The handset in the Mitel 5634 Desktop Programmer is restarted.
5. Place the unlicensed handset in the Mitel 5634 Desktop Programmer.
6. On the **Licenses** tab, select the handset online.
7. On the **License** menu, click **Refresh**.
   The handset in the Mitel 5634 Desktop Programmer is restarted.

### Move a License Using the WSM3/CPDM3 DM

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

   The handset is restarted.

### 5.1.4 Perform a Factory Reset

The factory reset of a handset can be performed using WinPDM/WSM3/CPDM3 DM or the handset. A factory reset restores all configuration settings to their default values. For example, PBX subscriptions, contacts, messages, certificate, and so on are removed. The software and licenses are left intact.

To perform a factory reset using WinPDM/WSM3/CPDM3 DM, perform the following steps:

1. In the **Devices** tab, mark the handset to be factory reset. Note that the handset must be online.
2. In the **Device** menu, select **Factory reset**. Alternatively, right-click the handset and select **Factory reset**.
3. In the **Reset devices** window that appears, click **Yes**. The handset restarts.

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

1. In the handset menu, select **Settings**.
2. Enter the Admin access code to access the Admin menu.
3. Select **Factory Reset**.
4. In the **Reset portable?** window that appears, click **Yes**. The handset restarts.

## 5.2 Handset Replacement

It is possible to replace with 5634, or a broken handset with a spare handset. Handsets registered in WinPDM/WSM3/CPDM3 DM are associated with a device type, device ID, and extension. During the replacement procedure, the broken/old handset’s device type and extension are associated with the spare handset’s device ID.

If the spare handset has been previously used, perform a factory reset. For more information, see 5.1.4 Perform a Factory Reset, page 69.

Handsets can be replaced in the following ways:

- Using the WinPDM/WSM3/CPDM3 DM with the network template already applied to the spare handset(s) to log in later. For more information, see 5.2.2 Replace the Handset using WSM3/CPDM3 DM, page 70.
- Using both WinPDM and the WSM3/CPDM3 DM with the network template not yet applied to the spare handset
(s) to log in later. For more information, see 5.2.3 Replace the Handset using WinPDM and WSM3/CPDM3 DM, page 71.
- Using only WinPDM. For more information, see 5.2.4 Replace the Handset using WinPDM, page 73.

The following data is replaced during a replacement:

- User parameters
- Contacts (entered by the user)

The following data is not replaced during a replacement:

- Call list
- Messages
- Company phone book
- Certificates
- Licenses

A handset’s license(s) can be moved to an unlicensed handset (Mitel 56xx).

For more information, see Replace and Move Licenses in the WSM3/CPDM3 DM, page 71.

### 5.2.1 Parameter Migration

The parameter migration feature allows templates and numbers of a certain handset variant to be applied to any compatible handset. Every 5624 and 5634 handset variant is compatible, which means that it is possible to replace a 5624 with a 5634.

The same template can be used for different 5634 variants, such as 5634 Alarm and 5634. 5634 Alarm specific parameters are ignored by the 5634.

It is not guaranteed that parameter migration results in the optimal configuration of the destination handset. For example, parameters related to features not present in the source handset are left at their default values in the destination handset. That is why, it is recommended to check the configuration of the destination handset after parameter migration and make sure that the configuration is correct.

### 5.2.2 Replace the Handset using WSM3/CPDM3 DM

The following two replacement procedures are available:

- If the broken/old handset and the spare handset have the same device type and functionality license. For more information, see Replace without Moving Licenses in the WSM3/CPDM3 DM, page 71.
- If the broken/old handset and the spare handset do not have the same device type or functionality license, or neither, the license must be moved to the spare handset.
For more information, see Replace and Move Licenses in the WSM3/CPDM3 DM, page 71.

### Replace without Moving Licenses in the WSM3/CPDM3 DM

1. In both handsets, go to the Admin menu and select **License** to check that the new handset is of the correct variant. For example, if you need alarm functionality, make sure that the handset is a 5634 Alarm.
   If the login screen is displayed in the spare handset, press **Info**, and select **License**.
2. If the broken/old handset is online in the WSM3/CPDM3 DM, switch off the handset to make it offline.
3. Take a spare handset prepared with the network settings (including the IP address to the WSM3/CPDM3).
4. Enter the broken/old handset's number and leave the password field blank. Press **Login**.
   The spare handset is automatically updated from the WSM3/CPDM3 DM and might be restarted depending on the changed settings. The last stored settings for the broken/old handset in the WSM3/CPDM3 DM are transferred to the spare handset.

### Replace and Move Licenses in the WSM3/CPDM3 DM

The spare handset must be an unlicensed Mitel 56xx to be able to move the licenses to the spare handset. To check that the handset is unlicensed, enter `*#34#` in idle mode and select **License**. Only Mitel 56xx must be displayed here.

1. Make sure that the broken/old handset is saved (indicated by a ✓) in the **Saved** column of the WSM3/CPDM3 DM. If not, right-click the broken/old handset in the **Numbers** tab and select **Save**.
2. Switch off the broken/old handset. The handset appears as offline in the WSM3/CPDM3 DM.
3. Take an unlicensed spare handset (Mitel 56xx) prepared with the network settings (including the IP address of the WSM3/CPDM3).
4. Enter the broken/old handset's number and leave the password field blank. Press **Login**. The handset is now online.
5. Switch off the spare handset. The handset appears as offline.
6. Switch on the broken/old handset. The handset appears as online.
7. Select the **Licenses** tab.
8. Right-click the broken/old handset and select **Move license…**.
9. In the **Move license** window, select the Mitel 56xx that should receive the license and press **OK**.
10. The broken/old handset restarts and has now become a Mitel 56xx. Switch off the broken/old handset. The handset appears as offline.
11. Switch on the spare handset. The handset appears as online.
12. Select the **Licenses** tab. Right-click the spare handset and select **Refresh**.
    The spare handset is automatically updated from the WSM3/CPDM3 DM and restarted. The last stored settings and licenses for the broken/old handset are transferred to the spare handset.

## 5.2.3 Replace the Handset using WinPDM and WSM3/CPDM3 DM

If the spare handset to be used must be factory reset or no network template has been applied, the network template needs to be applied to the spare handset in WinPDM. When the network template is added, the handset can log in to the WSM3/CPDM3 DM.

The following two replacement procedures are available:

- If the broken/old handset and the spare handset have the same device type and functionality license. For more information, see Replace without Moving Licenses Using WinPDM and WSM3/CPDM3 DM, page 72.

- If the broken/old handset and the spare handset do not have the same device type or functionality license, or neither, the license must be moved to the spare handset.
  For more information, see Replace and Move License Using WinPDM and WSM3/CPDM3 DM, page 72.

### Replace without Moving Licenses Using WinPDM and WSM3/CPDM3 DM

1. In both handsets, go to the Admin menu and select **License** to check that the new handset is of the correct variant. For example, if you need alarm functionality, make sure that the handset is a 5634 Alarm.
2. Make sure that the broken/old handset is saved (indicated by a ✓) in the **Saved** column of the WSM3/CPDM3 DM. If not, right-click the broken/old handset in the **Numbers** tab and select **Save**.
3. Switch off the broken/old handset. The handset appears as offline in the WSM3/CPDM3 DM.
   If the spare handset is not prepared with the basic network settings, also perform step Item 4., page 72 – step Item 7., page 72.
4. Open WinPDM.
5. Place the spare handset in the Mitel 5634 Desktop Programmer cradle.
6. Run the template with the basic network settings as follows (see 2.2.1.2 Create a Template in WinPDM/ WSM3/CPDM3 DM, page 4):
   - Network settings in **Network → General**:
     Under the respective network (**Network A**, **Network B**, **Network C**, or **Network D**), set the required parameters, for example, system settings for WLAN, such as **SSID**, **Security mode**, and any certificates for 802.1X. If using a security mode that requires certificates, also use an NTP server to assure the correct time in the handset, as certificates are only valid within a certain time.
   - VoIP settings in the **VoIP** menu:
     Configure, for example, VoIP information, SIP proxy ID and address.
   - Syslog settings in **Device → Log**:
     To be able to set the **Syslog server IP address**, the parameter **Syslog** must be enabled by selecting **On**.
   - Unite settings in **Device → Unite**:
     Enter the IP address and password (if any) to the WSM3/CPDM3.
7. Remove the handset from the Mitel 5634 Desktop Programmer cradle. The handset restarts, depending on the parameter changes.
8. Enter the broken/old handset's number and leave the password field blank. Press **Login**.
   The spare handset is automatically updated from the WSM3/CPDM3 DM and might be restarted depending on the changed settings. The last stored settings for the broken/old handset in the WSM3/CPDM3 DM are transferred to the spare handset.

### Replace and Move License Using WinPDM and WSM3/CPDM3 DM

The spare handset must be an unlicensed Mitel 56xx to be able to move the licenses to the spare handset. To check that the handset is unlicensed, enter `*#34#` in idle mode and select **License**. Only Mitel 56xx must be displayed here.

1. Make sure that the broken/old handset is saved (indicated by a ✓) in the **Saved** column of the WSM3/CPDM3 DM. If not, right-click the broken/old handset in the **Numbers** tab and select **Save**.
2. Switch off the broken/old handset to take the handset offline.
3. Open the WinPDM.
4. Place the unlicensed spare handset in the Mitel 5634 Desktop Programmer cradle.

5. Run the template with the basic network settings as follows (see 2.2.1.2 Create a Template in WinPDM/ WSM3/CPDM3 DM, page 4):
   - Network settings in **Network → General**:
     Under the respective network (**Network A**, **Network B**, **Network C**, or **Network D**), set the required parameters, for example, system settings for WLAN, such as **SSID**, **Security mode**, and any certificates for 802.1X. If using a security mode that requires certificates, also use an NTP server to assure the correct time in the handset, as certificates are only valid within a certain time.
   - VoIP settings in the **VoIP** menu:
     Configure, for example, VoIP information, SIP proxy ID and address.
   - Syslog settings in **Device → Log**:
     To be able to set the **Syslog server IP address**, the parameter **Syslog** must be enabled by selecting **On**.
   - Unite settings in **Device → Unite**:
     Enter the IP address and password (if any) to the WSM3/CPDM3.
6. Remove the handset from the Mitel 5634 Desktop Programmer cradle. The handset restarts, depending on the parameter changes.
7. Enter the broken/old handset’s number and leave the password field blank. Press **Login**.
8. Switch off the spare handset. The handset appears as offline.
9. Switch on the broken/old handset. The handset appears as online.
10. Select the **Licenses** tab.
11. Right-click the broken/old handset and select **Move license…**.
12. In the **Move license** window, select the Mitel 56xx that should receive the license and press **OK**.
13. The broken/old handset restarts and has now become a Mitel 56xx. Switch off the broken/old handset. The handset appears as offline.
14. Switch on the spare handset. The handset appears as online.
15. Select the **Licenses** tab. Right-click the spare handset and select **Refresh**.
    The spare handset is automatically updated from the WSM3/CPDM3 DM and restarted. The last stored settings and licenses for the broken/old handset are transferred to the spare handset.

### 5.2.4 Replace the Handset using WinPDM

Replacement through WinPDM is used in small VoWiFi systems or when WSM3/CPDM3 DM is not

available. The following two replacement procedures are available:

- If the broken/old handset and the spare handset have the same device type and functionality license.
  For more information, see Replace without Moving Licenses Using WinPDM, page 73.
- If the broken/old handset and the spare handset do not have the same device type or functionality license, or neither, the license must be moved to the spare handset.
  For more information, see Replace and Move Licenses Using WinPDM, page 74.

#### Replace without Moving Licenses Using WinPDM

1. In both handsets, go to the Admin menu and select **License** to check that the new handset is of the correct variant. For example, if you need alarm functionality, make sure that the handset is a 5634 Alarm.
   Alternatively, if the spare handset has been factory reset, press **Info** and select **License**.
2. Place the broken/old handset in the Mitel 5634 Desktop Programmer cradle.

3. Open the WinPDM.
4. Make sure that the broken/old handset is saved in the WinPDM (indicated by a ✓ ) in the **Saved** column. If not, right-click the broken/old handset in the **Numbers** tab and select **Save**.
5. Place the spare handset in the Mitel 5634 Desktop Programmer cradle.
6. A **Found Device Wizard** window appears. Select **Associate with Number** and click **Next >**.
7. In the list, select the broken/old handset to be replaced with the spare handset and click **OK**.

### Replace and Move Licenses Using WinPDM

The spare handset must be an unlicensed Mitel 56xx to be able to move the licenses to the spare handset. To check that the handset is unlicensed, enter `*#34#` in idle mode and select **License**. Only Mitel 56xx must be displayed here.

1. Place the broken/old handset in the Mitel 5634 Desktop Programmer cradle.
2. Make sure that the broken/old handset is saved in the WinPDM (indicated by a ✓ ) in the **Saved** column. If not, right-click the broken/old handset in the **Numbers** tab and select **Save**.
3. Remove the broken/old handset from the Mitel 5634 Desktop Programmer cradle.
4. Place the unlicensed spare handset in the Mitel 5634 Desktop Programmer cradle.
5. Run the template with the basic network settings as follows (see 2.2.1.2 Create a Template in WinPDM/ WSM3/CPDM3 DM, page 4):
   - Network settings in **Network → General**:
     Under the respective network (**Network A**, **Network B**, **Network C**, or **Network D**), set the required parameters, for example, system settings for WLAN, such as **SSID**, **Security mode**, and any certificates for 802.1X. If using a security mode that requires certificates, also use an NTP server to assure the correct time in the handset, as certificates are only valid within a certain time.
   - VoIP settings in the **VoIP** menu:
     Configure, for example, VoIP information, SIP proxy ID and address.
   - Syslog settings in **Device → Log**:
     To be able to set the **Syslog server IP address**, the parameter **Syslog** must be enabled by selecting **On**.
   - Unite settings in **Device → Unite**:
     Enter the IP address and password (if any) to the WSM3/CPDM3.
6. Place the broken/old handset in the Mitel 5634 Desktop Programmer cradle.
7. In the WinPDM, select the **Licenses** tab.
8. Right-click the broken/old handset and select **Move license…**.
9. In the **Move license** window, select the Mitel 56xx that should receive the license and select **Do nothing**. The broken/old handset restarts and has now become a Mitel 56xx.
10. Remove the broken/old handset from theMitel 5634 Desktop Programmer cradle.
11. Place the spare handset in the Mitel 5634 Desktop Programmer cradle.
    The spare handset is restarted and the licenses for the broken/old handset has been transferred to the spare handset.
12. In the **Found Device Wizard** window, select **Associate with number** and click **Next >**.
13. In the list, select the broken/old handset to be replaced with the spare handset and click **OK**.
    The spare handset can be restarted and the settings for the broken/old handset in the WinPDM are transferred to the spare handset.

## 5.3 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 WinPDM/WSM3/CPDM3 DM.
2. Open the **Numbers** tab, and select the handset to be updated with a new number.
3. In the Number menu, select **Rename…**. Alternatively, right-click the handset and select **Rename…** from the menu that appears.
4. In the **New prefix** field, enter the new prefix (if needed).
5. In the **New number** field, enter the new number.

   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/WSM3/CPDM3 DM.
6. Click **OK**.
   The new number is synchronized with the handset when it is connected to WinPDM/WSM3/CPDM3 DM.

## 5.4 Update Parameters Using WinPDM/WSM3/CPDM3 DM

The parameter update in WinPDM/WSM3/CPDM3 DM starts when the handset is idle and does not interrupt an ongoing call.

Select only the parameters that are changed, if all parameters are selected, the system performance decreases.

1. Open WinPDM/WSM3/CPDM3 DM.
2. Create a new template with only the parameters to be changed.
3. Select the numbers that should be updated and apply the template.
   The handsets are automatically updated from the WSM3/CPDM3 DM and can be restarted depending on which parameters are changed.

Templates can be applied for several handsets under the **Templates** tab . Parameters or templates can be set on individual handsets under the **Numbers** tab.

## 5.5 Perform a Security Upgrade Using WSM3/CPDM3 DM

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

To change the WLAN password/authentication, perform the following steps:

1. Open the WSM3/CPDM3 DM.
2. Create a new template with the new security settings.
   - Security mode:

All required settings for the WLAN. For example User name, Password, Regulatory domain, and so on.

3. Apply the new template to the handsets.
   The handsets are automatically updated from WSM3/CPDM3 DM and restarted.

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

4. Change the security settings for the APs. The handsets are now able to access the WLAN.

## 5.6 Upgrade the Template

The upgrade procedure of the templates definition version is described in the Installation and Operation Manual, Portable Device Manager for Windows (WinPDM) or User Manual, Device Manager in WSM3/CPDM3.

## 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 Installation and Operation Manual, Portable Device Manager for Windows (WinPDM) or User Manual, Device Manager in WSM3/CPDM3.

## 5.8 Logging

### 5.8.1 Syslog

Enables logging of system events to a syslog server.

1. In WinPDM/WSM3/CPDM3 DM, select **Device → Log**.
2. In the **Syslog** drop-down list, select **On** to enable logging.

### 5.8.2 PCAP Capturing

If enabled, the selected data is sent as PCAP logs to the indicated output.

**PCAP to file**

PCAP logging is started by performing the following steps:

1. In WinPDM/WSM3/CPDM3 DM, select **Device → Log**.
2. In the **PCAP Capturing** drop-down list, select **PCAP to file**.

When the necessary logs have been collected, stop PCAP logging by preforming the following steps:

1. In WinPDM/WSM3/CPDM3 DM, select **Device → Log**.
2. In the **PCAP Capturing** drop-down list, select **Off**.

The PCAP files are not encrypted and can be extracted with USB or SFTP, and can be viewed using, for example, Wireshark. To reduce the size of the generated files, RTP packets are not included.

**Remote PCAP**

Configure a PC that receives the logs (for example with Wireshark) and start PCAP logging by performing the following steps:

1. In WinPDM/WSM3/CPDM3 DM, select **Device → Log**.

2. In the **PCAP Capturing** drop-down list, select **RPCAP**.

When the necessary logs have been collected, stop PCAP logging by performing the following steps:

1. In WinPDM/WSM3/CPDM3 DM, select **Device → Log**.
2. In the **PCAP Capturing** drop-down list, select **Off**.

Packet capturing can also be configured in the Admin menu of the handset. For more information, see 3.4.21.1 Admin Menu Tree in the Handset, page 29.

### 5.8.3 Save Logs

The handset continuously generates encrypted logs that can be sent for investigation to Mitel support in case any issue occurs. The following procedure explains how to collect these logs.

Logs are normally kept in volatile memory for a short period before they are deleted.

When this function is enabled, all logs that are collected for the defined period of time are also saved to persistent storage.

Logs already stored in volatile memory when the function is enabled are also written to persistent storage. This means that the function **Save once now** can be used to store logs of a problem that has occurred a short while ago.

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

Use SFTP or USB transfer to retrieve the saved logs and send them to Mitel support.

Depending on the nature of the issue, it may be required to change the default log levels as described in 5.8.6 Trace Configuration, page 78. This controls which logs are generated and must be set before the problem occurs.

#### Save Logs after a Problem Has Occurred

Right after a problem has occurred, it is possible to save the logs that show the problem even if **Save logs** was not previously enabled.

1. In WinPDM/WSM3/CPDM3 DM, select **Device → Log**.
2. In the **Save logs** drop-down list, select **Save once now**.

#### Continuously Save Logs from Memory to Flash

To continuously save logs while trying to reproduce the problem, use one of the time-limited variants:

1. In WinPDM/WSM3/CPDM3 DM, select **Device → Log**.
2. In the **Save logs** drop-down list, select **Save for X time**.

Log saving can also be configured in the Admin menu of the handset. For more information, see 3.4.21.1 Admin Menu Tree in the Handset, page 29.

### 5.8.4 Enable Sending Logs over SFTP

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. In WinPDM/WSM3/CPDM3 DM, select **Device → Log**.
2. In the **Enable Sending Logs over SFTP** drop-down list, select **On**.

### 5.8.5 SFTP Server Settings

1. In WinPDM/WSM3/CPDM3 DM, select **Device → Log**.
2. The following SFTP parameters can be configured:
   - **SFTP server IP address** — Defines the IP address of the remote server, which the handset sends logs to over SFTP.
   - **SFTP server authentication identity** — The name is used when logs is about to be sent to a remote server using SFTP.
   - **SFTP remote server authentication password** — The password is used when the SFTP remote server requires a password.

### 5.8.6 Trace Configuration

In normal operation, all extended trace levels should be set to **Normal** since excessive logging can affect handset performance. When logs are enabled, it is indicated by the text `Trace active` on the idle screen.

1. In WinPDM/WSM3/CPDM3 DM, select **Device → Log**.
2. 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**
   - **Set SAS Trace**
   - **Set Bluetooth Trace**
3. Select one of the following logging levels:
   - **Normal**
   - **Verbose**
   - **Extreme**

   These settings only affect the encrypted internal handset logs, not the remote syslog functionality.

Restore the handset to **Normal** logging after logs are captured, since extra logging can affect handset performance.

Trace configuration can also be performed in the Admin menu of the handset. For more information, see 3.4.21.1 Admin Menu Tree in the Handset, page 29.

### 5.8.7 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. In WinPDM/WSM3/CPDM3 DM, select **Device → Log**.
2. In the **Low-Level WLAN debug** field, enter the required string.

### 5.8.8 SNMP

Simple Network Management Protocol (SNMP) with version 1.0 is supported using the standard port for SNMP: UDP port 161.

There is no server functionality, so the handset status cannot be requested.

To enable SNMP, perform the following steps:

1. In WinPDM/WSM3/CPDM3 DM, 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.

# 6 Troubleshooting

This section offers possible solutions for common operational errors. In case you need further assistance, contact Mitel support.

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

## 6.1 Fault Symptoms

| Fault | Probable cause | Action or comment |
|---|---|---|
| It is not possible to mute the handset by long-pressing the Sound off key/Mute button.<br>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, or muted or bad speaker/microphone | 1. 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.<br>2. Check if the handsets are muted.<br>3. 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**. |
| Voice quality is bad. | Increased traffic load or interference. | 1. Check if QoS is working in both directions. Voice traffic should be prioritized on both the LAN and the WLAN.<br>2. Connect to other phones (wired, analogue or external) to define if it is the other end that may cause bad quality.<br>3. Do a site survey and check for areas with too low or too high coverage and other interfering 802.11 systems.<br>4. Do a network performance test to ensure the wired LAN/backbone has adequate capacity.<br>5. Use a spectrum analyzer and look fornon–802.11interference. |

| Fault | Probable cause | Action or comment |
|---|---|---|
| Battery life is short. | DTIM might not be set correctly.<br>U-APSD is not used.<br>Cisco MSE or AiRISTA Flow location client settings need to be changed. | 1. Check the **Beacon interval** and **DTIM** settings in the AP.<br>2. Verify the coverage, since low signal strength will make the handset to constantly search for other APs and thereby consuming more power.<br>3. Use a sniffer and check the amount of broadcast traffic that is transmitted on the WLAN.<br>4. Check if correct models of the chargers are used.<br>5. Verify with another battery.<br>6. If using Cisco MSE or AiRISTA Flow location client, change the settings. |
| The handset has operational issues. | There might be a bug in the handset software. | 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:<br>1. Switch off the handset.<br>2. 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.<br>After a handset has started up correctly, using this procedure is not possible for security reasons. |

## 6.2 Display Information

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

**Table 4 Error Messages, Probable Cause, and Recommended Action**

| Display message | Probable cause | Action or comment |
|---|---|---|
| No access<br>Displayed in idle mode and indicated by simultaneous vibration (if enabled), beep signal, and a dialog window (if enabled by the system administrator). | 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 WSM3/CPDM3. | Acknowledge the dialog window (if enabled) or press the mute button (the later keeps the dialog window visible).<br>The No access warning can also be set to indicate repeatedly, or only once. See 3.4.15 No Network and No Access Warning, page 23.<br>1. Check if the handset is connected to the correct SSID by entering the WLAN info screen. (An unconfigured 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.<br>2. 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.<br>3. Check if it is possible to ping the handset, WSM3/CPDM3, and SIP proxy from another PC.<br>4. Check the VoIP settings in the handset and SIP proxy.<br>5. Restart the handset. |
| No network<br>Displayed in idle mode and indicated with a short beep repeated every minute for 30 minutes.<br>It is also indicated by simultaneous vibration (if enabled) and a dialog window (if enabled by the system administrator). | The handset has lost WLAN connection. | Acknowledge the dialog window (if enabled) or press the mute button (the latter keeps the dialog window visible).<br>The No network warning can also be set to indicate only once, or be turned off completely. See 3.4.15 No Network and No Access Warning, page 23.<br>ⓘ When leaving a bad state for another bad state, the dialog window reopens, and the beep sounds again (if enabled). |

**Table 4 Error Messages, Probable Cause, and Recommended Action (continued)**

| Display message | Probable cause | Action or comment |
|---|---|---|
| `No network` (continued) | The handset is out of coverage, or faulty handset.<br>The handset cannot find the wireless infrastructure with settings matching those configured in the handset. | The beeps can be stopped with the mute button. Then go into range.<br>ℹ When re-entering the coverage area it can take a couple of minutes before the handset automatically has registered into the system.<br>1. Check the SSID. The SSID configured in the handset must be identical to the SSID configured in the system infrastructure.<br>2. Check the security settings. The security settings, that is, authentication and encryption must match the settings in the system infrastructure.<br>3. 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.<br>4. Check which channels are used. By default, the handset uses channels 1, 6, and 11 in the 2.4 GHz range and UNII-1 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 UNII-1 as these are the recommended settings.<br>5. Check that the correct Network (A, B, C or D) setting is selected. |

**Table 4 Error Messages, Probable Cause, and Recommended Action (continued)**

| Display message | Probable cause | Action or comment |
|---|---|---|
| `Voice only` | The handset is configured to use both SIP proxy and the WSM3/CPDM3, but has lost contact with the WSM3/CPDM3. | 1. Check the WSM3/CPDM3 address. Try to ping the WSM3/CPDM3 from another PC.<br>2. Remove the handset from the Mitel 5634 Desktop Programmer. When connected to the WinPDM through USB on the Mitel 5634 Desktop Programmer, the handset cannot connect to the WSM3/CPDM3 and may show `Voiceonly`.<br>3. If messaging is not used in the system, verify that the |
| `Messaging only` | The handset is configured to use both a SIP proxy and the WSM3/CPDM3 but has lost contact with the SIP proxy. | 1. Check the SIP proxy address. Try to ping the SIP proxy from another wireless client.<br>2. Try to send a message. The idle connection check interval to the WSM3/CPDM3 is much longer than to the SIP proxy. Sometimes when all network connection is lost, the handset shows `Messaging only` 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 WSM3/CPDM3. In this case the handset will eventually change to `No access`.<br>3. If the handset is supposed to use SIP proxy discovery, verify that the configured SIP proxy IP address is 0.0.0.0.<br>4. 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. |

**Table 4 Error Messages, Probable Cause, and Recommended Action (continued)**

| Display message | Probable cause | Action or comment |
|---|---|---|
| `SERVICE NEEDED`<br>An additional message is also displayed describing the cause of the error.<br>This message is only shown in English. | Faulty handset. | 1. Select the **Reboot** option on the left soft key.<br>2.<br>3. If the problem persists, try one of the following:<br>– Power off the handset using the **Off** soft key in the middle and send the handset for service.<br>– Perform a factory reset by selecting the**Factory** soft key on the right. |
| `Enter PIN code` | Phone lock is activated. | Enter the required PIN code. If the PIN code has been lost, enter a new PIN code or do a factory reset using WinPDM/WSM3/CPDM3 DM. |
| `Battery low, charge now` | The battery level is low. | Charge the handset or replace or charge the battery. |
| `Phone book is not available at the moment.` | 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/WSM3/CPDM3 DM.<br>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` | There is no voice mail number defined in the handset. | Define a voice mail number using WinPDM/WSM3/CPDM3 DM. |

# 7 Related Documents

- Mitel 5634 VoWi-Fi Handset Data Sheet
- Mitel 5634 VoWi-Fi Handset Quick Reference Guide
- Mitel 5634 VoWi-Fi Handset User Guide
- Mitel 5634 Desktop Programmer Data Sheet
- Portable Device Manager for Windows (WinPDM) Data Sheet
- WinPDM Installation and Operation Manual
- WSM3/CPDM3 User Manual
- WSM3/CPDM3 Installation and Operation Manual
- IP-DECT System (Global) and WiFi System (EMEA) Wireless Handset Advanced Capability Licensing Guide

# Appendix A Templates

Templates enable the configuration of all parameters of a handset from sound volume to keypad shortcuts.

Your supplier can provide example templates for different PBX/Unified communication servers. The handset has full functionality towards the PBX/Unified communication server even without a template. However, by using a template, the handset is customized for that PBX/Unified communication server with menu options for functions specific to PBX/Unified communication server.

## A.1 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 a number of handsets.

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

1. Open the WinPDM/WSM3/CPDM3 DM.
2. In the **Numbers** tab, right-click on the required handset.
3. Select **Use as template...** and enter a descriptive name for it.
4. 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** — A text string displayed in idle mode. The parameter is located in **Device → Settings**.
   - **Phone lock PIN code** — The security code used to unlock the keypad. The parameter is located in **Device → Settings → Locks**.
   - **Endpoint ID** — The identity/name of the user registered in the PBX. The parameter is located in **VoIP → General**.
   - **Admin access code** — The password used to enter the Admin menu of the handset. The parameter is located in **Device → General**.
   - **SCEP password** — The password used to authenticate the handset towards the SCEP server. The parameter is located in **Device → SCEP**.
5. Click **OK**.

## A.2 Manage Templates using WinPDM and WSM3/CPDM3 DM

When creating a template in both WinPDM and the WSM3/CPDM3 DM, the templates must be identical to avoid that the parameters override each other when synchronizing the handset.

It is possible to export templates from one device manager and import them to the other. For more information, see A.2.1 Export a Template, page 88, A.2.2 Import a Parameter File, page 89, and A.2.3 Import a Template, page 89.

### A.2.1 Export a Template

1. Open WinPDM/WSM3/CPDM3 DM.
2. In the **Templates** tab, select the template to be exported.

3. Select **Template → Export**. Alternatively, right-click on the template and select **Export…**. The Export templates window is opened.
4. Give the template (`*.tpl`) a descriptive name and click **Save**.

### A.2.2 Import a Parameter File

If the parameter file (`*.def`) is not already included, it needs to be added to WinPDM/WSM3/CPDM3 DM before importing the template.

To import the parameter file, perform the following steps:

1. Open WinPDM/WSM3/CPDM3 DM.
2. Select **File → File management**.
3. On the **Parameter definition** tab, click **Add**. The Import files window is opened.
4. Locate the parameter file (`*.def`), or the package file (`*.pkg`) where the parameter file is included. For more information, ask the supplier.
5. Click **Open** to import the file.

### A.2.3 Import a Template

1. Open WinPDM/WSM3/CPDM3 DM.
2. Select **File → Import → Templates…**. The Import templates window is opened.
3. Locate the template to be imported.
4. Click **Open** to import the template.

# Appendix B Configure Custom Sounds

Applicable to 5634 Services and 5634 Alarm only.

Before configuring custom sounds, it is recommended to have a basic knowledge on notes.

The **Melody** in a custom sound is represented by a text string consisting of several elements. See below.

**Table 5 Elements, Melody Strings, and Parameters for Melodies**

| Element | | Sub element | Values |
|---|---|---|---|
| Note | > | Octave-prefix | *0 (A=55 Hz)<br>*1 (A=110 Hz)<br>*2<br>*3<br>*4 (default)<br>*5<br>*6<br>*7<br>*8 (A=14080 Hz)<br>If no octave prefix is added, the prefix *4 will be used. |
| | | Basic notes | c<br>d<br>e<br>f<br>g<br>a<br>b |
| | | Ess notes (flat notes) | &d<br>&e<br>&g<br>&a<br>&b |
| | | Iss notes (sharp notes) | #c<br>#d<br>#f<br>#g<br>#a |

**Table 5 Elements, Melody Strings, and Parameters for Melodies (continued)**

| Element | | Sub element | Values |
|---|---|---|---|
| | | Duration | 0 (Full-note)<br>1 (1/2-note)<br>2 (1/4-note)<br>3 (1/8-note)<br>4 (1/16-note)<br>5 (1/32-note) |
| Silence | > | Rest | r |
| | | Duration | 1 to 5 (1 = long pause, 5= short pause) |
| | | Duration specifier | . (Dotted note)<br>: (Double dotted note)<br>; (2/3 length) |
| Vibration | | N/A | Vibeon<br>Vibeoff |
| Repeat | | N/A | @0 (repeat forever)<br>@<number of repetitions>, for example: “@2” repeats the melody string 2 times. |

Figure 9. *Example of a Melody String*, page 91 and Table 6 Explanation of the Melody String Example, page 91 illustrates how to program a melody.

*Figure 9. Example of a Melody String*

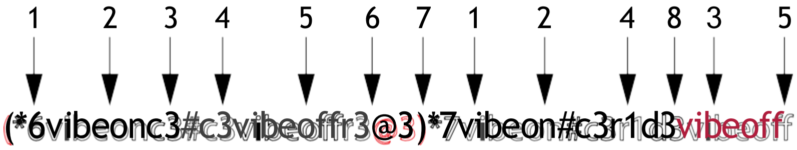


**Table 6 Explanation of the Melody String Example**

| | |
|---|---|
| 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 |

### Customize the Default Handset Beeps

If it is required to create a custom sound out of any of the default handset beeps (Beep 1–7 and Enhanced beeps 1–7), the default definition of each beep can be used as a starting point for further customizing the sound.

The default definitions are described below.

**Table 7 Definitions of Beeps**

| Beeps | Definition (default) |
|---|---|
| Custom sound 1: 1 beep | *5b4r4 |
| Custom sound 2: 2 beeps | (*5b4r4@2) |
| Custom sound 3: 3 beeps | (*5b4r4@3) |
| Custom sound 4: 3 tone chime | (*5b4r4@4) |
| Custom sound 5: 10 beeps | (*5b4r4@5) |
| Custom sound 6: Alarm sweep | (*5b4r4@10) |
| Custom sound 7: Alarm siren | (*6e4*6a4*6e4*6a4r4@10) |
| Custom sound 8 | Not predefined |
| Custom sound 9 | Not predefined |
| Custom sound 10 | Not predefined |

**Table 8 Definitions of Enhanced Beeps**

| Enhanced beeps | Definition (default) |
|---|---|
| Enhanced beep 1 | *6e2r2r1 |
| Enhanced beep 2 | *6e3r3e3r3r1 |
| Enhanced beep 3 | *6e4r4e4r4e4r4r1 |
| Enhanced beep 4 | *6c2r5:d2r5:e2r5r1 |
| Enhanced beep 5 | *6e4r4e4r4e4r3.e4r4e4r2e4r4e4r4e4r3.<br>e4r4e4r4r1 |
| Enhanced beep 6 | Beat 500,<br>(*5#f3g3#g3a3#a3b3*6c3#c3d3#d3e3r3@9) |
| Enhanced beep 7 | *6(c4e4@52) |

# Appendix C Easy Deployment

Easy deployment is done using a (staging) WLAN with a predefined SSID and security profile and a WSM3/CPDM3.

## C.1 Prerequisites

- The WLAN network needs at least one AP that allows access to the WSM3/CPDM3. The following default configuration is used, which cannot be changed:

| | |
|---|---|
| **SSID** | AWS-INIT |
| **Security mode** | WPA/WPA2-PSK |
| **WPA/WPA2 passphrase** | AWS-INIT |

- In the handset, all other network parameters must be at their default settings. See, 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** | UNII-1 |
| **World mode regulatory domain** | World mode (802.11d) |

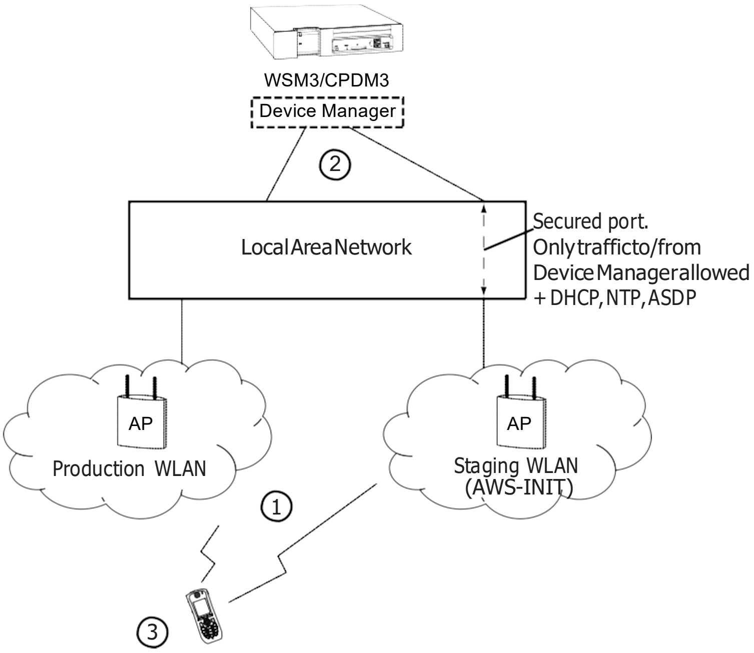
- If it is used in the WSM3/CPDM3, the password is needed to log in.
- The WSM3/CPDM3 port must be open and not blocked.
- No SSID for any of the networks A-D is configured in the handset.
- The DHCP offer for the AWS-INIT network must include an IP address of an NTP server to provide the handset with the correct system time (needed for the certificate validations).

The number to be used by a handset is entered using the handset’s keypad, after a successful first access to the WSM3/CPDM3.

Easy Deployment consists of the following three phases:

1. WLAN discovery
For more information, see C.2 WLAN Discovery, page 94.
2. WSM3/CPDM3 discovery
For more information, see C.3 WSM3/CPDM3 Discovery, page 95.
3. Parameter download
For more information, see C.4 Parameter Download, page 96.

*Figure 10. Easy Deployment*



## C.2 WLAN Discovery

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

If there is no WLAN network (SSID) configured in the handset, the handset tries to associate with a predefined default WLAN with SSID AWS-INIT, alternately on the 2.4 GHz frequency band and on the 5 GHz frequency band. See (1) in Figure 10. *Easy Deployment*, page 94.

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.

**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 WSM3/CPDM3 DM, and
services for Easy Deployment (like DHCP, NTP, ASDP). It prevents unauthorized access to the network.

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

The WLAN discovery process stops if any SSID for Network A–D is manually filled in, either by using the handset’s Admin menu or WinPDM/WSM3/CPDM3 DM.

The SSID can be accessed from the handset’s Admin menu in **Device info → WLAN info**. The `SSID (channel)`: field shows the SSID (network name). For more information, see 2.2.3 Deploy the Handset Using the Admin Menu, page 7.

If the wireless network connection bars (up in the left of the handset 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, `No network` is shown on the handset display.

## C.3 WSM3/CPDM3 Discovery

Once the handset has a WLAN connection, the second step is to automatically get the IP address to the WSM3/CPDM3, which runs the WSM3/CPDM3 DM, see (2) in Figure 10. *Easy Deployment*, page 94.

There are two ways of getting the IP address automatically:

- Using the vendor option functionality, Option 43 of a DHCP server. For more information, see C.3.1 Server Discovery Using the DHCP Option 43, page 95.
- Using the Ascom Service Discovery Protocol (ASDP) implemented in the handset. For more information, see C.3.2 Server Discovery Using the Ascom Service Discovery Protocol (ASDP), page 95.

In both cases, the received IP address is not saved, so this process is repeated on the next startup, unless a WSM3/CPDM3 IP address is set.

### C.3.1 Server Discovery Using the DHCP Option 43

A DHCP server can be configured to return a WSM3/CPDM3 IP address, as part of the DHCP response to the handset, with other needed DHCP parameters. The WSM3/CPDM3 IP address is sent using Option 43 (Vendor- Specific Data).

A DHCP request from a handset uses the Option 60 Vendor Class Identifier (VCI) to identify itself to the DHCP server. The VCI string Mitel_WLAN_Handset is the Object Identifier (OID) for the handset.

In this way, a DHCP server can be configured to return a WSM3/CPDM3 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 Messaging module, it tries to log in to the WSM3/CPDM3 DM. The DHCP Option 43 is ignored once the WSM3/CPDM3 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 D.1.2 Configuration Example of a Linux Server Using DHCP Option 43, page 104 and D.1.3 Configuration Example of an MS Windows 2003 Server, page 105, respectively.

### C.3.2 Server Discovery Using the Ascom Service Discovery Protocol (ASDP)

If the DHCP response does not contain a valid WSM3/CPDM3 IP address, the handset tries to find a WSM3/CPDM3 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.

A WSM3/CPDM3, configured to respond to ASDP discovery messages, responds with an ASDP offer as a unicast UDP message sent to the handset.

The protocol allows each WSM3/CPDM3 support different client services, and can separate different types of handsets (WLAN and DECT) to be serviced by different modules. If there are multiple WSM3/CPDM3s 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 unconfigured.

#### Configure the WSM3/CPDM3 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**.

## C.4 Parameter Download

After successfully receiving the WSM3/CPDM3 IP address, the handset tries to log in to the Messaging system.

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

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 **Numbers** tab of the WSM3/CPDM3 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 WSM3/CPDM3 DM. If the WLAN parameters are wrong, the handset cannot associate with neither the staging nor the production WLAN again.

If the wrong number is entered when the dialog window `Login:` is displayed, make a factory reset and start again. For more information, see 5.1.4 Perform a Factory Reset, page 69.

If there are no **Number records** already configured in the WSM3/CPDM3 DM before the handset logs in for the first time, perform the following steps:

1. In the WSM3/CPDM3 DM, check and save the automatically created **Numbers record** by right-clicking on the number's entry.
2. In the created record under **Device → Unite → IP address**, check that the IP address for the Messaging system is correct. Then the handset can log in to the same WSM3/CPDM3 DM again.

The WSM3/CPDM3 DM's IP address can also be checked using the Admin menu of the handset (in **Device Info → Network info → Device manager**).

## C.5 SCEP

Simple Certificate Enrollment Protocol (SCEP) is used for handling certificates in large VoWiFi systems. It can be configured using WinPDM/WSM3/CPDM3 DM or DHCP.

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).

### Configure SCEP Using WinPDM/WSM3/CPDM3 DM

To configure SCEP using WinPDM/WSM3/CPDM3 DM, perform the following steps:

1. In the **Numbers** tab, right-click the handset's number and select **Edit parameters**.
2. Select **Device → SCEP**.
3. Set the following:
   - **SCEP CA URL** — URL to the SCEP server. Example: http://myscepserver.example.com/certsrv/mscep/mscep.dll
     If left empty the handset uses SCEP configuration from the DHCP server, if available. For more information, see **Configure SCEP Using DHCP Option 43**, page 98.
   - **SCEP CA URL** — The URL of the SCEP server.
   - **Password** — Password used to authenticate the handset towards the SCEP server.
   - **Country** (optional) — Country name used in the generated certificate. It must be followed by the country code listed in https://www.ssl.com/csrs/country_codes/
   - **Organization name** (optional) — Organization name used in the generated certificate.
   - **Unit name** (optional) — Unit name used in the generated certificate.
   - **State name** (optional) — State or province name used in the generated certificate.
   - **Common name** (optional) — Common name used in the generated certificate. Different formats are allowed. MAC address in XXYYZZAABBCC format, or IPv4 address in abc.abc.abc.abc format, or string of printable characters. If left empty, the handset MAC address is used.
   - **Subject alternative name** (optional) — Subject alternative name extension used in the generated certificate.
   - **Key length** — The key length of the generated key pair.
   - **Validate server certificate** — Enables or disables the validation of the SCEP CA certificate.

### 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 Mitel_WLAN_Handset 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 the DHCP Option 43 is ignored until a new valid configuration is set.

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 9 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. |

**Table 9 Possible Key Value Pairs (continued)**

| | | |
|---|---|---|
| CN | String (max 32 characters) | Common name to be used in the generated certificate. Different formats are allowed. MAC address in XXYYZZAABBCC 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 D.1.2 Configuration Example of a Linux Server Using DHCP Option 43, page 104 and D.1.3 Configuration Example of an MS Windows 2003 Server, page 105, respectively.

# Appendix D Complementary Information for Easy Deployment

## D.1 DHCP Related

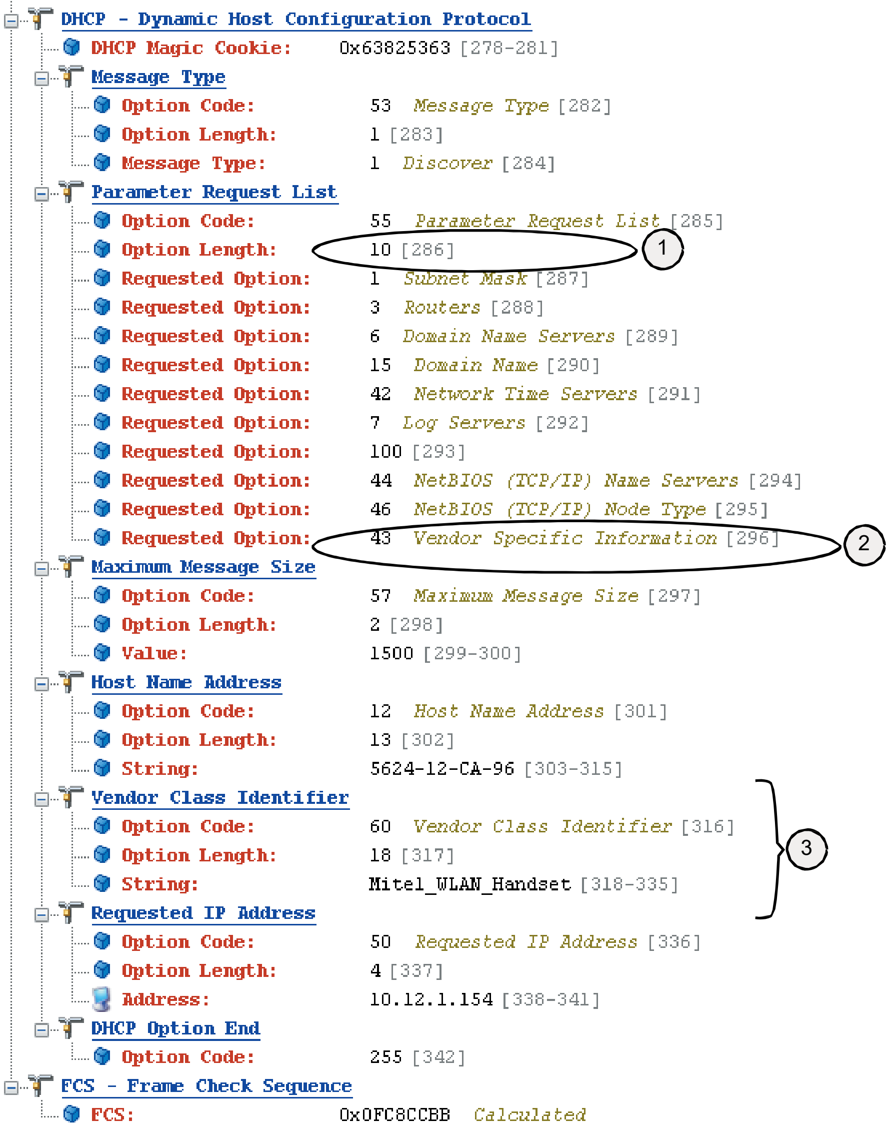
### D.1.1 DHCP Vendor Options Explained

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 11. *Example of a DHCP Discover Message (Omnipeek Trace)*, page 100.

*Figure 11. Example of a DHCP Discover Message (Omnipeek Trace)*

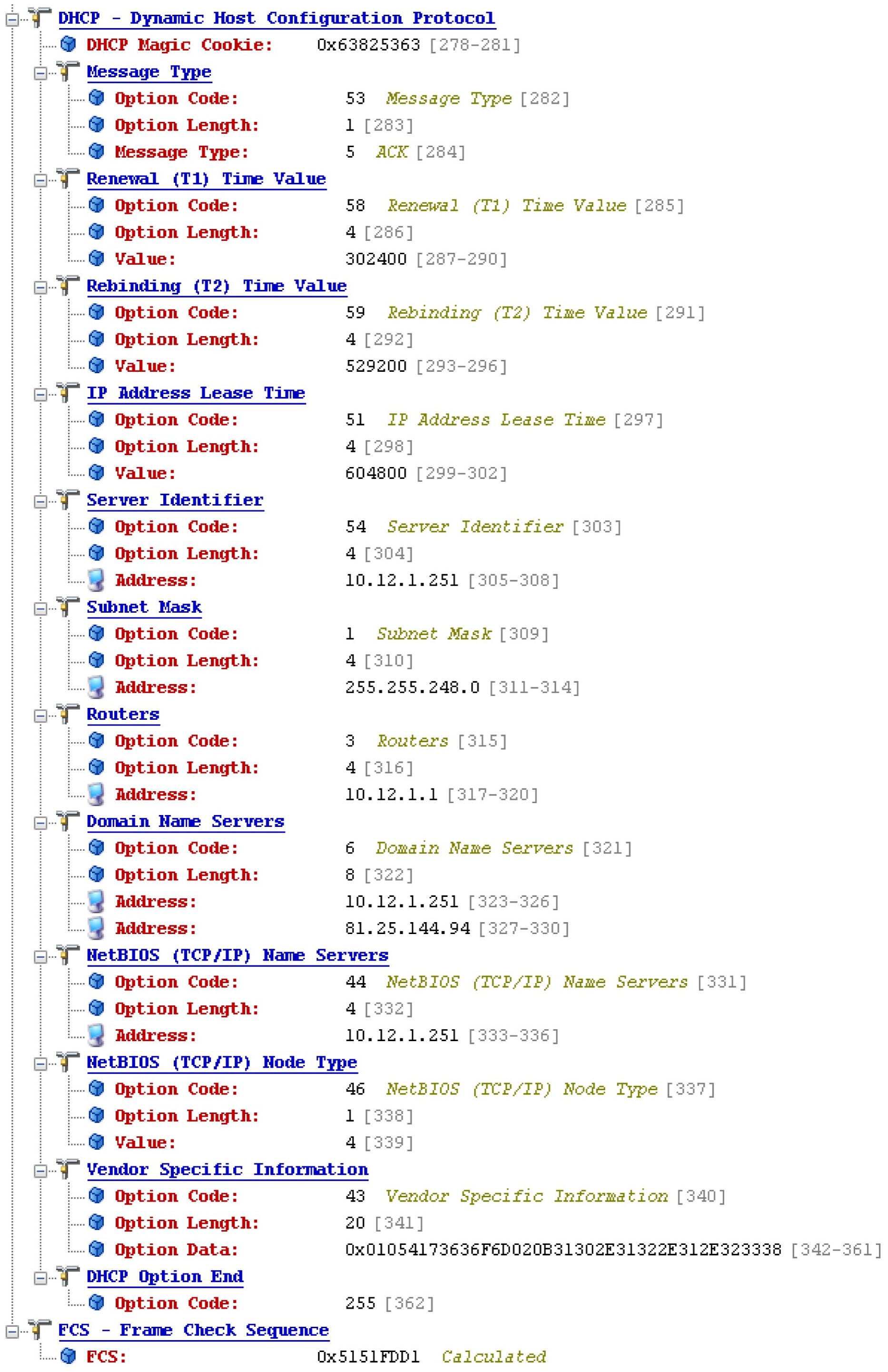


```
DHCP - Dynamic Host Configuration Protocol
  DHCP Magic Cookie:        0x63825363 [278-281]
  Message Type
    Option Code:            53  Message Type [282]
    Option Length:          1 [283]
    Message Type:           1  Discover [284]
  Parameter Request List
    Option Code:            55  Parameter Request List [285]
    Option Length:          10 [286]
    Requested Option:       1  Subnet Mask [287]
    Requested Option:       3  Routers [288]
    Requested Option:       6  Domain Name Servers [289]
    Requested Option:       15  Domain Name [290]
    Requested Option:       42  Network Time Servers [291]
    Requested Option:       7  Log Servers [292]
    Requested Option:       100 [293]
    Requested Option:       44  NetBIOS (TCP/IP) Name Servers [294]
    Requested Option:       46  NetBIOS (TCP/IP) Node Type [295]
    Requested Option:       43  Vendor Specific Information [296]
  Maximum Message Size
    Option Code:            57  Maximum Message Size [297]
    Option Length:          2 [298]
    Value:                  1500 [299-300]
  Host Name Address
    Option Code:            12  Host Name Address [301]
    Option Length:          13 [302]
    String:                 5624-12-CA-96 [303-315]
  Vendor Class Identifier
    Option Code:            60  Vendor Class Identifier [316]
    Option Length:          18 [317]
    String:                 Mitel_WLAN_Handset [318-335]
  Requested IP Address
    Option Code:            50  Requested IP Address [336]
    Option Length:          4 [337]
    Address:                10.12.1.154 [338-341]
  DHCP Option End
    Option Code:            255 [342]
FCS - Frame Check Sequence
  FCS:                      0x0FC8CCBB  Calculated
```

In Figure 11. *Example of a DHCP Discover Message (Omnipeek Trace)*, page 100, the numbered points illustrate the following:

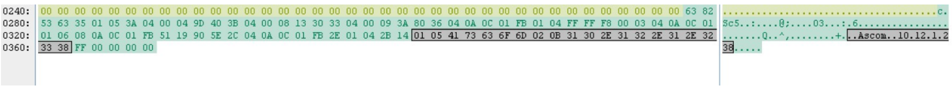
- The amount of options requested
- Vendor options requested by the handset
- A specific set of Vendor options requested by the handset, by sending a Vendor Class Identifier (VCI)

*Figure 12. Example of a DHCP Acknowledge (Omnipeek Trace)*



```
DHCP - Dynamic Host Configuration Protocol
    DHCP Magic Cookie:     0x63825363 [278-281]
    Message Type
        Option Code:           53  Message Type [282]
        Option Length:         1 [283]
        Message Type:          5  ACK [284]
    Renewal (T1) Time Value
        Option Code:           58  Renewal (T1) Time Value [285]
        Option Length:         4 [286]
        Value:                 302400 [287-290]
    Rebinding (T2) Time Value
        Option Code:           59  Rebinding (T2) Time Value [291]
        Option Length:         4 [292]
        Value:                 529200 [293-296]
    IP Address Lease Time
        Option Code:           51  IP Address Lease Time [297]
        Option Length:         4 [298]
        Value:                 604800 [299-302]
    Server Identifier
        Option Code:           54  Server Identifier [303]
        Option Length:         4 [304]
        Address:               10.12.1.251 [305-308]
    Subnet Mask
        Option Code:           1  Subnet Mask [309]
        Option Length:         4 [310]
        Address:               255.255.248.0 [311-314]
    Routers
        Option Code:           3  Routers [315]
        Option Length:         4 [316]
        Address:               10.12.1.1 [317-320]
    Domain Name Servers
        Option Code:           6  Domain Name Servers [321]
        Option Length:         8 [322]
        Address:               10.12.1.251 [323-326]
        Address:               81.25.144.94 [327-330]
    NetBIOS (TCP/IP) Name Servers
        Option Code:           44  NetBIOS (TCP/IP) Name Servers [331]
        Option Length:         4 [332]
        Address:               10.12.1.251 [333-336]
    NetBIOS (TCP/IP) Node Type
        Option Code:           46  NetBIOS (TCP/IP) Node Type [337]
        Option Length:         1 [338]
        Value:                 4 [339]
    Vendor Specific Information
        Option Code:           43  Vendor Specific Information [340]
        Option Length:         20 [341]
        Option Data:           0x01054173636F6D020B31302E31322E312E323338 [342-361]
    DHCP Option End
        Option Code:           255 [362]
FCS - Frame Check Sequence
    FCS:                   0x5151FDD1  Calculated
```

*Figure 13. Example of a DHCP ACK in Hex (Omnipeek Trace)*



```
0240: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 63 82 ......................................c.
0280: 53 63 35 01 05 3A 04 00 04 9D 40 3B 04 00 08 13 30 33 04 00 09 3A 80 36 04 0A 0C 01 FB 01 04 FF FF F8 00 03 04 0A 0C 01 Sc5..:....@;....03...:.6................
0320: 01 06 08 0A 0C 01 FB 51 19 90 5E 2C 04 0A 0C 01 FB 2E 01 04 2B 14 01 05 41 73 63 6F 6D 02 0B 31 30 2E 31 32 2E 31 2E 32 .......Q..^,........+...Ascom..10.12.1.2
0360: 33 38 FF 00 00 00 00                                                                                                     38.....
```

In Figure 12. *Example of a DHCP Acknowledge (Omnipeek Trace)*, page 101, 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 11. *Example of a DHCP Discover Message (Omnipeek Trace)*, page 100, 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.

### The Vendor Option 43 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 10 Option 60 String Values, page 102 lists some examples of Option 60 string values.

**Table 10 Option 60 String Values**

| Vendor | Device | String | Option 43 returned value |
|---|---|---|---|
| Aruba | Aruba AP | ArubaAP | Loopback address of the Aruba master controller |
| Cisco | Cisco AP | Cisco AP c1250 | IP address of the WLAN controller |

### 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 11 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.

### 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 Table 12 Information Bytes Format when Using *Encapsulated Vendor-specific Extensions*, page 103.

**Table 12 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, an administrator can enter each sub-option separately, or enter all values in a single concatenated string. Since each value contains a header, a length field, and the parameter itself, this can be difficult to enter correctly. Some servers require the entry of values in the hexadecimal format, while others use ASCII strings.

For the handset, the Option 43 sub-fields are defined according to Table 13 Option 43 Sub-fields, page 103.

**Table 13 Option 43 Sub-fields**

| Code (tag) | Length | Data items | Code | Length | Data items | Code (optional) |
|---|---|---|---|---|---|---|
| 01 | 5 | Mitel | 02 | 7–15 | IPv4 address to WSM/CPDM | 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, see C.5 SCEP, page 96.

When entering this information in a DHCP server, the administrator must observe that the field length of the IP address can vary, depending on the amount of digits used. If, for example, using the address 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 WSM3/CPDM3 DM with IP address 10.30.4.120, data is sent as Option 43 as follows:

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

The first option in the OEM string (made bold in the table above) is used to verify that the data received in the client is for the WLAN handset. This is called a magic number.

Search the internet for a tool that can assist in creating this string in hexadecimal format.

**Table 14 Vendor Class Identifier (VCI)**

| Vendor/OEM | Value |
|---|---|
| Mitel | Mitel_WLAN_Handset |

## D.1.2 Configuration Example of a Linux Server Using DHCP Option 43

The Code Example, page 104 is 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.ims code 2 = string;

class “vendors” {

match option vendor-class-identifier;

vendor-option-space easy;

}

subclass “vendors” “Mitel_WLAN_Handset” {

option easy.oem “Mitel”;
option easy.ims "10.30.4.120";
}
```

There are two options configured as code 1 and code 3, and both are defined as strings.

The server maps the string “Mitel_WLAN_Handset” 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.

### D.1.3 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.

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.

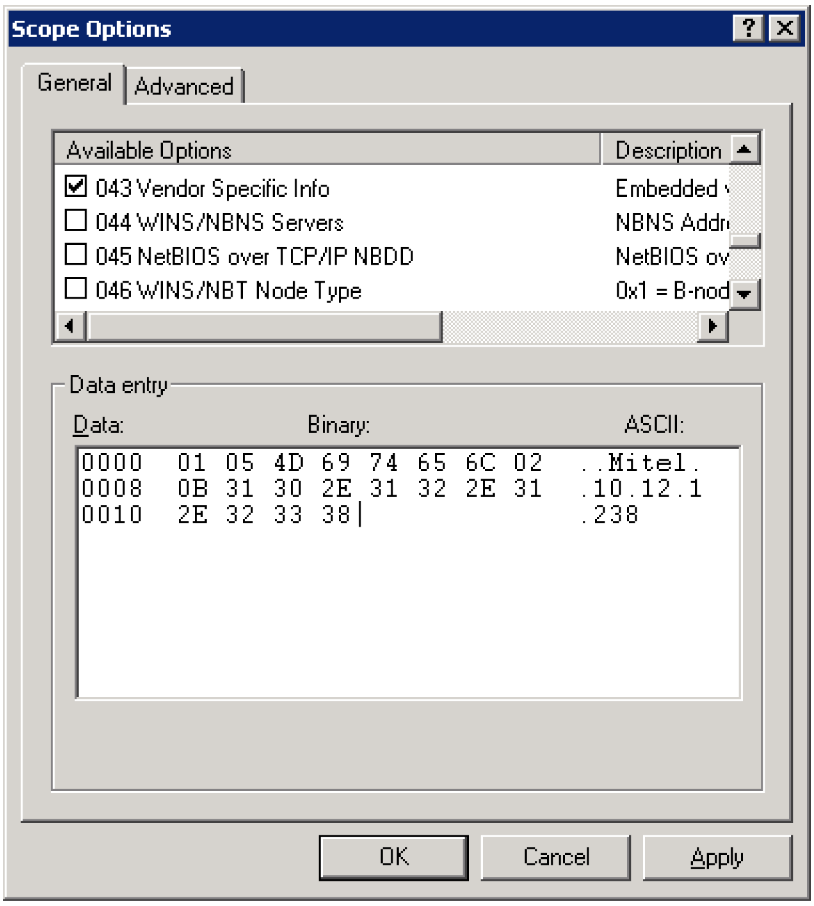
There are several documents on the internet that get this process wrong.

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. On the **General tab** (the default Standard DHCP class), scroll down, and select **043 Vendor Specific Info**.
3. In the data entry field, there are two ways of entering the information. Click to the left in the box to enter the string in binary, and to the right to enter the string in ASCII. It is possible to switch between binary and ASCII.
   Enter the values, as described in previous sections. Remember to get the length values in the TLV string correct.



| Available Options | Description |
|---|---|
| ☑ 043 Vendor Specific Info | Embedded |
| □ 044 WINS/NBNS Servers | NBNS Addr |
| □ 045 NetBIOS over TCP/IP NBDD | NetBIOS ov |
| □ 046 WINS/NBT Node Type | 0x1 = B-nod |

Data entry

```
Data:     Binary:                    ASCII:
0000      01 05 4D 69 74 65 6C 02    ..Mitel.
0008      0B 31 30 2E 31 32 2E 31    .10.12.1
0010      2E 32 33 38                .238
```

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

`01(“Mitel”)02(192.168.5.1)`

Click **OK** and save the new Option 43.

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

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

5. Test the configuration. If 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 `0203`.

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.

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.

### 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. For example, in the **Display name** field, enter **Mitel 5634 VoWiFi Handset**, and in the Description field, enter **Option 43 for Easy Deployment**. These fields are only used for displaying information for the administrator.
   In the ID field, enter the VCI string seen in the table in D.1.1 DHCP Vendor Options Explained, page 100 (**Mitel_WLAN_Handset**). Then click **OK**.

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

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

### Configure Sub-options for a Vendor Class in an MS Windows 2003 DHCP Server

The current sub-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 MitelX-brand and one with the IP-address of the WSM3/CPDM3 DM.

1. Right-click on the DHCP server and select **Set Predefined Options**.
2. Select the vendor class created earlier (in section Define New Vendor Class to Support Multiple Types of Clients, page 107) in **Option class** and click **Add**. The Option type window opens.
3. Enter a descriptive name for the first sub-option in the **Name:** field, for example, **VoWiFi Vendor**, and in the **Description:** field, enter, for example, **Vendor Magic ID**.
4. In the **Data type:** field, select **Binary** to allow entering more than one byte.
5. In the **Code:** field, enter `001`, then click **OK**.

   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).

6. For the second sub-option, repeat Item 1., page 107–Item 2., page 107.
7. Enter a descriptive name for the second sub-option in the **Name:** field, for example, **IP address**, and copy it to the **Description:** field.
8. In the **Data type:** field, select **Binary** to allow entering more than one byte.
9. In the **Code:** field, enter `002003`, then click **OK**.
10. Add the two sub-options to a scope and assign the values needed as follows:

Right-click on your scope, then select **Scope Options → Configure Options**.

11. Select the **Advanced** tab. In the **Vendor class:** field, select the new vendor class that was created in section Define New Vendor Class to Support Multiple Types of Clients, page 107 (Mitel 56xxX-brand handset). Check the two sub-options that appear (**001 VoWiFi Vendor** and **002 Unite module IP address**.

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

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

    Remove `00` that is displayed by default.

    A length value (in the **Data:** field) is not needed to be entered here (as normally done, when entering a TLV record). Click **OK**.

13. Select the second sub-option **002003 WSM IP address** and enter the WSM IP address in binary/ hexadecimal or ASCII. Click **OK**.
14. Test the configuration by factory-resetting a handset. If the configuration does not work, do a trace with a sniffer to see why.

    Install Wireshark on the DHCP server and filter on the `bootp` protocol to view the packet exchange when a handset is started up.

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

If a predefined DCHP 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.

### D.1.4 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 "VCI string of the handset"
    ```

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. For the VCI string, use the value above. The quotation marks must be included.
   Add the Option 43 line with the following syntax:
   `option 43 hex <hexadecimal string>`
   This hexadecimal string is assembled as a sequence of the TLV values for the Option 43 sub-option: Type + Length + Value, as described in Configure Sub-options for a Vendor Class in an MS Windows 2003 DHCP Server, page 107.

## D.2 Easy Deployment and VLAN

In a VoWiFi system, the WSM3/CPDM3 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 WSM3/CPDM3 DM used for Easy Deployment.

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 WSM3/CPDM3 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.

## D.3 Easy Deployment and Certificates

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 WSM3/CPDM3 DM used for Easy Deployment, and then select the required application certificate. Perform the steps, as described below in this section.

If there is no application certificate in the WSM3/CPDM3 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. Perform the steps of association according to Item 3., page 110 and Item 5., page 110.

   For more information on certificates, see *WinPDM Installation and Operation Manual* and in WSM3/CPDM3 User Manual.
3. In the **Numbers** tab, right-click the handset's number and 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. Click **Close**.
5. In the **Numbers** tab, right-click the handset's number and select **Edit parameters**.
6. Select **Network X** (X represents A, B, C, or D).
7. In the **Security mode** drop-down list, select **EAP-TLS**.
8. In the **EAP application certificate** drop-down list, select the application certificate to be used. Click **OK**.

# Appendix E Interactive Messaging in Handsets

The **interactiveMessage** service in the Open Access Protocol (OAP) client application is used to send an IM to the handset. OAP is an XML-based protocol that enables the exchange of data between external applications or systems and the WSM3/CPDM3.

The following list contains the XML tags for interactive messaging supported by the handsets:

- Messaging
  - Subject
  - Body
  - Break through of silent mode
  - Beep characteristics/Number of beeps
  - Number of indications
  - Time between indications
  - Message priority used by handset
  - Message ID
  - Time to live in handset
  - Allow later erase of message
- IM-specific
  - Update existing IM
  - Sticky mode
  - Time between indications before option selection
  - Time between indications after option selection
- Options
  - Option text
  - Option ID
  - Assigned soft key
  - Requested call number
  - Display layer

- On option selection
  - Number to call
  - Request for call number
  - Disconnect ongoing call
  - Data to send when call is disconnected
  - Data to send
  - Erase specified option
  - Erase message
  - Update message time to live
  - Show prompt text and request data from user
  - Destination address for sent response
  - Enable Option ID
  - Display specified layer
  - Close message
  - Sticky mode
  - Change message priority
  - Feedback on selection
- IM response
  - Data received from handset
  - Data entered by user
  - Device ID from handset

**Manufactured by**
**Mitel Deutschland GmbH**
Zeughofstrasse 1
10997 Berlin, Germany

58016277 / October 2020

Mitel
Powering connections