FXS 7224
Cerberus Mobile
Commissioning

IP 7
Imprint

Technical specifications and availability subject to change without notice.

Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights created by patent grant or registration of a utility model or design patent are reserved.

Issued by:
Siemens Switzerland Ltd.
Building Technologies Division
International Headquarters
Theilerstrasse 1a
CH-6300 Zug
Tel. +41 58 724-2424
www.siemens.com/buildingtechnologies

Edition: 2018-08-29
Document ID: A6V10418718_d_en_--

© Siemens Switzerland Ltd, 2013
# Table of contents

1 About this document.......................................................................................... 5
  1.1 Applicable documents.................................................................................. 8
  1.2 Download center......................................................................................... 8
  1.3 Technical terms and abbreviations............................................................... 8
  1.4 Revision history .......................................................................................... 9

2 Safety ............................................................................................................... 10
  2.1 Safety instructions ...................................................................................... 10
  2.2 Safety regulations for the method of operation .......................................... 11
  2.3 Standards and directives complied with.................................................... 13
  2.4 Release Notes ............................................................................................ 13
  2.5 Cyber security disclaimer ........................................................................... 14

3 Commissioning - Overview ........................................................................... 15
  3.1 Requirements for operation ....................................................................... 15
  3.2 Commissioning the router ......................................................................... 16
  3.3 Connecting the router to the 'station' ......................................................... 16
  3.4 Setting up a home network ......................................................................... 17

4 App installation .............................................................................................. 18

5 Establishing a connection to the 'station'....................................................... 19
  5.1 Connection via mobile telecommunications ................................................. 19
    5.1.1 Activating the Internet connection via mobile telecommunications on the router .............................................................. 20
    5.1.2 Activating the dynamic DNS service on the router ......................... 21
    5.1.3 Setting up a VPN connection on the router ...................................... 22
    5.1.4 Activating a VPN connection on the router ..................................... 27
    5.1.5 Configuring a VPN connection on a smartphone ........................... 28
    5.1.6 Starting a VPN connection on a smartphone ................................. 29
    5.1.7 Deactivating a VPN connection on a smartphone ......................... 30
  5.2 Connection via WLAN wireless network ................................................. 30
    5.2.1 Activating a WLAN connection on the router .................................. 31
    5.2.2 Activating WLAN encryption on the router .................................... 32

6 Configuring a 'station' for smartphones......................................................... 33
  6.1 Configuring visibility for Cerberus Mobile ................................................. 33
  6.2 Configuring connection event for Cerberus Mobile ............................... 34
  6.3 Specifying the operation mode for Cerberus Mobile .............................. 35
  6.4 Enable smartphone .................................................................................... 36
  6.5 Removing a smartphone ........................................................................... 37
  6.6 Access level .............................................................................................. 37
7 General commissioning steps ...............................................................38
  7.1 Detector test .............................................................................................. 38
  7.2 Control test ................................................................................................ 40
  7.3 Switching off 'Zone' .................................................................................... 41
  7.4 Switching on 'Zone' .................................................................................... 42
  7.5 Adapting preferences ................................................................................. 43
8 General operations ..............................................................................45
  8.1 Acknowledging an 'ALARM' ....................................................................... 45
  8.2 Resetting an 'ALARM' ................................................................................ 46
  8.3 Acknowledge fault ..................................................................................... 46
  8.4 Execute commands ................................................................................... 47
  8.5 Displaying events ..................................................................................... 48
  8.6 Exiting Cerberus Mobile ............................................................................. 48
9 Testing detectors ................................................................................49
10 Control test ...........................................................................................50
Glossary .....................................................................................................51
Index .........................................................................................................52
## 1 About this document

### Goal and purpose
In this document you will find information and work steps for commissioning the FXS7224 'Cerberus Mobile' app. You will find more information about installing, commissioning, servicing, and troubleshooting the FS720 fire detection system and operating fire control panels and fire terminals in the FS720 fire detection system under 'Applicable documents' in the corresponding documentation.

### Scope
The information contained in this document is valid for the market package IP 7.

<table>
<thead>
<tr>
<th>![WARNING]</th>
<th><strong>WARNING</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>No compliance with EN 54</strong></td>
</tr>
<tr>
<td></td>
<td>The following commands are not EN 54-compliant in the case of 'Cerberus Mobile':</td>
</tr>
<tr>
<td></td>
<td>- Acknowledge 'ALARM'</td>
</tr>
<tr>
<td></td>
<td>- Reset 'ALARM'</td>
</tr>
<tr>
<td></td>
<td>- Switch off 'Zone'</td>
</tr>
<tr>
<td></td>
<td>- Switch on 'Zone'</td>
</tr>
</tbody>
</table>
## Target groups

The information in this document is intended for the following target groups:

<table>
<thead>
<tr>
<th>Target group</th>
<th>Activity</th>
<th>Qualification</th>
</tr>
</thead>
</table>
| System owner          | • According to EN 50110-1, 'nominated person with the overall responsibility to ensure the safe operation of the electrical installation by setting rules and organisation or framework.' | • 'This person can be the owner, employer, proprietor or a delegated person.'
                                                                                     |                                                                                                          | • 'Some of these duties can be delegated to others as required. For large or complex electrical installations or networks, the duties can be delegated for parts of the installations or the network.' |                                                                                                          |
| Installation personnel| • Assembles and installs the product components at the place of installation.  
• Carries out a function check following installation.    | • Has received specialist training in the area of building installation technology or electrical installations. |
| Commissioning personnel| • Configures the product at the place of installation according to customer-specific requirements.  
• Checks the product operability and releases the product for use by the operator.  
• Searches for and corrects malfunctions. | • Has obtained suitable specialist training for the function and for the products.  
• Has attended the training courses for commissioning personnel. |
| Operating personnel   | • Carries out procedures to correctly operate the product.                | • No particular basic training is needed.  
• Has been instructed by the commissioning personnel. |
| Maintenance personnel | • Carries out all maintenance work.  
• Checks that the products are in perfect working order.  
• Searches for and corrects malfunctions. | • Has obtained suitable specialist training for the function and for the products. |

## Source language and reference document

- The source/original language of this document is German (de).
- The reference version of this document is the international version in English. The international version is not localized.
Document identification
The document ID is structured as follows:

<table>
<thead>
<tr>
<th>ID code</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID_ModificationIndex_Language_COUNTRY-- = multilingual or international</td>
<td>A6V10215123_a_de_DE</td>
</tr>
<tr>
<td></td>
<td>A6V10215123_a_en--</td>
</tr>
<tr>
<td></td>
<td>A6V10315123_a_----</td>
</tr>
</tbody>
</table>

Date format
The date format in the document corresponds to the recommendation of international standard ISO 8601 (format YYYY-MM-DD).

Conventions for text marking
Markups
Special markups are shown in this document as follows:

<table>
<thead>
<tr>
<th>&gt;</th>
<th>Requirement for a behavior instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 2.</td>
<td>Behavior instruction with at least two operation sequences</td>
</tr>
<tr>
<td>-</td>
<td>Version, option, or detailed information for a behavior instruction</td>
</tr>
<tr>
<td>⇢</td>
<td>Intermediate result of a behavior instruction</td>
</tr>
<tr>
<td>⇣</td>
<td>End result of a behavior instruction</td>
</tr>
<tr>
<td>●</td>
<td>Numbered lists and behavior instructions with an operation sequence</td>
</tr>
<tr>
<td>[⇒ X]</td>
<td>Reference to a page number</td>
</tr>
<tr>
<td>’Text’</td>
<td>Quotation, reproduced identically</td>
</tr>
<tr>
<td>&lt;Key&gt;</td>
<td>Identification of keys</td>
</tr>
<tr>
<td>&gt;</td>
<td>Relation sign and for identification between steps in a sequence, e.g., ‘Menu bar’ &gt; ‘Help’ &gt; ‘Help topics’</td>
</tr>
<tr>
<td>↑ Text</td>
<td>Identification of a glossary entry</td>
</tr>
</tbody>
</table>

Supplementary information and tips
The 'i' symbol identifies supplementary information and tips for an easier way of working.
1.1 Applicable documents

<table>
<thead>
<tr>
<th>Document ID</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>A6V10210362</td>
<td>Planning</td>
</tr>
<tr>
<td>A6V10229261</td>
<td>List of compatibility</td>
</tr>
<tr>
<td>A6V10211076</td>
<td>FC72x / FT724 Fire Control Panel / Fire Terminal, Operation</td>
</tr>
<tr>
<td>A6V10210424</td>
<td>FS720 Fire Detection System, Configuration</td>
</tr>
<tr>
<td>A6V10210355</td>
<td>System description</td>
</tr>
<tr>
<td>A6V10210416</td>
<td>FS720 Fire Detection System, Commissioning / Maintenance / Troubleshooting</td>
</tr>
</tbody>
</table>

1.2 Download center

You can download various types of documents, such as data sheets, installation instructions, and license texts via the following Internet address: https://siemens.com/bt/download

- Enter the document ID in the search field.

You will also find information about search variants and links to mobile applications (apps) for various systems on the home page.

1.3 Technical terms and abbreviations

<table>
<thead>
<tr>
<th>Term</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>UMTS</td>
<td>Universal Mobile Telecommunications System</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>LRC</td>
<td>Lifecycle Responsibility Concept</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless LAN</td>
</tr>
<tr>
<td>WPA</td>
<td>WiFi Protected Architecture</td>
</tr>
</tbody>
</table>

You will find details of further technical terms and abbreviations in the ‘Glossary’ chapter.
1.4 Revision history

The reference document's version applies to all languages into which the reference document is translated.

The first edition of a language version or a country variant may, for example, be version 'd' instead of 'a' if the reference document is already this version.

The table below shows this document's revision history:

<table>
<thead>
<tr>
<th>Version</th>
<th>Edition date</th>
<th>Brief description</th>
</tr>
</thead>
<tbody>
<tr>
<td>d</td>
<td>2018-08-29</td>
<td>Edition for IP 7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New: 'Configuring connection event for Cerberus Mobile'</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Revised: 'Establishing a connection to the station', 'Configuring a station' for smartphones, 'Requirements for operation', 'App installation'</td>
</tr>
<tr>
<td>c</td>
<td>2017-05-16</td>
<td>Revised: Graphic updated in chapter 'Configuring visibility for Cerberus Mobile'</td>
</tr>
<tr>
<td>b</td>
<td>2015-12-15</td>
<td>Edition for IP 6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New: Cyber security disclaimer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Revised: Referenced documents updated, chapter 'Smartphone license' removed, information on smartphone licenses removed from the document</td>
</tr>
<tr>
<td>a</td>
<td>2013-11-25</td>
<td>First edition</td>
</tr>
</tbody>
</table>
2 Safety

2.1 Safety instructions

The safety notices must be observed in order to protect people and property.

The safety notices in this document contain the following elements:

- Symbol for danger
- Signal word
- Nature and origin of the danger
- Consequences if the danger occurs
- Measures or prohibitions for danger avoidance

Symbol for danger

This is the symbol for danger. It warns of **risks of injury**. Follow all measures identified by this symbol to avoid injury or death.

Additional danger symbols

These symbols indicate general dangers, the type of danger or possible consequences, measures and prohibitions, examples of which are shown in the following table:

<table>
<thead>
<tr>
<th>General danger</th>
<th>Explosive atmosphere</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voltage/electric shock</td>
<td>Laser light</td>
</tr>
<tr>
<td>Battery</td>
<td>Heat</td>
</tr>
</tbody>
</table>

Signal word

The signal word classifies the danger as defined in the following table:

<table>
<thead>
<tr>
<th>Signal word</th>
<th>Danger level</th>
</tr>
</thead>
<tbody>
<tr>
<td>DANGER</td>
<td>'DANGER' identifies a dangerous situation, which <strong>will result directly in death or serious injury</strong> if you do not avoid this situation.</td>
</tr>
<tr>
<td>WARNING</td>
<td>'WARNING' identifies a dangerous situation, which <strong>may result in death or serious injury</strong> if you do not avoid this situation.</td>
</tr>
<tr>
<td>CAUTION</td>
<td>'CAUTION' identifies a dangerous situation, which could result in <strong>slight to moderately serious injury</strong> if you do not avoid this situation.</td>
</tr>
<tr>
<td>NOTICE</td>
<td>'NOTICE' identifies a possibly harmful situation or possible damage to property that may result from non-observance. 'NOTICE' does not relate to possible bodily injury.</td>
</tr>
</tbody>
</table>
How risk of injury is presented
Information about the risk of injury is shown as follows:

⚠️ WARNING

Nature and origin of the danger
Consequences if the danger occurs
• Measures / prohibitions for danger avoidance

How possible damage to property is presented
Information about possible damage to property is shown as follows:

❗️ NOTICE

Nature and origin of the danger
Consequences if the danger occurs
• Measures / prohibitions for danger avoidance

2.2 Safety regulations for the method of operation

National standards, regulations and legislation
Siemens products are developed and produced in compliance with the relevant European and international safety standards. Should additional national or local safety standards or legislation concerning the planning, mounting, installation, operation or disposal of the product apply at the place of operation, then these must also be taken into account together with the safety regulations in the product documentation.

Electrical installations

⚠️ WARNING

Electric voltage
Electric shock
• Work on electrical installations may only be carried out by qualified electricians or by instructed persons working under the guidance and supervision of a qualified electrician, in accordance with the electrotechnical regulations.

• Wherever possible disconnect products from the power supply when carrying out commissioning, maintenance or repair work on them.
• Lock volt-free areas to prevent them being switched back on again by mistake.
• Label the connection terminals with external voltage using a ‘DANGER External voltage’ sign.
• Route mains connections to products separately and fuse them with their own, clearly marked fuse.
• Fit an easily accessible disconnecting device in accordance with IEC 60950-1 outside the installation.
• Produce earthing as stated in local safety regulations.
Safety
Safety regulations for the method of operation

<table>
<thead>
<tr>
<th>CAUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Noncompliance with the following safety regulations</td>
</tr>
<tr>
<td>Risk of injury to persons and damage to property</td>
</tr>
<tr>
<td>● Compliance with the following regulations is required.</td>
</tr>
</tbody>
</table>

- Specialist electrical engineering knowledge is required for installation.
- Only an expert is permitted to carry out installation work.
Incorrect installation can take safety devices out of operation unbeknown to a layperson.

Mounting, installation, commissioning and maintenance
- If you require tools such as a ladder, these must be safe and must be intended for the work in hand.
- When starting the fire control panel ensure that unstable conditions cannot arise.
- Ensure that all points listed in the 'Testing the product operability' section below are observed.
- You may only set controls to normal function when the product operability has been completely tested and the system has been handed over to the customer.

Testing the product operability
- Prevent the remote transmission from triggering erroneously.
- If testing building installations or activating devices from third-party companies, you must collaborate with the people appointed.
- The activation of fire control installations for test purposes must not cause injury to anyone or damage to the building installations. The following instructions must be observed:
  - Use the correct potential for activation; this is generally the potential of the building installation.
  - Only check controls up to the interface (relay with blocking option).
  - Make sure that only the controls to be tested are activated.
- Inform people before testing the alarm devices and allow for possible panic responses.
- Inform people about any noise or mist which may be produced.
- Before testing the remote transmission, inform the corresponding alarm and fault signal receiving stations.

Modifications to the system design and the products
Modifications to the system and to individual products may lead to faults, malfunctioning and safety risks. Written confirmation must be obtained from Siemens and the corresponding safety bodies for modifications or additions.
Modules and spare parts

- Components and spare parts must comply with the technical specifications defined by Siemens. Only use products specified or recommended by Siemens.
- Only use fuses with the specified fuse characteristics.
- Wrong battery types and improper battery changing lead to a risk of explosion. Only use the same battery type or an equivalent battery type recommended by Siemens.
- Batteries must be disposed of in an an environmentally friendly manner. Observe national guidelines and regulations.

Disregard of the safety regulations

Before they are delivered, Siemens products are tested to ensure they function correctly when used properly. Siemens disclaims all liability for damage or injuries caused by the incorrect application of the instructions or the disregard of danger warnings contained in the documentation. This applies in particular to the following damage:

- Personal injuries or damage to property caused by improper use and incorrect application
- Personal injuries or damage to property caused by disregarding safety instructions in the documentation or on the product
- Personal injury or damage to property caused by poor maintenance or lack of maintenance

2.3 Standards and directives complied with

A list of the standards and directives complied with is available from your Siemens contact.

2.4 Release Notes

Limitations to the configuration or use of devices in a fire detection installation with a particular firmware version are possible.

<table>
<thead>
<tr>
<th>WARNING</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Limited or non-existent fire detection</strong></td>
</tr>
<tr>
<td>Personal injury and damage to property in the event of a fire.</td>
</tr>
<tr>
<td>- Read the ’Release Notes’ before you plan and/or configure a fire detection installation.</td>
</tr>
<tr>
<td>- Read the ’Release Notes’ before you carry out a firmware update to a fire detection installation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NOTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incorrect planning and/or configuration</strong></td>
</tr>
<tr>
<td>Important standards and specifications are not satisfied. Fire detection installation is not accepted for commissioning. Additional expense resulting from necessary new planning and/or configuration.</td>
</tr>
<tr>
<td>- Read the ’Release Notes’ before you plan and/or configure a fire detection installation.</td>
</tr>
<tr>
<td>- Read the ’Release Notes’ before you carry out a firmware update to a fire detection installation.</td>
</tr>
</tbody>
</table>
2.5 Cyber security disclaimer

Siemens provides a portfolio of products, solutions, systems and services that includes security functions that support the secure operation of plants, systems, machines and networks. In the field of Building Technologies, this includes building automation and control, fire safety, security management as well as physical security systems. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement - and continuously maintain - a holistic, state-of-the-art security concept. Siemens' portfolio only forms one element of such a concept.

You are responsible for preventing unauthorized access to your plants, systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For additional information, please contact your Siemens sales representative or visit https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html.

Siemens’ portfolio undergoes continuous development to make it more secure. Siemens strongly recommends that updates are applied as soon as they are available and that the latest versions are used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. Siemens strongly recommends to comply with security advisories on the latest security threats, patches and other related measures, published, among others, under https://www.siemens.com/cert/en/cert-security-advisories.htm.
3 Commissioning - Overview

3.1 Requirements for operation

Devices required

With 'Cerberus Mobile', up to 5 smartphones can access a Site simultaneously with 'Limited access (view only)' or 'Full access (view/operation)'.

The following devices are required to use the 'Cerberus Mobile' smartphone app:

- A smartphone with Android operating system version 7.x or higher
- A router with the latest firmware version
  The FRITZ!Box router is used in the commissioning and configuration example in this document.
- A network cable to connect the router to the 'Station'
- A PC to configure the router

The following devices are required to set up a mobile connection via UMTS:

- The router must support VPN and UMTS
- A USB modem for broadband Internet access
- A SIM card with public dynamic IP
  Additional subscriptions may be required for mobile use of the Internet with the necessary SIM card. You should contact the network operator prior to commissioning.

The following devices are required to set up a connection via WLAN:

- The router must support WLAN
- The smartphone must support WLAN

Applications required

The following applications are required to connect the smartphone to the 'Station':

- The 'Cerberus Mobile' smartphone app
- 'Cerberus-Engineering-Tool' to configure visibility for the smartphone

For mobile connection:

- A VPN application for the router
  The 'Set up FRITZ!Box remote access' application was used in the configuration example in this document.
- A dynamic DNS service to generate a static domain name

Licenses required

The following licenses are required to commission 'Cerberus Mobile':

- A suitable license key for the station
  License keys are needed to enable stations for network functions. The required license key must support the 'Cerberus Mobile' function.

You will find more information about license keys in document A6V10210362. See chapter 'Applicable documents'.
3.2 Commissioning the router

A router is required to connect a smartphone to the Station. If the connection is to be established via mobile telecommunications, the router must support VPN and UMTS. If the connection is established via WLAN, the router must support WLAN. The FRITZ!Box router is used in the commissioning and configuration example in this document.

The FRITZ!Box can be commissioned following the manufacturer's instructions in the 'Setup and operation' manual. The manual can be downloaded from the manufacturer's Internet site. If you are using a similar router, we recommend following the manufacturer's commissioning instructions in the corresponding manual.

3.3 Connecting the router to the 'Station'

To connect the router to the 'Station', proceed as follows:

1. Plug the network cable into the Ethernet port on the 'Station'.
2. Plug the free end of the cable into the Ethernet port (LAN) on the router.
   ➤ The router is now connected to the 'Station'.
3.4 Setting up a home network

A router home network must be set up to commission ‘Cerberus Mobile’. The manufacturer's manual describes how to set up a home network on the FRITZ!Box. The manual can be downloaded from the manufacturer's Internet site or opened from via the user interface of the FRITZ!Box configuration system. If you are using a different router, you must obtain the manual from the manufacturer.

To set up the home network on the FRITZ!Box, proceed as follows:

1. Open the user interface of the router.
2. Select ‘Home network’ > ‘Network’.
3. Enter the value ‘192.168.200.10’ under ‘IPv4 address’.
4. Check the ‘Activate DHCP server’ checkbox.
5. Enter the value ‘192.168.200.20’ under ‘From’.
6. Enter the value ‘192.168.200.200’ under ‘To’.

You have set up a home network on the router.

![FRITZ!Box 3370](image)

Figure 1: Setting up a home network
4 App installation

'Cerberus Mobile' can be downloaded from the 'Google Play' platform online. The Android operating system includes a link to 'Google Play'. 'Cerberus Mobile' cannot be downloaded from other operating system platforms.

'Cerberus Mobile' can only be installed in an Android operating system version 7.x or higher.
5 Establishing a connection to the 'station'

### WARNING

Connection failure to the station due to 'Doze' mode on the mobile device

Mobile devices with Android 6.0 and higher switch to 'Doze' mode to reduce power consumption when they are not connected to the mains and the screen is off. It is therefore not possible to establish a continuous connection between the 'Cerberus Mobile' app and the station in 'Doze' mode. This means that the station cannot transmit alarms, fault messages, and other events to the 'Cerberus Mobile' app in real time.

- Actively check the pending events in the 'Cerberus Mobile' app at regular intervals.
- Always keep the mobile device connected to the mains whenever possible.
- If the mobile device is not connected to the mains, wake it up at regular intervals by unlocking it.

The 'Cerberus Mobile' app reconnects to the station automatically. The 'Cerberus Mobile' app receives all events from the station.

With 'Cerberus Mobile', up to 5 smartphones can access a Site simultaneously with 'Limited access (view only)' or 'Full access (view/operation)'.

To operate the ↑ 'Station' with 'Cerberus Mobile', you need a connection between the smartphone and the 'Station'. The following connection options are available:

- Connection via mobile telecommunications [➙ 19]
- Connection via WLAN wireless network [➙ 30]

The 'Station' must also be configured for the connection with a smartphone. You will find more information on configuring the 'Station' in chapter 'Configuring a 'station' for smartphones [➙ 33}'.

#### 5.1 Connection via mobile telecommunications

To connect the smartphone to the ↑ 'Station' via mobile telecommunications, you must start up the router and establish a connection with the 'Station' via a network cable.

Check that your router's user interface is set to 'Advanced view' in the system settings. You will find more information about setting up the advanced view in the router's user interface in the manufacturer's user manual.

To connect the smartphone to the ↑ 'Station' via mobile telecommunications, proceed as follows:

- You have set the advanced view in the FRITZ!Box.

1. Activate the Internet connection via mobile telecommunications on the router. Link [➙ 20]
2. Activate the dynamic DNS service on the router. Link [➙ 21]
3. Set up a VPN connection on the router. Link [➙ 22]
4. Activate the VPN connection on the router. Link [➙ 27]
5. Configure the VPN connection on the smartphone. Link [➙ 28]
6. Start the VPN connection on the smartphone. Link [➙ 29]

Your smartphone is connected to the 'Station'.
5.1.1 Activating the Internet connection via mobile telecommunications on the router

Broadband Internet access can be activated on the router with a USB modem and a compatible SIM card. A 'FRITZ!Box' router is used in the commissioning example described below.

The manufacturer's manual describes how to set up Internet access via mobile telecommunications on the FRITZ!Box. The manual can be downloaded from the manufacturer's Internet site or opened from the user interface of the FRITZ!Box configuration system. If you are using a different router, you must obtain the manual from the manufacturer.

The following figure shows the example configuration after Internet access via mobile telecommunications has been activated on the FRITZ!Box.

![Figure 2: FRITZ!Box settings for activating Internet access via mobile telecommunications]
5.1.2 Activating the dynamic DNS service on the router

Whenever the router is connected to the Internet via mobile telecommunications, it is assigned a dynamic IP address. For access to the 'Station' with the smartphone, the router must be accessible from the Internet under a fixed domain name. To specify a domain name, a user name, and a password, you must register with a dynamic DNS provider.

'Dynamic DNS' must be activated for the FRITZ!Box configuration example. The manufacturer's manual describes how to activate 'Dynamic DNS'. The manual can be downloaded from the manufacturer's Internet site or opened from via the user interface of the FRITZ!Box configuration system. If you are using a different router, you must obtain the manual from the manufacturer.

The following figure shows the example configuration after 'Dynamic DNS' has been activated on the FRITZ!Box. The 'Dynamic DNS provider', 'Domain name', 'User name', and 'Password' fields must be completed using the registration information from the dynamic DNS provider.

Figure 3: FRITZ!Box settings for activating dynamic DNS

To set up the dynamic DNS service, proceed as follows:

1. Check the 'Use dynamic DNS' checkbox.
2. Enter the domain name of your dynamic DNS provider in the 'Domain name' field.
3. Enter the name of your domain in the 'Domain name' field.
4. Enter the user name of your account with the dynamic DNS provider in the 'User name' field.
5. Enter the password of your account with the dynamic DNS provider in the 'Password' field.
5.1.3 Setting up a VPN connection on the router

To establish secure access to the fire detection system network, you must set up a VPN connection. A VPN connection requires a VPN configuration file. In the FRITZ!Box example configuration, the VPN configuration file is created with the 'Set up FRITZ!Box remote access' software. The following steps describe how to create a VPN configuration file.

An active VPN connection deactivates all other data connections. If you need to access the Internet while a VPN connection is active, check the 'Send all data via VPN tunnel' checkbox in the 'Specify IP network for your FRITZ!Box' dialog window. See step 10.

1. Install the 'Set up FRITZ!Box remote access' software.
2. Start the 'Set up FRITZ!Box remote access' software.
3. Select 'New'.
4. Select 'Set up remote access for a user'.

![Figure 4: Setting up VPN for a user](image)

5. Select 'iPhone / iPod touch / iPad' as the device.

![Figure 5: Device type 'iPhone / iPod touch / iPad'](image)
6. Enter the user name. You must enter the name of the user who wants to use his or her smartphone to connect to the station. Avoid using special characters and the @ character.

7. Enter the domain name of your router. To use a domain name, you must previously have registered with a dynamic DNS provider.

8. Select 'Use a different IP network'.

9. Enter the IP address '192.168.200.0' for the FRITZ!Box in the 'IP network' text box.
10. Enter the IP address of the user in the 'IP address of the user on the FRITZ!Box network' text box. The first user is assigned the unique IP address '192.168.200.11'. For each additional user, the last digit of the IP address increases by 1 (12, 13, 14, etc.).

- Optional: Check the 'Send all data via VPN tunnel' checkbox if you require Internet access when a VPN connection is active.

11. Select a key and enter a password.
12. Select 'Show directory containing the configuration files'. The directory displayed contains a subdirectory named after the user. This subdirectory contains the VPN user file with all the information the user needs to activate the VPN on his or her smartphone.

![Figure 10: Display directory with configuration file](image)

- You have created a VPN connection for the FRITZ!Box. The VPN connection has been enabled for a user.

**Configure VPN connection for additional users**

If additional users are to be enabled via a VPN connection for the FRITZ!Box, proceed as follows:

1. Start the 'Set up FRITZ!Box remote access' software.
2. Select the domain name of the VPN connection you have set up followed by 'New'.

![Figure 11: Select domain name](image)
3. Select 'Set up remote access for a user' followed by the domain name of your router.

![Figure 12: Select domain name](image)

4. Proceed as described under 'Setting up a VPN connection', point 5.
5.1.4 Activating a VPN connection on the router

The following steps describe how to activate the VPN connection that has been set up on the router.

1. Open the user interface of your router. In FRITZ!Box example configuration, select 'Enable' from the 'Internet' menu.

2. Select the 'VPN' tab.

3. Press the 'Browse' button to load a configuration file.

4. Navigate to the directory created when the VPN connection was set up. Open the VPN configuration file with the file extension '.cfg'.

5. Select 'Import VPN settings'. If an additional VPN user has been added for an existing domain name, the VPN configuration file must be re-opened and the VPN settings must be re-imported.
5.1.5 Configuring a VPN connection on a smartphone

A VPN connection to the router must be set up to connect a smartphone to the station. Use the VPN application in the Android operating system to do this. You can configure the VPN settings in the 'Settings' > 'More settings' > 'VPN' menu. To set up a VPN connection, proceed as follows:

1. Select 'Add VPN network'.
2. Enter a name for the connection in the 'Name' field.
3. Select the value 'IPSec Xauth PSK' in the 'Type' field.
4. Enter the domain name of the router in the 'Server address' field. You will find the domain name in the VPN user file under 'Server'.
5. Enter the user name in the 'IPSec Identifier' field. You will find the user name in the VPN user file under 'Group name'.
6. Enter the key in the 'IPsec Pre-shared Key' field. You will find the key in the VPN user file under 'Shared Secret'.
7. Save the configuration.

You have configured the VPN connection to the router.
5.1.6 Starting a VPN connection on a smartphone

An Internet connection on the smartphone is required to establish a VPN connection between the smartphone and the station. The Internet connection can be established via mobile telecommunications or WLAN.

The following steps describe how to start the configured VPN connection in the VPN application in the Android operating system.

If the connection is interrupted, the VPN application in the Android operating system will not start a new one. After a connection interruption, you must restart the VPN connection manually.

1. Select the configured VPN connection.
2. Enter the user name in the 'User name' field. You will find the user name in the VPN user file under 'Account'.
3. Enter the password in the 'Password' field. You will find the password in the VPN user file under 'Password'.
4. Select 'Connect'.

You have established the VPN connection between your smartphone and the router.
5.1.7 Deactivating a VPN connection on a smartphone

The following steps describe how to deactivate an active VPN connection in the Android operating system.

1. Drag the top edge of the screen down to open the system toolbar.
2. Select 'VPN activated'.
3. Select 'Disconnect connection'.

You have deactivated the VPN connection between your smartphone and the router.

5.2 Connection via WLAN wireless network

We recommend using a mobile data connection to connect a smartphone to the 'Station'. Connections via WLAN are limited in range and are not entirely suitable for connecting a smartphone to the 'Station'.

To connect a smartphone to the 'Station' via WLAN, you must start up the router and establish a connection with the 'Station' via a network cable.

Check that your router's user interface is set to 'Advanced view' in the system settings. You will find more information about setting up the advanced view in the router's user interface in the manufacturer's user manual.
To connect a smartphone to the 'Station' via WLAN, proceed as follows:

1. Activate the WLAN connection on the router. Link [→ 31]
2. Activate the WLAN encryption on the router. Link [→ 32]
3. Connect the smartphone to the router's WLAN wireless network.
   ➔ Your smartphone is connected to the 'Station'.

5.2.1 Activating a WLAN connection on the router

WLAN Internet access must be activated on the router. A 'FRITZ!Box' router is used in the commissioning example described below.

The manufacturer's manual describes how to set up Internet access via WLAN on the FRITZ!Box. The manual can be downloaded from the manufacturer's Internet site or opened from the user interface of the FRITZ!Box configuration system. If you are using a different router, you must obtain the manual from the manufacturer.

The following figure shows the example configuration after Internet access via WLAN has been activated on the FRITZ!Box. The 'Name of WLAN wireless network (SSID)' field must be completed with your commissioning information.

Figure 17: FRITZ!Box settings for activating Internet access via WLAN
5.2.2 Activating WLAN encryption on the router

Activating WLAN encryption protects the WLAN wireless network against unauthorized use.

The following steps describe how to activate WLAN encryption on the router:

1. Open the user interface of your router. In FRITZ!Box example configuration, select 'Security' from the 'WLAN' menu.
2. Select 'WLAN encryption'.
3. Select 'WPA2 (CCMP)' mode in the 'WPA mode' field.
4. Enter a WLAN network key.
5. Press the 'Apply' button.

Figure 18: Activate WPA encryption
6 Configuring a 'station' for smartphones

With 'Cerberus Mobile', up to 5 smartphones can access a Site simultaneously with 'Limited access (view only)' or 'Full access (view/operation)'.

The configuration of the 'Station' is required for the smartphone to access the 'Station'. To configure the 'Station', proceed as follows:

1. Configure visibility for 'Cerberus Mobile'. Link [➡ 33]
2. Optional: Configure a connection event for 'Cerberus Mobile'. Link [➡ 34]
3. Specify the operation mode for 'Cerberus Mobile'. Link [➡ 35]
4. Issue the enable for the smartphone. Link [➡ 36]

6.1 Configuring visibility for Cerberus Mobile

To configure 'Visibility' for smartphones in FXS 7212, proceed as follows:

1. Select 'Operation' > 'Station' in the task card.
2. Create the 'Cerberus Mobile' element for the 'Station'.
3. Open 'Cerberus Mobile' in the tree view.
4. Select 'Standard visibility'.
5. Select 'Assign'.
6. In the 'Assign' window, select the 'Station' on which you want to set 'Visibility' for smartphones and confirm your choice by clicking 'Assign'.
7. Go to the tree view and select the assigned 'Station'. Then select the 'Overview' tab.
8. Activate the 'ALL event categories visible' option.
   - 'Visibility' for smartphones has now been specified.
   - All 'Event categories of the 'Station' are visible for smartphones.

Figure 19: Configuring visibility
6.2 Configuring connection event for Cerberus Mobile

A station can be configured so that it issues an event when a mobile device establishes a connection to the station via the 'Cerberus Mobile' application. All stations that have corresponding visibility of the station then display a corresponding message on the display of the Person Machine Interface. At the same time, the station records the event in the event memory.

Configuration process

- You have already configured the 'Cerberus Mobile' application for a station. You will find information on this in chapter 'Configuring visibility for Cerberus Mobile [➙ 33]'.
- You have already registered at least one mobile device on the 'PMI' of the station. You will find information on this in chapter 'Enable smartphone [➙ 36]'.

1. Highlight the following element in the 'Operation' task card under the station on which you have registered the mobile device: 'Cerberus Mobile' > 'Cerberus Mobile client'

   **Information:** Each 'Cerberus Mobile client' element represents a mobile device enabled at the station.

2. Select the 'Events' tab in the detail editor.

3. Open the 'Cerberus Mobile connected' event in the tab.

4. Put a check mark next to the 'Enabled' property or remove it, depending on whether the station should issue the event or not.

5. Repeat the previous configuration steps for all mobile devices for which you want to configure this behavior.

6. Save the configuration.

**See also**

- Enable smartphone [➙ 36]
- Configuring visibility for Cerberus Mobile [➙ 33]
6.3 Specifying the operation mode for Cerberus Mobile

Specification of operation mode on the 'Station'

The 'Cerberus Mobile' element must be configured manually in Cerberus-Engineering-Tool for a 'Station'.

You can configure a permanent operation mode for 'Cerberus Mobile' in 'Cerberus-Engineering-Tool'. If 'Permanent Cerberus Mobile access' is configured, you do not need to define the operation mode on the 'Station'.

1. Select 'Main menu' > 'Topology'.
2. Select the 'Hardware tree' subtree.
3. Navigate to 'Station' > 'Mobile'.
4. Press the 'More Options' softkey.
5. Select 'Execute Commands' and confirm with <ok>.  
   ⇨ The 'Select command' window is open.
6. Select the 'Enable full access' or 'Enable view access' command and confirm with <ok>.  
   ⇨ The operation mode for 'Cerberus Mobile' is now specified.

Deactivation of operation mode on the 'Station'

If you have permanently configured the operation mode in 'Cerberus-Engineering-Tool', you must deactivate the operation mode in 'Cerberus-Engineering-Tool'.

Proceed as for 'Specification of operation mode on the 'Station'' and select the 'Disable access' command in the 'Select command' window.
6.4 Enable smartphone

You can use Cerberus Mobile in a fire detection installation with networked 'Stations' to gain global 'Visibility'. Just one license key is needed for this per network in the 'Station' to which 'Cerberus Mobile' is connected.

You will find more information about license keys in document A6V10210362. See chapter 'Applicable documents'.

To enable a smartphone at the 'Station', proceed as follows:

- You have specified the Visibility for smartphones in 'Cerberus-Engineering-Tool'.
- You have specified the operation mode for Cerberus Mobile at the 'Station'.
- You have established a connection with the 'Station' on your smartphone.
- You have installed 'Cerberus Mobile' on your smartphone.
- You have started 'Cerberus Mobile' on your smartphone.
- The 'New client found' message is displayed. The IMEI number of the smartphone is displayed for identification purposes. For more information, see the example display at the end of this chapter.

1. Select 'Client' or, in the 'Message summary' main menu, select the 'Information' menu followed by 'Client'.
2. Press the 'Execute Commands' softkey.
3. Optional: Select the 'Set customer text' command.
4. Optional: Enter the required Customer text for the smartphone and confirm with <ok>.
   - The Customer text for the smartphone has now been entered.
5. Select the 'Accept Cerberus Mobile client' command and confirm with <ok>.
   - The smartphone is enabled on the 'Station'.

<table>
<thead>
<tr>
<th>Remote transmission activated</th>
<th>004 Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>1/1</td>
</tr>
<tr>
<td>837622498004</td>
<td>New client found</td>
</tr>
<tr>
<td></td>
<td>004</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Execute Commands</th>
<th>Show Intervention text</th>
<th>More Options</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1: Example display: Smartphone visible on station
6.5 Removing a smartphone

To remove a smartphone from a 'Station', proceed as follows:

1. Select 'Main menu' > 'Topology'.
   ⇨ The three partial trees of the topology tree are indicated.
2. Select 'Hardware tree'.
3. Select the 'Station'.
4. Select 'Mobile'.
5. Select the smartphone.
6. Press the 'Execute Commands' softkey.
7. Select the 'Remove Cerberus Mobile client' command and confirm with <ok>.
   ⇨ The smartphone is removed at the 'Station'.

6.6 Access level

In the case of 'Cerberus Mobile', the same 'PINs' apply as in the case of 'Station'.

**Enter 'PIN' in 'Cerberus Mobile'**

1. Select the 'Topology view' button.
   ⇨ The 'Login' dialog window opens.
2. Enter the 'PIN' for the station.
   ⇨ You have entered the 'PIN' in 'Cerberus Mobile'.
7 General commissioning steps

The following chapters contain general commissioning steps that are referred to in several chapters.

You will find more information on commissioning an FS720 fire detection system and/or a 'Station' in document A6V10210416.

7.1 Detector test

The 'Detector test' is a hardware function test for the devices and their assignment to 'Detection tree'.

You will find information about 'Detector test' in document A6V10211076. See chapter 'Applicable documents'.

Switch on 'Detector test' with 'Cerberus Mobile'

1. Select the 'Topology' button from the toolbar on the start page of 'Cerberus Mobile'.
   - The 'Topology' opens.
2. Select 'Detection tree'.
3. Navigate to the element you want to switch to test mode: 'Area', 'Section', or 'Zone'.
4. Press and hold down the element until the action bar is displayed.
5. Select the 'Detector test' command from the action bar or the overflow menu.
   - You will find the icon for the overflow menu on the right-hand side of the action bar.

Figure 20: Commands in the overflow menu

- The element is in test mode for the 'Detector test'.

Switch off 'Detector test' with 'Cerberus Mobile'

Proceed as for 'Switch on 'Detector test' and select the 'Detector test END' command from the action bar or the overflow menu.

Figure 21: Commands in the overflow menu
7.2 Control test

The 'Control test' tests the function of the configured 'Controls' as in normal operation, but the outputs are not activated. The 'Control test' checks the function of configured controls.

During the 'Control test', the controls function in the same way as during normal operation; however, the hardware is not actuated.

An activation message is generated for all configured effects, such as the actuation of digital outputs and sounders or the execution of commands. The hardware concerned does not receive a signal and is not activated.

Depending on their configuration, all controls can be set to 'Control test'.

Switch on 'Control test' with 'Cerberus Mobile'

1. Select the 'Topology' button from the toolbar on the start page of 'Cerberus Mobile'.
   - The 'Topology' opens.
2. Select 'Control tree'.
3. Navigate to an 'Control' you want to switch to test mode.
4. Press and hold down the element until the action bar is displayed.
5. Select the 'Control test' command from the action bar or the overflow menu.

![Figure 22: Commands in the overflow menu]

- The element is in test mode for the 'Control test'.
Switch off 'Control test' with 'Cerberus Mobile'
Proceed as for 'Switch on 'Control test' and select the 'Control test END' command from the action bar or the overflow menu.

Figure 23: Commands in the overflow menu

7.3 Switching off 'Zone'

<table>
<thead>
<tr>
<th>WARNING</th>
</tr>
</thead>
<tbody>
<tr>
<td>No compliance with EN 54</td>
</tr>
<tr>
<td>Switching off a 'Zone' with 'Cerberus Mobile' does not comply with EN 54.</td>
</tr>
</tbody>
</table>

1. Select the 'Topology' button from the toolbar on the start page of 'Cerberus Mobile'.
2. Navigate to the 'Zone' you want to switch off.
3. Press and hold down the 'Zone' until the action bar is displayed.

Figure 24: 'Select command'

4. Select the 'OFF' command from the action bar.

\(\Rightarrow\) The 'Zone' is switched off.
7.4 Switching on 'Zone'

⚠️ WARNING
No compliance with EN 54
Switching on a 'Zone' with 'Cerberus Mobile' does not comply with EN 54.

1. Select the 'Topology' button from the toolbar on the start page of 'Cerberus Mobile'.
2. Navigate to the 'Zone', you want to switch on.
3. Press and hold down the 'Zone' until the action bar is displayed.
4. Select the 'ON' command from the action bar or the overflow menu.

![Figure 25: 'Select command'](#)

- The 'Zone' is switched on.
7.5 Adapting preferences

To adapt 'Preferences' in 'Cerberus Mobile, proceed as follows:

1. Press the menu button on the left of the start screen button on the smartphone.
   a) The menu opens.
2. Select 'Preferences'.
   a) The 'Preferences' dialog window opens.
3. Press a category to configure the 'Preferences'.

The categories of 'Preferences' are described in the next section.

'Panel settings'

- **IP address/Host name**: IP address of the 'Station'
- **Host ID**: Address of 'Station' at which 'Cerberus Mobile' was configured

Figure 26: 'Panel settings'

'Local settings'

- **Auto start**: This setting specifies whether 'Cerberus Mobile' is to be started automatically when the smartphone operating system starts up.
- **Alarm tone**: Selection of ring tone for new messages
- **Notification tone**: Selection of audible signal for new messages

Figure 27: 'Local settings'

'Notification options foreground' / 'Notification options background'

You can make settings for audible notifications if 'Cerberus Mobile' is active in the foreground or background.

The following table lists the message options that can be configured for the 'Notification options foreground' and 'Notification options background' categories.
General commissioning steps
Adapting preferences

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>'Notification mode'</td>
<td>Notification mode for new messages</td>
</tr>
<tr>
<td></td>
<td>● 'None': No audible notifications are output</td>
</tr>
<tr>
<td></td>
<td>● 'Alarm tone': The ring tone for new messages is output¹</td>
</tr>
<tr>
<td></td>
<td>● 'Notification tone': The audible signal for new messages is output</td>
</tr>
<tr>
<td></td>
<td>● 'Text to speech': New messages are read out via automatic voice output</td>
</tr>
<tr>
<td>'ALARMS'</td>
<td>Notification of 'ALARMS'</td>
</tr>
<tr>
<td>'Pre-ALARMS'</td>
<td>Notification of 'Pre-ALARMS'</td>
</tr>
<tr>
<td>'Faults'</td>
<td>Notification of 'Faults'</td>
</tr>
<tr>
<td>'Test activations'</td>
<td>Notification of 'Test activations'</td>
</tr>
<tr>
<td>'Technical messages'</td>
<td>Notification of 'Technical messages' e.g., 'Sabotage ALARM' for key depot</td>
</tr>
</tbody>
</table>

¹ Category 'Notification options background' only.

Example configurations

**Notification mode foreground**

- none
- Notification tone
- Text to speech

![Figure 28: 'Notification mode foreground']

**Notification options background**

- none
- Alarm tone
- Notification tone
- Text to speech

![Figure 29: 'Notification mode background']
8 General operations
The following chapters describe general operations that are referred to in several chapters. In 'Cerberus Mobile' you cannot perform all of the operations that can be performed on the 'Station'. The operations that are available in 'Cerberus Mobile' are the same as those on the 'Station'.

You will find more information about operating a 'Station' in document A6V10211076.

8.1 Acknowledging an 'ALARM'

<table>
<thead>
<tr>
<th>WARNING</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No compliance with EN 54</strong></td>
</tr>
<tr>
<td>Acknowledging an 'ALARM' with 'Cerberus Mobile' does not conform to EN-54.</td>
</tr>
</tbody>
</table>

- Press the 'Acknowledge' button on the start screen in 'Cerberus Mobile'.

![Figure 30: Acknowledge alarm](image)

- The alarm is acknowledged.
- The buzzer is switched off.
- With ↑ 'AVC', countdown t2 for examining the cause of 'ALARM' starts.

You will find information about how to proceed in the event of an 'ALARM' in document A6V10211076. See chapter 'Applicable documents'.
8.2 Resetting an 'ALARM'

<table>
<thead>
<tr>
<th>WARNING</th>
</tr>
</thead>
</table>
| No compliance with EN 54  
Resetting an 'ALARM' with 'Cerberus Mobile' does not conform to EN-54. |

The alarm message must be acknowledged before an alarm is reset. If the cause of an alarm is not remedied, a new alarm event will be triggered once an alarm has been reset.

1. Press the menu button on the left of the start screen button on the smartphone.  
   - The menu opens.
2. Select 'Reset'.  
   - The ALARM is reset.

You will find information about how to proceed in the event of an 'ALARM' in document A6V10211076. See chapter 'Applicable documents'.

8.3 Acknowledge fault

1. Press the 'Acknowledge' button on the start screen in 'Cerberus Mobile'.
2. Read the location of the cause of the 'Fault' displayed from the display.
3. Go to the location of the cause.
4. Remove the cause of the 'Fault'.  
   - or  
5. Contact service if you are unable to remove the cause of the 'Fault' yourself.

You will find information about how to proceed in the event of a fault in document A6V10211076. See chapter 'Applicable documents'.

8.4 Execute commands

You will find commands for elements or events on the action bar. The number of
commands on the action bar is determined by the size of the smartphone screen.
All other commands can be found in the action bar overflow menu.

Executing commands for elements in the topology
1. In the topology, navigate to the element for which you wish to execute a
   command.
2. Press and hold down the element until the action bar is displayed.
3. Select a command from the action bar or press the button for the overflow
   menu and select a command from the overflow menu.

Executing commands for events on the start screen
You can execute commands for current events directly from the start screen.
1. Press and hold down the event until the action bar is displayed.
2. Select a command from the action bar or press the button for the overflow
   menu and select a command from the overflow menu.

Close action bar
If no commands are to be executed, the action bar can be closed again after
opening.
● Press the button with the check mark on the left-hand side of the action bar.
❖ The action bar closes.
8.5 Displaying events

Display all events
All current events are displayed on the start screen in 'Cerberus Mobile'.

Extended view
The extended view shows a 4-line depiction of the selection. Additional information such as e.g. additional customer texts can be displayed this way.
- Press an event on the start screen in 'Cerberus Mobile'.
  ➤ The advanced view for an event is switched on.

![Figure 31: Details for event](image)

Filter events
In the example description of the operations, events in the 'Information' category are filtered.
1. Open the 'ALL' drop-down menu.
2. Select 'Information'.
  ➤ 'Information' type events are displayed.

8.6 Exiting Cerberus Mobile
1. Press the menu button on the left of the start screen button on the smartphone.
  ➤ The menu opens.
2. Select 'Exit'.
  ➤ You have exited 'Cerberus Mobile'.
9 Testing detectors

'Cerberus Mobile' makes it easy to test a detector. The steps of the operation can be executed in 'Cerberus Mobile'. No entries need to be made at the ↑ 'Station'. The following detector properties can be checked with 'Cerberus Mobile':

- 'Activation'
- 'Customer text'
- Assignment to 'Zone'

To check a detector, proceed as follows:

1. Switch on the 'Detector test' in 'Cerberus Mobile'. Link [→ 38]
2. Trigger the detector with the appropriate means. You will find information about triggering detectors in document A6V10212047. See chapter 'Applicable documents'.
3. Check 'Cerberus Mobile' to see if the detector has been activated.
4. Check the 'Cerberus Mobile' of the detector in 'Customer text'.
5. In 'Cerberus Mobile', check the assignment of the detector to 'Zone'.
6. Switch off the 'Detector test' in 'Cerberus Mobile'. Link [→ 38]

Next steps after the detector test

1. Optional: Change the customer text of the detector in 'Cerberus Mobile'.
2. Optional: In 'Cerberus-Engineering-Tool', check the assignment of the detector to a 'Zone'.
10 Control test

'Cerberus Mobile' makes it easy to test a control. The steps of the operation can be executed in 'Cerberus Mobile'. No entries need to be made at the 'station'. Multiple controls can be tested one after the other.

To test a control, proceed as follows:

1. Switch on the control test in 'Cerberus Mobile'. Link [→ 40]
2. Trigger all detectors necessary to activate the control cause with the appropriate means. You will find information about triggering detectors in document A6V10212047. See chapter 'Applicable documents'.
3. Check 'Cerberus Mobile' to see if the control has been activated.
4. Acknowledge the alarm. Link [→ 45]
5. Reset the alarm. Link [→ 46]
6. Switch off the control test in 'Cerberus Mobile'. Link [→ 40]
Glossary

AVC
Abbreviation for 'Alarm Verification Concept'.

Detection tree
Diagram of the geographical and organizational arrangements of sensors in a building. This is a hierarchical structure comprising the area, section, and zone.

Detector line
Electrical connection between the detectors and the fire control panel. There are collective detector lines and addressed detector lines.

Effect
An impact caused by a control, e.g., activation of a hardware output or a command.

Hardware tree
Depiction of the hardware of a fire detection installation.

Isolation
Status of one part of the fire detection installation, which suppresses the evaluation of all signals.

License key
Hardware modules for activating functions.

Normal operation
The fire detection installation is supplied with mains voltage.

Section
Level in detection tree of the fire detection system. The section is assigned to the area. It is used for combining zones.

Soft keys
Softkeys are buttons which you can use to carry out functions and which are displayed in the three fields of the softkey line on the display. These three black fields contain the names of the functions in white font. The functions of the softkeys change dynamically depending on the situation and the contents of the display. Always the most important functions are assigned to the softkeys 1 and 2.

Station
Unit for system control. Fire control panel or fire terminal.

Visibility
Defines which part of a site is visible and can be operated on a station.
Index

A
Access level.................................................... 37
Acknowledge
  Alarm............................................................. 45
  Fault.................................................................. 46
Alarm
  Acknowledge.................................................. 45
C
Connection
  Station.......................................................... 19
Control test..................................................... 40
  Check activation............................................. 50
  ON.................................................................. 40
  Switching off................................................. 41
D
Detector test.................................................... 38
  Check activation............................................. 49
  Check customer text....................................... 49
  Check zone.................................................... 49
  ON.................................................................. 38
  Switching off................................................. 39
Download......................................................... 18
Download center
  URL.................................................................. 8
Dynamic DNS service........................................ 21
E
Enable............................................................ 36
Encryption......................................................... 32
Event
  Extended view................................................ 48
  Filter.................................................................. 48
  Indicators......................................................... 48
Execute command............................................. 47
Extended view
  Event................................................................ 48
F
Fault
  Acknowledge.................................................. 46
Filter
  Event................................................................ 48
H
Home network.................................................. 17
I
Indicators
  Event................................................................ 48
Installation....................................................... 18
Internet connection
  Activation....................................................... 20, 31
  Mobile telecommunications............................ 19
  WLAN.............................................................. 30
L
Local settings.................................................... 43
O
Operating requirements
  Applications.................................................... 15
  Device............................................................. 15
  License........................................................... 15
Operation......................................................... 45
Original language.............................................. 6, 6
P
PIN .................................................................. 37
R
Remove.......................................................... 37
Router............................................................. 16
  Connecting...................................................... 16
  Dynamic DNS service....................................... 21
  Encryption....................................................... 32
  Internet connection......................................... 20, 31
  Setting up a home network............................... 17
S
Settings............................................................ 43
  Smartphone..................................................... 43
  Station............................................................ 43
Source language............................................... 6, 6
Start Screen
  Execute command........................................... 47
Station
  Connection...................................................... 19
  Enabling a smartphone.................................... 36
  Removing a smartphone.................................... 37
<table>
<thead>
<tr>
<th>W</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLAN ..................... 30</td>
<td>Zone</td>
</tr>
<tr>
<td>WPA ..................... 32</td>
<td>ON .................................................................. 42</td>
</tr>
<tr>
<td></td>
<td>Switch off ........................................ 41</td>
</tr>
</tbody>
</table>