A MITEL
PRODUCT
GUIDE

Unify OpenScape Alarm Response Professional

OScAR Mobile Client V5

Service Documentation
07/2024

P31003-S1750-S103-01-7620

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

1 Overview and Reference Documents

Overview

This chapter gives you an overview of the manual and refers to other OScAR product documentations that can be of further help for you.

Content

This chapter consists of the following sub-sections:

1.1 Overview of the other chapters in this document

This manual contains the following chapters:

Chapter 2, “Conventions and Operating Instructions"	This chapter specifies the conventions employed and provides advice on how to use this manual.
Chapter 3, “About OScAR Mobile Client (DMC)"	This chapter gives you an overview of the DMC system basic components as well as a general description of the functions of DMC.
Chapter 4, “Install and uninstall DMC app"	This chapter shows you how to install the software "DMC-Proxy V1.0x" and the DMC application from the various stores, and also how to remove both again from your system.
Chapter 5, “Initial Startup and Configuration of DMC Proxy and DMC"	This chapter shows you how to configure DMC proxy and runs you through the first-time startup of OScAR Mobile Client on smartphones. In addition, it gives you an overview of the icons used by DMC, including their significance.
Chapter 6, “OScAR Mobile Client Redundancy Concept"	This chapter covers the redundancy concept for backup of DMC systems and gives you an overview of the reasons that lead to the automatic switch-over to the other system.

Table 1-1 Overview of chapters

1.2 Reference manuals

The below-listed tetronik documents offer information that can be of additional assistance when working with OScAR:

- OScAR Mobile Client User and Administrator Manual
- OScARpro Server Configuration Manual V9.x
- OScAR-TT User Manual
- OScAReco, OScARmed, OScARindico Server Manual

2 Conventions and Operating Instructions

Overview

This chapter specifies the conventions employed and provides advice on how to use this manual.

Content

This chapter consists of the following sub-sections:

Note:
OScAR Mobile Client (hereinafter abbreviated: DMC) constitutes the tetronik designation of the product that is documented in this manual.
When marketed and sold as a product through Unify GmbH und Co. KG (short: Unify), the product name reads: OScAR Mobile Client (OMC).
The terms and screenshots found in this document generally refer to the product or product names of tetronik. The explanations and descriptions, however, equally shall be understood to apply to the Unify product.

2.1 Notations and symbols

Notations

The following definitions are used in this document:

`Text`	All texts copied from files that are described in this document and all entries that are added to these files are output in the monospace font Courier.
The password 123456...	Details and instructions in the continuous text that are of particular importance or must be heeded are output in bold print. Buttons are also in bold print.
The file `global.cfg`	`Files` and `directories` are output in the monospace font Courier.
"Name"	Field names, menu names and window descriptions are placed in "quotation marks".
<Placeholder>	Entries and outputs, both of which may vary dependent on the individual situation in which they appear, are placed in <angle brackets> and output in italics.

Table 2-1 Notations

Symbols

The following symbols are used in this User Manual:

Note:
The info "i" is used to indicate additional helpful information.

Important information and warnings
Important information and warnings describe e.g. hazards that can damage or destroy the hardware or software, or lead to the loss of data.

2.2 Data protection and data security

The system described in this document may draw on and process both personal and corporate data.

In Germany, the processing and application of use of this data is subject to various regulations, including the Federal Data Protection Act (Bundesdatenschutzgesetzes, BDSG). Please be careful to follow the laws and regulations for the protection of personal data that are in force in the country in which you work.

The purpose of data protection is to protect the individual against any infringement of his or her personal rights through the misuse of personal data.

In addition, the goal of the data Protection Regulations is the safeguard of the data from misuse during the different processing phases and consequently to counter any impairment caused to external or internal legitimate interests.

Please help ensure complete data protection and data security by being aware of these issues as you work:

- Always make sure that only authorized persons have access to personal data.
- Assign passwords whenever you can. Do not grant unauthorized persons access to your passwords, for example by writing them down.
- Always make sure that no unauthorized persons can process or utilize personal data in any way, for example by saving, editing, communicating, blocking, deleting or in any other way using this information.
- Always make sure that no unauthorized persons have access to data storage media, for example to backup disks or printouts of logfiles or protocols. This applies both to service work provided directly at the customer and to the storage and transport of data carriers.
- Always make sure that every data storage medium that is no longer needed is properly and fully destroyed. Also be careful not to leave behind any papers that could become openly accessible to others.

We urge all readers to work together closely with the contact persons of your clients. This not only helps to build trust but will also help you reduce your own workload.

3 About OScAR Mobile Client (DMC)

Overview

This chapter gives you an overview of the DMC system basic components as well as a general description of the functions of DMC.

Note:
OScARpro supports a topology with external proxy.
➤ see Image 3-1

OScAReco and OScARmed support both integrated and external proxy topology.

For more detailed information on DMC please see the corresponding sections of this manual.

Content

This chapter consists of the following sub-sections:

3.1 DMC system for OScAR with external DMC proxy

The DMC system usually consists of the following components:

- a OScAR server,
- a DMC proxy,
- a Push-Notification Service and
- the DMC clients that communicate with the OScAR server via the DMC proxy either in the WLAN or through the internet.

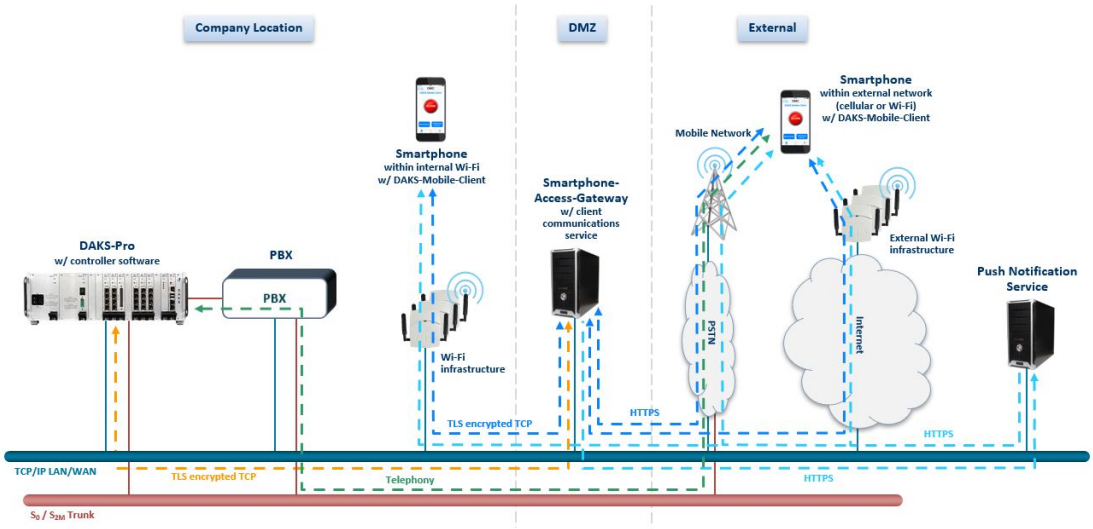


Image 3-1 DMC system - basic system components

3.2 DMC system for OScAR with integrated DMC proxy

The DMC system usually consists of the following components:

- a OScAR server,
- an integrated DMC proxy, and
- the DMC clients that communicate with the OScAR server via the DMC proxy in the WLAN

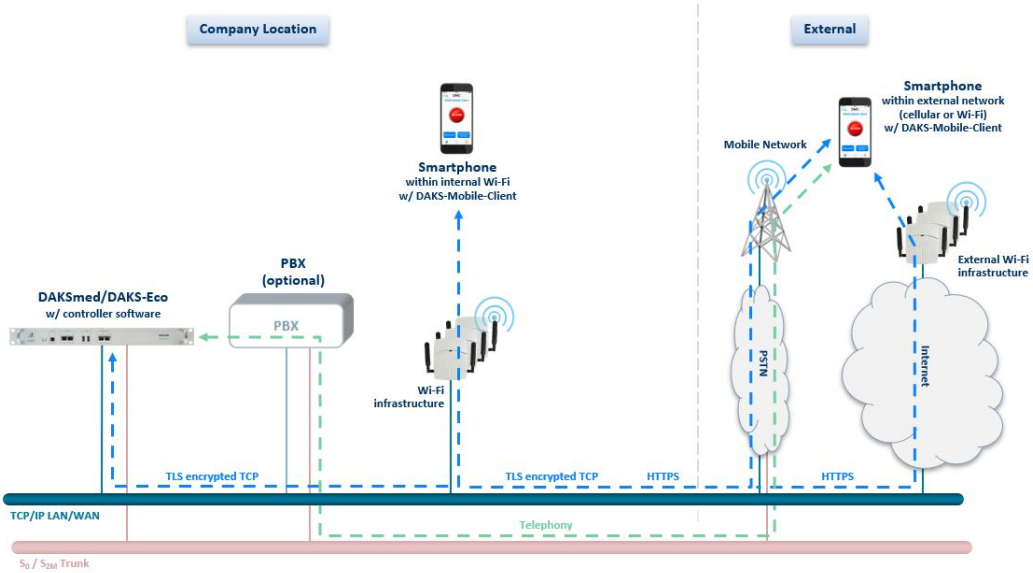


Image 3-2 DMC system - basic system components

4 Install and uninstall DMC app

Overview

This chapter shows you how to install the software "DMC-Proxy V1.0x" and the DMC application from the various stores, and also how to remove both again from your system.

Content

This chapter consists of the following sub-sections

4.1 Install the DMC app

This section shows you how to install the DMC application on smartphones through the pertinent app stores.

4.1.1 Install DMC via App Store

How to install DMC via App Store, step by step:

No.	Step
1.	Open the application "App Store" on the iPhone on which you want to install DMC. Note: To do so, you need internet access and an Apple ID.
2.	Under "Find" enter "DMC - OScAR Mobile Client". This will take you to the DMC app with the following icon:  Now, install the app.
3.	For more details on the installation of the app: ➤ see Section 5.4, "Initial configuration of DMC".

Table 4-1 Install DMC via app store

4.1.2 Install DMC via Google Play Store

How to install DMC via the Google Play Store, step by step:

No.	Step
1.	Open the application "Play Store" on the Android device on which you want to install DMC, and log in with your Google account. Note: To do so, you need internet access and a Google account.
2.	Under "Find" enter "DMC - OScAR Mobile Client". This will take you to the DMC app with the following icon:  Install the app.
3.	For more details on the installation of the app: ➤ see Section 5.4, "Initial configuration of DMC".

Table 4-2 Install DMC via Google Play Store

4.2 Uninstall the DMC App

4.2.1 Uninstall DMC from iPhone, step by step

No.	Step
1.	Press the DMC icon until it is displayed as follows. 
2.	Tippen Sie auf folgendes Symbol  und die App wird deinstalliert.

Table 4-3 Install DMC from iPhone

4.2.2 Uninstall DMC from Android, step by step

No.	Step
1.	Press the DMC icon until a recycle bin appears in the display.
2.	Move the DMC icon to the trash and the app will be uninstalled.

Table 4-4 Uninstall DMC from Android

5 Initial Startup and Configuration of DMC Proxy and DMC

Overview

This chapter shows you how to configure DMC proxy and runs you through the first-time startup of OScAR Mobile Client on smartphones. In addition, it gives you an overview of the icons used by DMC, including their significance.

Content

This chapter consists of the following sub-sections:

5.1 The Software "DMC proxy"

This section shows you how to install the software "DMC proxy" on a Windows® PC, and also how to remove (uninstall) it again.

Caution!
If you are working with both a main and a redundancy OScAR server, you must install two DMC proxy installations, as each OScAR server communicates via its own DMC proxy.

5.1.1 Install the DMC proxy

How to install the DMC proxy, step by step:

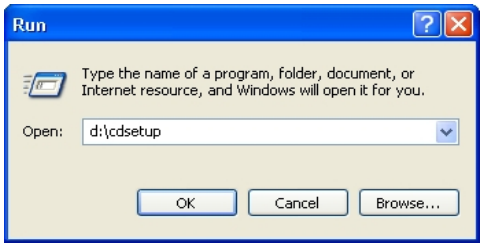
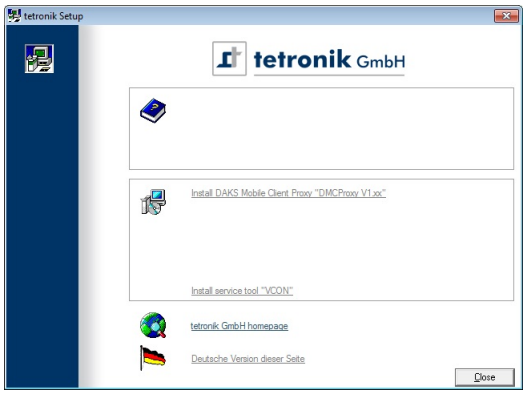
No.	Step	Window
1.	Insert the installation CD in the CD-ROM drive. If the installation software fails to start automatically, please start the CD installation manually from the Windows® interface using the command "Run menu". To do so, use the menu command: "Run...". Go to the command line above Start and enter the command: <CD-Rom drive>:\cdsetup e.g.: d:\cdsetup Confirm with OK.	
2.	Click the menu item: "Install the OScAR Mobile Client Proxy „DMC proxy V1.xx"	
3.	Select the language you want to use and confirm with OK.	

Table 5-1 Install DMC proxy

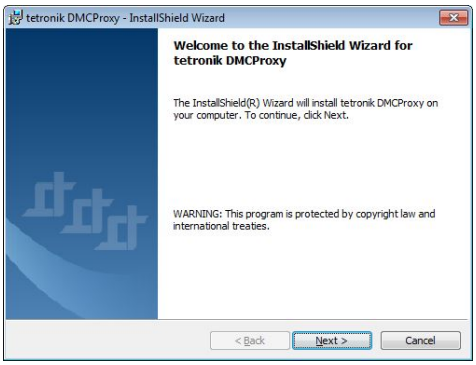
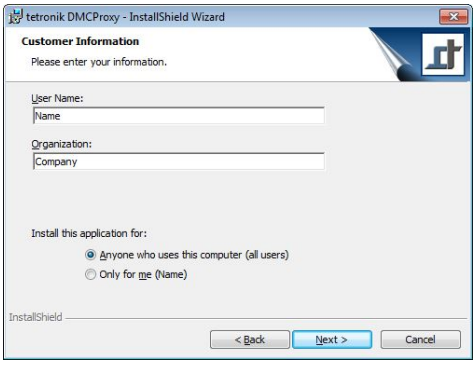
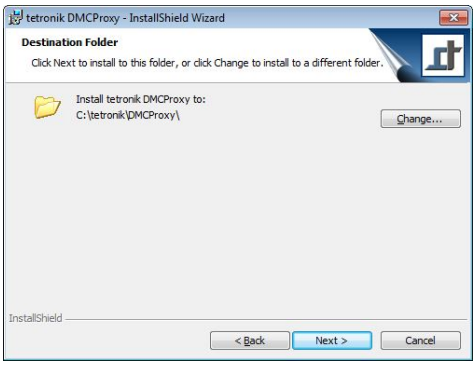
No.	Step	Window
4.	The installation is now initialized.	
5.	Click Next to make all installation settings.	
6.	Enter the user name and the name of the organization or company. Specify if you want the software to be installed for all users of this PC, or only for you. Now click Next.	
7.	In necessary, adjust the destination folder. To do so, click Change.... If you want to use the default destination folder, click Next.	

Table 5-1 Install DMC proxy

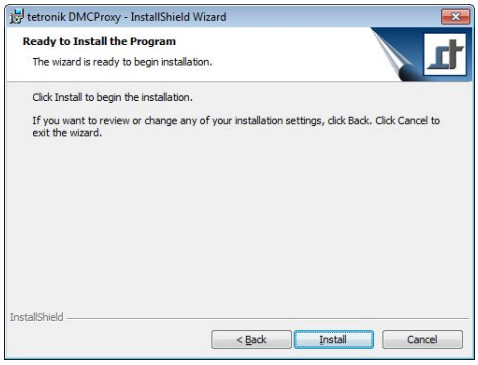
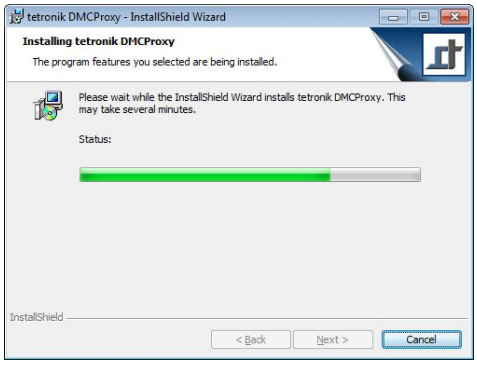
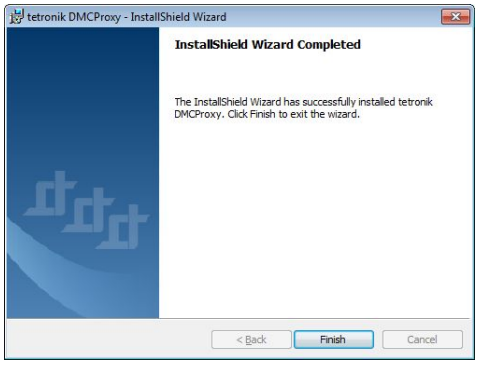
No.	Step	Window
8.	Next, proceed to install the DMCproxy software on your PC. Click Install.	
9.	The software is now installed in the selected directory. The progress of the installation is shown with a progress bar.	
10.	Complete the installation process. To do so, click Finish.	

Table 5-1 Install DMC proxy

5.1.2 Uninstall DMC proxy

How to remove the DMC proxy, step by step:

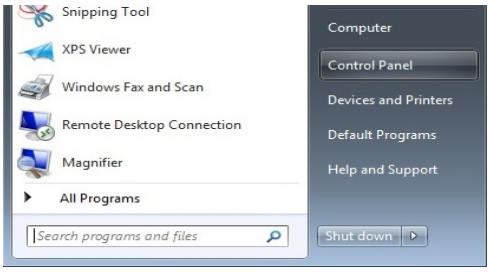
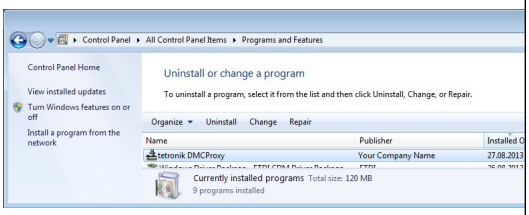
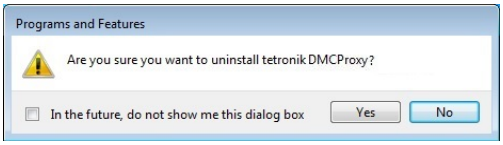
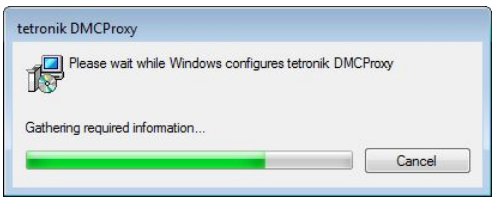
No.	Step	Window
1.	Open the Windows® Control Panel.	
2.	Open "Programs and Functions".	
3.	Select the entry: " tetronik DMCProxy" . Next, click Change. This will start the program to uninstall "tetronik DMCProxy".	
4.	Confirm the security prompt. To do so, click Yes.	
5.	"tetronik DMCProxy" is now removed from your system.	

Table 5-2 Uninstall DMC proxy

5.2 Configure DMC Proxy

To carry out the configuration for the DMC proxy as described below, you must first set up the access to the DMC proxy in the OScAR service and configuration tool: VCON

Note:
The service and configuration tool VCON is covered in detail the following tetronik manual:

➤ see "OScARpro Server Configuration Manual"
➤ see „OScAReco Server Manual“

5.2.1 Configure the IP parameters of DMC proxy via VCON

Parameters:

Parameters	Value range [Default setting]	Description
Tree structure: Server ➤ IP Manager Service ➤ VCON access		
VCON Port	IP-Port [2180]	The IP port for the VCON access to DMC proxy
VCON Whitelist 1... 10	IP-address [0.0.0.0]	The IP addresses entitled to access DMC proxy via VCON. If no entries are made in this list there is no access restriction at all.
Tree structure: Server ➤ IP Manager Service ➤ IP #1		
IP V4 address	IP-address [0.0.0.0]	Output of the IP address of the system on which the DMC proxy runs
IP V4 address for dns #1	IP-address [0.0.0.0]	IP address of the DNS server
IP V4 address for dns #2	IP-address [0.0.0.0]	IP address of the DNS server (alternative)
Tree structure: Server ➤ DMC Proxy Application ➤ Parameter		
Use HTTPS only	[no], yes	Exclusive use of HTTPS
IP-Port HTTP	IP-Port [80]	The IP port at which the web interface of DMC proxy can be reached via HTTP
IP-Port HTTPS	IP-Port [443]	IP port at which the web interface of DMC-Proxy can be reached via HTTPS
use APNS	[no], yes	Use Apple Push Notification Service
IP-Port DGMP	IP-Port [4013]	The IP port at which the DMC proxy can be reached by the OScAR server via DGMP
No-Poll timeout [sec]	1.. 60 s [30 s]	The maximum time that may elapse between the sending of a response by DMC proxy and the receipt of a renewed inquiry from DMC. Otherwise, the DMC is switched to the offline mode.
Poll timeout [sec]	1.. 60 s [30 s]	The maximum time by which DMC proxy will delay a response to an inquiry from DMC, if no current information is available.
Offline timeout [min]	5..10.000 min [30 min]	The maximum length of time during which DMC proxy waits for the OScAR Mobile Client (DMC) to respond to a message. Otherwise the DMC proxy ends the connection.

Table 5-3 Parameters DMC-Proxy

Parameters	Value range [Default setting]	Description
Send timeout [sec]	1.. 20 s [20 s]	The maximum time that the OScAR server must wait for messages from DMC proxy installations.
Max. number of connection	1...9999 [2000]	The maximum number of OScAR Mobile Clients (DMCs) that may connect with the OScAR server
Interval for push notifications [sec]	15.. 9999 s [60 s]	Maximum number of clients allowed to connect to the OScAR server

Table 5-3 Parameters DMC-Proxy

5.2.2 Configure SSL parameters via VCON

Full description

The area "SSL" is used to list and administrate imported certificates.

Note:
The service and configuration tool VCON is covered in detail the following tetronik manual:

➤ see "OScARpro Server Configuration Manual"

Parameters:

Parameters	Value range [Default setting]	Description
Tree structure: Server ➤ SSL Service		
Allow self signed	yes, [no]	Allow certificates that are self-signed.
Allow unknown issuer (CA)	yes, [no]	Allow certificates also if their issuer (CA) is unknown.
Allow outdated	yes, [no]	Allow certificates also if their validity date has expired.
Sign certificates with sha256	[yes], no	Sign certificates with sha256.
Ciphers	SSLv3 and better TLS v 1.2 HIGH and up only [TLS v 1.0 and up]	Version of the encryption protocol.
AES coding	AES-128 AES-256 [AES-128 and AES-256]	Supported key length of the encryption method.
SHA support	SHA1 allowed [SHA1 prohibited],	Use of SHA1 • SHA1 prohibited: Connections with SHA1 not allowed • SHA1 allowed: Connections with SHA1 allowed
FIPS 140-2 mode	yes, [no]	Enabling the FIPS 140-2 mode
sign with expiration in	1 year, 2 years, 3 years, 5 years, 10 years	Certificate validity period
Add IPs to CN	[yes], no	Use IP address in certificate
Add IPs to SAN	[yes], no	Use IP address in "Subject alternative name"
Add Hostname to SAN	[yes], no	Use host name in "Subject alternative name"
Tree structure: Server ➤ SSL ➤ Machine Certificate		
This area is used for the certificate that is currently used by the OScAR server.		
Tree structure: Server ➤ SSL ➤ Issuer		
This area is used for details on the issuer of the certificate.		
Tree structure: Server ➤ SSL ➤ Trusted Certificates		

Table 5-4 Parameter SSL

Parameters	Value range [Default setting]	Description
This area is used to list all certificates that have been uploaded to the memory of trusted certificates.		
Tree structure: Server ➤ SSL ➤ Trusted Certificates ➤ Certificate		
Action	[none], remove certificate	Use 'remove certificate' to delete a certificate
Tree structure: Server ➤ SSL ➤ Trusted Certificates ➤ Issuer		
This area is used for details on the issuer of the certificate.		
Tree structure: Server ➤ SSL ➤ Temporary Certificates		
This area is used to list all certificates that are allowed on a temporary, i.e. time-limited basis.		
Action	[none], add to „Trusted certificates“	Use the parameter 'add to trusted certificates' to add certificates to the memory of trusted certificates.
Tree structure: Server ➤ SSL ➤ Temporary Certificates ➤ Issuer		
This area is used for details on the issuer of the certificate.		

Table 5-4 Parameter SSL

5.3 DMC-Proxy Firewall-Setting for APNs

To use the Apple Push Notification System (APNs), the following ports must be enabled for address block 17.0.0.0/8:

- TCP port 5223: for communication with the APNs
- TCP port 2195: for sending notifications to the APNs
- TCP port 2196: for the APNs feedback service
- TCP port 443: only for switching back to WLAN, only if the devices are not able to connect to the APNs via port 5223

5.4 Initial configuration of DMC

As you carry out the initial startup configuration of OScAR Mobile Client, the DMC home window will consist of the components described below.

Note:
Depending on the smartphone you are using and the size of the screen, the locations where the individual elements are placed on the display may differ.

Note:
For the DMC app to be able to connect with the OScAR server, the user data must be properly administrated in the OScAR server.

➤ see "OScARpro User Manual".

The DMC home window of iPhone or Android devices is subdivided into the following areas:

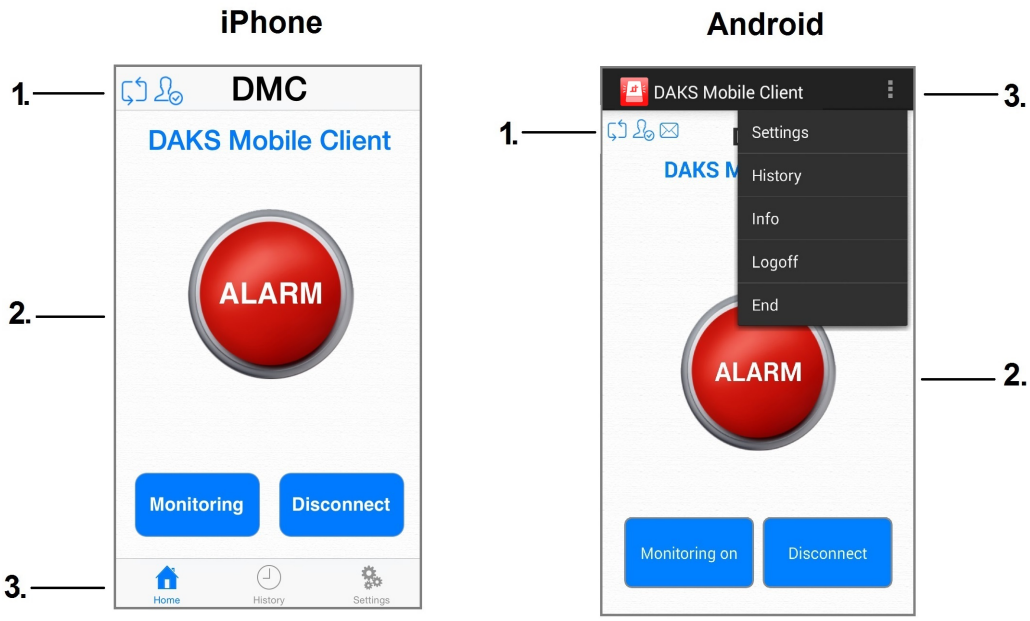


Image 5-1 DMC Home window

1. Header

   The header carries different icons that offer information on the state of the DMC.

2. Control window:

   The control window carried various control elements to operate with the DMC.

3. Menu bar

   Depending on the operating system, you can toggle the menu bar to jump to the Home screen (applies only to iPhone), the History or the Settings.

   ➤ see OScAR Mobile Client User and Administrator Manual

Fist-time configuration of DMC, step by step:

No.	Step
1.	Start the DMC app. Log in using the default login data: • Name: admin • Password: admin-t Note: If you make wrongs entries here, a new login will be temporarily blocked. For the first wrong entry, the blocking will last 10 seconds, for the second 30 seconds and for the third and every additional wrong entry the blocking will last 60 seconds.
2.	Go to the menu bar and click "Settings". You can change the default administrator user login data under "Administrator login". • Name: Enter the new administrator user name • Password: Enter the new administrator password • Repeat password: Repeat the new password Finally, click Save.
3.	You can administrate the login data of the default user under "Default user login". • Name: Enter the new name of the default user • Password: Enter the new password of the default user • Repeat password: Repeat the new password Finally, click Save. Note: For the DMC app to be able to connect with the OScAR server, the user data must be properly stored in the OScAR server. ➤ see "OScARpro User Manual"
4.	Enter the telephone number of the smartphone under "Device ID". Together with the login data this number will be used as further authentication feature when registering at the OScAR server. In addition, the smartphone can be reached at this number in the event of an emergency, should no data connection be available. Finally, click Save. Note: For the DMC app to be able to connect with the OScAR server, the device ID must be properly registered in the OScAR server. ➤ see "OScARpro User Manual"
5.	Go to "DMC proxy URLs" and configure the URLs of the DMC proxy installation of the main OScAR server and, if applicable, also of the backup OScAR server. To do so, enter the addresses of the DMC proxy 1 and DMC proxy 2: e.g.: **`https://192.168.69.12`** Note: The URLs of both DMC proxy 1 and DMC proxy 2 must be entered in accordance with the URL requirements. Finally, click Save.

Table 5-5 DMC initial configuration

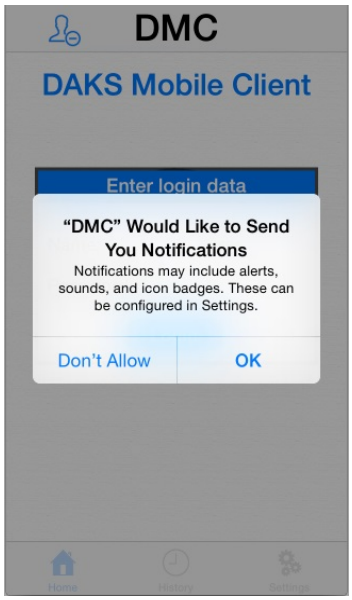
No.	Step	
6.	The initial configuration of DMC is now finished. You can now log in to DMC with the default user login data or the administrator login data. After you have successfully logged in the home window of DMC will automatically pop up.	
	Note: With the iPhone operation system iOS 8, the user authorize the DMC app to send messages. For this purpose, a message box will automatically appear when the first DMC message is received. Confirm the message box with OK.	

Table 5-5 DMC initial configuration

6 OScAR Mobile Client Redundancy Concept

Overview

This chapter covers the redundancy concept for backup of DMC systems and gives you an overview of the reasons that lead to the automatic switch-over to the other system.

Content

This chapter consists of the following sub-sections:

6.1 General Information on the DMC Redundancy System

A DMC system consists of a OScAR server and a corresponding DMC proxy. Systems that are designed for redundancy DMC installations consist of a main DMC system and a (backup) redundancy DMC system.

If a component of the active DMC system fails or breaks down, the OScAR Mobile Client clients (DMCs) will automatically switch over the other system.

6.2 Reasons for a switch-over

The following situations can cause a switch-over from the main to the redundancy system:

- The DMC proxy reports that it has no connection to the OScAR server.
- The OScAR server reports that it is in the hot standby mode.
- The OScAR server reports that it is in a red alarm.
- No connection to the DMC proxy, even though an allowed network connection available.

6.3 Switch-over details

If one of the aforementioned situations occurs, a switch-over to the redundant system is carried out automatically.

You can configure at any time if you want OScAR Mobile Client to inform you with a message box of the reason that caused the switch-over, and/or if you want DMC to inform you when the actual switch-over was successfully carried out.

DMC automatically generates a corresponding entry in the DMC History. When a switch-over is made from the main to the redundancy DMC system and the login there fails, OScAR Mobile Client will automatically try alternately to register at either of the two servers.

In this case, in order to keep the energy consumption of the device as low as possible, the first 5 login attempts will be initiated every seconds, the next five login attempts every 10 seconds, and all further login attempts only every 20 seconds.

As soon as DMC is registered at the redundancy DMC system, it will regularly check every 1 minute if the main DMC system can be reached again. As soon as it becomes available again, DMC will automatically switch back to the main DMC system

Caution!
A switch-over from a functioning main DMC system to a backup redundancy DMC system can only be carried out by the administrator for test purposes!