

# Technische Dokumentation Fernzugriff Hekatron Remote





---

## Inhalt

|                                               |    |
|-----------------------------------------------|----|
| 1. Einleitung .....                           | 5  |
| 2. Bestimmungsgemäße Verwendung .....         | 5  |
| 3. Sicherheitshinweise .....                  | 6  |
| 4. Produktbeschreibung .....                  | 6  |
| 4.1 Übersicht .....                           | 6  |
| 4.2 Anwendungen .....                         | 7  |
| 5. Schnittstellen .....                       | 8  |
| 5.1 VPN-Router LAN .....                      | 8  |
| 5.2 VPN-Router Mobilfunk (LTE/LAN) .....      | 9  |
| 6. Projektierung .....                        | 10 |
| 6.1 Allgemeines .....                         | 10 |
| 6.2 Voraussetzungen .....                     | 11 |
| 6.3 Projektierungsbeispiele .....             | 13 |
| 6.4 Sicherheitskonzept .....                  | 15 |
| 7. Montage .....                              | 16 |
| 7.1 Antennenmontage .....                     | 16 |
| 8. Installation .....                         | 17 |
| 8.1 IP-Adressvergabe .....                    | 17 |
| 8.2 Gerätekonfiguration .....                 | 18 |
| 8.3 Anschluss VPN-Router LAN .....            | 20 |
| 8.4 Anschluss VPN-Router Mobilfunk .....      | 20 |
| 9. Programmierung .....                       | 21 |
| 9.1 IP Adressen vergeben .....                | 21 |
| 9.2 Fernbedienfelder anlegen .....            | 22 |
| 9.3 Benutzer anlegen .....                    | 23 |
| 9.4 Benutzer zuordnen .....                   | 25 |
| 9.5 Push Nachrichten .....                    | 26 |
| 9.6 Integral Mail .....                       | 27 |
| 9.7 Verzögerung Störung Fremdsystem .....     | 29 |
| 9.8 Freigabe/Sperre über Element Extern ..... | 31 |

---

|                                              |           |
|----------------------------------------------|-----------|
| <b>10. Checkliste</b>                        | <b>34</b> |
| 10.1 Planungsphase:                          | 34        |
| 10.2 Durchführungsphase                      | 35        |
| <b>11. Fehlermeldungen</b>                   | <b>36</b> |
| <b>12. Remote Mein HPlus Adminoberfläche</b> | <b>37</b> |
| 12.1 Stationen                               | 38        |
| 12.2 Menüleiste                              | 42        |
| 12.3 Aktivitäten                             | 43        |
| 12.4 Org.Einheiten                           | 44        |
| 12.5 Benutzer                                | 45        |
| 12.6 Gruppen                                 | 48        |
| 12.7 Router                                  | 49        |
| 12.8 VPNs                                    | 50        |
| 12.9 Wartung                                 | 50        |
| <b>13. Bedienung</b>                         | <b>51</b> |
| 13.1 Remote Standard                         | 51        |
| 13.2 Remote Mobile                           | 55        |
| <b>14. Instandhaltung</b>                    | <b>60</b> |
| <b>15. Technische Daten</b>                  | <b>62</b> |
| 15.1 VPN-Router LAN                          | 62        |
| 15.2 VPN-Router Mobilfunk                    | 62        |
| <b>16. Maßbild</b>                           | <b>63</b> |
| <b>17. Bestelldaten</b>                      | <b>63</b> |

## 1. Einleitung

Diese Technische Dokumentation gilt für den Fernzugriff Hekatron Remote über VPN-Router, im weiteren Text meist Fernzugriff oder Hekatron Remote genannt. Dieses Dokument ist gültig ab Produktversion 30-4800013-0x-01.

### Symbole und Signalwörter

In dieser Betriebsanleitung werden folgende Symbole und Signalwörter verwendet:

| Symbol/<br>Signalwort                                                             | Bedeutung                                                                                |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| <b>GEFAHR</b>                                                                     | Warnhinweis, der bei Nichtbeachtung zu schweren Verletzungen oder zum Tod führt.         |
| <b>WARNUNG</b>                                                                    | Warnhinweis, der bei Nichtbeachtung zu schweren Verletzungen oder zum Tod führen kann.   |
| <b>VORSICHT</b>                                                                   | Warnhinweis, der bei Nichtbeachtung zu leichten oder mittleren Verletzungen führen kann. |
| <b>ACHTUNG</b>                                                                    | Warnhinweis, der bei Nichtbeachtung zu Sachschäden oder Funktionsstörungen führen kann.  |
|  | Hinweis auf zusätzliche Information                                                      |
|  | Handlungsanweisung                                                                       |
|  | Ergebnis einer Handlung                                                                  |
| -                                                                                 | Aufzählung                                                                               |

Die Warnhinweise sind wie folgt aufgebaut:

#### **SIGNALWORT**

Art und Quelle der Gefahr

Folgen bei Nichtbeachtung

► Maßnahmen zur Gefahrenabwehr

## 2. Bestimmungsgemäße Verwendung

- Verwendung an einer Brandmelderzentrale für den Fernzugriff über PC (per Browser) oder mobile Endgeräte (per App) zur Echtzeit-Information und Bedienung

### Nicht bestimmungsgemäße Verwendung

- Keine Verwendung an anderen Anlagen als einer Brandmelderzentrale

Wenn der Router nicht bestimmungsgemäß verwendet wird, haftet die Hekatron Vertriebs GmbH nicht für Schäden, die daraus resultieren.

### 3. Sicherheitshinweise

Wenn die Sicherheits- und Bedienungshinweise nicht beachtet werden, bestehen keine Haftungs- und Gewährleistungsansprüche gegenüber der Hekatron Vertriebs GmbH.

#### Allgemein

- Für einen ordnungsgemäßen und sicheren Gebrauch des Routers die Anleitung vollständig lesen und den Anweisungen folgen
- Die Anleitung für ein späteres Nachschlagen aufbewahren
- Das Gerät nur in unbeschädigtem Zustand betreiben
- Das Gerät nicht öffnen, umbauen oder modifizieren
- Die Typenschilder und Kennzeichnungen auf dem Gerät nicht entfernen, überschreiben oder unkenntlich machen

### 4. Produktbeschreibung

Hekatron Remote („remote“ = fern, entfernt) bezeichnet generell einen Fernzugriff auf die Brandmelderzentrale Integral über das Intranet (internes Netzwerk) oder Internet, um zu jeder Zeit von jedem Ort Informationen abzurufen, Bedienvorgänge durchzuführen oder Programmiertätigkeiten nach geltenden Normen vorzunehmen.

- Informationen abrufen z. B. Zustandsanzeige oder Empfang von programmierten Meldungen (Alarmer, Störungen)
- Bedienvorgänge durchführen z. B. abgesetzte Bedienung (Leitstelle, Pforte) oder Unterstützung bei Bedienungsschwierigkeiten
- Servicetätigkeiten vornehmen z. B. Vorbereitung eines Instandhaltungseinsatzes oder Assistenz bei Fehlersuche und Programmierung

Bei Hekatron Remote wird generell zwischen 2 Zugriffsarten unterschieden, die vom eingesetzten Endgerät (Windows-PC oder mobiles Endgerät) abhängig sind. Während der Fernzugriff mit dem Windows-PC über die Integral Software erfolgt, ist bei mobilen Endgeräten eine spezielle kostenfreie App (Integral Mobile) erforderlich. Zusätzlich unterstützt die Zentrale auch den automatischen Versand von E-Mails (Integral Mail).

#### 4.1 Übersicht

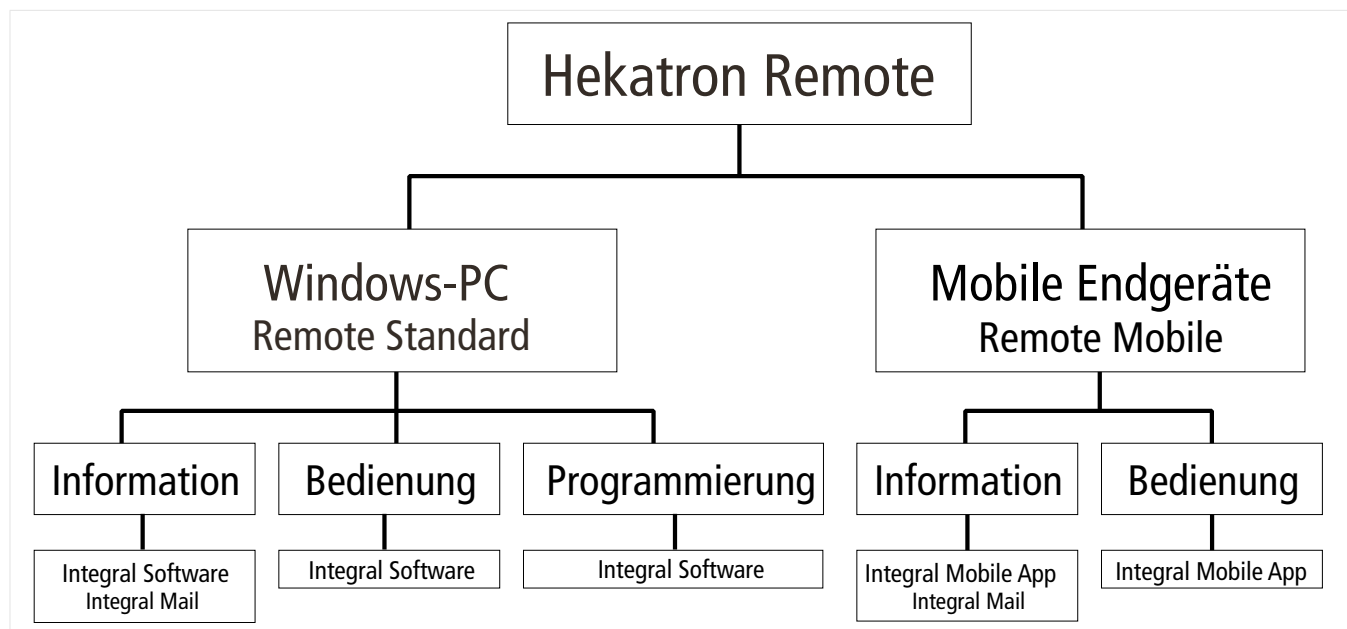


Abb. 1: Übersicht Hekatron Remote

## 4.2 Anwendungen

### Integral Software

Software mit entsprechendem Dongle zur Bereitstellung von Anwendungen auf einem Windows-PC. Folgende Anwendungen können über Hekatron Remote genutzt werden.

- Loader
- Peripherie Assistant
- Service Assistant
- Integral Desktop (virtuelles Integral Bedienfeld, ehemals VirtualMAP)

Die Anwendung Integral Desktop steht auch als eigenständige Lösung mit entsprechendem Dongle ohne Integral Software zur Verfügung.



Abb. 2: Integral Software

### Integral Mobile

App zur Bereitstellung des Integral Desktop (virtuelles Integral Bedienfeld) auf mobilen Endgeräten. Mit Push Nachrichten zur automatischen Benachrichtigung bei Auftreten eines Ereignisses (z. B. Alarm oder Störung) und Geo Check zur Einschränkung des Bedienungsradius.



Abb. 3: Integral Mobile

### Integral Mail

Funktion zum automatischen E-Mail Versand durch die Brandmelderzentrale bei Auftreten eines Ereignisses wie z. B. Alarm oder Störung an einen oder mehrere Empfänger auf PC oder mobilen Endgeräten.



Abb. 4: Integral Mail

Der Fernzugriff auf die Zentrale wird über die Remote Mein HPlus Adminoberfläche gesteuert, die alle notwendigen Daten zur Verbindung von PC oder mobilem Endgerät zu den Zentralen enthält. Die Anbindung der Brandmelderzentralen erfolgt über speziell konfigurierte VPN-Router (LAN oder Mobilfunk) mit Zertifikat.

PCs greifen mit entsprechender VPN-Software (z. B. OpenVPN), Zertifikat und Dongle, mobile Endgeräte über Zugangsdaten (Benutzername, Passwort) und eine verschlüsselte Verbindung auf die Zentrale zu.

## 5. Schnittstellen

Es werden nur die jeweils relevanten Schnittstellen auf den Geräten für die Anwendung Hekatron Remote beschrieben.

**ACHTUNG**

Router wird auf Werkseinstellungen zurückgesetzt und die Vorkonfiguration auf Anwendung Hekatron Remote gelöscht.  
Zur Neukonfiguration muss der Router an Hekatron eingeschickt werden.

- Keinesfalls einen Reset über die Taste RST am Router durchführen

### 5.1 VPN-Router LAN

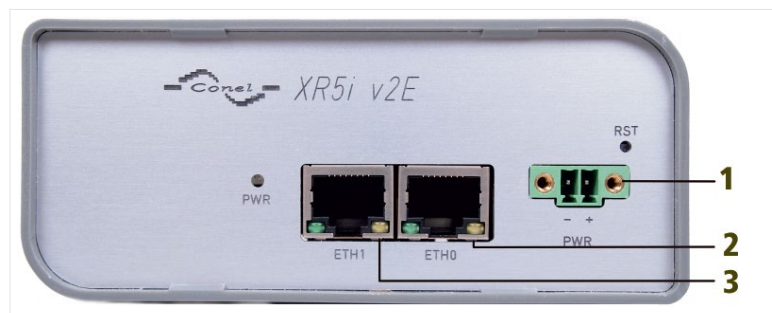


Abb. 5: Schnittstellen am VPN-Router LAN

|   |                                     |
|---|-------------------------------------|
| 1 | Anschlusstecker Stromversorgung     |
| 2 | Anschlusstecker Ethernet (Zentrale) |
| 3 | Anschlusstecker Ethernet (Netzwerk) |

#### 1 - Anschlusstecker Stromversorgung

|                   |                                |
|-------------------|--------------------------------|
| Betriebsspannung  | 10 bis 30 V DC                 |
| Mechanisch        | 2-polige Schraubklemme         |
| LED-Anzeige (PWR) | grün blinkend - betriebsbereit |

| Klemme | Bezeichnung | Funktion |
|--------|-------------|----------|
| 1      | +           | 24 V (+) |
| 2      | -           | GND (-)  |

#### 2/3 - Anschlusstecker Ethernet

|                 |                                                                                                                       |
|-----------------|-----------------------------------------------------------------------------------------------------------------------|
| Richtung        | bidirektional, voll duplex                                                                                            |
| Geschwindigkeit | max. 100 Mbit/s                                                                                                       |
| Leitungslänge   | max. 100 m                                                                                                            |
| Mechanisch      | RJ 45 Buchse, 8 polig<br>für Kabel ab Kategorie Cat-5                                                                 |
| LED-Anzeige     | grün an - 100 Mbit/s<br>grün aus - 10 Mbit/s<br>gelb an - Netzkabel angeschlossen<br>gelb blinkend - Datenübertragung |

| Klemme | Bezeichnung | Funktion      | Drahtfarbe  |
|--------|-------------|---------------|-------------|
| 1      | TX+         | Transmit Data | weiß/grün   |
| 2      | TX-         | Transmit Data | grün        |
| 3      | RX+         | Receive Data  | weiß/orange |
| 4      |             |               | blau        |
| 5      |             |               | weiß/blau   |
| 6      | RX-         | Receive Data  | orange      |
| 7      |             |               | weiß/braun  |
| 8      |             |               | braun       |



## 5.2 VPN-Router Mobilfunk (LTE/LAN)



Abb. 6: Schnittstellen am VPN-Router Mobilfunk (LTE/LAN)

|   |                                     |
|---|-------------------------------------|
| 1 | Steckplatz SIM-Karte                |
| 2 | Anschlusstecker Stromversorgung     |
| 3 | Anschlusstecker Ethernet (Zentrale) |
| 4 | Anschlusstecker GSM-Antenne         |

### 1 - Steckplatz SIM-Karte

|                  |                           |
|------------------|---------------------------|
| Betriebsspannung | 1,8 oder 3 V              |
| LED-Anzeige      | gelb an - SIM-Karte aktiv |

### 2 - Anschlusstecker Stromversorgung

|                   |                                |
|-------------------|--------------------------------|
| Betriebsspannung  | 10 bis 30 V DC                 |
| Mechanisch        | 2-polige Schraubklemme         |
| LED-Anzeige (PWR) | grün blinkend - betriebsbereit |

| Klemme | Bezeichnung | Funktion |
|--------|-------------|----------|
| 1      | +           | 24 V (+) |
| 2      | -           | GND (-)  |

### 3 - Anschlusstecker Ethernet

Zum Anschluss der BMZ nach TIA-568A. Der ETH2 Anschluss ist für eine zusätzliche (optionale) LAN-Verbindung vorgesehen.

|                 |                                                                                                                       |
|-----------------|-----------------------------------------------------------------------------------------------------------------------|
| Richtung        | bidirektional, voll duplex                                                                                            |
| Geschwindigkeit | max. 100 Mbit/s                                                                                                       |
| Leitungslänge   | max. 100 m                                                                                                            |
| Mechanisch      | RJ 45 Buchse, 8 polig<br>für Kabel ab Kategorie Cat-5                                                                 |
| LED-Anzeige     | grün an - 100 Mbit/s<br>grün aus - 10 Mbit/s<br>gelb an - Netzkabel angeschlossen<br>gelb blinkend - Datenübertragung |

| Klemme | Bezeichnung | Funktion      | Drahtfarbe  |
|--------|-------------|---------------|-------------|
| 1      | TX+         | Transmit Data | weiß/grün   |
| 2      | TX-         | Transmit Data | grün        |
| 3      | RX+         | Receive Data  | weiß/orange |
| 4      |             |               | blau        |
| 5      |             |               | weiß/blau   |
| 6      | RX-         | Receive Data  | orange      |
| 7      |             |               | weiß/braun  |
| 8      |             |               | braun       |

### 4 - Anschlusstecker GSM-Antenne

|                   |                              |
|-------------------|------------------------------|
| Mechanisch        | SMA-Steckverbinder           |
| LED-Anzeige (GSM) | rot blinkend - Kommunikation |
| LED-Anzeige (PPP) | gelb an - PPP Verbindung     |

## 6. Projektierung

Die Projektierung muss gemäß den geltenden Normen und Richtlinien durchgeführt werden.

### 6.1 Allgemeines

Zur Projektierung ist je nach gewünschter Anwendung die im folgenden aufgeführte Hardware mit entsprechender Software zu berücksichtigen.

|                               | Remote<br>Standard | Remote<br>Mobile | Integral<br>Mail |
|-------------------------------|--------------------|------------------|------------------|
| Brandmelderzentrale           | X                  | X                | X <sup>1)</sup>  |
| VPN-Router mit VPN-Zertifikat | X                  | X                | X                |
| DSL-Modem/Netzwerk            | X <sup>2)</sup>    | X <sup>2)</sup>  | X <sup>2)</sup>  |
| PC/Laptop                     | X <sup>3)</sup>    | X                | X <sup>4)</sup>  |
| Mobile Endgeräte              | -                  | X <sup>5)</sup>  | X <sup>4)</sup>  |
| Dongle                        | X                  | -                | -                |

Tab. 1: Benötigte Komponenten je nach Anwendung

Zusätzlich fällt für jede Hekatron Remote Verbindung (jeden Router) eine einmalige Gebühr für die Konfiguration der Hard- und Software und Einrichtung auf der Remote Mein HPlus Adminoberfläche an. Voraussetzung zur Nutzung der Anwendung ist zudem ein unterschriebener Lizenzvertrag, der eine jährliche Lizenzgebühr beinhaltet und den Zugang zur Remote Mein HPlus Adminoberfläche mit einer unbegrenzten Anbindung von Routern ermöglicht.

### Systemgrenzen

Generell können über Remote Standard maximal 8 Benutzer zur Bedienung und 1 Benutzer zur Programmierung gleichzeitig auf die Brandmelderzentrale zugreifen. Über Remote Mobile sind maximal 4 gleichzeitige Benutzer zur Bedienung möglich, die maximale Gesamtanzahl von 8 Benutzern darf aber auch im Mischbetrieb der beiden Anwendungen nicht überschritten werden.

Pro Brandmelderzentrale sind als übergeordnete Systemgrenze maximal 10 Netzwerkverbindungen möglich. Diese setzen sich zusammen aus bis zu 4 Netzwerkfunktionen (Modbus-TCP, ISP-IP, Integral Message und Integral Mail) und bis zu 8 Fernbedienfeldern (Integral Desktop) für den Fernzugriff.

Sind also z. B. bereits 3 Netzwerkfunktionen belegt, verbleiben lediglich 7 freie Netzwerkverbindungen für den gleichzeitigen Fernzugriff. Zusätzlich ist noch die Gesamtanzahl von maximal 16 Bedienfeldern (Summe aus externen und internen Bedienfeldern sowie B5-MMI-PIP und Integral Desktop) pro Brandmelderzentrale zu beachten.

<sup>1)</sup> Der Versand von E-Mails kann auch über den direkten Anschluss der Brandmelderzentrale an ein DSL-Modem erfolgen, dann sind jedoch nur unverschlüsselte E-Mails möglich, ab Integral Plattform B8/B9/B10 sind auch verschlüsselte Mails möglich

<sup>2)</sup> Nur erforderlich bei Einsatz eines LAN-Routers

<sup>3)</sup> VPN-Zertifikat erforderlich

<sup>4)</sup> Zum Empfang von E-Mails

<sup>5)</sup> Lizenz erforderlich

## Anzahl Benutzer Remote Standard

In der Integral Software können bis zu 254 Benutzer pro Teilzentralenring angelegt werden. Jeder Benutzer kann wie folgt programmiert werden.

- Der Bedienfeldbenutzer besitzt ein numerisches Passwort und kann sich nur an einem Bedienfeld anmelden um Bedienvorgänge durchzuführen (z. B. interne oder externe Bedienfelder). Integral Desktop nur, wenn er auch Remote Access Benutzer ist
- Der Remote Access Benutzer besitzt einen Namen und ein Passwort (beides alphanumerisch) und kann damit eine Verbindung per Fernzugriff zur Zentrale aufbauen (z. B. mit Integral Desktop oder der Integral Software). Ist er auch Bedienfeldbenutzer kann er auch Bedienvorgänge durchführen

Pro Bedienfeld können bis zu 31 Benutzer zugeordnet werden. Bei bis zu 8 Fernbedienfeldern können somit für den Fernzugriff bis zu 248 Benutzer eingerichtet werden.

## Anzahl Benutzer Remote Mobile

Benutzer für Remote Mobile werden über die Remote Mein HPlus Adminoberfläche angelegt, die Anzahl der Benutzer ist hier unbegrenzt. Je nach Leistungspaket können max. 2 oder max. 4 Benutzer gleichzeitig auf die Brandmelderzentrale zugreifen.

## 6.2 Voraussetzungen

Nachfolgend werden die Voraussetzungen für die einzelnen Komponenten beschrieben.

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Brandmelderzentrale | <ul style="list-style-type: none"> <li>- Ab B5-, B6- bzw. B7-Plattform, zur Hochrüstung von alten Plattformen stehen spezielle Upgrade Kits zur Verfügung</li> <li>- Netzwerkbaugruppe mit Ethernetschnittstelle (LAN-Port). An Baugruppen mit 2 getrennten Ethernetanschlüssen kann auch ein Anschluss für lokalen (Intranet) und ein Anschluss für globalen (Internet) Fernzugriff genutzt werden</li> <li>- Ab Integral Software 7.3 für Programmierung und Zugriff</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| VPN-Router          | <ul style="list-style-type: none"> <li>- VPN-Router als LAN- oder Mobilfunk-Variante mit integrierter Firewall zur Sicherheit gegenüber dem Fremdnetz (Internet)</li> <li>- Bei Mobilfunk-Variante SIM-Karte mit Datenflatrate (kein Prepaid), bei Volumentarifen wird mindestens 1 GB empfohlen. Näherungswerte für normale Nutzung App ca. 300 MB/Monat, Programmierung ca. 20 MB pro Vorgang</li> <li>- Verfügbare Datenübertragungsraten von mindestens 384 kbit/s (Upload) bzw. 1 Mbit/s (Download)</li> <li>- Distanz zwischen BMZ und Router bis zu 100 m</li> <li>- Komplette Vorkonfiguration, bei Mobilfunk müssen lediglich noch die Verbindungsdaten für den Mobilfunk eingetragen werden</li> <li>- Standardeinstellung dynamische IP, auf fixe IP umstellbar</li> <li>- Über den Hutschielenanschluss in eine Zentrale oder einen Schrank mit Hutschiene (z. B. Hutschielenschrank B6-CTR-2) montierbar</li> </ul> |

- DSL-Modem/Netzwerk  
(nur bei LAN-Router)

- Separater Internetzugang nur für die Brandmelderzentrale über DSL-Modem (empfohlen) oder Internetzugang über ein bestehendes Kundennetzwerk
  - Vertrag mit entsprechendem Internet Provider
  - Wenn die vorkonfigurierten Grundeinstellungen des Routers nicht verändert werden, muss am LAN Port des DSL-Modems DHCP aktiviert sein
  - Freigabe folgender Ports an der Firewall im Kundennetzwerk für ausgehende Verbindungen
    - Port 443 (HTTPS) bei Betrieb des VPN-Routers im Netzwerk
    - Port 8181 (WebSocket) bei Betrieb von Remote Mobile im WLAN
    - Port 8191 (FlashSocket) bei Betrieb der Remote Mein HPlus Adminoberfläche im Netzwerk
- PC/Laptop

- Betriebssystem ab Windows 10
  - USB-Schnittstelle für Dongle
  - Ethernetschnittstelle (LAN-Port) oder Hardware für Mobilfunkzugang
  - Vertrag mit entsprechendem Internet Provider
  - Verfügbare Datenübertragungsraten von mindestens 384 kbit/s (Upload) bzw. 1 Mbit/s (Download)
  - VPN-Zertifikat für PC, dieses wird in der Remote Mein HPlus Adminoberfläche einem Benutzer zugeordnet
  - VPN-Software (z. B. OpenVPN)
  - Browser zur Nutzung der Remote Mein HPlus Adminoberfläche
- Mobile Endgeräte

- Betriebssystem iOS ab 6.0 oder Android ab 4.0
  - Auflösung ab 960 x 640 Pixel
  - Vertrag mit entsprechendem Internet Provider
  - Verfügbare Datenübertragungsraten von mindestens 384 kbit/s (Upload) bzw. 1 Mbit/s (Download)
  - App Integral Mobile (kostenfrei über die entsprechenden App-Stores)
  - Lizenz für 2 oder 4 gleichzeitige Zugriffe
  - Browser zur Nutzung der Remote Mein HPlus Adminoberfläche
- Dongle

Je nach Anwendung muss der entsprechende Dongle am PC/Laptop eingesetzt werden.

|                                  | Integral Desktop-Dongle | Basis-Dongle      | Basis-Dongle Erweiterung Remote |
|----------------------------------|-------------------------|-------------------|---------------------------------|
| Anwendung                        | Virtuelles Bedienfeld   | Integral Software | Integral Software               |
| Fernzugriff lokal über Intranet  | Ja                      | Ja                | -                               |
| Fernzugriff global über Internet | Ja                      | Nein              | Ja                              |

Tab. 2: Übersicht Donglevarianten

### 6.3 Projektierungsbeispiele

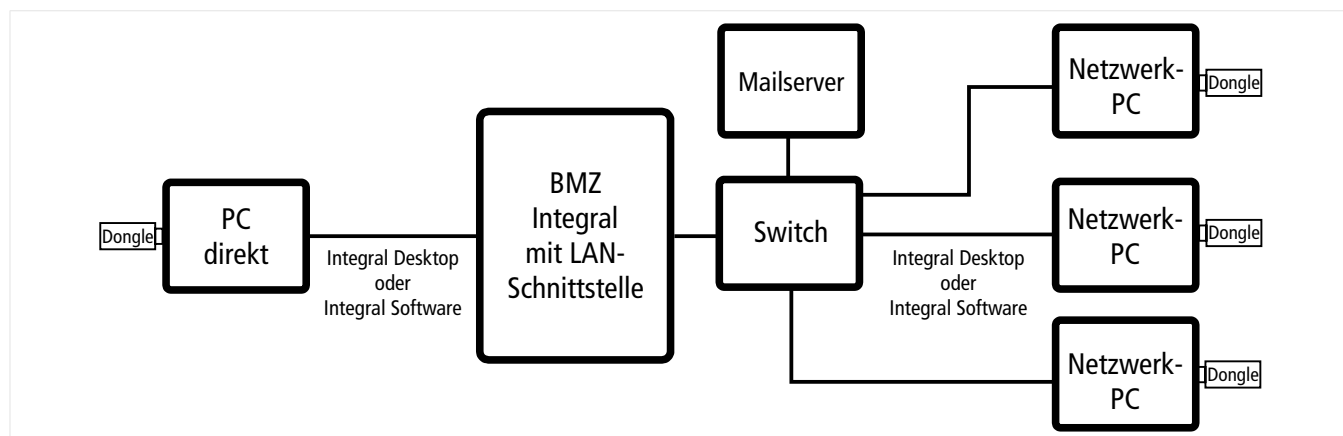


Abb. 7: Remote Standard (lokal) mit Integral Mail über internen Mailserver (max. 8 gleichzeitige Zugriffe)

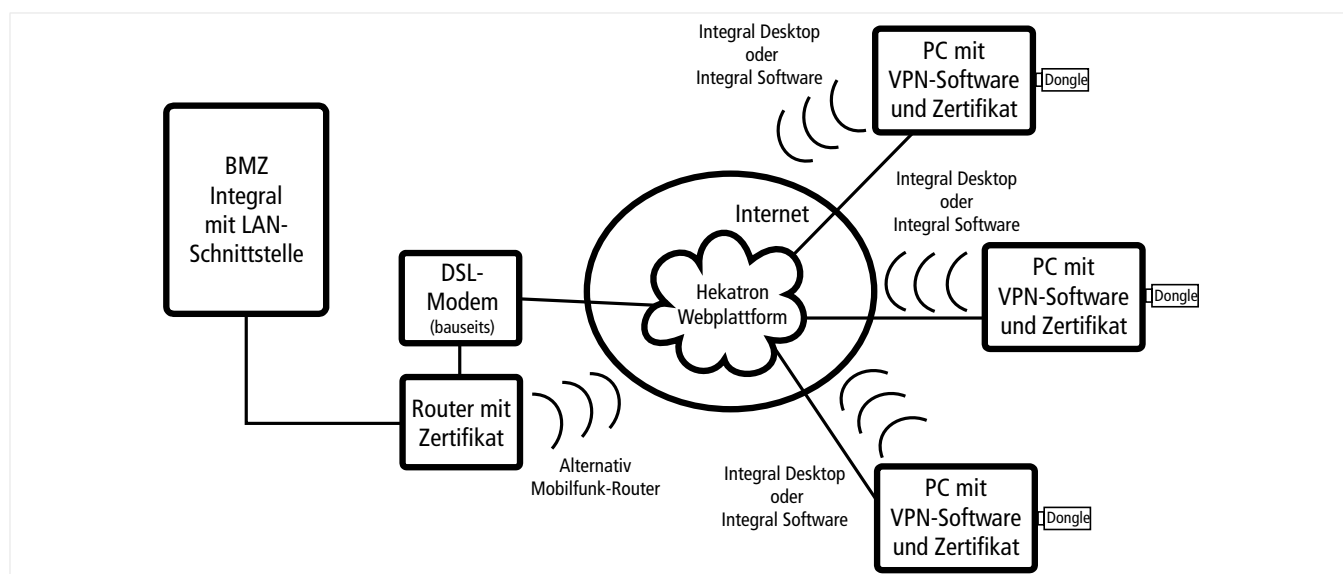


Abb. 8: Remote Standard (global) mit Integral Mail (max. 8 gleichzeitige Zugriffe)

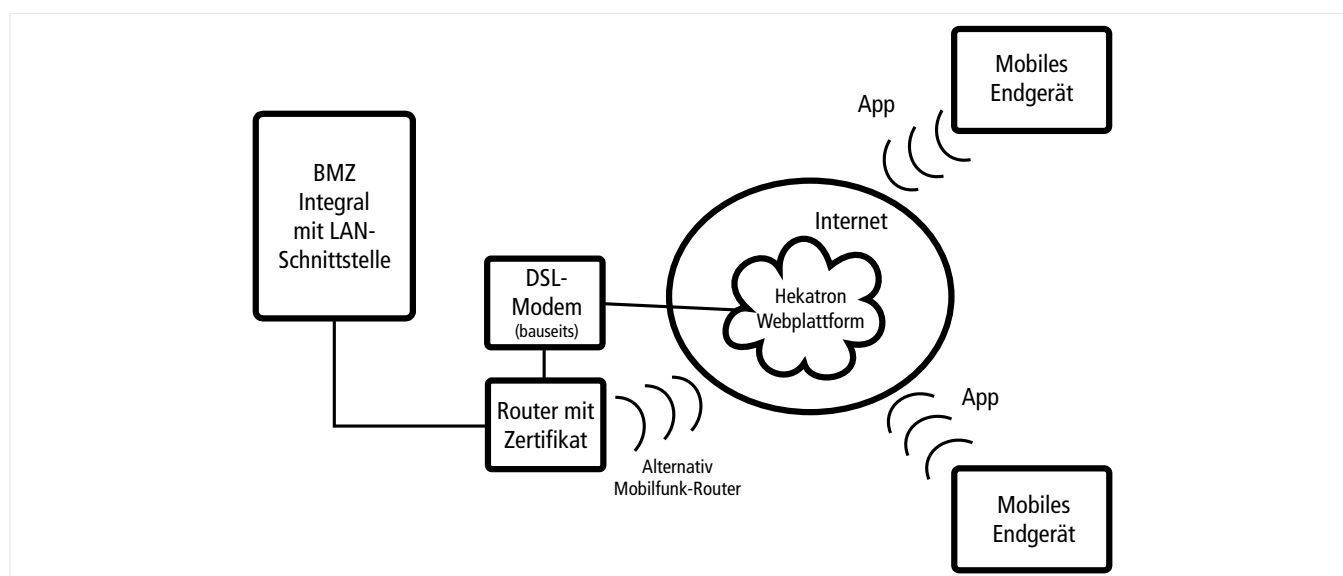


Abb. 9: Remote Mobile (global) mit Integral Mail (max. 2 gleichzeitige Zugriffe)

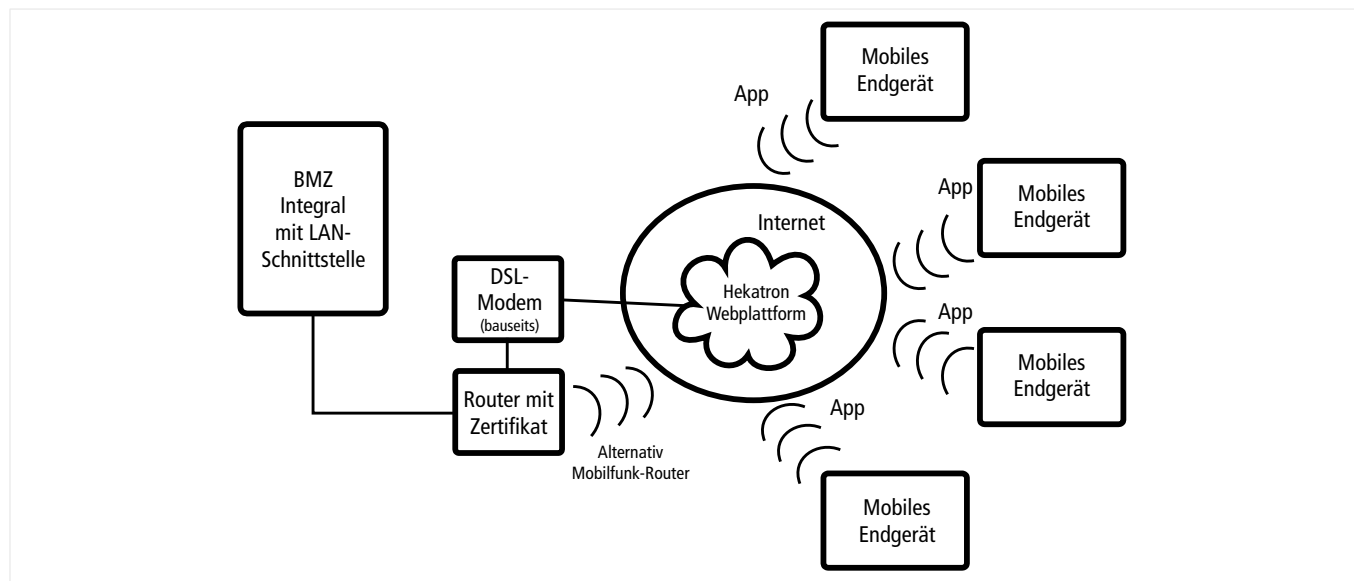


Abb. 10: Remote Mobile (global) mit Integral Mail (max. 4 gleichzeitige Zugriffe)

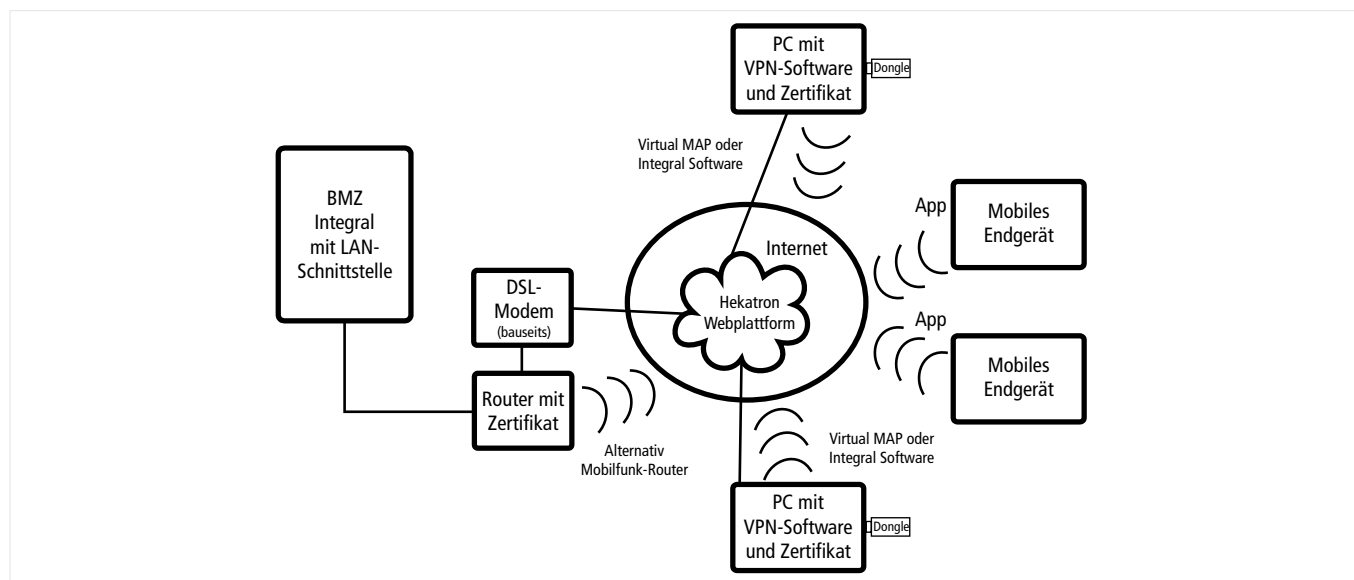


Abb. 11: Remote Standard und Remote Mobile (global) mit Integral Mail (max. 8 gleichzeitige Zugriffe, davon max. 4 über Remote Mobile)

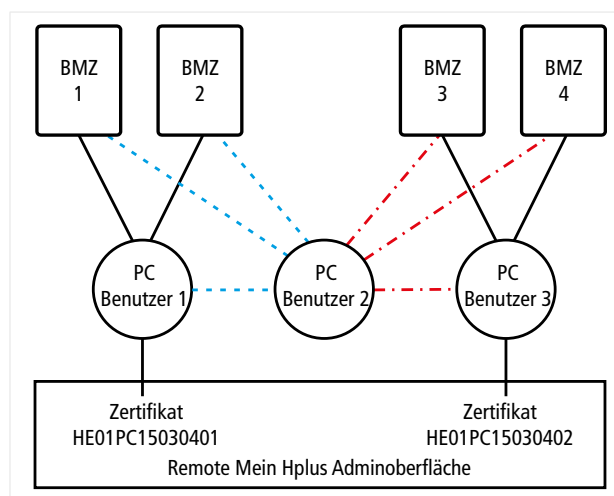


Abb. 12: Benutzerzertifikate für Remote Standard

Ein PC-Zertifikat kann über die Remote Mein HPlus Adminoberfläche maximal einem PC-Benutzer zugeordnet und auf bestimmte Zentralen freigegeben werden.

Im Beispiel ist dem Benutzer 1 und 3 jeweils ein PC-Zertifikat zugeordnet. Mit diesem kann Benutzer 1 auf BMZ 1 und 2 und Benutzer 3 auf BMZ 3 und 4 zugreifen. Weitere Benutzer können das Zertifikat für den Zugriff auch verwenden, haben dann aber die gleichen Zugriffsrechte. So kann Benutzer 2 mit dem Zertifikat von Benutzer 1 auf BMZ 1 und 2 und mit dem Zertifikat von Benutzer 3 auf BMZ 3 und 4 zugreifen. Ein gleichzeitiger Zugriff von 2 Benutzern über ein Zertifikat ist nicht möglich.

## 6.4 Sicherheitskonzept

Nach VDE 0833-1 dürfen folgende Tätigkeiten auch aus der Ferne durchgeführt werden. Je nach Tätigkeit ist vorab eine Freigabe an der BMZ vor Ort erforderlich.

- Fernabfrage (z. B. Meldungs-, Störungs-, Betriebs- und Systemzustände oder Abfrage des Ereignisspeichers)
- Fernsteuerung (z. B. Rücksetzen von Meldungs- und Störungszuständen oder Abschalten von Betriebsmitteln)
- Fernreparatur (z. B. zur Beseitigung von Systemfehlern)
- Fernparametrierung (z. B. zur Funktionsänderung)

Hekatron Remote bietet ein mehrstufiges Sicherheitskonzept. Die Verbindung zur Zentrale wird generell über gesicherte Verbindungen und entsprechende Zertifikate hergestellt. Über die Benutzerverwaltung der Brandmelderzentrale können Zugriffsrechte nur für einen bestimmten Benutzerkreis eingerichtet werden. Für jeden Benutzer kann ein Passwort für den Zugriff und ein Code für die Bedienung vergeben werden. Es kann zudem individuell festgelegt werden, welche Tätigkeiten der Benutzer per Fernzugriff ausführen darf.

Für den Zugriff über Remote Standard wird die entsprechende Integral Software und ein Dongle benötigt.

Bei Remote Mobile gibt es eine Benutzerauthentifizierung für die App und die Bedienung kann über einen Geo Check eingeschränkt werden.

Darüber hinaus ist eine unmittelbare Freigabe durch den Betreiber vor Ort am Bedienfeld der BMZ erforderlich. Die Verbindung zur Brandmelderzentrale kann durch den Betreiber jederzeit wieder gesperrt werden.

 Die Zugangsberechtigung zwischen Betreiber und Hekatron Remote Nutzer sollte schriftlich festgehalten werden. Jeder Fernzugriff und die in diesem Zusammenhang durchgeführten Änderungen sollten vom Betreiber im Betriebsbuch dokumentiert werden.

## 7. Montage

- Den im Lieferumfang des Routers enthaltenen Plastikclip an der Unterseite oder Rückseite des Routers befestigen.
- Den Router auf der optionalen Hutschiene im Zentralengehäuse (akkugepufferte Stromversorgung über das Netzgerät der Zentrale), im Hutschienenschrank B6-CTR-2 oder einem entsprechenden bauseitigen Schrank direkt an der Brandmelderzentrale montieren.
- Die Kabeleinführung über die Rückseite der Zentrale oder des Schrankes durchführen.

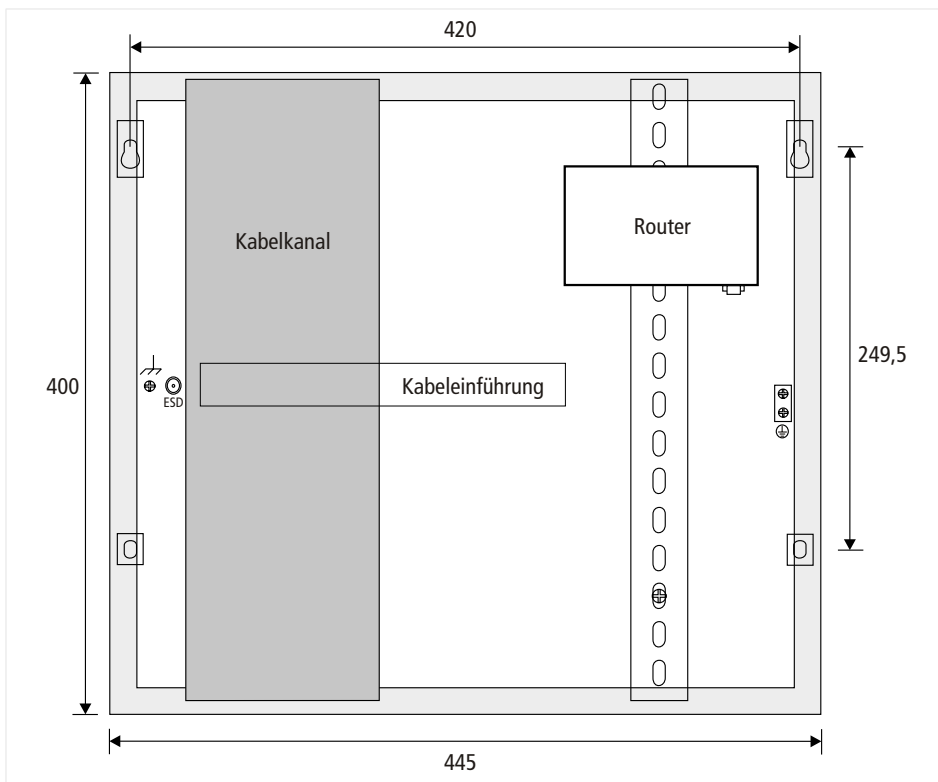


Abb. 13: Montage im Hutschienenschrank B6-CTR-2 (Angaben in mm)

### 7.1 Antennenmontage

- i** Vor der Montage unbedingt den Empfangspegel am geplanten Montageort messen, z. B. mit einem beliebigen Mobiltelefon in das die SIM-Karte, die später im Router betrieben wird, eingelegt wird.
- Die im Lieferumfang des Mobilfunk-Routers enthaltene Magnetfussantenne (Länge Anschlusskabel 2,5 m) außerhalb des Schrankes montieren.
- Den Magnetfuss der Antenne immer auf einer metallischen Oberfläche anbringen (Groundplane-Antenne).
- Wird nur eine Antenne über den Hauptanschluss ANT des Routers genutzt, diese entweder horizontal oder vertikal positionieren.
- Wird auch die zweite Antenne über den Antennenanschluss DIV genutzt (für HSPA+ Verbindungen), eine Antenne horizontal und eine Antenne vertikal anbringen (cross-polarisiert).
- Die Antennen nicht im Außenbetrieb verwenden und nicht in unmittelbarer Nähe von Brandmelderleitungen, Teilzentralenverbindungen, MMI-BUS Leitungen oder anderen Datenleitungen. Der Mindestabstand beträgt 1 m.



## 8. Installation

Der Anschluss an die Brandmelderzentrale erfolgt über die Ethernetschnittstelle (LAN-Port) auf der Hauptplatine oder einer NET- oder LAN-Baugruppe. Der Router bietet mit seiner integrierten Firewall Sicherheit gegenüber dem Fremdnetz (Internet) und wird daher zwischen Fremdnetz und dem internen Netzwerk mit der Brandmelderzentrale angeschlossen.

- Das DSL-Modem dient nur zur Verbindungsherstellung mit dem Internet. Für den Router eine feste IP-Adresse vergeben oder am LAN Port des DSL-Modems DHCP aktivieren, damit der Router automatisch eine Adresse für den Internetzugang bekommt.
- Wird die Brandmelderzentrale im Kundennetzwerk betrieben, folgende Ports für ausgehende Verbindungen an der Firewall freigeben:

| Port               | Zweck                                                                          | Ziel                    |
|--------------------|--------------------------------------------------------------------------------|-------------------------|
| 443 (HTTPS)        | Betrieb VPN-Router im Netzwerk                                                 | hekatron2.s2service.com |
| 8181 (WebSocket)   | Betrieb Remote Mobile im WLAN                                                  | remote.meinhplus.de     |
| 8191 (FlashSocket) | Bei Betrieb der browserbasierten Remote Mein HPlus Adminoberfläche im Netzwerk |                         |
| 843 (Browser)      |                                                                                |                         |

Tab. 3: Freizugebende Ports für ausgehende Verbindungen

### 8.1 IP-Adressvergabe

Router sind Netzwerkgeräte, die mehrere Rechnernetze koppeln oder trennen. Im Fall von Hekatron Remote das interne Netzwerk (BMZ und Router) mit dem Internet. Daher benötigt der Router sowohl für das interne Netzwerk als auch für den VPN-Tunnel und den Zugang ins Internet eine IP-Adresse.

- Folgende 3 private IP-Adressbereiche für die Anwendung nutzen:

| Netzklasse | Netzadressbereich               |
|------------|---------------------------------|
| A          | 10.0.0.0 bis 10.255.255.255     |
| B          | 172.16.0.0 bis 172.31.255.255   |
| C          | 192.168.0.0 bis 192.168.255.255 |

Tab. 4: IP-Adressbereiche

Die IP-Adresse für das interne Netzwerk aus Netzklasse C ist im Router bereits vorkonfiguriert, die IP-Adresse für den VPN-Tunnel aus Netzklasse A, mit der der Router später über den Fernzugriff angesprochen wird, ist im Router ebenfalls vorkonfiguriert.

- Für die Brandmelderzentrale eine IP-Adresse für das interne Netzwerk aus Netzklasse C programmieren (siehe Kapitel 9.1), diese darf nicht identisch mit der IP-Adresse des Routers sein.
- Für das DSL-Modem (Internetzugang) eine IP-Adresse aus Netzklasse A, B oder C vergeben, bei Nutzung einer Klasse A oder Klasse C Adresse darf diese nicht identisch mit der IP-Adresse des Routers sein.

| Gerät                | IP-Adresse intern                                      | IP-Adresse extern         |
|----------------------|--------------------------------------------------------|---------------------------|
| BMZ<br>(TZ 1 bis 16) | 192.168.193.1 bis 192.168.193.16                       | -                         |
| Router               | 192.168.193.100 <sup>6)</sup>                          | 10.94.0.138 <sup>6)</sup> |
| DSL-Modem            | Klasse A außer 10.94.x.x, B oder C außer 192.168.193.x |                           |

Tab. 5: Beispiel für eine IP-Adressvergabe

<sup>6)</sup> IP-Adresse wird werkseitig projektbezogen voreingestellt, diese dürfen bei Anwendung im Kundennetzwerk nicht anderweitig vergeben sein

## 8.2 Gerätekonfiguration

Beim VPN-Router LAN und Mobilfunk muss vor der Gerätekonfiguration zuerst der Anschluss der Stromversorgung sichergestellt sein.

- i

Eine SIM-Karte (keine Prepaid) darf beim Mobilfunk-Router erst nach dem Anschalten und Konfigurieren der PIN (der SIM-Karte) eingelegt werden.
- Für das Einlegen der SIM-Karte die gelbe Taste neben dem SIM-Kartensteckplatz drücken um den Kartenhalter auszuwerfen.
  - Die Karte in den Halter einsetzen (mit Ecke nach links unten) und diesen wieder in den Router einstecken.
  - Zum Abruf der Routerinformationen und Eintrag der Verbindungsdaten für den Mobilfunk einen PC über Patchkabel mit dem Router (ETH Port) verbinden und im Browser 192.168.193.100/module/guest/ eingeben.

Anmeldedaten für den Router:

Benutzername: guest

Passwort: guest

Das Routermenü beinhaltet folgende Punkte:

|               |                        |                                               |
|---------------|------------------------|-----------------------------------------------|
| Status        | Mobile WAN             | Anzeige der Daten der mobilen Verbindung      |
|               | Network                | Anzeige der Daten des Netzwerks               |
|               | System Log             | Anzeige der Logdaten (Ereignisspeicher)       |
| Configuration | PPP                    | Eingabe der Verbindungsdaten für Mobilfunk    |
|               | WAN                    | Zuordnung einer festen IP- und Gatewayadresse |
|               | SMS                    | Information wenn Datenlimit erreicht ist      |
| Customization | Set SMS Service Center | Eingabe der Nummer (wenn erforderlich)        |
|               | Change Password        | Neue Passwortvergabe für den guest            |
|               | Unlock SIM Card        | Entsperren der SIM-Karte (Eingabe PUK)        |
|               | Admin Login            | Admin Zugang (nur für interne Zwecke)         |

Tab. 6: Punkte im Routermenü

### Mobile WAN

Hier werden die Daten der mobilen Verbindung angezeigt (Signalstärke mit Statistik, Datenverkehrstatistik).

|                                                                                                                                                                                                                                                                                                |                                                                         |  |  |  |  |  |  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|--|--|--|--|--|--|
| <div>Status</div> <div>Mobile WAN</div> <div>Network</div> <div>System Log</div> <div>Configuration</div> <div>PPP</div> <div>WAN</div> <div>SMS</div> <div>Customization</div> <div>Set SMS Service Center</div> <div>Change Password</div> <div>Unlock SIM Card</div> <div>Admin Login</div> | Mobile WAN Status                                                       |  |  |  |  |  |  |
|                                                                                                                                                                                                                                                                                                | Mobile Network Information                                              |  |  |  |  |  |  |
|                                                                                                                                                                                                                                                                                                | Registration : Home Network                                             |  |  |  |  |  |  |
|                                                                                                                                                                                                                                                                                                | Operator : Telekom.de                                                   |  |  |  |  |  |  |
|                                                                                                                                                                                                                                                                                                | Technology : EDGE                                                       |  |  |  |  |  |  |
|                                                                                                                                                                                                                                                                                                | PLMN : 26201                                                            |  |  |  |  |  |  |
|                                                                                                                                                                                                                                                                                                | Cell : CAED                                                             |  |  |  |  |  |  |
|                                                                                                                                                                                                                                                                                                | LAC : 5218                                                              |  |  |  |  |  |  |
|                                                                                                                                                                                                                                                                                                | Channel : 32                                                            |  |  |  |  |  |  |
|                                                                                                                                                                                                                                                                                                | Signal Strength : -77 dBm                                               |  |  |  |  |  |  |
|                                                                                                                                                                                                                                                                                                | Neighbours : -101 dBm (44), -103 dBm (89), -108 dBm (40), -108 dBm (46) |  |  |  |  |  |  |
|                                                                                                                                                                                                                                                                                                | » More Information «                                                    |  |  |  |  |  |  |
| Mobile Network Statistics                                                                                                                                                                                                                                                                      |                                                                         |  |  |  |  |  |  |
| Signal Min : -86 dBm    Yesterday : --- dBm    This Week : -86 dBm    Last Week : -89 dBm    This Period : -89 dBm    Last Period : --- dBm                                                                                                                                                    |                                                                         |  |  |  |  |  |  |
| Signal Avg : -77 dBm    Yesterday : --- dBm    This Week : -77 dBm    Last Week : -77 dBm    This Period : -77 dBm    Last Period : --- dBm                                                                                                                                                    |                                                                         |  |  |  |  |  |  |
| Signal Max : -77 dBm    Yesterday : --- dBm    This Week : -77 dBm    Last Week : -71 dBm    This Period : -71 dBm    Last Period : --- dBm                                                                                                                                                    |                                                                         |  |  |  |  |  |  |
| Cells : 1    Yesterday : 0    This Week : 1    Last Week : 2    This Period : 2    Last Period : 0                                                                                                                                                                                             |                                                                         |  |  |  |  |  |  |
| Availability : 95.3%    Yesterday : 0.0%    This Week : 95.3%    Last Week : 42.3%    This Period : 44.9%    Last Period : 0.0%                                                                                                                                                                |                                                                         |  |  |  |  |  |  |
| Traffic Statistics for Primary SIM card                                                                                                                                                                                                                                                        |                                                                         |  |  |  |  |  |  |
| Rx Data : 3864 KB    Yesterday : 0 KB    This Week : 3864 KB    Last Week : 14360 KB    This Period : 18224 KB    Last Period : 0 KB                                                                                                                                                           |                                                                         |  |  |  |  |  |  |
| Tx Data : 219 KB    Yesterday : 0 KB    This Week : 219 KB    Last Week : 834 KB    This Period : 1053 KB    Last Period : 0 KB                                                                                                                                                                |                                                                         |  |  |  |  |  |  |
| Connections : 2    Yesterday : 0    This Week : 2    Last Week : 1    This Period : 3    Last Period : 0                                                                                                                                                                                       |                                                                         |  |  |  |  |  |  |

Abb. 14: Konfiguration Mobile WAN

## Network

Hier werden die Daten des Netzwerks angezeigt, unter anderem die IP-Adressen für den Router (eth0) und den VPN-Tunnel (tun0).

| Status                                                                                                                                                              | Network Status                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Mobile WAN</a><br><a href="#">Network</a><br><a href="#">System Log</a>                                                                                 | <b>Interfaces</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Configuration</b><br><a href="#">PPP</a><br><a href="#">WAN</a><br><a href="#">SMS</a>                                                                           | <pre>eth0      Link encap:Ethernet  HWaddr 00:0A:14:81:72:5C           inet addr:192.168.193.100  Bcast:192.168.193.255  Mask:255.255.255.0           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1           RX packets:2899 errors:0 dropped:0 overruns:0 frame:0           TX packets:3580 errors:0 dropped:0 overruns:0 carrier:0           collisions:0 txqueuelen:32           RX bytes:320872 (313.3 KB)  TX bytes:4126658 (3.9 MB)           Interrupt:23  lo        Link encap:Local Loopback           inet addr:127.0.0.1  Mask:255.0.0.0           UP LOOPBACK RUNNING  MTU:16436  Metric:1           RX packets:1 errors:0 dropped:0 overruns:0 frame:0           TX packets:1 errors:0 dropped:0 overruns:0 carrier:0           collisions:0 txqueuelen:0           RX bytes:76 (76.0 B)  TX bytes:76 (76.0 B)  ppp0      Link encap:Point-Point Protocol           inet addr:10.22.54.192  P-t-P:192.168.254.254  Mask:255.255.255.255           UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1           RX packets:881 errors:0 dropped:0 overruns:0 frame:0           TX packets:712 errors:0 dropped:0 overruns:0 carrier:0           collisions:0 txqueuelen:3           RX bytes:670365 (654.6 KB)  TX bytes:69547 (67.9 KB)  tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00           inet addr:10.1.0.182  P-t-P:10.1.0.181  Mask:255.255.255.255           UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1           RX packets:0 errors:0 dropped:0 overruns:0 frame:0           TX packets:0 errors:0 dropped:0 overruns:0 carrier:0           collisions:0 txqueuelen:100           RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)</pre> |
| <b>Customization</b><br><a href="#">Set SMS Service Center</a><br><a href="#">Change Password</a><br><a href="#">Unlock SIM Card</a><br><a href="#">Admin Login</a> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Abb. 15: Konfiguration Network

## PPP

Hier können die Verbindungsdaten für den Mobilfunk eingetragen werden (in Klammer Beispiel für T-Mobile).

- APN = Access Point Name (internet.telekom)
- Username = Nutzernamen (telekom)
- Password = Passwort (tm)
- PIN = Persönliche Identifikationsnummer der SIM-Karte
- Die rot markierten Felder müssen ausgefüllt werden, alle anderen Felder sind nicht relevant.

| Status                                                                                                                                                              | Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Mobile WAN</a><br><a href="#">Network</a><br><a href="#">System Log</a>                                                                                 | <input checked="" type="checkbox"/> Create connection to mobile network<br><b>Primary SIM card</b><br><div> <div>APN *</div> <div>Username *</div> <div>Password *</div> </div> <div> <div>Authentication</div> <div>PAP or CHAP</div> </div> <div> <div>IP Address *</div> <div>Phone Number *</div> <div>Operator *</div> </div> <div> <div>Network Type</div> <div>automatic selection</div> </div> <div> <div>PIN *</div> </div> <div> <div>MRU</div> <div>1500</div> </div> <div> <div>MTU</div> <div>1500</div> </div> |
| <b>Customization</b><br><a href="#">Set SMS Service Center</a><br><a href="#">Change Password</a><br><a href="#">Unlock SIM Card</a><br><a href="#">Admin Login</a> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Abb. 16: Konfiguration PPP

### 8.3 Anschluss VPN-Router LAN

- ▶ DSL-Modem über WAN-Port mit dem Internet und über LAN-Port mit dem ETH1 Port am Router verbinden.
- ▶ Ethernet Port der BMZ mit dem ETH0 Port am Router verbinden (Netzadapter 230 V und 2 Patchkabel 1,5 m sind im Lieferumfang enthalten).

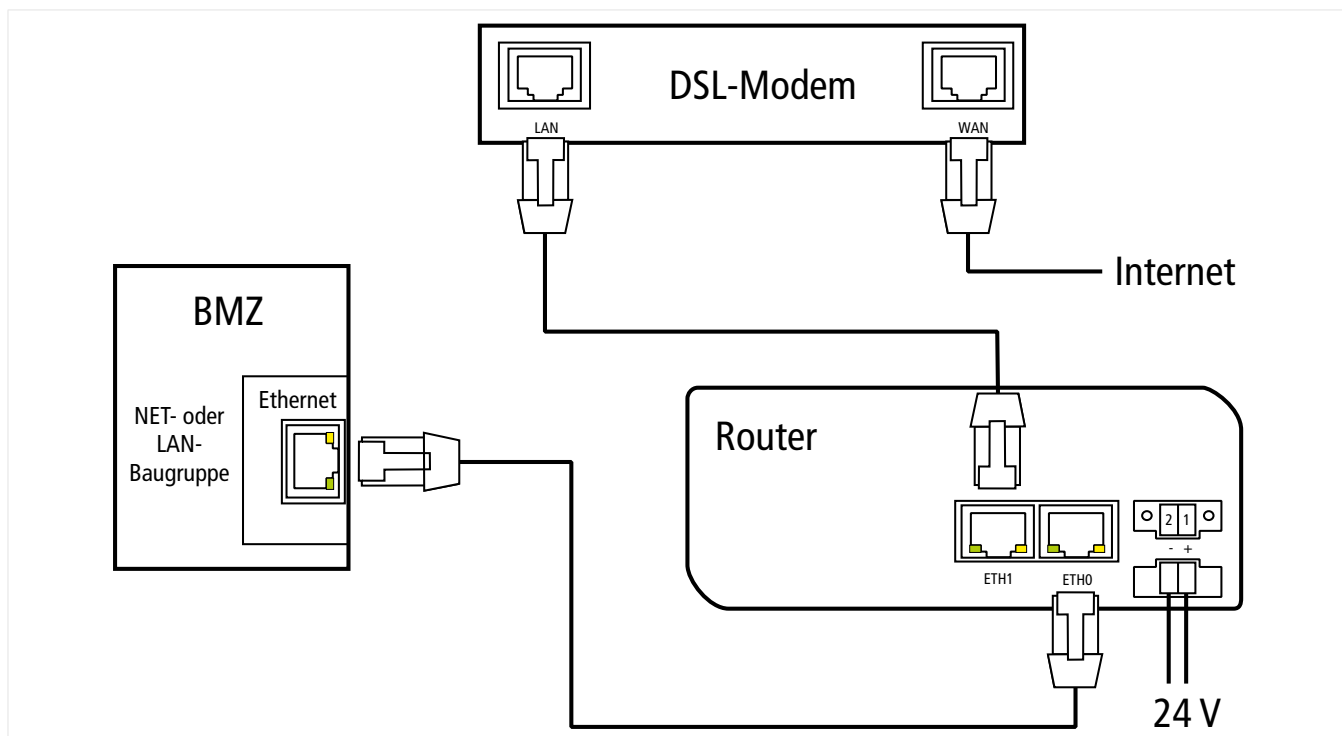


Abb. 17: Anschluss LAN-Router

### 8.4 Anschluss VPN-Router Mobilfunk

- ▶ Ethernet Port der BMZ mit dem ETH Port am Router verbinden (Netzadapter 230 V und 2 Patchkabel 1,5 m sind im Lieferumfang enthalten).
- ▶ Magnetfussantenne unter ANT und bei HSPA+ zusätzlich unter DIV (Antennendiversität) am Router anschließen.

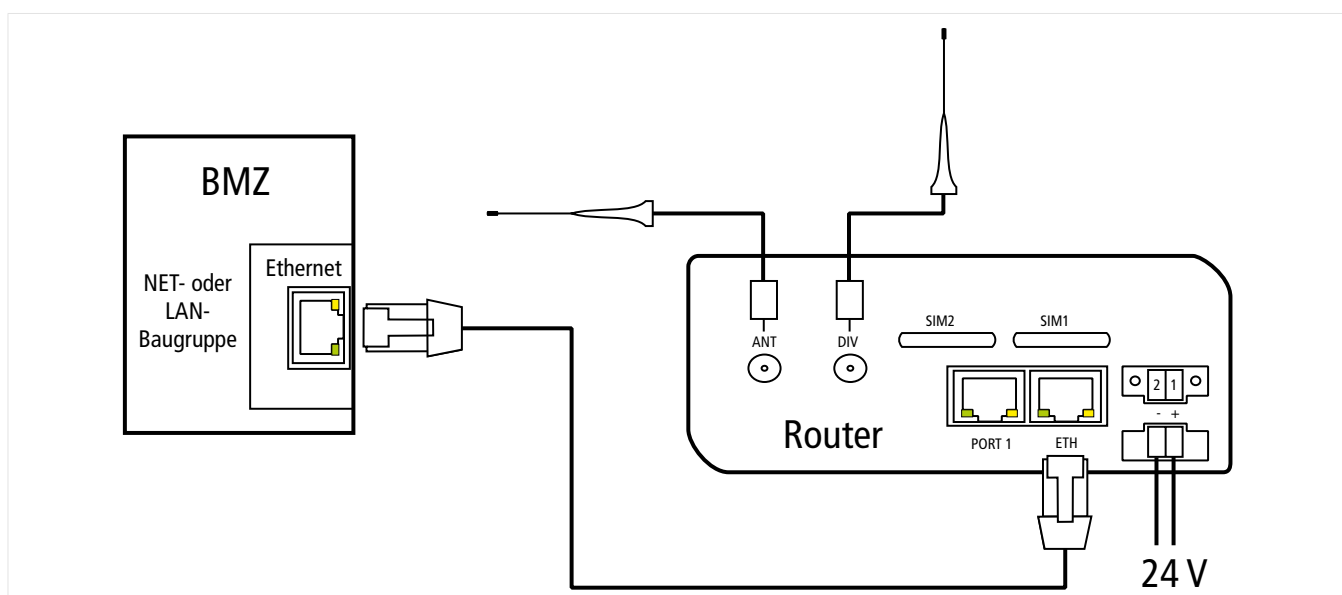


Abb. 18: Anschluss Mobilfunk-Router

## 9. Programmierung

Zur Programmierung von Remote Standard, Remote Mobile und Integral Mail wird mindestens Integral Software 7.3 benötigt.

### 9.1 IP Adressen vergeben

- i** Die eingetragenen Gerätedaten werden erst nach dem Einspielen in die Zentrale über den Loader wirksam. Wird die Brandmelderzentrale mit der Funktion Integral Mail direkt an einem DSL-Modem betrieben, so muss die IP-Adresse des DSL-Modems unter Gateway **3** und DNS1 **4** eingetragen werden und die IP-Adresse der Brandmelderzentrale muss im gleichen IP-Adressbereich wie das DSL-Modem liegen.

Zur Identifikation im Netzwerk kann bis zu 16 Zentralen eines Teilzentralenringes eine IP-Adresse zugeordnet werden.

- Unter Übersicht „Verbindung“ den Reiter „IP-Adresszuordnung“ auswählen um die Geräteparameter einzustellen.
- Für die an Hekatron Remote angebundene Zentrale unter **1** die IP-Adresse 192.168.193.1, unter **2** die Subnetzmaske 255.255.255.0 und unter **3** das Gateway 192.168.193.100 (Routeradresse) eintragen.

Mit dem jeweiligen Pfeilbutton rechts daneben werden die Einträge ab der markierten Zentrale automatisch auf die weiteren Zentralen übertragen bzw. hochgezählt.

Abb. 19: IP-Adressen zuordnen

- DNS1 **4** ebenfalls auf die Gatewayadresse 192.168.193.100 und DNS2 **5** auf 8.8.8.8 einstellen.

Wird ein NTP Zeitserver **6** (Network Time Protocol) eingetragen, übernimmt dieser die Zeitsynchronisierung der Brandmelderzentralen im Netzwerk.

Abb. 20: DNS einstellen

- Im Reiter „Anwendungen“ unter Verbindungsart eine Voreinstellung der TCP/IP-Verbindung **7** festlegen (lokal oder global), die dann in jeder verbindungs-fähigen Anwendung voreingestellt ist.
- Bei lokaler Verbindung die IP-Adresse der Zentrale, bei globaler Verbindung die IP-Adresse des VPN-Tunnels (tun0) eintragen.

Abb. 21: Verbindungsart festlegen

## 9.2 Fernbedienfelder anlegen

**i** Ab Integral Software 8.2 ist dieser Punkt bereits voreingestellt. Für vorherige Versionen oder wenn 4 gleichzeitige Zugriffe eingesetzt werden ist dieses Kapitel zu beachten. Pro Fernbedienfeld vermindert sich die Anzahl anschaltbarer physikalischer Bedienfelder um 1, da jeweils eine logische Bedienfeldadresse belegt wird.

Zur Nutzung von Remote Mobile sind entsprechende Fernbedienfelder erforderlich. Bis zu 8 Fernbedienfelder können nach Öffnen der jeweiligen Hauptrechnereinheit im Configurator unter „Hardware“ angelegt werden.

Aufbau Log.Nummer für Fernbedienfeld:

6 = Fernbedienfeld

01 = Teilzentrale 1

01 = Fernbedienfeld Nummer 1

- Für den Service-PC das Fernbedienfeld 60101 anlegen (in der Vorlage bereits voreingestellt).
- Bei 2 gleichzeitigen Remote Mobile Zugriffen die Fernbedienfelder 60102 und 60103 anlegen (in der Vorlage bereits voreingestellt).
- Bei 4 gleichzeitigen Remote Mobile Zugriffen zusätzlich die Fernbedienfelder 60104 und 60105 anlegen.

| B5-MCUA (1)      |                                           |
|------------------|-------------------------------------------|
| Eigenschaften    |                                           |
| SD-Karte         | keines                                    |
| Fernbedienfeld 1 |                                           |
| Log. Nummer      | <input checked="" type="checkbox"/> 60101 |
| Fernbedienfeld 2 |                                           |
| Log. Nummer      | <input checked="" type="checkbox"/> 60102 |
| Fernbedienfeld 3 |                                           |
| Log. Nummer      | <input checked="" type="checkbox"/> 60103 |
| Fernbedienfeld 4 |                                           |
| Log. Nummer      | <input type="checkbox"/>                  |

Abb. 22: Fernbedienfelder anlegen

## 9.3 Benutzer anlegen

**i** Um im Ereignisspeicher leicht nachvollziehen zu können, wer einen Fernzugriff durchgeführt hat, empfiehlt es sich, jeden Berechtigten als Benutzer anzulegen.

Wird an der Brandmelderzentrale ein Softwareupdate von Version 7 auf Version 8 durchgeführt, so müssen vorab die erstellten Remote Mobile Benutzer (Benutzer und Push) gelöscht werden, da diese in den Vorlagen der Version 8 bereits standardmäßig vorhanden sind und sonst doppelt angelegt werden.

Damit eine Verbindung zu den Fernbedienfeldern aufgebaut werden kann, müssen Benutzer für die Fernbedienfelder angelegt werden. Im Configurator unter „Benutzer“ sind in der Vorlage bereits Standardbenutzer angelegt.

- ▶ Über „Neu“ **1** weitere Benutzer anlegen (bis max. 254).
- ▶ Den Namen **2** frei wählen, dieser muss bei späterem Fernzugriff über die Integral Software als Legitimation eingegeben werden.
- ▶ Unter Bedienfeldbenutzer **3** einen Zugangscode und eine Berechtigungsebene für die spätere Freigabe der Bedienung am virtuellen Bedienfeld (Software oder App) frei wählen.
- ▶ Unter RemoteAccess Benutzer **4** ein Passwort wählen, dieses dient wie der Benutzername später als Legitimation für den Fernzugriff über die Integral Software.
- ▶ Über Rechte auswählen, auf was und wie der Benutzer zugreifen kann. So können bestimmte Tätigkeiten nie freigeschaltet sein, sofort oder erst nach erfolgter Freigabe durch den Betreiber vor Ort.

Dies Rechte sind wie folgt zugeordnet:

Bedienung - Integral Desktop

Firmware Download - Loader

Konfiguration - Peripherie Assistant

Servicefunktionen - Service Assistant

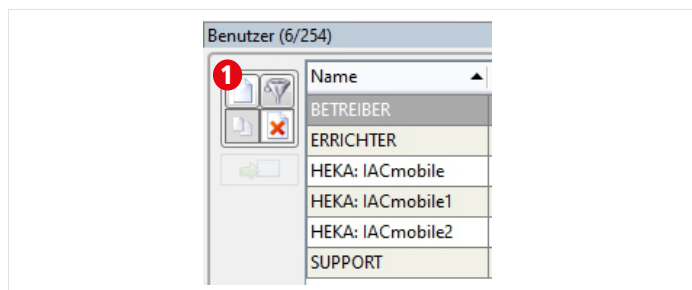


Abb. 23: Neuen Benutzer anlegen

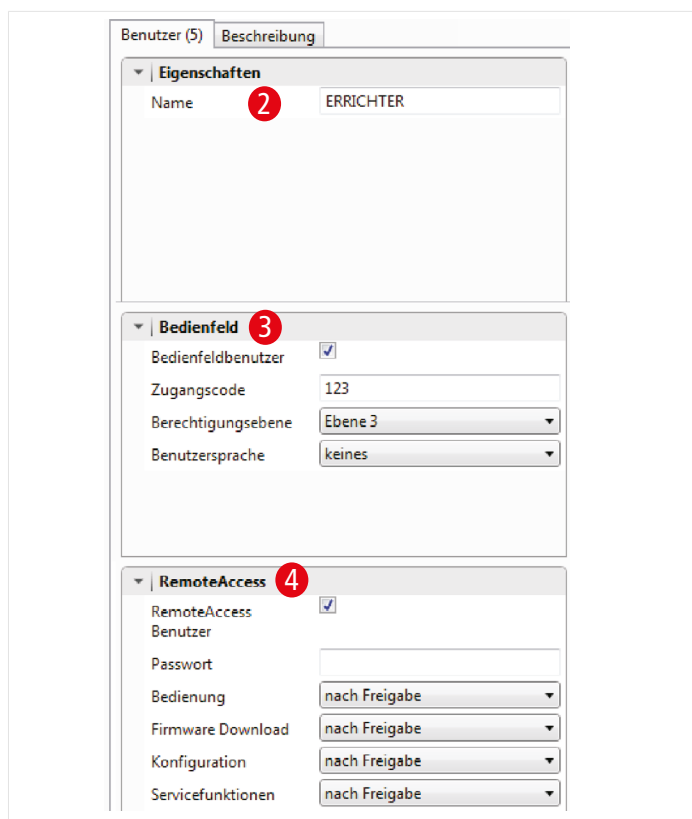


Abb. 24: Benutzerdaten einstellen

## Remote Mobile Benutzer

Für jeden Zugriff über Remote Mobile müssen zusätzlich spezielle Benutzer angelegt werden. Es können bis zu 4 Benutzer definiert werden, die später gleichzeitig über die App zugreifen können.

- Die Benutzer mit vorgegebenem Namen und Passwort als RemoteAccess Benutzer konfigurieren (kein Bedienfeldbenutzer!) und alle Rechte auf „nie“ einstellen. In der Vorlage sind 2 Benutzer (IACmobile1 und IACmobile2) bereits angelegt.
- Bei 4 gleichzeitigen Zugriffen die weiteren Benutzer nach folgendem Schema anlegen:

Benutzer 3

Name: IACmobile3

Passwort: iacmobile3

Benutzer 4

Name: IACmobile4

Passwort: iacmobile4

Groß-/Kleinschreibung beachten!

The screenshot shows the configuration window for 'Benutzer (2)' with the 'Beschreibung' tab selected. The 'Eigenschaften' section shows the 'Name' as 'IACmobile1'. The 'Bedienfeld' section has 'Bedienfeldbenutzer' unchecked, 'Zugangscode' set to '0', 'Berechtigungsebene' set to a dropdown, and 'Benutzersprache' set to 'keines'. The 'RemoteAccess' section has 'RemoteAccess' checked, and 'Benutzer', 'Passwort' (set to 'iacmobile1'), 'Bedienung', 'Firmware Download', 'Konfiguration', and 'Servicefunktionen' all set to 'nie'.

Abb. 25: Remote Mobile Benutzer anlegen

## Push Nachrichten

- Sollen später über Remote Mobile auch die Push Nachrichten genutzt werden, zusätzlich einen Fremdsystembenutzer (IACmobile) anlegen, dieser ist in der Vorlage bereits angelegt.

The screenshot shows the configuration window for 'Benutzer (1)' with the 'Beschreibung' tab selected. The 'Eigenschaften' section shows the 'Name' as 'IACmobile'. The 'Leit-/Fremdsystem' section has 'Leit-/Fremdsystem' checked, and 'Benutzer' and 'Passwort' (set to 'iacmobile') are filled in.

Abb. 26: Fremdsystembenutzer anlegen



## 9.4 Benutzer zuordnen

**i** Ab Integral Software 8.2 ist dieser Punkt bereits voreingestellt. Für vorherige Versionen oder wenn 4 Fernbedienfelder eingesetzt werden ist dieses Kapitel zu beachten.

**i** Die Fernzugriffsanfragen werden von der Zentrale in der Reihenfolge der angelegten Fernbedienfelder und den dort hinterlegten Benutzern abgearbeitet. Es empfiehlt sich daher, die Benutzer von Remote Standard und Remote Mobile über jeweils separate Benutzernamen klar zu differenzieren (z. B. Errichter und Errichter mobil) und diese innerhalb der jeweiligen Anwendung mehreren Fernbedienfeldern zuzuordnen (z. B. Errichter dem Fernbedienfeld 2 und 3 und Errichter mobil dem Fernbedienfeld 60102 und 60103). So wird verhindert, dass Benutzer der einen Anwendung Fernbedienfelder der anderen blockieren. Außerdem kann dem Benutzer bei belegtem Fernbedienfeld ein weiteres freies zugewiesen werden. Alternativ können den Benutzern auch feste Fernbedienfelder zugeordnet werden.

Nach Anlage der Fernbedienfelder und der Benutzer müssen die Fernbedienfelder konfiguriert und Benutzern zugeordnet werden um festzulegen, welcher Benutzer auf welches Fernbedienfeld zugreifen darf.

- Im Configurator unter „Logisch“ das Element „Bedienfeld“ öffnen und die Konfigurationseinstellungen der Fernbedienfelder unter dem Reiter Bedienfeld Subtyp 2 so wählen, dass sie denen des physikalischen Bedienfeldes an der Zentrale entsprechen.
- Über den Reiter „Berechtigung“ kann die Berechtigungsstruktur für das jeweilige Bedienfeld definiert werden.



Abb. 27: Konfigurationseinstellungen

- Über Bedienungsberechtigung **1** dem Bedienfeld Benutzer zuordnen, die dann mit ihrem Code über die App oder die Integral Software einen Berechtigungswechsel am Fernbedienfeld durchführen können. Maximal 31 Benutzer pro Bedienfeld sind möglich.
- Bei Fernbedienfeldern 60102 bis 60105 für Remote Mobile immer zusätzlich zu den Standard Benutzern auch die IACmobile (1 bis 4) Benutzer auswählen.
- Unter Menü **2** für das jeweilige Bedienfeld festlegen, ab welcher Benutzerebene der jeweilige Menüpunkt verfügbar sein soll.

In diesem Beispiel wurden dem Fernbedienfeld 60103 die Benutzer IACmobile1, IACmobile2, Betreiber, Errichter und Support zugeordnet.

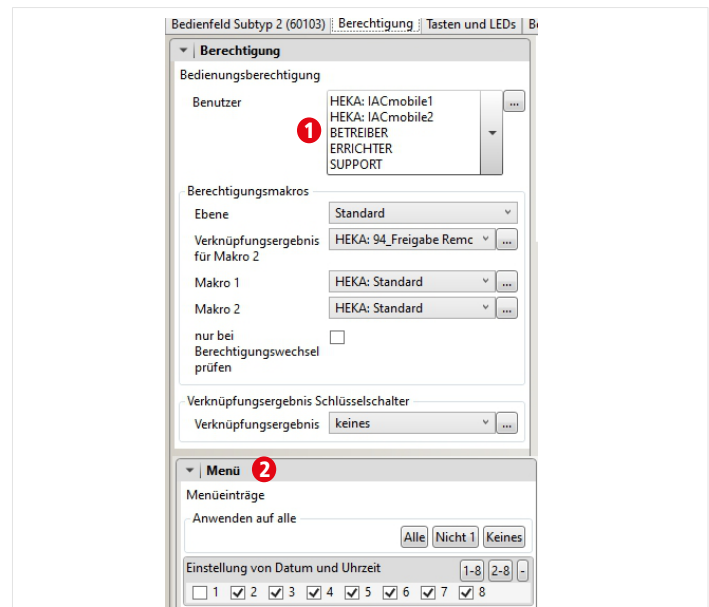


Abb. 28: Bedienungsberechtigung

## 9.5 Push Nachrichten

**i** Ab Integral Software 8.2 ist dieser Punkt bereits voreingestellt. Für vorherige Versionen ist dieses Kapitel zu beachten.

- Für die Verwendung der Funktion Push Nachrichten ein zusätzliches Fremdsystem erstellen.
- Dazu im Configurator unter „Hardware“ ein Fremdsystem **1** anlegen und dieses mit einer Verbindung vom Typ LAN **2** mit der BMZ verbinden.
- Zur Änderung der Eigenschaften **3** das Fremdsystem doppelklicken. Es wird empfohlen den voreingestellten Namen in Push Nachrichten zu ändern, die logische Nummer kann zwischen 1 und 65534 liegen, als Protokoll ISP-IP auswählen.

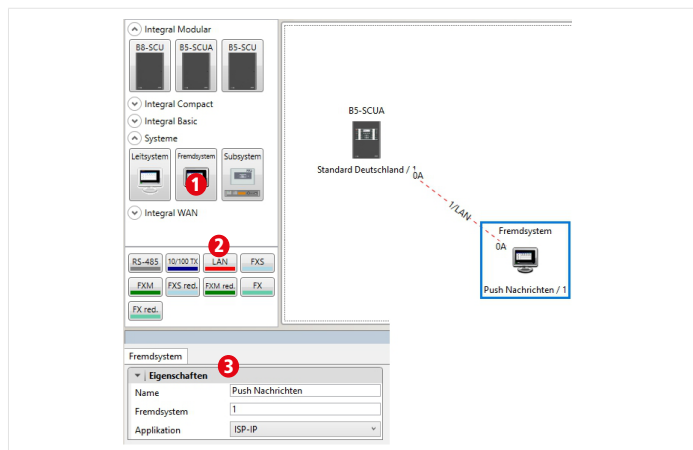


Abb. 29: Fremdsystem erstellen

- Unter „Logisch“ und „Fremdsystem“ das Standard Berechtigungsmakro **4** setzen.
- Unter Benutzer **5** den im Kapitel 9.3 definierten Benutzer IACmobile zuordnen. In der App selbst kann dann ausgewählt werden ob Alarmer, Störungen oder Sonstige (alle weiteren Ereignisse) als Push Nachrichten übertragen werden sollen.
- Über Bereichs- und Meldungsfilter **6** die Ereignisse genauer definieren.

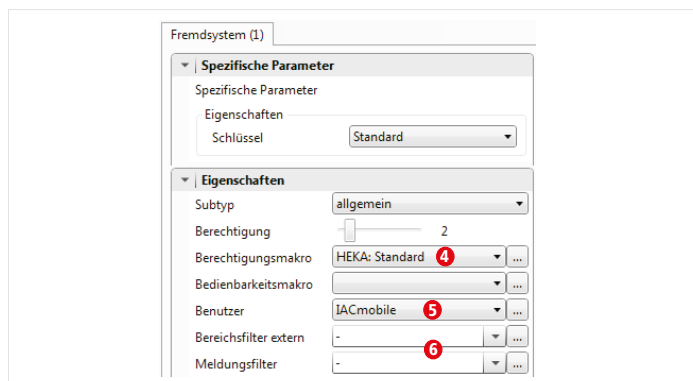


Abb. 30: Logische Eigenschaften

## 9.6 Integral Mail

**i** Jedem Router wird werkseitig eine E-Mail Adresse auf der Remote Mein HPlus Adminoberfläche zugeteilt, die zum Versenden von E-Mails genutzt werden kann.

Zum Versenden von E-Mails benötigt die Brandmelderzentrale Zugriff auf einen internen oder externen E-Mail Server (Standard SMTP Server Spezifikation), der über das LAN bzw. Internet erreichbar sein muss. Es werden nur unverschlüsselte Verbindungen unterstützt, ab Integral Plattform B8/B9/B10 sind auch verschlüsselte Mails möglich

- Für die Verwendung der Funktion Integral Mail ein zusätzliches Fremdsystem erstellen.
- Dazu im Configurator unter „Hardware“ ein Fremdsystem **1** anlegen und dieses mit einer Verbindung vom Typ LAN **2** mit der BMZ verbinden.
- Zur Änderung der Eigenschaften **3** das Fremdsystem doppelklicken. Es wird empfohlen den vor-eingestellten Namen in Integral Mail zu ändern, die logische Nummer kann zwischen 1 und 65534 liegen, als Protokoll Integral Mail auswählen.

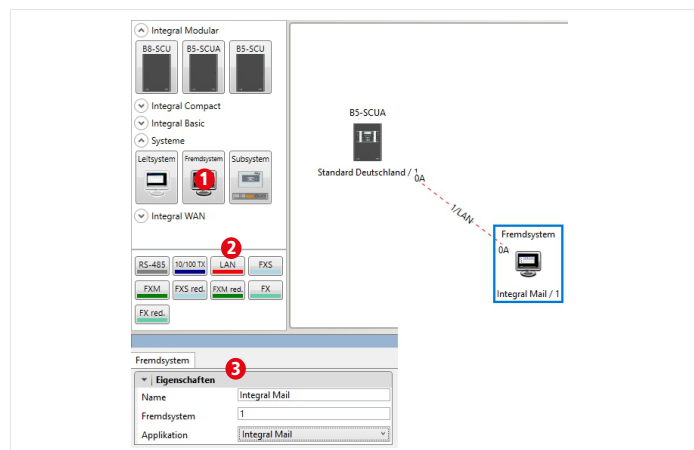


Abb. 31: Fremdsystem erstellen

- Unter „Logisch“ und „Fremdsystem“ das Standard Berechtigungsmakro **4** setzen.
- Über Bereichs- und Meldungsfilter **5** die Ereignisse genauer definieren.

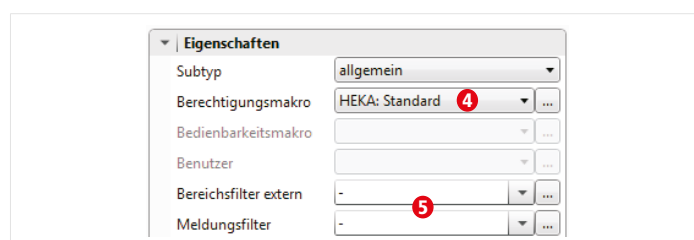


Abb. 32: Logische Eigenschaften

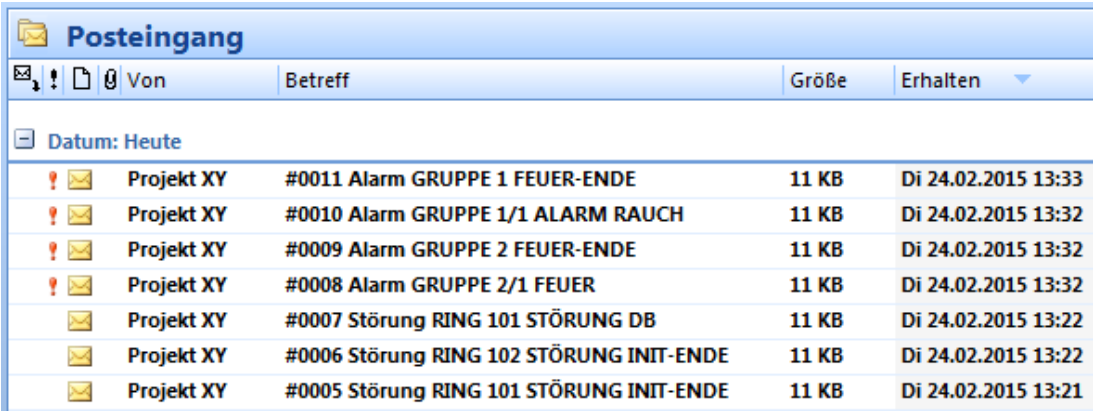
Unter spezifische Parameter können die zu übertragenden Zustände ausgewählt werden. Zur Auswahl stehen Alarme, Störungen und andere Zustände (alle weiteren Ereignisse). Für jeden Zustand kann eine separate Einstellung festgelegt werden. Beispielhaft wird hier der Zustand Alarme beschrieben.

- Priorität **1** setzen, mit der die E-Mail beim Empfänger angezeigt wird (hoch, mittel oder niedrig).
- Unter Absender **2** die von der Remote Mein HPlus Adminoberfläche zugeteilte Mailadresse eintragen und unter Absendername den Namen, unter dem die E-Mails verschickt werden sollen.
- Unter Serverparameter **3** die Parameter des Mailservers zu dieser Mailadresse eintragen. Dies sind IP-Adresse oder Hostname (SMTP, generell mail-remote.meinhplus.de) und Port (unverschlüsselt Port 25 bzw. verschlüsselt Port 465 oder Port 587). Unter Benutzername und Passwort die von der Remote Mein HPlus Adminoberfläche zugeteilte Mailadresse und das Passwort für die Anmeldung am Mailserver eintragen.
- Den Haken bei zyklische Verbindungsprüfung **4** setzen, wenn die Verbindung zum Mailserver im eingetragenen Zyklus (100 s bis 18 h) überprüft werden soll. Bei nicht erreichbarem Mailserver wird eine Störung des Fremdsystems angezeigt.
- Den Haken unter Sendeverzögerung **5** setzen und Zeitangabe (0 s bis 18 h) eintragen, wenn die Mails zeitlich versetzt versendet werden sollen. Treten mehrere Ereignisse gleichzeitig auf, werden auch mehrere E-Mails gleichzeitig versendet, was manche Mailserver als SPAM interpretieren und den Absender eventuell auf eine Schwarze Liste setzen.

Abb. 33: Spezifische Parameter Integral Mail

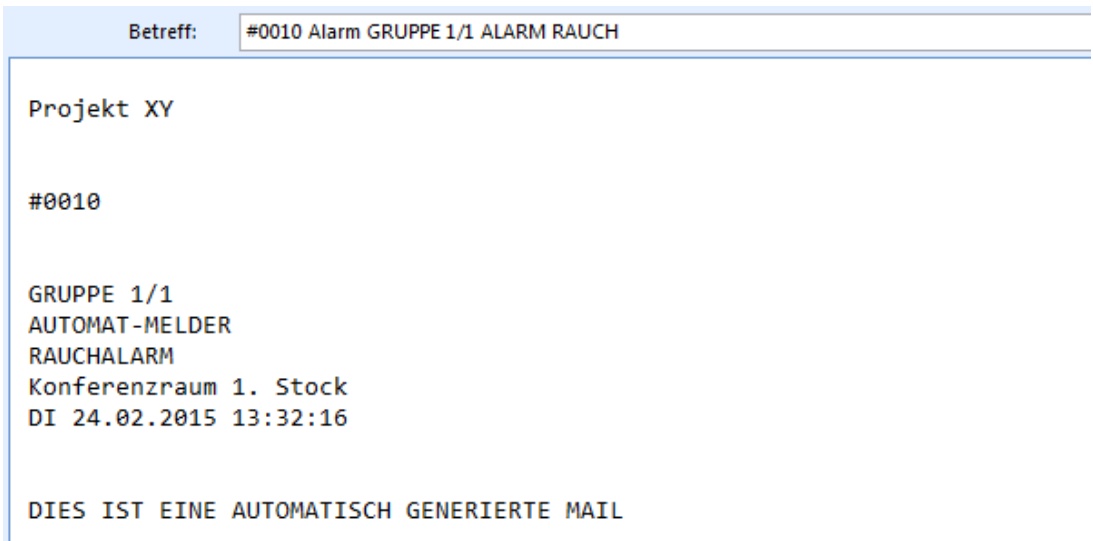
- Unter Empfänger **6** alle E-Mail Adressen eintragen, die eine E-Mail erhalten sollen (max. 99 Zeichen). Mehrere Empfänger jeweils mit einem Komma trennen, alternativ kann eine Sammeladresse mit Verteilerliste verwendet werden. Zusätzlich können Kopie- und Blindkopieempfänger und ein Betreff eingetragen werden. Den Haken bei „Zustandstext des Elements in Betreff“ **7** setzen, wenn zusätzlich der Zustandstext im Betreff eingesetzt werden soll.
- Unter Nachricht **8** den Inhaltstext und Betreff einer Testmail eintragen, die über das Bedienfeld verschickt werden kann (Fremdsystem/Weitere Befehle/Prüfen). Den Haken bei „Zustand-Ende Meldungen übertragen“ **9** setzen, wenn auch eine Mail bei Ende eines anstehenden Zustandes gesendet werden soll.

Im Beispiel unten wurden die E-Mails mit Priorität hoch, „Zustandstext des Elements in Betreff“ und „Zustand-Ende Meldungen übertragen“ konfiguriert. Nach Einspielen einer neuen oder geänderten Programmierung beginnt die Nummerierung der E-Mails wieder bei 0001.



| Posteingang  |                                          |       |                     |
|--------------|------------------------------------------|-------|---------------------|
| Von          | Betreff                                  | Größe | Erhalten            |
| Datum: Heute |                                          |       |                     |
| Projekt XY   | #0011 Alarm GRUPPE 1 FEUER-ENDE          | 11 KB | Di 24.02.2015 13:33 |
| Projekt XY   | #0010 Alarm GRUPPE 1/1 ALARM RAUCH       | 11 KB | Di 24.02.2015 13:32 |
| Projekt XY   | #0009 Alarm GRUPPE 2 FEUER-ENDE          | 11 KB | Di 24.02.2015 13:32 |
| Projekt XY   | #0008 Alarm GRUPPE 2/1 FEUER             | 11 KB | Di 24.02.2015 13:32 |
| Projekt XY   | #0007 Störung RING 101 STÖRUNG DB        | 11 KB | Di 24.02.2015 13:22 |
| Projekt XY   | #0006 Störung RING 102 STÖRUNG INIT-ENDE | 11 KB | Di 24.02.2015 13:22 |
| Projekt XY   | #0005 Störung RING 101 STÖRUNG INIT-ENDE | 11 KB | Di 24.02.2015 13:21 |

Abb. 34: Eingehende E-Mails



|                                                                                                |                                    |
|------------------------------------------------------------------------------------------------|------------------------------------|
| Betreff:                                                                                       | #0010 Alarm GRUPPE 1/1 ALARM RAUCH |
| Projekt XY                                                                                     |                                    |
| #0010                                                                                          |                                    |
| GRUPPE 1/1<br>AUTOMAT-MELDER<br>RAUCHALARM<br>Konferenzraum 1. Stock<br>DI 24.02.2015 13:32:16 |                                    |
| DIES IST EINE AUTOMATISCH GENERIERTE MAIL                                                      |                                    |

Abb. 35: Inhalt E-Mails

9.7 Verzögerung Störung Fremdsystem

Nach einer dauerhaften Nutzung von maximal 24 Stunden wird ein Internetzugang in der Regel durch den Provider getrennt (Zwangstrennung). Wenn Fremdsysteme für Push Nachrichten und Integral Mail programmiert sind, erzeugt diese Zwangstrennung eine Störung Fremdsystem an der Brandmelderzentrale.

Soll diese Störung unterdrückt werden kann ab Integral Software 8.0 unter den logischen Eigenschaften des Fremd-systems ein Haken bei „Verbindungsstörung unterdrücken“ gesetzt werden, dann werden jedoch alle Verbindungs-störungen unterdrückt (auch die nicht durch eine Zwangstrennung verursachten).

Alternativ kann ein Meldungsfilter programmiert werden. Um die Verbindungsstörungen, die nicht durch eine Zwangs-trennung verursacht wurden, trotzdem anzuzeigen kann zusätzlich eine Boolesche Definition programmiert werden, die eine bestehende Verbindungsstörung anzeigt, falls diese auch noch nach mindestens einer Minute besteht.

Meldungsfilter

- Einen neuen Meldungsfilter erstellen (z. B. Zwangstrennung) und unter dem Reiter „Elementzuordnung“ bei den Elementtypen Leitung (früher Verbindung) und Fremdsystem die Verbindungsstörung herausfiltern. Zusätzlich kann ein Bereichsfilter erstellt werden, wenn nicht alle Leitungen und Fremdsysteme gefiltert werden sollen.

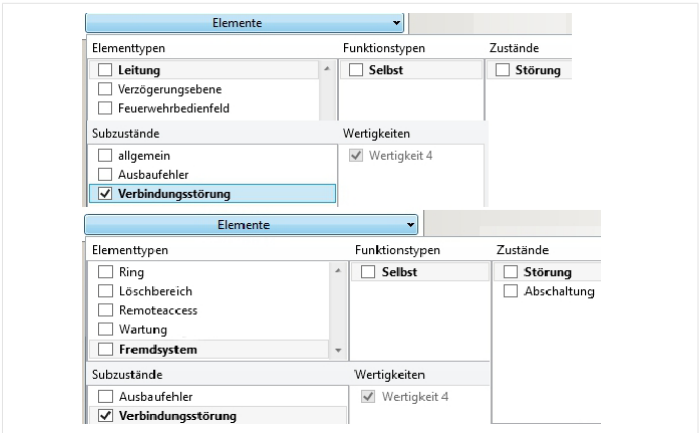


Abb. 36: Meldungsfilter erstellen

- Den neu erstellten Meldungsfilter in den logischen Eigenschaften von Fremdsystem, Bedienfeld, Leitsystem, Steuerung (Störungsweiterleitung) und Hauptzentrale zuordnen.

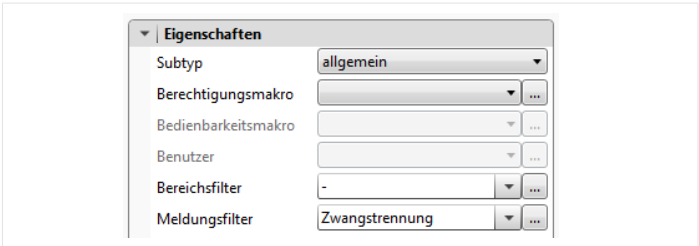


Abb. 37: Meldungsfilter zuordnen

Boolesche Definition

- Eine neue Boolesche Definition erstellen (z. B. Zwangstrennung), die Zeit der positiven Flanke sollte mindestens 1 min betragen.

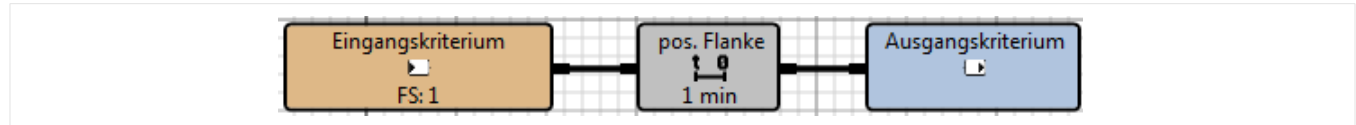


Abb. 38: Boolesche Definition erstellen

- Unter Eingangskriterium bei Elementtyp und Nummer das betreffende Fremdsystem eintragen und unter Zustand Störung den Subzustand Verbindungsstörung auswählen.

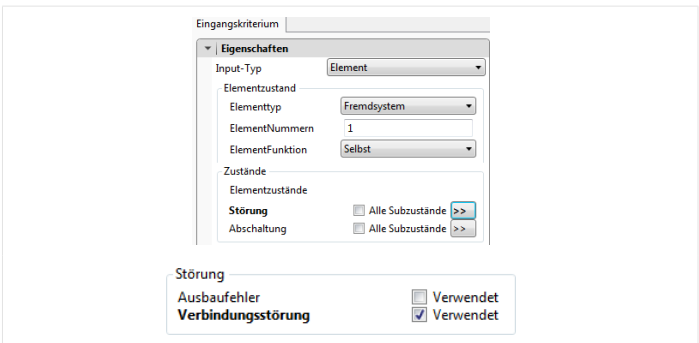


Abb. 39: Einstellungen Eingangskriterium

- Ein neues Element Extern anlegen und unter „Störung bei“ als Verknüpfungsergebnis die Boolesche Definition zuordnen.

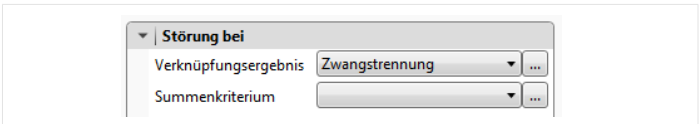


Abb. 40: Verknüpfung zuordnen

## 9.8 Freigabe/Sperre über Element Extern

**i** Ab Integral Software 8.2 ist dieser Punkt bereits voreingestellt. Für vorherige Versionen ist dieses Kapitel zu beachten.

Bei Remote Standard kann in der Benutzerprogrammierung „nach Freigabe“ ausgewählt werden, damit bei einem Fernzugriff vor Bedienung zuerst eine Freischaltung durch den Betreiber an der Zentrale erfolgen muss.

Alternativ kann dies bei einem Zugriff über Remote Standard oder Remote Mobile auch über 2 Boolesche Definitionen programmiert werden. Eine regelt die Aktivierung eines Elementes Extern, die andere die automatische Rücksetzung (z. B. um 23:00 Uhr), wenn das Element vom Betreiber nicht selbst wieder rückgesetzt wird.

Dazu vorab ein Element Extern mit der Nummer 65000 anlegen, das nicht weiter programmiert werden muss.

### Boolesche Definition 1

- Eine neue Boolesche Definition erstellen (z. B. Freigabe Remote).
- Das Eingangskriterium unter Eigenschaften als Element Extern mit der Nummer 65000 programmieren.
- Unter dem Elementzustand Ansteuerung alle Subzustände auswählen.

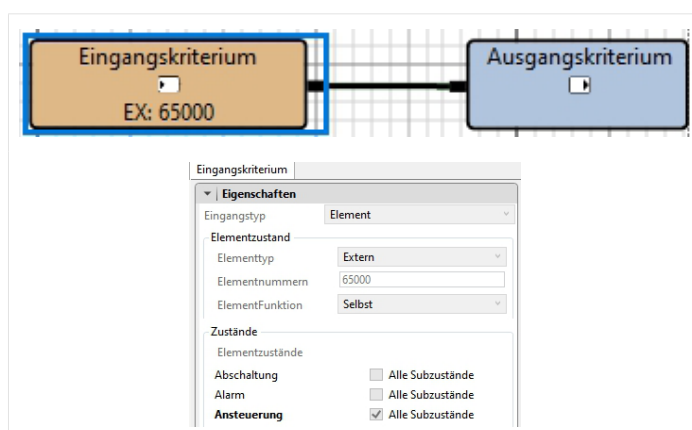


Abb. 41: Boolesche Definition 1 erstellen

### Boolesche Definition 2

- Eine neue Boolesche Definition erstellen (z. B. Ende Freigabe Remote).
- Das Eingangskriterium als Datum/Uhrzeit mit der entsprechenden Stunde/Minute angeben, an der die Bedienfreigabe wieder automatisch aufgehoben werden soll, wenn der Betreiber dies nicht direkt nach Abschluss des Fernzugriffs macht.

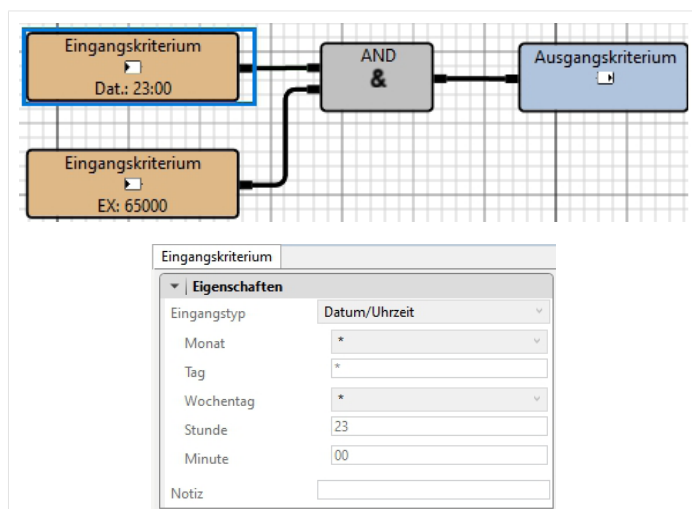


Abb. 42: Boolesche Definition 2 erstellen

## Berechtigungsmakro

Das Berechtigungsmakro „Standard Remote“ ist in der Vorlage bereits angelegt.

- Alternativ ein eigenes Berechtigungsmakro erstellen (z. B. Nicht bedienbar). und den Elementtypen die gewünschten Berechtigungen zuordnen.

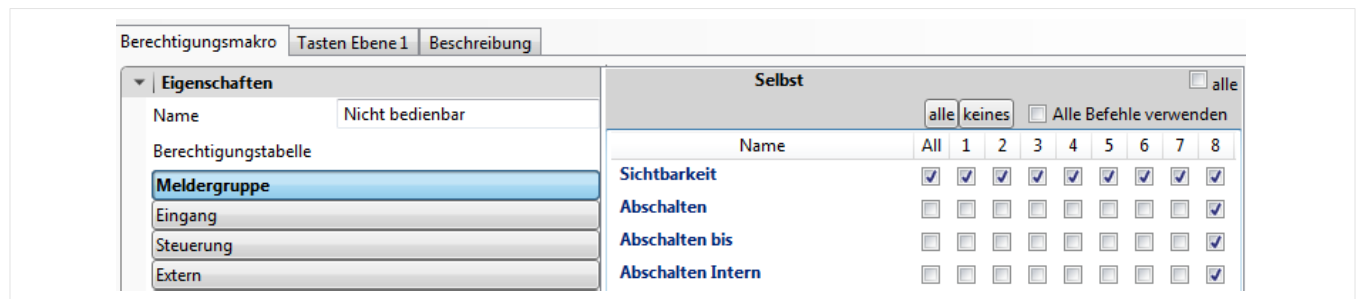


Abb. 43: Berechtigungsmakro erstellen

- Unter dem Reiter Tasten Ebene 1 die Haken bei den gewünschten Berechtigungen setzen.



Abb. 44: Berechtigungen für Tasten Ebene 1



## Meldung

- Eine neue Meldung erstellen (z. B. Ende Freigabe Remote) und die Boolesche Definition Ende Freigabe Remote zuordnen.
- Niedrige Priorität auswählen und Haken bei Neuansteuerung und Aktiv setzen.
- Den Elementtyp Extern auswählen, Funktionstyp Element selbst und den Befehl Rücksetzen.
- Bei der Elementnummer von-bis jeweils 65000 eintragen. Somit wird bei Rücksetzen des Element Extern um 23:00 Uhr eine entsprechende Meldung ausgegeben.

Abb. 45: Meldung erstellen

## Zuordnung zu Fernbedienfeldern

- Den Fernbedienfeldern (z. B. 60102, 60103 usw.) unter dem Reiter Berechtigung die Boolesche Definition „Freigabe Remote“ und das Berechtigungsmakro „Standard Remote“ zuordnen.

Abb. 46: Berechtigung einrichten

## 10. Checkliste

Zur einfachen Übersicht über die wichtigsten Eckpunkte zu Hekatron Remote, die bei der Projektplanung und Projektdurchführung zu berücksichtigen sind.

In der letzten Spalte steht die entsprechende Seite in dieser Dokumentation.

### 10.1 Planungsphase:

| Projektname                                                |                                                                                        | Bearbeiter                                                                                                                                                            |    |
|------------------------------------------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Brandmelderzentrale                                        | B8 <input type="checkbox"/> B9 <input type="checkbox"/> B10 <input type="checkbox"/>   | LAN-Port erforderlich                                                                                                                                                 | 11 |
| Upgrade-Kit erforderlich?                                  | ja <input type="checkbox"/> nein <input type="checkbox"/>                              | Nur bei B3 und B4                                                                                                                                                     | 11 |
| Vorhandene Software                                        |                                                                                        | Mindestens Version 7.3 erforderlich                                                                                                                                   | 11 |
| Art des Fernzugriffs                                       | intern <input type="checkbox"/> extern <input type="checkbox"/>                        | Intranet bzw. Internet                                                                                                                                                | 11 |
| Router                                                     | LAN <input type="checkbox"/> Mobilfunk <input type="checkbox"/>                        | Mind. 384 kbit/s (Up) bzw. 1 Mbit/s (Down)<br>SIM-Karte mit Internettarif, kein Prepaid                                                                               | 11 |
| Internetzugang                                             | separat nur für BMZ <input type="checkbox"/><br>über Netzwerk <input type="checkbox"/> | DSL-Modem mit Freigabe Port 443 (HTTPS)<br>in der Firewall für ausgehende Verbindungen                                                                                | 12 |
| IP-Adressen                                                | dynamisch <input type="checkbox"/> fix <input type="checkbox"/>                        | Standardeinstellung dynamisch                                                                                                                                         | 11 |
| Anzahl PC Benutzer                                         |                                                                                        | Über Software, max. 248 Benutzer<br>max. 8 gleichzeitige Zugriffe<br>Betriebssystem ab Windows 10<br>Mind. 384 kbit/s (Up) bzw. 1 Mbit/s (Down)                       | 11 |
| Anzahl PC Benutzer über<br>Integral Desktop                |                                                                                        | Nur Bedienfeld über Integral Desktop Dongle                                                                                                                           | 11 |
| Anzahl PC Benutzer über<br>Integral Software               |                                                                                        | Loader, Peripherie Assistant, Service Assistant und<br>Integral Desktop über Erweiterung des Basis-Dongle                                                             | 11 |
| Anzahl PC Zertifikate                                      |                                                                                        | Pro Zertifikat ein Benutzer zuweisbar,<br>mehrere Benutzer pro Zertifikat möglich                                                                                     | 14 |
| Anzahl Benutzer<br>mobile Endgeräte<br>(Tablet/Smartphone) |                                                                                        | Über App, unbegrenzte Anzahl Benutzer<br>max. 4 gleichzeitige Zugriffe<br>Betriebssystem iOS ab 6.0 oder Android ab 4.0<br>Mind. 384 kbit/s (Up) bzw. 1 Mbit/s (Down) | 11 |
| Mobiler Zugriff                                            | 2 Zugriffe <input type="checkbox"/><br>4 Zugriffe <input type="checkbox"/>             | Gleichzeitige Zugriffe                                                                                                                                                | 12 |
| Freigabe durch Betreiber?                                  | ja <input type="checkbox"/> nein <input type="checkbox"/>                              | Fernzugriff erst nach Freigabe des<br>Betreibers am Bedienfeld möglich                                                                                                | 15 |
| Push Nachrichten?                                          | ja <input type="checkbox"/> nein <input type="checkbox"/>                              | Meldungen auch bei nicht aktiver App empfangen                                                                                                                        | 58 |
| Integral Mail<br>(E-Mail Versand)?                         | ja <input type="checkbox"/> nein <input type="checkbox"/>                              | Verschlüsselt über E-Mail Adresse der<br>Remote Mein HPlus Adminoberfläche                                                                                            | 27 |

Tab. 7: Checkliste Planungsphase

## 10.2 Durchführungsphase

|                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                               |    |
|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| <b>Organisatorisches</b>                                         | <ul style="list-style-type: none"> <li>▶ Vorab SIM-Karte freischalten lassen.</li> <li>▶ Foto mit SIM-Kartennummer und VPN-ID an <a href="mailto:remoteservice@hekatron.de">remoteservice@hekatron.de</a> schicken.</li> </ul>                                                                                                                                                                                |    |
| <b>Router einrichten</b>                                         | ▶ Router mit Spannung versorgen, Antennen anschließen und über Netzkabel mit dem Notebook verbinden.                                                                                                                                                                                                                                                                                                          | 20 |
|                                                                  | ▶ Browser öffnen und die IP-Adresse <a href="http://192.168.193.100/module/guest/">http://192.168.193.100/module/guest/</a> eingeben.<br>Benutzername: guest Passwort: guest                                                                                                                                                                                                                                  | 18 |
|                                                                  | <ul style="list-style-type: none"> <li>▶ Unter Menü Configuration auf PPP klicken und bei Primary SIM Card bei APN <a href="http://internet.m2mportal.de">internet.m2mportal.de</a> eingeben.</li> <li>▶ Nach unten scrollen und mit Apply speichern.</li> </ul>                                                                                                                                              | 19 |
|                                                                  | ▶ Verbindung zum Router trennen und die SIM-Karte einsetzen.                                                                                                                                                                                                                                                                                                                                                  | 18 |
|                                                                  | ▶ Router über blaues Netzkabel mit der Zentrale verbinden.                                                                                                                                                                                                                                                                                                                                                    | 20 |
| <b>Zentrale programmieren</b>                                    | In der Vorlage ab V8.2 ist fast alles für Remote voreingestellt.                                                                                                                                                                                                                                                                                                                                              |    |
|                                                                  | <ul style="list-style-type: none"> <li>▶ Für die angebundene Teilzentrale die IP-Adresse 192.168.193.1 eintragen.</li> <li>▶ Subnetzmaske 255.255.255.0 eintragen.</li> <li>▶ Gateway 192.168.193.100 (Routeradresse) eintragen.</li> </ul>                                                                                                                                                                   | 21 |
|                                                                  | <ul style="list-style-type: none"> <li>▶ Für den Benutzer SUPPORT ein Passwort vergeben.</li> <li>▶ Bedienfeld Zugangscode: 1604786</li> <li>▶ RemoteAccess Passwort: Das E-Mailversand Passwort (Zettel liegt Router bei oder in der Remote Mein HPlus Adminoberfläche).</li> </ul>                                                                                                                          | 23 |
| <b>Zusätzliche Programmierung bei hochgezogenen Anlagen</b>      | ▶ Fernbedienfelder für Remote Mobile mit den logischen Nummern 60102 und 60103 auf der Teilzentrale mit der IP-Adresse 192.168.193.1 anlegen.                                                                                                                                                                                                                                                                 | 22 |
|                                                                  | <ul style="list-style-type: none"> <li>▶ Dem Fernbedienfeld 60102 den Benutzer „IACMobile1“ und „IACMobile2“ zuordnen.</li> <li>▶ Dem Fernbedienfeld 60103 den Benutzer „IACMobile1“ und „IACMobile2“ zuordnen</li> <li>▶ Zur Bedienung per App den Fernbedienfeldern weitere Benutzer zuordnen, z. B. Benutzer BETREIBER</li> </ul>                                                                          | 25 |
|                                                                  | <ul style="list-style-type: none"> <li>▶ Für Push Nachrichten Fremdsystem mit der Applikation ISP-IP anlegen und eine LAN-Verbindung zu der Teilzentrale mit der IP-Adresse 192.168.193.1 herstellen.</li> <li>▶ Dem Fremdsystem den Benutzer „IACmobile“ zuordnen.</li> <li>▶ Das Flag „Verbindungsstörung unterdrücken“ setzen, damit die Zentrale keine Störung bei Verbindungsabbruch auslöst.</li> </ul> | 26 |
| <b>Benutzer in der Remote Mein HPlus Adminoberfläche anlegen</b> | Wenn die App genutzt werden soll, müssen in der Remote Mein HPlus Adminoberfläche Benutzer angelegt werden.                                                                                                                                                                                                                                                                                                   |    |
|                                                                  | ▶ Mit den per E-Mail vom RemoteService erhaltenen Logindaten unter <a href="http://remote.meinhplus.de/admin/">remote.meinhplus.de/admin/</a> anmelden.                                                                                                                                                                                                                                                       | 37 |
|                                                                  | <ul style="list-style-type: none"> <li>▶ In der Menüleiste Benutzer auswählen.</li> <li>▶ „Neuen Benutzer hinzufügen“ auswählen.</li> <li>▶ Daten des Benutzers eintragen, Einstellungen vornehmen und speichern.</li> </ul>                                                                                                                                                                                  | 45 |
| <b>App einrichten</b>                                            | <ul style="list-style-type: none"> <li>▶ Benutzername und Passwort in den Einstellungen speichern.</li> <li>▶ Push Nachrichten aktivieren.</li> </ul>                                                                                                                                                                                                                                                         | 58 |
| <b>VPN Tunnel aufbauen</b>                                       | <ul style="list-style-type: none"> <li>▶ OpenVPN herunterladen und installieren.</li> <li>▶ VPN-Zertifikat in der Mein HPlus Adminoberfläche herunterladen oder auf CD erhalten.</li> <li>▶ Heruntergeladenes VPN-Zertifikat entpacken und beide Dateien in den Ordner C:\Programme\OpenVPN\config kopieren.</li> <li>▶ OpenVPN als Administrator starten und eine Verbindung herstellen.</li> </ul>          | 51 |

Tab. 8: Checkliste Durchführungsphase

## 11. Fehlermeldungen

Sollte Hekatron Remote nach Anschaltung und Programmierung nicht ordnungsgemäß funktionieren, zuerst folgende Lösungsansätze prüfen. Ist das Problem damit nicht behoben bitte die Hekatron Hotline verständigen.

Fehlermeldungen bei der Anmeldung an der Konfigurationsoberfläche der Remote Mein HPlus Adminoberfläche siehe Kapitel 12. Fehlermeldungen bei der Anmeldung über ein mobiles Endgerät siehe Kapitel 13.2.

### Router baut keine VPN-Verbindung auf

| Mögliche Ursache                                                 | Abhilfe / Lösungsansatz                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Anschaltung fehlerhaft                                           | Verbindungen am Router prüfen, Antenne angeschlossen? (siehe Kapitel 8.3/8.4).                                                                                                                                                                                             |
| SIM-Karte nicht eingelegt                                        | SIM-Karte in den Router einlegen (keine Prepaid).                                                                                                                                                                                                                          |
| SIM-Karte gesperrt                                               | SIM-Karte mit PUK entsperren.                                                                                                                                                                                                                                              |
| Fehlerhafte Konfiguration des Routers                            | Konfiguration des Routers prüfen (siehe Kapitel 8.2).                                                                                                                                                                                                                      |
| Fehlerhafte Konfiguration von Kundennetzwerk oder Kundenfirewall | Statt Router einen PC mit IP-Adresse des Routers an das Netzwerk anbinden und Verbindungsaufbau über OpenVPN testen. Bei Verbindung OK ist Netzwerk richtig konfiguriert, bei Verbindung NOK Konfiguration prüfen (bei Firewall wird ausgehend TCP auf Port 443 benötigt). |

Tab. 9: Fehlermeldungen Router

### VPN-Verbindung steht, aber keine Verbindung über Software oder App

| Mögliche Ursache                                               | Abhilfe / Lösungsansatz                                                                                                                                                                                               |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fehlerhafte Konfiguration der BMZ                              | Über Loader mit BMZ verbinden und IP-Adresszuordnung abgleichen (siehe Kapitel 9.1). Prüfen ob Fernbedienfelder angelegt und die entsprechenden Integral Mobile Benutzer zugewiesen sind (siehe Kapitel 9.2 und 9.4). |
| Fehlerhafte Zuordnung in der Remote Mein HPlus Adminoberfläche | Das VPN-Zertifikat dem Benutzer zuordnen oder den Router dem Benutzer zuordnen.                                                                                                                                       |

Tab. 10: Fehlermeldungen VPN-Verbindung

### Zentrale versendet keine E-Mails

| Mögliche Ursache                                                 | Abhilfe / Lösungsansatz                                                                                                                                                                      |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentifizierung fehlgeschlagen, keine Namensauflösung möglich  | Mit der BMZ verbinden und im Service Assistant die Einträge unter Befehle/ Fehlerzähler kontrollieren.                                                                                       |
| Fehlerhafte Konfiguration der BMZ                                | Konfiguration überprüfen (siehe Kapitel 9.6).                                                                                                                                                |
| SMTP-Server akzeptiert keine unverschlüsselten Verbindungen      | SMTP-Server einsetzen der unverschlüsselte Verbindungen akzeptiert (z. B. über Remote Mein HPlus).                                                                                           |
| Fehlerhafte Konfiguration von Kundennetzwerk oder Kundenfirewall | Statt Router einen PC mit IP-Adresse des Routers an das Netzwerk anbinden. Mail-Client mit den Daten aus der Anlagenkonfiguration einrichten und E-Mail Versand über den Mail-Client testen. |

Tab. 11: Fehlermeldungen Zentrale

### Kein Empfang von Push Nachrichten

| Mögliche Ursache                                                         | Abhilfe / Lösungsansatz                                                                                                                                                    |
|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fehlerhafte Konfiguration der BMZ                                        | Konfiguration überprüfen, Fremssystem angelegt und über LAN verbunden? (siehe Kapitel 9.5), Integral Mobile Benutzer angelegt und zugewiesen? (siehe Kapitel 9.3 und 9.4). |
| Push Nachrichten in der App nicht aktiviert                              | Push Nachrichten in der App aktivieren.                                                                                                                                    |
| Push Nachrichten in den Einstellungen des mobilen Endgerätes deaktiviert | In den Einstellungen Push Nachrichten für die App aktivieren.                                                                                                              |

Tab. 12: Fehlermeldungen Push Nachrichten

## 12. Remote Mein HPlus Adminoberfläche

Nach Programmierung der Brandmelderzentrale müssen abschließend auch die Einstellungen in der Remote Mein HPlus Adminoberfläche vorgenommen werden. Hier können Daten eingetragen und Informationen abgerufen werden, z. B.

- Zustandsübersicht über alle verwalteten Brandmelderzentralen und Benutzer
- Name einer Brandmelderzentrale oder eines Benutzers ändern
- Passwörter und Berechtigungen von Benutzern ändern
- Benutzer neu hinzufügen oder löschen
- Brandmelderzentralen zu Benutzern zuordnen
- Geo Check einrichten
- Zugangssperren durch falsche Benutzer- oder Passworteingabe aufheben

Ein entsprechender Zugang zur Remote Mein HPlus Adminoberfläche mit Benutzername und Passwort wird im Rahmen der Erstbestellung von Hekatron Remote durch Hekatron eingerichtet. Jeder weitere Router wird dann automatisch durch Hekatron dem bestehenden Zugang zugeordnet.

### Anmeldung

- Im Browser  
**<https://remote.meinhplus.de/admin>** eingeben.
- In der Anmeldemaske Benutzername und Passwort eingeben. Mit Anmelden bestätigen.

Abb. 47: Anmeldung Remote Mein HPlus Adminoberfläche

| Fehlermeldung                                                      | Beschreibung                                                                                                                                                                                               |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Error: The user name or password is incorrect                      | Ein falscher Benutzername oder ein falsches Passwort wurde eingegeben                                                                                                                                      |
| Error: User is locked                                              | Der Benutzer ist gesperrt, da der Benutzername oder das Passwort mehrfach hintereinander falsch eingegeben wurde. Der Benutzer kann nur über die Remote Mein HPlus Adminoberfläche wieder entsperrt werden |
| Error: User does not have administrator privileges. Access denied. | Der Benutzer ist als User ohne Administratorrechte angelegt. Soll der Benutzer Zugang zur Remote Mein HPlus Adminoberfläche erhalten, muss er als Admin eingerichtet werden                                |

Tab. 13: Fehlermeldungen bei Anmeldung in der Remote Mein HPlus Adminoberfläche

12.1 Stationen

Nach erfolgreicher Anmeldung erscheint der Menüpunkt Stationen, dies sind alle dem Zugang zugeordneten Anlagen, die über Remote Mobile bedient werden können.

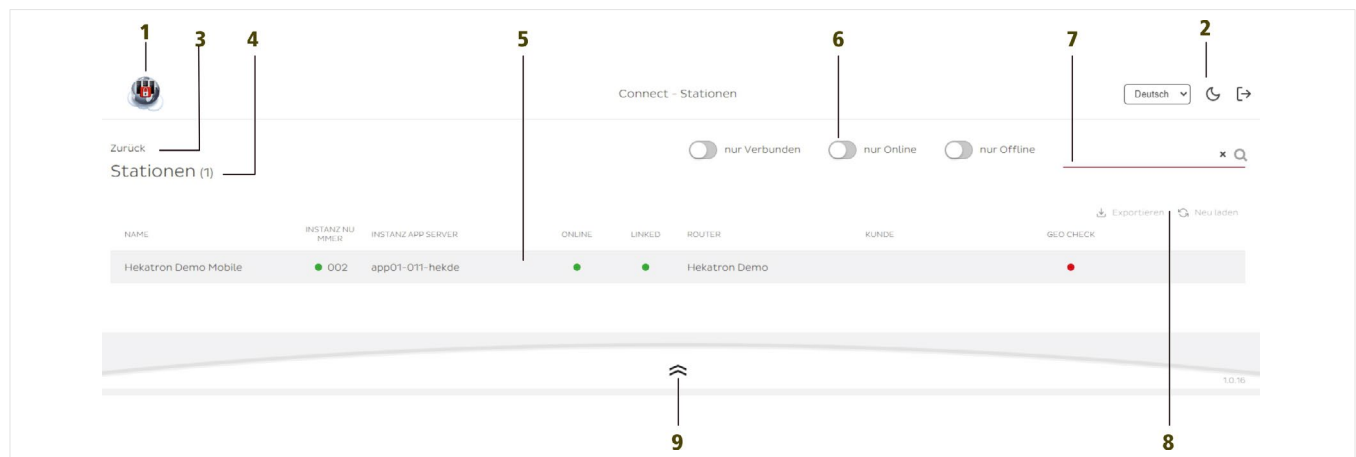


Abb. 48: Übersicht Stationen

|   |                                     |                    |   |                                                                                      |
|---|-------------------------------------|--------------------|---|--------------------------------------------------------------------------------------|
| 1 | Home (in jedem Menü vorhanden)      |                    |   | Link zurück zur Startseite „Stationen“                                               |
| 2 | Allgemein (in jedem Menü vorhanden) | Sprache            |   | Auswahl zwischen Deutsch und Englisch                                                |
|   |                                     | Darkmode           |   | Auswahl zwischen hellem und dunklem Webdesign                                        |
|   |                                     | Abmelden           |   | Abmelden des Benutzers                                                               |
| 3 | Zurück                              |                    |   | Zurück zur Übersichtsseite, z. B. wenn über Suchfeld gefiltert wurde                 |
| 4 | Anzahl Stationen                    |                    |   | In Klammer Anzeige der Anzahl der Stationen in der Stationsübersicht                 |
| 5 | Stationsübersicht                   | Name               |   | Name der Station                                                                     |
|   |                                     | Instanznummer      | ● | Server, auf dem der Dienst läuft ist bereit + Nummer des Dienstes                    |
|   |                                     |                    | ● | Server, auf dem der Dienst läuft ist nicht bereit                                    |
|   |                                     | Instanz App Server |   | Server, auf dem der Dienst läuft                                                     |
|   |                                     | Online             | ● | Integral Mobile am Server ist bereit                                                 |
|   |                                     |                    | ● | Integral Mobile am Server ist nicht bereit                                           |
|   |                                     | Linked             | ● | Brandmelderzentrale ist verbunden                                                    |
|   |                                     |                    | ● | Brandmelderzentrale ist nicht verbunden                                              |
|   |                                     | Router             |   | Name des Routers                                                                     |
|   |                                     | Kunde              |   | Name des zugewiesenen Kunden (Betreiber)                                             |
| 6 | Filter                              | nur Verbunden      |   | Anzeige Stationen in der Stationsübersicht, die nur verbundenen sind                 |
|   |                                     | nur Online         |   | Anzeige Stationen in der Stationsübersicht, die nur online sind                      |
|   |                                     | nur Offline        |   | Anzeige Stationen in der Stationsübersicht, die nur offline sind                     |
| 7 | Sucheingabefeld                     |                    |   | Suche nach einer bestimmten Station in der Übersicht                                 |
| 8 | Export/Aktualisieren                | Exportieren        |   | Export der Stationsübersicht in eine csv-Datei                                       |
|   |                                     | Neu laden          |   | Anzeige der Stationsübersicht wird aktualisiert                                      |
| 9 | Menüleiste                          |                    |   | Bei Klicken wird das Menü eingeblendet, bei nochmaligem Klicken wieder ausgeblendet. |

Tab. 14: Inhalte unter Stationen

Wird die Maus über einer Station positioniert, erscheinen rechts weitere Menüpunkte.

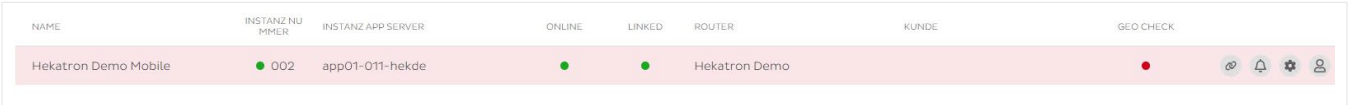


Abb. 49: Weitere Menüpunkte in der Stationsübersicht

| Menü                       | Beschreibung                                                                                                                                                  |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connect to Station         | Eingabe von Benutzername und Passwort, um eine Verbindung zu der Station über den Integral Browser herzustellen                                               |
| Open Notification Settings | Anzeige welche Push Benachrichtigungen die Benutzer in der App Integral Mobile aktiviert haben                                                                |
| Control Panel Settings     | Festlegen der Beschriftung der frei programmierbaren LEDs und Tasten. Mit dieser Beschriftung werden die LEDs und Tasten in der App Integral Mobile angezeigt |
| Show Assigned Users        | Anzeige der Benutzer, die der Station zugewiesen sind                                                                                                         |

Control Panel Settings

Für den Zugriff über die App Integral Mobile können die Beschriftungstexte der frei programmierbaren LEDs und Tasten am Bedienfeld in unterschiedlichen Sprachen erstellt werden.

- Über Hinzufügen die Anzahl der benötigten Zeilen wählen.
- Die Field ID eintragen (26/29 LED links bzw. rechts, 43/44 Taste links bzw. rechts). Den gewünschten Text in der Spalte der jeweiligen Sprache eintragen.
- Einzelne Texte über das Papierkorbsymbol oder alle Texte über „Alle Einträge löschen“ entfernen.
- Speichern drücken.

Bedienteil Einstellungen (Hekatron Demo Mobile)

|  | Field ID | German       | English | Czechian |
|--|----------|--------------|---------|----------|
|  | 26       | Linke LED    |         |          |
|  | 29       | Rechte LED   |         |          |
|  | 43       | Linke Taste  |         |          |
|  | 44       | Rechte Taste |         |          |
|  |          |              |         |          |

HINZUFÜGEN

ALLE EINTRÄGE ENTFERNEN

ABRECHEN

SPEICHERN

Abb. 50: Festlegen Beschriftung LEDs und Tasten

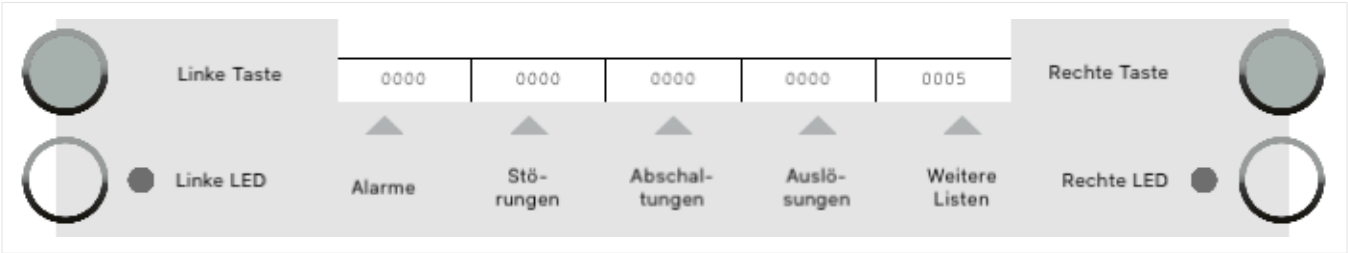


Abb. 51: Beschriftete LEDs/Tasten in der App Integral Mobile

Durch Klick auf den Namen einer Station kann diese konfiguriert werden. Unter Allgemein kann nur der Name geändert werden, alle anderen Einstellungen sind fest hinterlegt. Dies gilt auch für die E-Mail- und VPN-Einstellungen.

Zurück

Station Hekatron Demo Mobile

SPEICHERN

Status

Allgemein

Name \*

Hekatron Demo Mobile

Verbindungszeichenfolge \*

10.144.21.37:7002

Interne Verbindungszeichenfolge

10.144.21.37:7003

Kunde

Routers

Hekatron Demo

Integral-IP Einstellungen

Plananzeige

Fortbestehen lassen

Fortlaufendes Intervall

2000

Rückmeldungszeit

00:01:00

Eingriffszeit

00:04:00

Geokodierung

Geo Check

E-Mail Einstellungen

E-Mail Account

E-Mail Passwort

VPN Einstellungen

VPN Netzwerk

Keine Auswahl

VPN Zertifikat

Keine Auswahl

Abb. 52: Übersicht Stationen

Integral IP Einstellungen

|                                                                                           |                                                                                     |           |                                                                                                                                                  |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Plananzeige (vorein-<br>gestellt, nicht änderbar)                                         |  | Aktiviert | Plan-Schaltfläche in der Push Benachrichtigung ist aktiv um die<br>Feuerwehrlaufkarte anzuzeigen                                                 |
| Fortbestehen lassen und<br>Fortlaufendes Intervall<br>(voreingestellt, nicht<br>änderbar) |  | Aktiviert | Die Verbindung zwischen App Integral Mobile und Station bleibt aktiv.<br>Das eingestellte Intervall wird unter Fortlaufendes Intervall angezeigt |
| Rückmeldungszeit                                                                          |                                                                                     |           | Einstellung der Quittierzeit, in der die Taste Erkundung in der App Integral<br>Mobile gedrückt werden kann um die Erkundungszeit zu starten     |
| Eingriffszeit                                                                             |                                                                                     |           | Einstellung der Erkundungszeit, nach deren Ablauf der Alarm an die<br>Feuerwehr weitergeleitet wird                                              |

Tab. 15: Konfiguration der Integral IP Einstellungen



## Geo Check

Die Bedienung über die App Integral Mobile kann auf einen bestimmten Bereich (z. B. das Betriebsgelände) beschränkt werden. Dieser Bereich kann durch einen Kreis oder ein Polygon nachgebildet werden.

|           |                                                                                   |             |                   |
|-----------|-----------------------------------------------------------------------------------|-------------|-------------------|
| Geo Check |  | Aktiviert   | Geo Check aktiv   |
|           |  | Deaktiviert | Geo Check inaktiv |

Tab. 16: Konfiguration Geo Check

- ▶ Im Feld „Auf Karte suchen“ eine Adresse eingeben z. B. Stadt, Straße, Hausnummer und Enter drücken. Alternativ Eingabe von Breiten- und Längengrad.
- ▶ Das Kreis- oder Polygonsymbol auswählen.  

- ▶ Den Startpunkt über das Kreuz setzen.
- ▶ Den Kreis auf die gewünschte Radiusgröße ziehen.
- ▶ Beim Polygon einen Start und Zwischenpunkte setzen und die Linie am Startpunkt wieder schließen.
- ▶ Oben wird der Breiten- (Lat) und Längengrad (Lng) sowie die Radiusgröße angezeigt.
- ▶ Über „Form entfernen“ kann die Form wieder gelöscht werden.

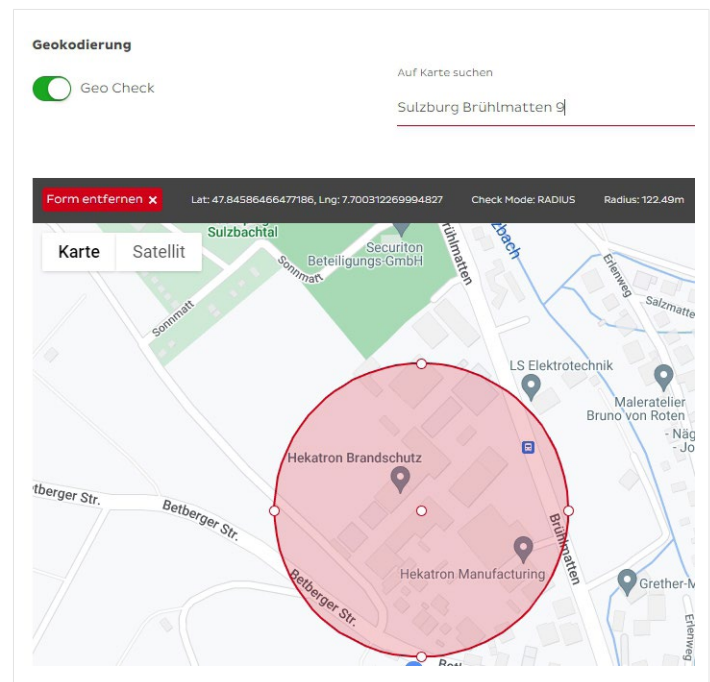


Abb. 53: Geo Check über einen Kreis

12.2 Menüleiste

In der Menüleiste können die verschiedenen Menüpunkte ausgewählt werden.

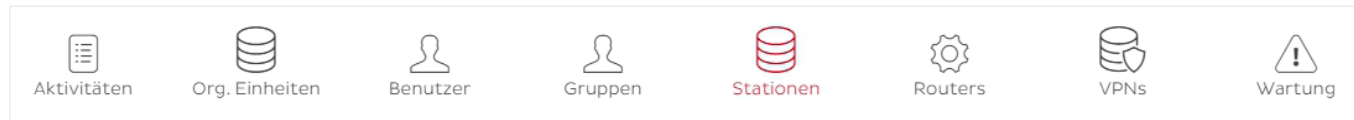


Abb. 54: Menüpunkte in der Menüleiste

| Menü                   | Beschreibung                                                                                                                                                                                                                                                                                |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aktivitäten            | <ul style="list-style-type: none"><li>- Aktivitäten/Ereignisse verbundener Anlagen anzeigen</li></ul>                                                                                                                                                                                       |
| Organisationseinheiten | <ul style="list-style-type: none"><li>- Hierarchische Organisationseinheiten erstellen</li><li>- Benutzer zuweisen</li><li>- Stationen zuweisen</li><li>- Router zuweisen</li><li>- VPN-Zertifikate zuweisen</li></ul>                                                                      |
| Benutzer               | <ul style="list-style-type: none"><li>- Benutzer anzeigen/ändern/löschen/entsperren/neu anlegen</li><li>- Stationen zuweisen</li><li>- Router zuweisen</li><li>- VPN-Zertifikate zuweisen</li></ul>                                                                                         |
| Gruppen                | <ul style="list-style-type: none"><li>- Gruppen anzeigen/ändern/löschen/neu anlegen</li><li>- Benutzer zuweisen</li><li>- Stationen zuweisen</li><li>- Router zuweisen</li></ul>                                                                                                            |
| Stationen              | <ul style="list-style-type: none"><li>- Stationen anzeigen</li><li>- Status anzeigen</li><li>- Stationseinstellungen ändern</li><li>- Beschriftungstexte für die App Integral Mobile</li><li>- Geo Check einrichten (Polygon, Radius)</li><li>- Push Benachrichtigungen verwalten</li></ul> |
| Routers                | <ul style="list-style-type: none"><li>- Router anzeigen</li><li>- IP-Adresse des Remote Mein HPlus VPN-Routers anzeigen</li><li>- Routername ändern</li></ul>                                                                                                                               |
| VPNs                   | <ul style="list-style-type: none"><li>- VPN-PC-Zertifikate herunterladen</li></ul>                                                                                                                                                                                                          |
| Wartung                | <ul style="list-style-type: none"><li>- Aktuelle Hinweise und geplante Wartungsarbeiten anzeigen</li></ul>                                                                                                                                                                                  |

Tab. 17: Inhalte unter den Menüpunkten

## 12.3 Aktivitäten

Ereignisse von Anlagen werden 92 Tage lang gespeichert und angezeigt, Push-Nachrichten nur für 31 Tage.



Abb. 55: Übersicht Aktivitäten

|   |                                                                                                     |                |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---|-----------------------------------------------------------------------------------------------------|----------------|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Anzahl Aktivitäten                                                                                  |                |  | In Klammer Anzeige der Anzahl der Aktivitäten in der Aktivitätenübersicht                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 2 | Allgemein                                                                                           | Filter         |  | Ein- oder Ausblenden der Filterkriterien                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|   |                                                                                                     | Exportieren    |  | Export der Aktivitätenübersicht in eine csv-Datei                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|   |                                                                                                     | Neu laden      |  | Anzeige der Aktivitätenübersicht wird aktualisiert                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 3 | Filterkriterien                                                                                     | Nachrichtentyp |  | Suche oder Mehrfachauswahl aus den Typen Info, Push Message, Warning, Error, Fatal. Die Anzahl der ausgewählten Typen wird im schwarzen Feld angezeigt                                                                                                                                                                                                                                                                                                                                                                        |
|   |                                                                                                     | Zeitpunkt      |  | Eingabe eines Datums im Format DD.MM.YYYY oder Auswahl über die Kalenderansicht, alternativ kann nach folgenden Kriterien gefiltert werden (die Auswahl des Datums wird dadurch gelöscht): <ul style="list-style-type: none"> <li>- Heute</li> <li>- Letzten 7 Tage</li> <li>- Letzten 30 Tage</li> </ul>                                                                                                                                                                                                                     |
|   |                                                                                                     | Nachricht      |  | Schlagwortsuche in der Nachricht                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|   |                                                                                                     | Stationsname   |  | Schlagwortsuche nach einem Stationsnamen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|   |                                                                                                     | Benutzername   |  | Schlagwortsuche nach einem Benutzernamen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 4 | Aktivitätenübersicht<br>(In der Titelleiste einer Spalte kann auf- oder absteigend sortiert werden) | Nachrichtentyp |  | Anzeige des Nachrichtentyps als Symbol <div>  Info  Push Message  Warning  Error  Fatal </div> |
|   |                                                                                                     | Zeitpunkt      |  | Anzeige des Zeitpunkts, an dem die Aktivität aufgetreten ist                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|   |                                                                                                     | Nachricht      |  | Anzeige des Nachrichtentextes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|   |                                                                                                     | Stationsname   |  | Anzeige des Stationsnamens                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|   |                                                                                                     | Benutzername   |  | Anzeige des Benutzernamens                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

Tab. 18: Inhalte unter Aktivitäten

## 12.4 Org.Einheiten

Die Organisationseinheit (z. B. eine Firma) unter der die Stationen und Router administriert werden.

- ▶ Eine angezeigte Organisationseinheit auswählen, suchen oder Neue Einheit hinzufügen.
- ▶ Über den Pfeil links neben einer Organisationseinheit können die Unter-Einheiten eingeblendet werden.

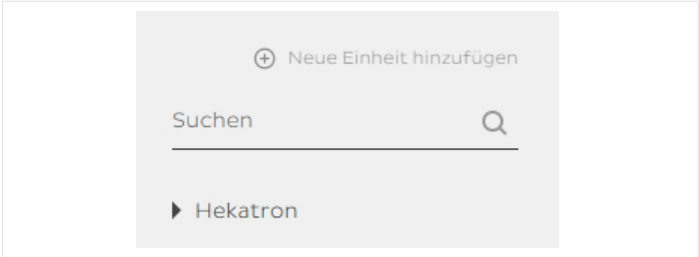


Abb. 56: Einstiegsmenü Org.Einheiten

### Auswahl einer bestehenden Organisationseinheit

Nach Auswahl werden die dieser Organisationseinheit zugewiesenen Nutzer, Stationen, Router und VPN-Zertifikate angezeigt.

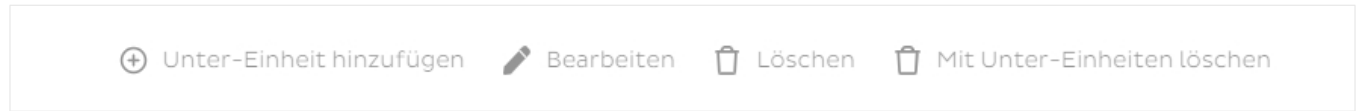


Abb. 57: Menüpunkte in der Menüleiste

|                             |                                                                                                              |
|-----------------------------|--------------------------------------------------------------------------------------------------------------|
| Unter-Einheit hinzufügen    | Erstellen einer untergeordneten Organisationseinheit. Ist identisch mit dem Punkt „Neue Einheit hinzufügen“. |
| Bearbeiten                  | Zuweisung von angelegten Benutzern, Stationen, Routern und VPN-Zertifikaten zur Organisationseinheit         |
| Löschen                     | Löschen der Unter-Einheit. Dazu die Sicherheitsabfrage mit OK bestätigen.                                    |
| Mit Unter-Einheiten löschen | Identisch mit dem Punkt „Löschen“                                                                            |

Tab. 19: Inhalte unter Org.Einheiten

- i

Wird unter „Bearbeiten“ die Maus über einem Benutzer der Organisationseinheit positioniert, erscheint rechts ein Papierkorbsymbol zum Löschen des Benutzers. Damit wird der Benutzer komplett gelöscht! Zum Löschen des Benutzers aus der Organisationseinheit diesem über das Menü „Benutzer“ eine neue Organisationseinheit zuweisen.

### Neue Einheit hinzufügen oder Unter-Einheit hinzufügen

- ▶ Einen Namen und eine Beschreibung der Unter-Einheit eingeben und speichern.
- ▶ Die Benutzer, Stationen, Router und VPN-Zertifikate der Unter-Einheit zuweisen.
- ▶ Dazu die gewünschten Einträge unter „Verfügbar“ suchen.
- ▶ Über + vor dem Eintrag diesen zuweisen oder über – die Zuweisung wieder entfernen.
- ▶ Mit Speichern abschließen.

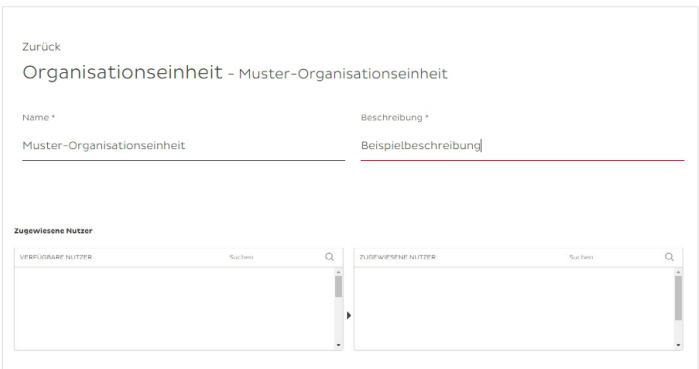


Abb. 58: Neue Unter-Einheit anlegen

## 12.5 Benutzer

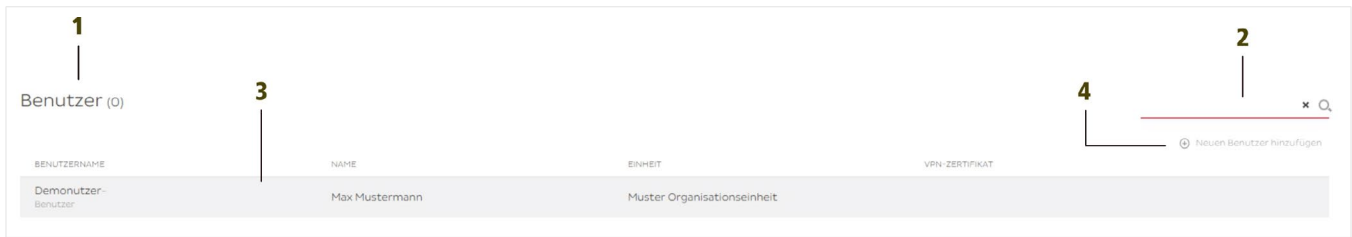


Abb. 59: Übersicht Benutzer

|   |                           |                |  |                                                                                                                                                               |
|---|---------------------------|----------------|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Anzahl Benutzer           |                |  | In Klammer Anzeige der Anzahl der Benutzer in der Benutzerübersicht                                                                                           |
| 2 | Sucheingabefeld           |                |  | Suche nach einem bestimmten Benutzer in der Übersicht                                                                                                         |
| 3 | Benutzerübersicht         | Benutzername   |  | Anmeldename des Benutzers                                                                                                                                     |
|   |                           | Name           |  | Vorname und Nachname des Benutzers                                                                                                                            |
|   |                           | Einheit        |  | Organisationseinheit, zu der der Benutzer zugeordnet wurde. Jeder Benutzer kann nur einer Einheit zugeordnet werden (Organisationseinheit oder Unter-Einheit) |
|   |                           | VPN-Zertifikat |  | VPN-Zertifikat, das dem Benutzer zugeordnet wurde                                                                                                             |
| 4 | Neuen Benutzer hinzufügen |                |  | Anlegen eines neuen Benutzers                                                                                                                                 |

Tab. 20: Inhalte unter Benutzer

Wird die Maus über einem Benutzer positioniert, erscheint rechts ein Papierkorbsymbol zum Löschen des Benutzers. Das Symbol anklicken und die Sicherheitsabfrage mit OK bestätigen.

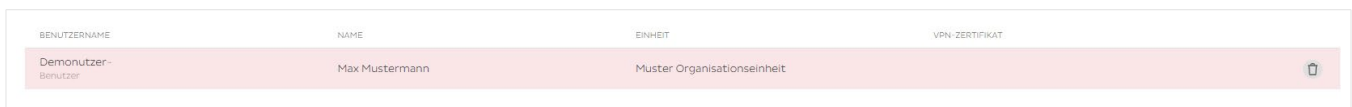


Abb. 60: Löschen eines Benutzers



Ein dem gelöschten Benutzer zugeordnetes VPN-Zertifikat wird ebenfalls gelöscht. Damit können auch weitere Benutzer, die das Zertifikat ebenfalls genutzt haben, nicht mehr zugreifen. Vor dem Löschen von Benutzern sollten bestehende Zertifikate daher auf andere Nutzer übertragen werden.

Bearbeiten eines Benutzers oder Neuen Benutzer hinzufügen

Durch Klick auf den Benutzernamen kann der Benutzer bearbeitet werden. Über „Neuen Benutzer hinzufügen“ kann ein neuer Benutzer angelegt werden.

Zurück

SPEICHERN

Nutzer Demonutzer

Nutzer

Benutzername\*

Demonutzer

Kennwort\*

Vorname

Max

Nutzerrollen\*

Benutzer

Nachname

Mustermann

Organisationseinheit\*

Muster Organi...

E-Mail Wartungsnachricht

Email:

Einstellungen

☐ Ist Administrator

☐ Ist Browser-Benutzer

☐ Geo-Check ignorieren

☒ Ist VPN-Benutzer

☐ Ist App-Benutzer

☐ App/Browser-Betrieb erlaubt

VPN-Einstellungen

VPN-Netzwerk

Keine Auswahl

Ausgeschlossen

☐ Ist gesperrt

Zugewiesene Stationen

VERFÜGBARE STATIONEN

Suchen

ZUGEWIESENE STATIONEN

Suchen

Zugewiesener Router

VERFÜGBARE ROUTER

Suchen

ZUGEWIESENER ROUTER

Suchen

Zugewiesene VPN Zertifikate

VERFÜGBARE VPN-ZERTIFIKATE

Suchen

ZUGEWIESENE VPN ZERTIFIKATE

Suchen

Abb. 61: Neuen Benutzer anlegen oder bestehenden Benutzer bearbeiten

|                          |                      |                                                                                                                                                                                                                           |
|--------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nutzer                   | Benutzername         | Benutzername zur Anmeldung in der App Integral Mobile und in der Remote Mein HPlus Adminoberfläche                                                                                                                        |
|                          | Vorname              | Vorname des Benutzers                                                                                                                                                                                                     |
|                          | Nachname             | Nachname des Benutzers                                                                                                                                                                                                    |
|                          | Kennwort             | Kennwort zur Anmeldung in der App Integral Mobile und in der Remote MeinHPlus Adminoberfläche .Das Kennwort muss aus mindestens 6 Zeichen bestehen, einen Großbuchstaben, einen Kleinbuchstaben und eine Ziffer enthalten |
|                          | Nutzerrollen         | Zuordnung einer Rolle an den Benutzer, zur Auswahl stehen User mit einfachen Rechten oder Installer mit erweiterten Rechten                                                                                               |
|                          | Organisationseinheit | Zuordnung des Benutzers zu einer Organisationseinheit                                                                                                                                                                     |
| E-Mail Wartungsnachricht | E-Mail               | E-Mail, an die Informationen zu geplanten Wartungsarbeiten gesendet werden                                                                                                                                                |

|                |                      |                                                                                     |             |                                                                                                                                                                                  |
|----------------|----------------------|-------------------------------------------------------------------------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Einstellungen  | Ist Administrator    |    | Aktiviert   | Der Benutzer ist berechtigt, sich auf der Remote MeinHPlus Adminoberfläche anzumelden                                                                                            |
|                |                      |    | Deaktiviert | Der Benutzer ist nicht berechtigt, sich auf Remote MeinHPlus Adminoberfläche anzumelden                                                                                          |
|                | Ist Browser-Benutzer |    | Aktiviert   | Der Benutzer ist berechtigt Integral Browser zu verwenden                                                                                                                        |
|                |                      |    | Deaktiviert | Der Benutzer ist nicht berechtigt Integral Browser zu verwenden                                                                                                                  |
|                | Geo-Check ignorieren |    | Aktiviert   | Der unter Stations aktivierte Geo Check wird für den Benutzer ignoriert                                                                                                          |
|                |                      |    | Deaktiviert | Der unter Stations aktivierte Geo Check ist für den Benutzer gültig                                                                                                              |
|                | Ist VPN-Benutzer     |    | Aktiviert   | Dem Benutzer kann ein VPN-Zertifikat zugewiesen werden. Wird ein Benutzer mit zugewiesenem VPN-Zertifikat gelöscht, wird aus Sicherheitsgründen auch das VPN-Zertifikat gelöscht |
|                |                      |    | Deaktiviert | Dem Benutzer kann kein VPN-Zertifikat zugewiesen werden.                                                                                                                         |
|                | Ist App-Benutzer     |    | Aktiviert   | Der Benutzer ist berechtigt die App Integral Mobile zu verwenden                                                                                                                 |
|                |                      |    | Deaktiviert | Der Benutzer ist nicht berechtigt die App Integral Mobile zu verwenden.                                                                                                          |
| Ausgeschlossen | Ist gesperrt         |   | Aktiviert   | Der Benutzer ist berechtigt die Anlage zu bedienen                                                                                                                               |
|                |                      |  | Deaktiviert | Der Benutzer ist nicht berechtigt die Anlage zu bedienen. Die Eingabe eines Berechtigungscodes ist nicht möglich, lediglich die Anzeige der Meldungen und Ort-Info-Angaben       |
|                |                      |  | Deaktiviert | Der Benutzer ist nicht gesperrt                                                                                                                                                  |

Tab. 21: Inhalte unter Benutzer bearbeiten/hinzufügen

- Abschließend die Stationen, Router und VPN-Zertifikate dem Benutzer zuweisen. Die kann vereinfacht für mehrere Benutzer auch durch Gruppierung und Zuordnung über Organisationseinheiten erfolgen.
- Dazu die gewünschten Einträge unter „Verfügbar“ suchen.
- Über + vor dem Eintrag diesen zuweisen oder über – die Zuweisung wieder entfernen.
- Mit Speichern abschließen.

12.6 Gruppen

Über Gruppen können beispielsweise Stationen und Router zu einer Region zugewiesen werden. Sollte ein neuer Benutzer Zugriff auf diese Stationen und Router benötigen, kann er dieser Gruppe zugewiesen werden.

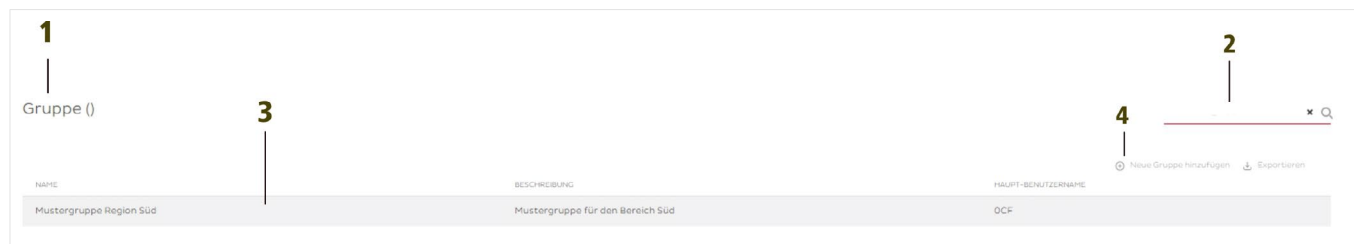


Abb. 62: Übersicht Gruppen

|   |                  |                        |  |                                                                   |
|---|------------------|------------------------|--|-------------------------------------------------------------------|
| 1 | Anzahl Gruppen   |                        |  | In Klammer Anzeige der Anzahl der Gruppen in der Gruppenübersicht |
| 2 | Sucheingabefeld  |                        |  | Suche nach einer bestimmten Gruppe in der Übersicht               |
| 3 | Gruppenübersicht | Name                   |  | Name der Gruppe                                                   |
|   |                  | Beschreibung           |  | Beschreibung der Gruppe                                           |
|   |                  | Haupt-Benutzername     |  | Übergeordneter Benutzer, z. B. mit der Nutzerrolle Installer      |
| 4 | Allgemein        | Neue Gruppe hinzufügen |  | Anlegen einer neuen Gruppe                                        |
|   |                  | Exportieren            |  | Export der Gruppenübersicht in eine csv-Datei                     |

Tab. 22: Inhalte unter Gruppen

Wird die Maus über einer Gruppe positioniert, erscheint rechts ein Papierkorbsymbol zum Löschen der Gruppe. Das Symbol anklicken und die Sicherheitsabfrage mit OK bestätigen.

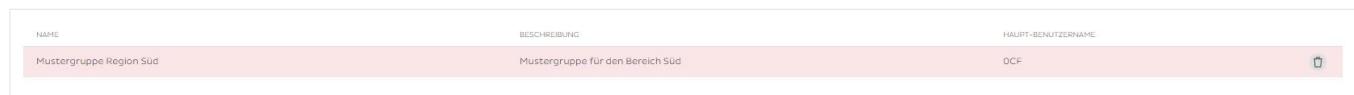


Abb. 63: Löschen einer Gruppe

Bearbeiten einer Gruppe oder Neue Gruppe hinzufügen

Durch Klick auf den Namen kann die Gruppe bearbeitet werden. Über „Neuen Gruppe hinzufügen“ kann eine neue Gruppe angelegt werden.

Zurück

Gruppe-m

SPEICHERN

Allgemeines

Name\*

Beschreibung

Haupt-Benutzername

Mustergruppe Region Süd

Mustergruppe für den Bereich Süd

Keine Auswahl

Abb. 64: Neue Gruppe anlegen oder bestehende Gruppe bearbeiten

- ▶ Gruppendaten bearbeiten oder für neue Gruppe Namen, Beschreibung und Haupt-Benutzername eingeben
- ▶ Mit Speichern abschließen.



12.7 Router

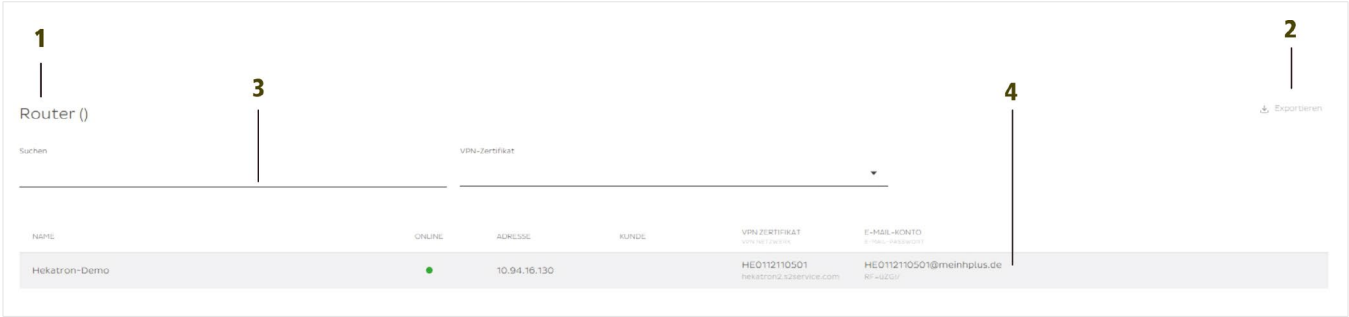


Abb. 65: Übersicht Router

|   |                 |                                   |  |                                                                                                                                                                                                                  |
|---|-----------------|-----------------------------------|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Anzahl Router   |                                   |  | In Klammer Anzeige der Anzahl der Router in der Routerübersicht                                                                                                                                                  |
| 2 | Exportieren     |                                   |  | Export der Gruppenübersicht in eine csv-Datei                                                                                                                                                                    |
| 3 | Sucheingabefeld | Suchen                            |  | Suche nach einem bestimmten Router in der Übersicht                                                                                                                                                              |
|   |                 | VPN-Zertifikat                    |  | Suche nach einem bestimmten VPN-Zertifikat in der Übersicht                                                                                                                                                      |
| 4 | Routerübersicht | Name                              |  | Name der Gruppe                                                                                                                                                                                                  |
|   |                 | Online                            |  | Der Router ist mit dem VPN-Netzwerk verbunden                                                                                                                                                                    |
|   |                 |                                   |  | Der Router ist nicht mit dem VPN-Netzwerk verbunden                                                                                                                                                              |
|   |                 | Adresse                           |  | IP-Adresse des Remote Mein HPlus VPN-Routers im Remote Mein HPlus-Netzwerk. Über diese IP-Adresse kann eine Verbindung aufgebaut werden. Als Voraussetzung muss ein VPN-Zertifikat vorhanden und zugewiesen sein |
|   |                 | Kunde                             |  | Name des Kunden                                                                                                                                                                                                  |
|   |                 | VPN-Zertifikat<br>VPN-Netzwerk    |  | Über die VPN-ID wird jeder Router eindeutig im VPN-Netzwerk identifiziert. Diese ID kann nicht verändert werden und muss bei Erweiterungen angegeben werden, z. B. VPN-Zertifikate                               |
|   |                 | E-Mail-Account<br>E-Mail-Passwort |  | Für jeden Remote MeinHPlus VPN-Router wird automatisch ein E-Mail-Konto mit Passwort erstellt                                                                                                                    |

Tab. 23: Inhalte unter Router

Bearbeiten eines Routers

Durch Klick auf den Namen kann der Router bearbeitet werden (Änderung Name). Außerdem können weitere Router zugewiesen werden, z. B. bei Verbindungen über Integral WAN.

12.8 VPNs

In diesem Dialog können die vorhandenen VPN-Client-Zertifikate für den Verbindungsaufbau über einen PC heruntergeladen werden.

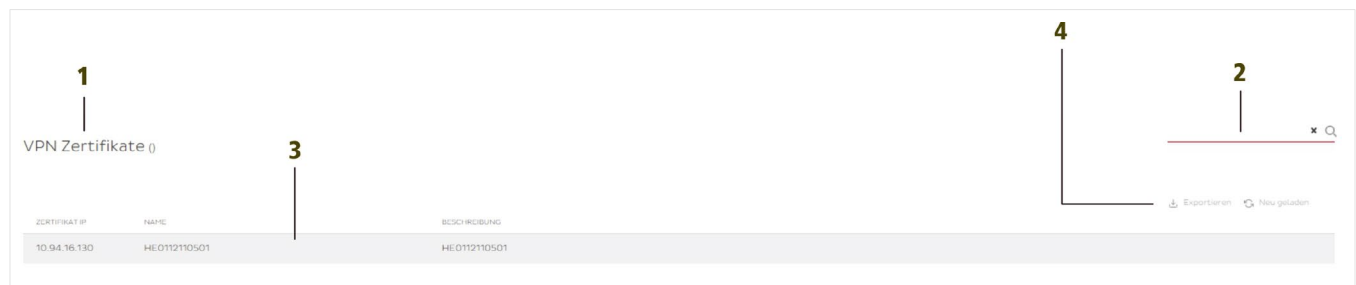


Abb. 66: Übersicht VPNs

|   |                      |               |  |                                                                               |
|---|----------------------|---------------|--|-------------------------------------------------------------------------------|
| 1 | Anzahl VPNs          |               |  | In Klammer Anzeige der Anzahl der VPN-Zertifikate in der Zertifikatsübersicht |
| 2 | Sucheingabefeld      |               |  | Suche nach einem bestimmten VPN-Zertifikat in der Übersicht                   |
| 3 | Zertifikatsübersicht | Zertifikat IP |  |                                                                               |
|   |                      | Name          |  |                                                                               |
|   |                      | Beschreibung  |  |                                                                               |
| 4 | Allgemein            | Exportieren   |  | Export der VPN-Zertifikatsübersicht in eine csv-Datei                         |
|   |                      | Neu geladen   |  | Anzeige der VPN-Zertifikatsübersicht wird aktualisiert                        |

Tab. 24: Inhalte unter VPNs

Wird die Maus über einem Zertifikat positioniert, erscheint rechts ein weiterer Menüpunkt.



Abb. 67: Weiterer Menüpunkt in der VPNs Übersicht

| Menü                       | Beschreibung                                                              |
|----------------------------|---------------------------------------------------------------------------|
| Download User Certificates | Download des VPN-Zertifikats zum Aufbau des VPN über die Software OpenVPN |

Tab. 25: Inhalte im weiteren Menüpunkt

12.9 Wartung

Aktuelle Hinweise und geplante Wartungsarbeiten werden angezeigt.

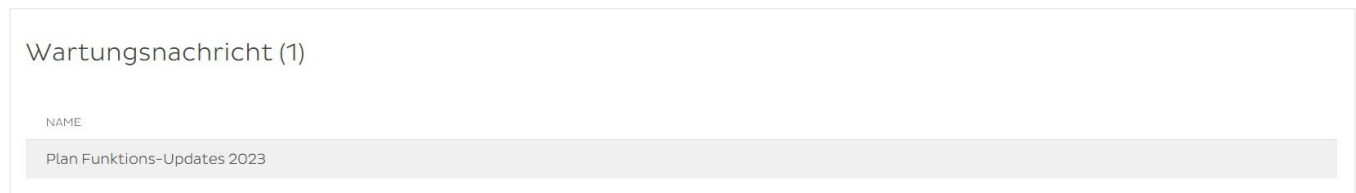


Abb. 68: Anzeige Wartungsarbeiten

## 13. Bedienung

- i** Die Zugangsberechtigung zwischen Betreiber und Hekatron Remote Nutzer sollte schriftlich festgehalten werden. Jeder Fernzugriff und die in diesem Zusammenhang durchgeführten Änderungen sollten vom Betreiber im Betriebsbuch dokumentiert werden.

### 13.1 Remote Standard

Zur Herstellung einer Verbindung über Remote Standard wird ein Windows-PC, eine VPN-Software (z. B. OpenVPN) und ein VPN-Zertifikat für den PC benötigt. Das Zertifikat bestätigt die Zugriffsberechtigung des Benutzers. Im VPN-Router an der Brandmelderzentrale ist ein solches Zertifikat bereits vorinstalliert, das VPN-PC-Zertifikat wird separat zugeschickt oder kann über die Remote Mein HPlus Adminoberfläche heruntergeladen werden. Weiterhin ist ein gültiger Integral Dongle für den Fernzugriff erforderlich.

- ▶ OpenVPN auf dem Windows-PC installieren.
- ▶ Nach der Installation Rechtsklick auf die OpenVPN Verknüpfung und Eigenschaften auswählen.
- ▶ Im Reiter Kompatibilität unter Berechtigungsstufe Haken bei „Programm als Administrator ausführen“ setzen.
- ▶ Anschließend das VPN-PC-Zertifikat im Ordner C:\Benutzer\OpenVPN\config ablegen.

- ▶ OpenVPN starten.
- ▶ Über das Symbol in der Statusleiste mit rechter Maustaste das Menü aufrufen und „Connect“ auswählen.
- ▶ Sind mehrere einzelne Zertifikate hinterlegt (z. B. verschiedene Anlagen) vorab die gewünschte Anlage aus dem Menü auswählen.

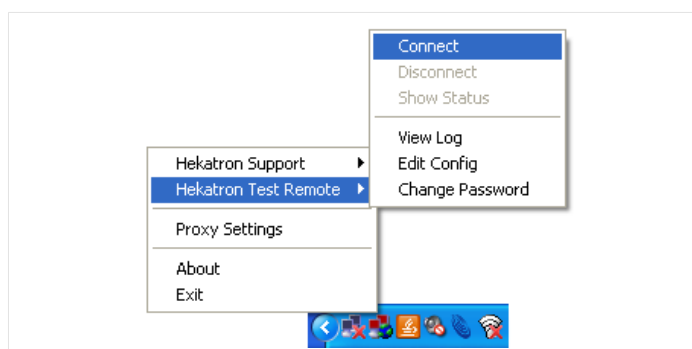


Abb. 69: OpenVPN starten

Es öffnet sich ein Fenster, das den Aufbau der Verbindung anzeigt. Wurde der Aufbau erfolgreich durchgeführt wird dies mit der Meldung „...is now connected“ bestätigt.

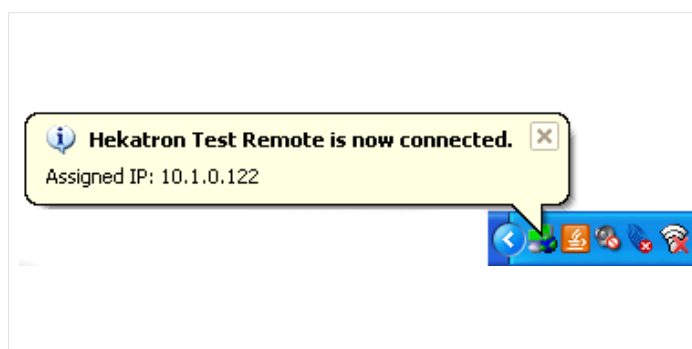


Abb. 70: Bestätigung Verbindung

- i** Für die Verbindung zur Brandmelderzentrale muss die im Router hinterlegte IP-Adresse für den VPN-Tunnel verwendet werden! Für lokale Verbindungen über das interne Netzwerk (Intranet) ist keine VPN-Verbindung erforderlich, hier kann direkt mit den Anwendungen auf die Brandmelderzentrale zugegriffen werden.

Mit bestehender Verbindung kann nun die Verbindung zur Brandmelderzentrale aufgebaut werden.

Dazu die gewünschte Anwendung in der Integral Software öffnen. Unterstützt werden:

- Loader z. B. Anlagendaten rücklesen, mit Berechtigung Anlagendaten programmieren
- Peripherie Assistant z. B. Melderverschmutzung auslesen, mit Berechtigung Ringdaten programmieren
- Service Assistant z. B. Ereignisspeicher auslesen, mit Berechtigung Befehle senden
- Integral Desktop (Integriert in die Software und als eigenständige Anwendung) z. B. aktuellen Zustand der BMZ anzeigen lassen, mit Berechtigung Bedienungsvorgänge durchführen

Im folgenden wird exemplarisch der Zugriff über Integral Desktop beschrieben, die Zugriffe auf die anderen Anwendungen sind identisch.

- Anwendung Integral Desktop in der Integral Software starten.
- Unter TCP/IP-Verbindung **1** die IP-Adresse des VPN-Tunnels (tun0) eintragen und auf das Verbinden Symbol **2** drücken um eine Verbindung zum System herzustellen.
- Soll der Zugriff über das interne Netzwerk (lokale Verbindung) erfolgen, unter TCP/IP-Verbindung die IP-Adresse der Zentrale eintragen. Befindet sich der PC im gleichen Adressbereich wie die Zentrale reicht ein Basis-Dongle aus.

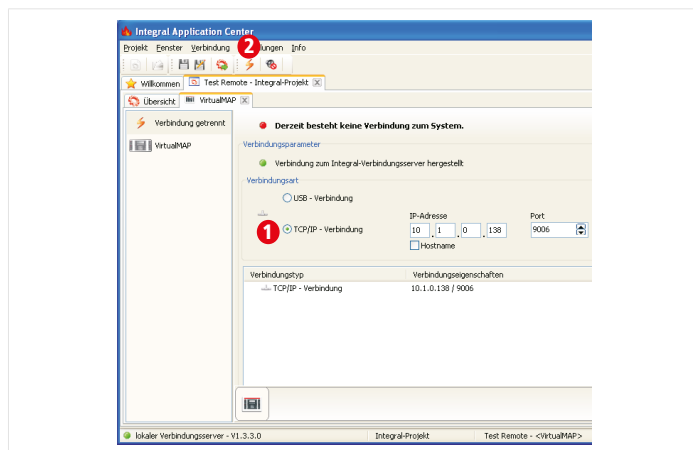


Abb. 71: Eingaben unter Integral Desktop

Ist der Basis-Dongle für den netzwerkübergreifenden Fernzugriff (Internet) nicht lizenziert, wird eine entsprechende Meldung angezeigt. In diesem Fall muss der Basis-Dongle um die Erweiterung Remote Access ergänzt werden.

Ist die Verbindung hergestellt, wird Benutzername und Passwort abgefragt.

- Hier die unter „Benutzer“ in der Programmierung hinterlegten Daten innerhalb von 2 min (bei lokaler Verbindung gibt es keine Zeitvorgabe) eintragen.

⇒ Nach erfolgter Anmeldung wird das Integral Desktop eingeblendet.

Wurde in der Benutzerprogrammierung „nach Freigabe“ ausgewählt, erscheint die Meldung, dass vor Bedienung zuerst eine Freischaltung an der Zentrale erfolgen muss.

Wird trotzdem versucht einen Berechtigungswechsel durchzuführen, so erscheint eine zweite Fehlermeldung.

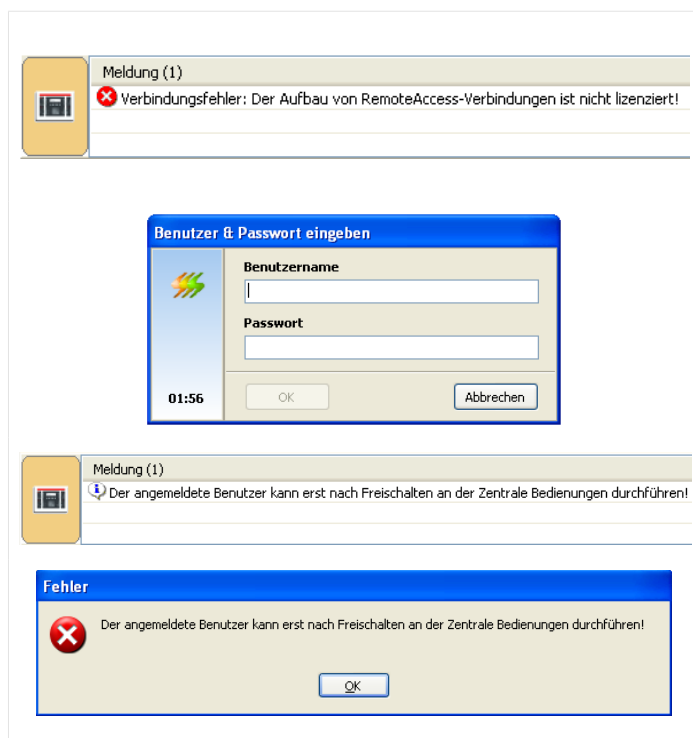


Abb. 72: Über Fernzugriff anmelden

An der Zentrale vor Ort wird die Fernzugriffsanfrage nun als Aktivierung im Bedienfeld angezeigt. Über die Taste weitere Listen kann der berechtigte Bediener vor Ort die Aktivierungen einsehen.

Aktiv Remote heißt, es besteht bereits eine aktive Verbindung von Benutzer-ID 0 (z. B. lokale Verbindung über Netzwerk). Vor-Aktiv Remote ist die aktuelle Anfrage von Benutzer-ID 2, die auf Freigabe wartet.

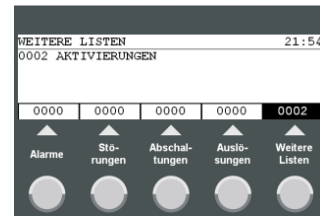
- Über die Pfeiltasten auf Vor-Aktiv Remote Access scrollen und mit Enter bestätigen.
  - Bei Anzeige Elementbedienung die Taste Setzen/Rücksetzen drücken.
- ⇒ Der Fernzugriff über Remote Standard ist jetzt freigeschaltet und die Funktionen des virtuellen Bedienfeldes können genutzt werden.
- Zum Beenden der Verbindung wieder auf das Verbinden Symbol drücken (oder Menüpunkt Verbindung).

Alternativ kann der Bediener vor Ort den Zugriff über die Taste Setzen/Rücksetzen wieder sperren.

Bei Fernzugriff über das Element Extern erscheint Remote Access Aktiv.

- Die Taste „Weitere Elemente“ drücken und das Element Extern über die Pfeiltasten auswählen.
  - Die Nummer 65000 eingeben und Enter drücken.
  - Die Taste „Setzen/Rücksetzen“ drücken.
- ⇒ Der Fernzugriff ist jetzt freigeschaltet und die Funktionen des virtuellen Bedienfeldes können genutzt werden. Das Element Extern wird zur programmierten Zeit automatisch wieder rückgesetzt.

- Unter dem Menüpunkt Einstellungen die Pa-nelsprache umstellen oder die Akustik ein- und ausschalten (oder über Akustik Symbol).



| AKTIVIERUNGEN |                      |      |      |      |
|---------------|----------------------|------|------|------|
| 1             | AKTIV REMOTE ACC     |      |      | 1/0  |
| 2             | VOR-AKTIV REMOTE ACC |      |      | 1/2  |
| 0000          | 0000                 | 0000 | 0000 | 0002 |

| ELEMENTBEDIENUNG |      |      |      |      |
|------------------|------|------|------|------|
| REMOTEACCESS     |      | 1/2  |      |      |
| VOR-AKTIV        |      |      |      |      |
|                  |      |      |      |      |
| 0000             | 0000 | 0000 | 0000 | 0002 |

| ELEMENTBEDIENUNG |      |      |      |      |
|------------------|------|------|------|------|
| REMOTEACCESS     |      | 1/2  |      |      |
| AKTIV            |      |      |      |      |
|                  |      |      |      |      |
| 0000             | 0000 | 0000 | 0000 | 0002 |

Abb. 73: Fernzugriff freischalten

| ELEMENTBEDIENUNG |      |      |      |      |
|------------------|------|------|------|------|
| REMOTEACCESS     |      | 1/2  |      |      |
| AKTIV            |      |      |      |      |
| 0000             | 0000 | 0000 | 0000 | 0000 |

| AUSLÖSUNGEN |      |      |      |       |
|-------------|------|------|------|-------|
| EXTERN      |      |      |      | 65000 |
| AKTIV       |      |      |      |       |
| 0000        | 0000 | 0000 | 0001 | 0000  |

Abb. 74: Fernzugriff über Element Extern freischalten

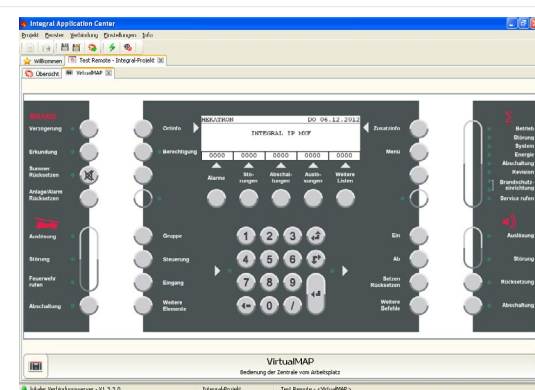


Abb. 75: Virtuelles Bedienfeld

## Integral Desktop als eigenständige Lösung

Neben dem in der Integral Software integrierten Integral Desktop kann dieses auch als eigenständige Lösung separat installiert werden (z. B. für Betreiber, die lediglich einen Fernzugriff auf das Bedienfeld wünschen). Für diese Anwendung steht ein spezieller Integral Desktop Dongle zur Verfügung, auf dem nur das virtuelle Bedienfeld freigeschaltet ist.

- i** Im Gegensatz zu der in der Integral Software integrierten Version des Integral Desktop kann mit der eigenständigen Anwendung mit Integral Desktop Dongle sowohl lokal als auch global auf die Brandmelderzentrale zugegriffen werden. Bei globalem Zugriff unter TCP/IP-Verbindung die IP-Adresse des VPN-Tunnels (tun0) eintragen und auf das Verbinden Symbol drücken um eine Verbindung zum System herzustellen. Wurde in der Benutzerprogrammierung „nach Freigabe“ ausgewählt, erscheint auch hier die Meldung, dass vor Bedienung zuerst eine Freischaltung an der Zentrale erfolgen muss.

- ▶ Anwendung Integral Desktop starten.
  - ▶ Unter TCP/IP-Verbindung **1** die IP-Adresse der Zentrale (192.168.193.1) eintragen und auf das Verbinden Symbol **2** drücken um eine Verbindung zum System herzustellen.
  - ▶ Ist die Verbindung hergestellt wird Benutzername und Passwort abgefragt. Hier die unter „Benutzer“ in der Programmierung hinterlegten Daten eintragen.
- ⇒ Der Fernzugriff über Remote Standard ist jetzt freigeschaltet und die Funktionen des virtuellen Bedienfeldes können genutzt werden. Zum Beenden der Verbindung wieder auf das Verbinden Symbol drücken (oder Menüpunkt Verbindung).

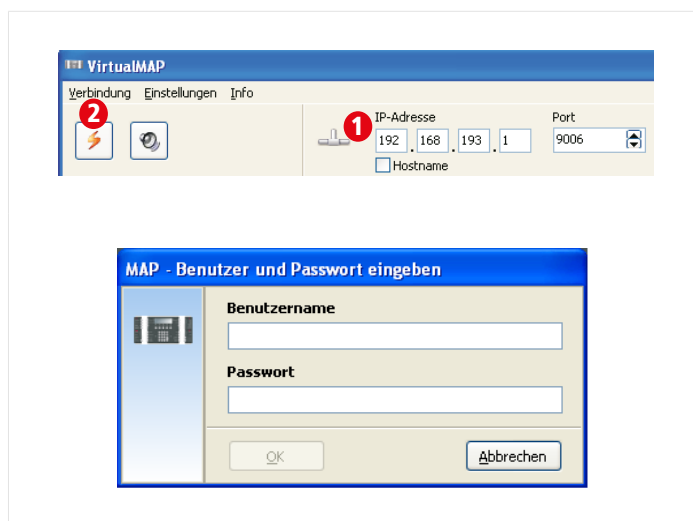


Abb. 76: Verbindung herstellen

- ▶ Unter dem Menüpunkt Einstellungen die Panelsprache umstellen oder die Akustik ein- und ausschalten (oder über Akustik Symbol).
- ▶ Unter dem Menüpunkt Verbindung aktuelle Verbindungsdaten als Verknüpfung speichern.



Abb. 77: Virtuelles Bedienfeld

## 13.2 Remote Mobile

Zur Herstellung einer Verbindung über Remote Mobile wird eine spezielle App „Integral Mobile“ benötigt, die in den entsprechenden Stores kostenfrei zur Verfügung steht. Nach der Installation erscheint eine Abfrage, ob der Standort des mobilen Endgerätes ermittelt werden darf. Wird mit Nein bestätigt, ist über die App nur die Anzeige aber keine Bedienung möglich.

Es erscheint eine weitere Abfrage, ob die App „Integral Mobile“ Push-Mitteilungen senden darf.

- Wenn dies gewünscht wird entsprechend bestätigen.

Beide Einstellungen können jederzeit auch nachträglich am mobilen Endgerät wieder geändert werden.

- ⇒ Nun wird die App auf dem mobilen Endgerät angezeigt und kann gestartet werden. Nach Laden der Anwendung erscheint der Anmeldebildschirm.

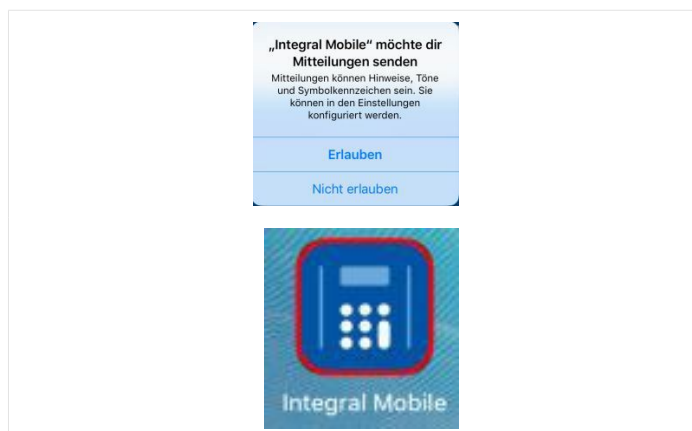


Abb. 78: App starten

## Bedienung mit dem Tablet

- Zur Anmeldung und Verbindung mit der Brandmelderzentrale den Benutzer und das Passwort eingeben und mit Login bestätigen.

Folgende Fehlermeldungen können auftreten:

- Invalid username/password  
Der Benutzer hat einen falschen Benutzernamen oder ein falsches Passwort angegeben
- User locked by system  
Der Benutzername oder das Passwort wurden mehrfach hintereinander falsch eingegeben. Der Benutzer wurde gesperrt und kann nur über Remote Mein HPlus wieder entsperrt werden
- User is locked  
Ein gesperrter Benutzer versucht sich anzumelden ohne dass zuvor die Entsperrung über die Remote Mein HPlus Adminoberfläche erfolgt ist
- No station online...  
Die Brandmelderzentrale ist nicht verbunden
- No configured station...  
Dem Benutzer wurden in der Remote Mein HPlus Adminoberfläche keine Brandmelderzentralen zugeordnet

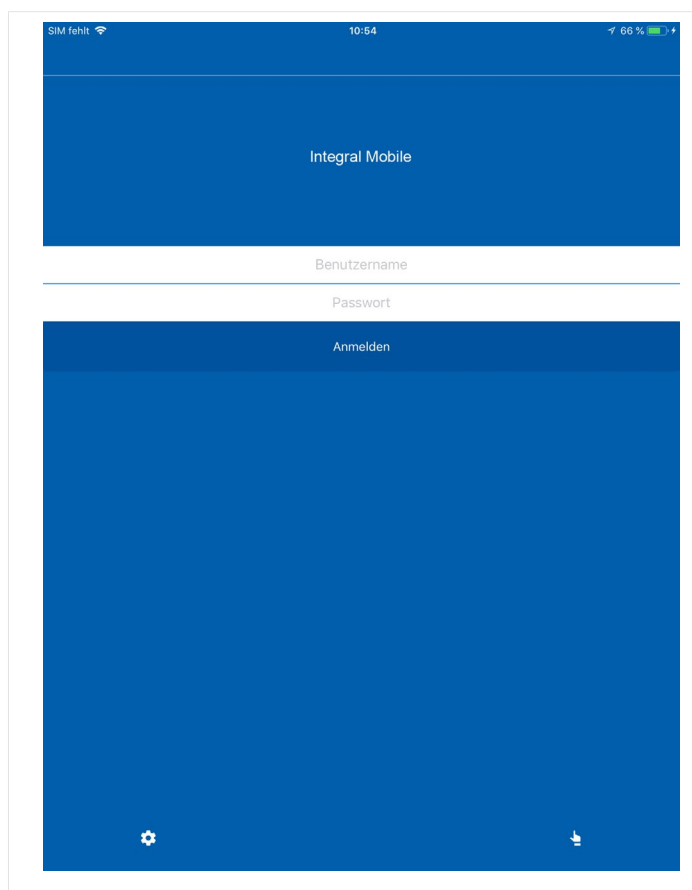


Abb. 79: Anmelden

Sind dem Benutzer mehrere Brandmelderzentralen zugeordnet, so kann über den Pfeil rechts das Auswahlfenster geöffnet werden.

- Im Auswahlfenster auswählen, mit welcher Zentrale eine Verbindung hergestellt werden soll.

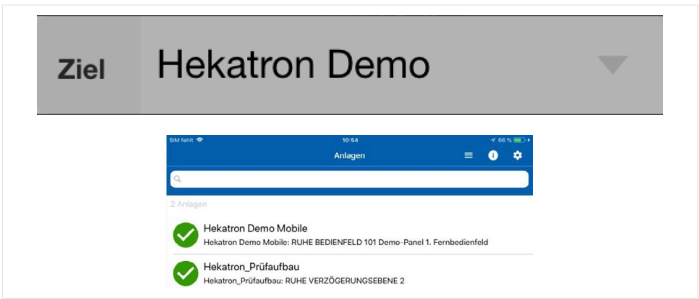


Abb. 80: Zentrale auswählen

**i** Die Anlage und Änderung von Benutzern sowie die Zuordnung von Brandmelderzentralen zu Benutzern kann über die Remote Mein HPlus Adminoberfläche durchgeführt werden.

- ⇒ Nach erfolgreicher Anmeldung wird die Verbindung zur Zentrale hergestellt und das virtuelle Bedienfeld angezeigt.

Im Hochformat ist nur ein kleiner Ausschnitt des Bedienfeldes sichtbar. Durch Drehen des Tablets (Kippfunktion) ins Querformat wird das Bedienfeld automatisch komplett angezeigt und alle Funktionen des virtuellen Bedienfeldes können genutzt werden.

Ist der Geo Check aktiviert und man befindet sich außerhalb des definierten Bedienungsradius oder Polygons, so ist lediglich die Anzeige im Hochformat möglich. Ein Drehen des Tablets ins Querformat zur weiteren Bedienung ist damit nicht möglich.



Abb. 81: Anzeige am Tablet

Der Status der Brandmelderzentrale wird oben in der Leiste angezeigt (grün für Betrieb, rot für Alarm und gelb für Störung).

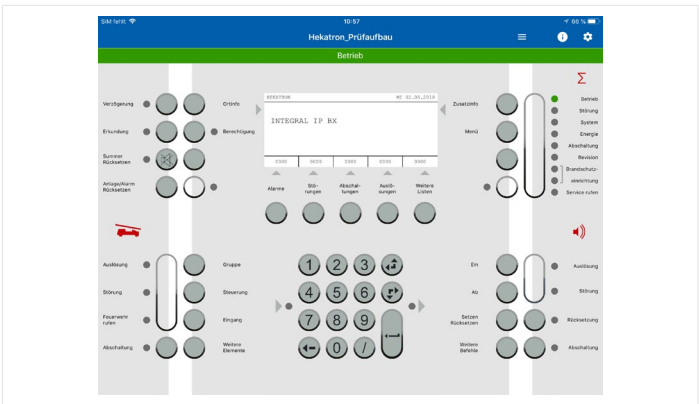


Abb. 82: Virtuelles Bedienfeld





Über dieses Symbol öffnet sich das Einstellungsmenü mit folgenden Einträgen, siehe Abbildung links.



Über dieses Symbol öffnet sich das Einstellungsmenü mit folgenden Einträgen, siehe Abbildung rechts.

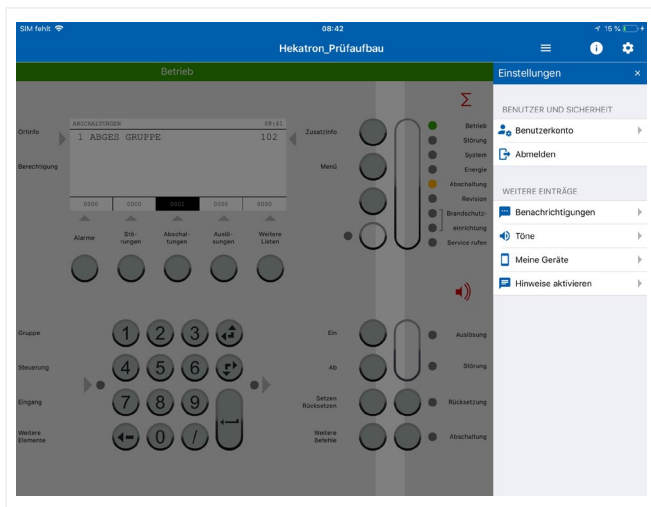


Abb. 83: Menü Einstellungen 1

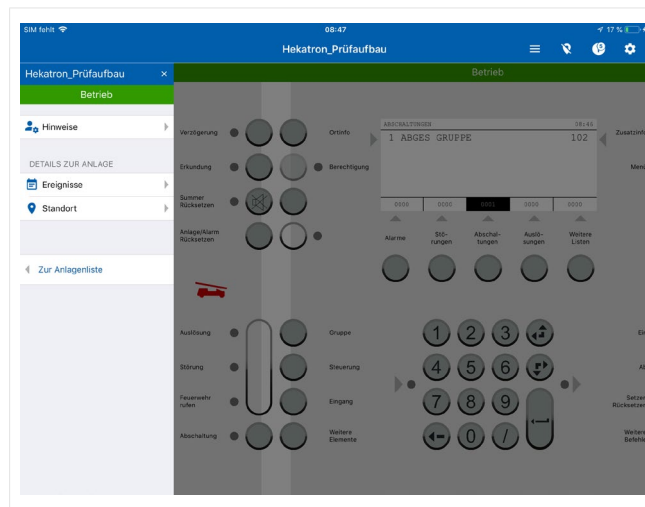


Abb. 84: Menü Einstellungen 2

|                     |                                                                                                                                                            |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Benutzerkonto       | Anzeige der Einstellungen des Benutzerkontos, z. B. Passwort                                                                                               |
| Abmelden            | Benutzer abmelden                                                                                                                                          |
| Benachrichtigungen  | Aktivierung von Push- und E-Mailnachrichten für die aktuell verbundene Anlage                                                                              |
| Töne                | Einstellung der Töne                                                                                                                                       |
| Meine Geräte        | Alle Endgeräte werden bei der ersten Anmeldung von der App gespeichert und in der Liste aufgeführt. Über das Papierkorbsymbol können diese gelöscht werden |
| Hinweise aktivieren | Aktivierung der Hinweise                                                                                                                                   |
| Hinweise            | Anzeige relevante Hinweise                                                                                                                                 |
| Ereignisse          | Anzeige der Ereignisse                                                                                                                                     |
| Standort            | Anzeige des aktivierten Geo Checks                                                                                                                         |

Unter Standort wird der Bereich des aktivierten Geo Checks (Bild rechts Polygon) dargestellt. Zusätzlich wird der Name der Brandmelderzentrale angezeigt, mit der man über die App verbunden ist. Bei Einstellung eines Radius erfolgt die Darstellung über einen Kreis.

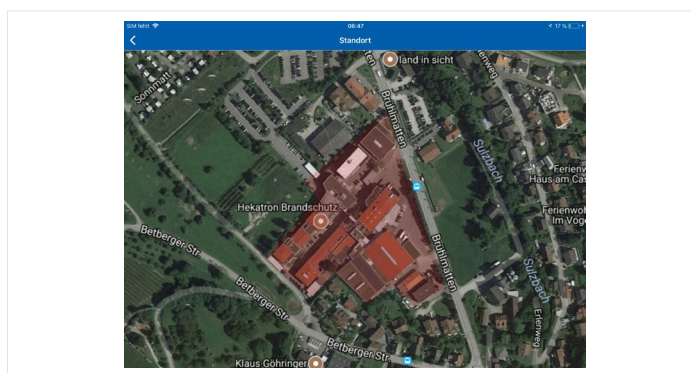


Abb. 85: Anzeige Geo Check

- ▶ Unter Benachrichtigungen bei gewünschter Aktivierung von Push Nachrichten den obersten Regler nach rechts schieben.
- ▶ Je nach gewünschter Aktivierung die Regler für Push Alarm, Push Störung, Push Verbindung und Push Sonstige nach rechts schieben.
- ▶ Das Gleiche im Feld darunter für E-Mail-benachrichtigungen durchführen.

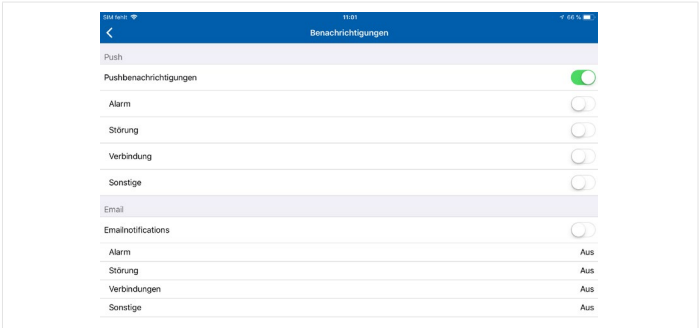


Abb. 86: Push und E-Mailbenachrichtigungen

Zusätzlich kann für die Zustände Alarm, Störung und Sonstige auch jeweils eine E-Mailadresse angegeben werden, an die die App die entsprechenden Informationen verschickt.

- ▶ Über den Button „Email-Adresse hinzufügen“ eine neue Adresse eingegeben. Über „Alle löschen“ können alle Adressen gelöscht werden.

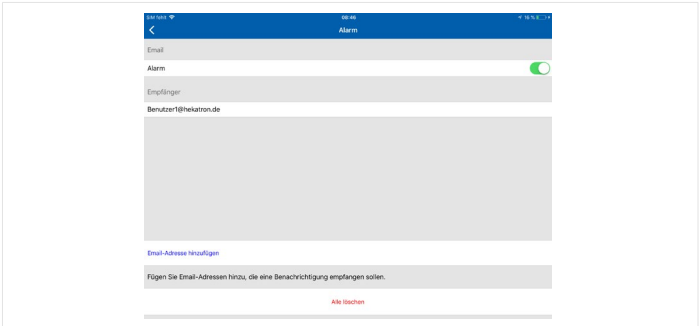


Abb. 87: E-Mailadresse hinzufügen

⇒ Nun werden auch bei nicht gestarteter App die entsprechenden Zustände der Brandmelderzentrale als Benachrichtigung am Bildschirm des mobilen Endgerätes angezeigt. Von dort kann über „Anzeigen“ direkt in die App gewechselt werden.

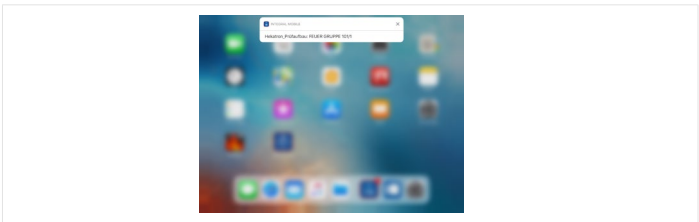


Abb. 88: Anzeige am Bildschirm

- ▶ Zum Ändern des Passworts das alte und neue Passwort eingeben, das neue Passwort bestätigen und mit „Passwort ändern“ speichern.

Das neue Passwort muss aus mindestens 6 Zeichen bestehen, davon mindestens ein Großbuchstabe, ein Kleinbuchstabe und eine Zahl.

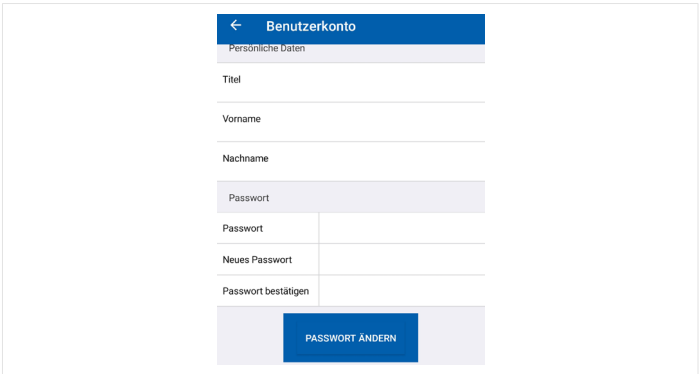


Abb. 89: Passwort ändern

**i** Das persönliche Passwort sollte aus Sicherheitsgründen in regelmäßigen Abständen geändert werden.

## Bedienung mit dem Smartphone

Die Anmeldung über Smartphone ist identisch zur Anmeldung über Tablet.

Nach erfolgreicher Anmeldung wird die Verbindung zur Zentrale hergestellt und das virtuelle Bedienfeld angezeigt. Im Hochformat ist nur ein kleiner Ausschnitt des Bedienfeldes sichtbar (Anzeige 1).

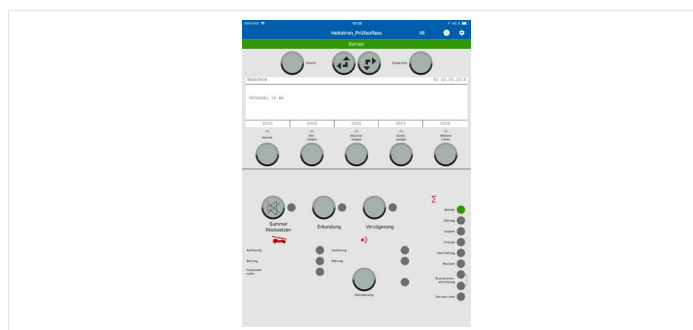


Abb. 90: Anzeige 1

Im Gegensatz zum Tablet (Kippfunktion) werden auch die weiteren Bereiche des Bedienfeldes beim Smartphone im Hochformat über Wischen angezeigt.

- Einmal Wischen von rechts nach links blendet die Anzeige 2 ein. Einmal Wischen von links nach rechts wieder Anzeige 1.

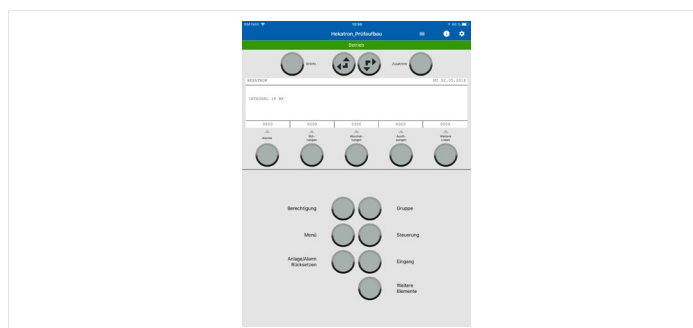


Abb. 91: Anzeige 2

- Befindet man sich nun auf Anzeige 2, so kommt man durch einmal Wischen von rechts nach links zu Anzeige 3.
- Einmal Wischen von links nach rechts blendet wieder Anzeige 2 ein.
- Erneutes Wischen von links nach rechts blendet wieder Anzeige 1 ein.

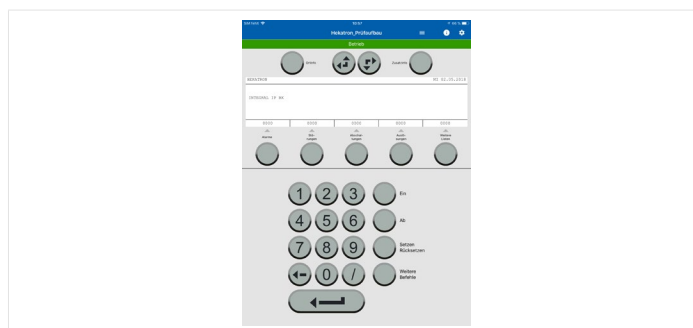


Abb. 92: Anzeige 3

- Von Anzeige 3 kommt man durch erneutes Wischen von rechts nach links zur Anzeige 4.

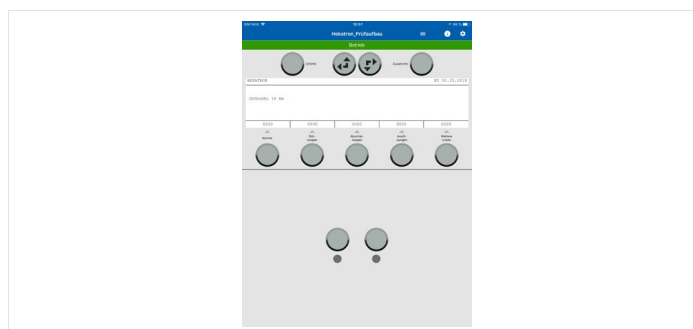


Abb. 93: Anzeige 4

# 14. Instandhaltung

Die Instandhaltung muss gemäß den geltenden Normen und Richtlinien durch zertifiziertes Fachpersonal durchgeführt werden.

**i** Die herstellerseitig notwendigen Arbeiten an der Anwendung Hekatron Remote finden in einem regelmäßigen Wartungsfenster jeden 3. Dienstag im Monat von 09:00 Uhr bis 12:00 Uhr statt. In diesem Zeitraum steht die Anwendung nur eingeschränkt zur Verfügung.

Zur Vorbereitung eines Instandhaltungseinsatzes kann über Hekatron Remote die Melderverschmutzung ausgelesen werden. Dazu die Verbindung zur Zentrale im Peripherie Assistant wie im Kapitel 13.1 beschrieben herstellen.

- Auf DCU gehen, mit rechter Maustaste Menü aufrufen und „Ausbau lesen“ oder „Ausbau mit Seriennummern lesen“ **1** auswählen um die Ringteilnehmer an allen Teilzentralen einzulesen.

Alternativ kann diese Funktion auch auf der SCU (Ringteilnehmer der Teilzentrale), der DAI/DXI (Ringteilnehmer der Ringleitungsbaugruppe) und auf dem Ring (Ringteilnehmer des Rings) ausgeführt werden.

- Erneut auf DCU gehen, mit rechter Maustaste Menü aufrufen und „Assistenten“ sowie im zweiten Fenster „Teilnehmerdaten“ auswählen.

Auch hier kann diese Funktion alternativ auf der SCU, der DAI/DXI und auf dem Ring ausgeführt werden.

- Über „Alle lesen“ **2** die Abfrage aller Teilnehmer durchführen.

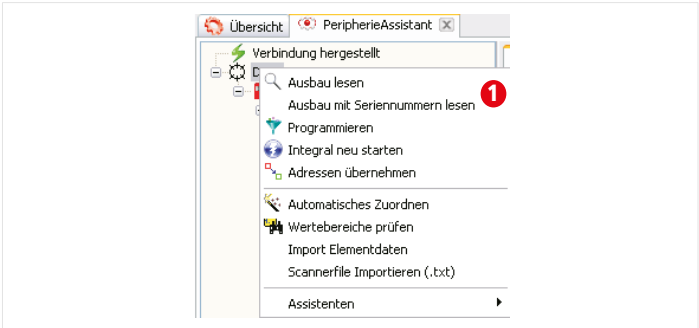


Abb. 94: Ausbau lesen

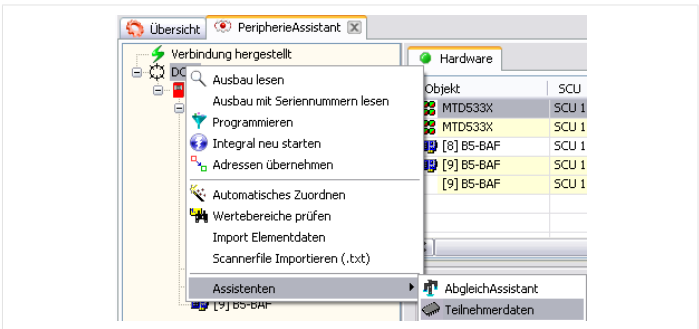


Abb. 95: Teilnehmerdaten auswählen

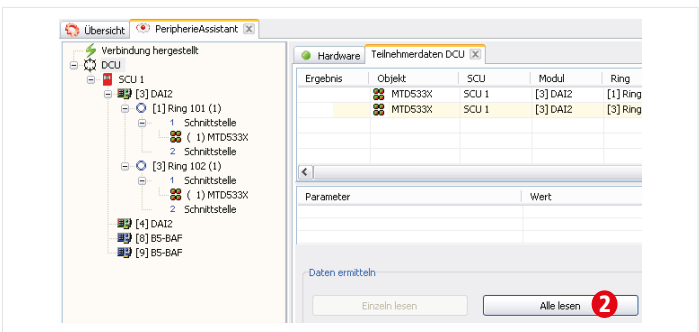


Abb. 96: Alle lesen

- ⇒ Die durchgeführte Abfrage der Teilnehmer wird über einen grünen Haken in der Spalte Ergebnis angezeigt.
- Über „Ausgabe speichern...“ **3** die Informationen abspeichern. Es wird empfohlen den voreingestellten Pfad und Dateinamen beizubehalten.

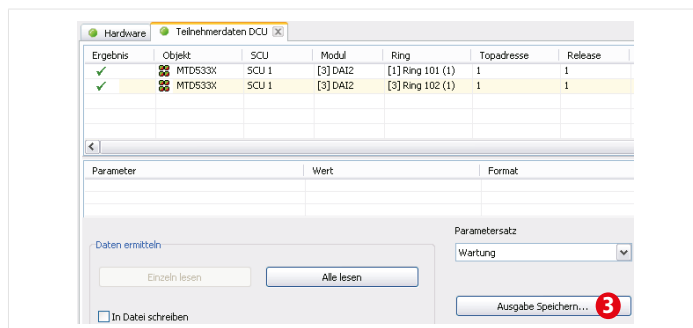


Abb. 97: Ausgabe speichern

- Zur Auswertung der Daten die Anwendung Integral Analysis starten.
- Entsprechende .xml Datei auswählen und mit OK bestätigen.

Alternativ kann eine externe Datei geöffnet werden.

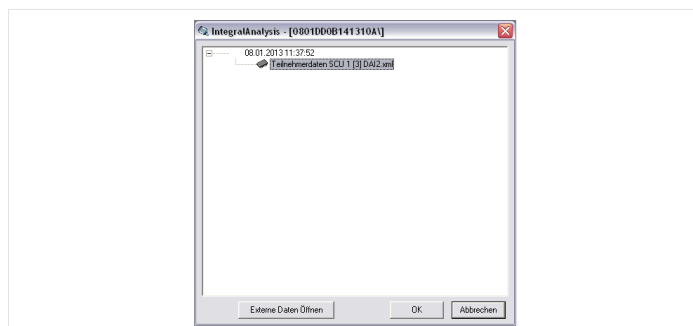


Abb. 98: .xml Datei auswählen

- ⇒ Nun werden die Daten der einzelnen Ringteilnehmer angezeigt.

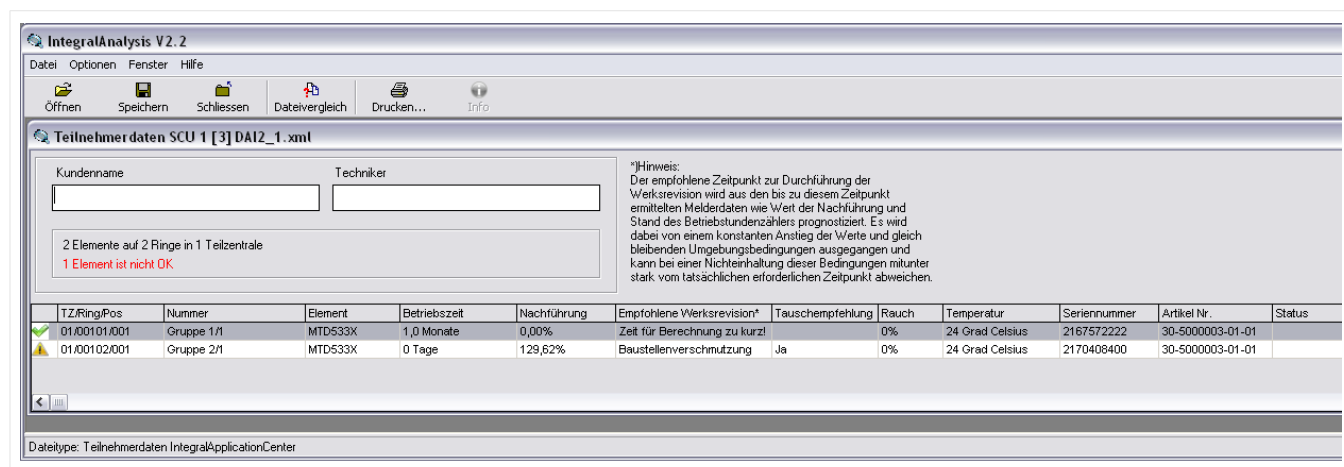


Abb. 99: Anzeige der Ringteilnehmer

- Die Übersicht entweder komplett oder nur für die Elemente mit Tauschempfehlung ausdrucken oder die Daten für eine Weiterverarbeitung im .csv Format speichern.

## 15. Technische Daten

### 15.1 VPN-Router LAN

#### Allgemein

|                          |                    |
|--------------------------|--------------------|
| Zul. Umgebungstemperatur | -30 °C bis +60 °C  |
| Schutzart                | IP20               |
| Abmessungen (H x B x T)  | 49 x 116 x 90 mm   |
| Gehäuse                  | Kunststoff schwarz |
| Gewicht                  | 200 g              |

#### Elektrische Werte

|                                |                |
|--------------------------------|----------------|
| Betriebsspannung <sup>7)</sup> | 10 bis 30 V DC |
|--------------------------------|----------------|

### 15.2 VPN-Router Mobilfunk

#### Allgemein

|                          |                                 |
|--------------------------|---------------------------------|
| Mobilfunkstandards       | 4G/LTE/UMTS/HSDPA+<br>GPRS/EDGE |
| Frequenzband             |                                 |
| LTE                      | 800, 900, 1800 ,2100, 2600 MHz  |
| UMTS (WCDMA/FDD)         | 900, 2100 MHz                   |
| GSM                      | 900, 1800 MHz                   |
| Zul. Umgebungstemperatur | -30 °C bis +60 °C               |
| Schutzart                | IP20                            |
| Abmessungen (H x B x T)  | 49 x 116 x 90 mm                |
| Gehäuse                  | Kunststoff schwarz              |
| Gewicht                  | 200 g                           |

#### Elektrische Werte

|                                |                |
|--------------------------------|----------------|
| Betriebsspannung <sup>7)</sup> | 10 bis 30 V DC |
|--------------------------------|----------------|

<sup>7)</sup> Netzadapter für Anschluss an 230 V AC im Lieferumfang enthalten

## 16. Maßbild

Alle Angaben in mm.

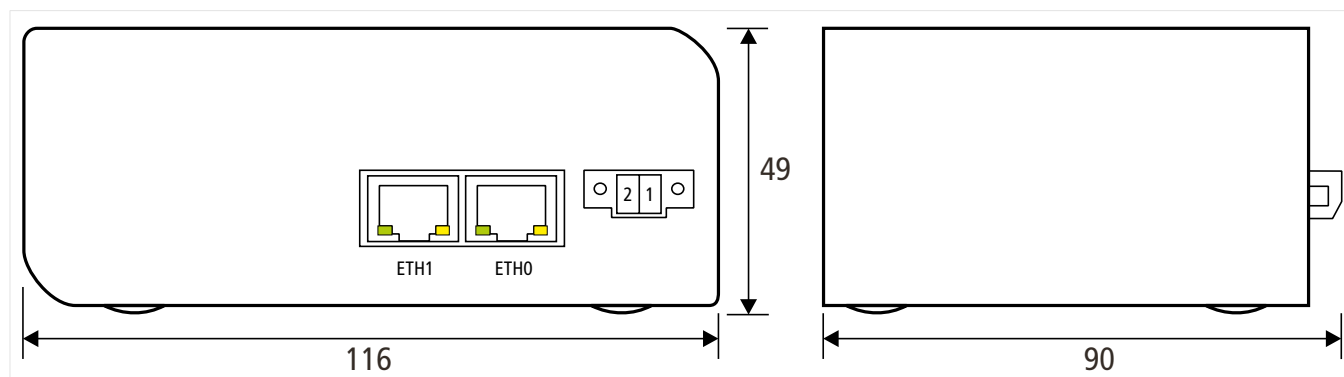


Abb. 100: Front- und Seitenansicht Router

## 17. Bestelldaten

### Varianten

| Bezeichnung          | Beschreibung                   | Bestellnummer    |
|----------------------|--------------------------------|------------------|
| VPN-Router LAN       | Router für LAN-Anbindung       | 30-4800013-01-xx |
| VPN-Router Mobilfunk | Router für Mobilfunk-Anbindung | 30-4800013-02-xx |

xx - Platzhalter für die aktuelle Produktversion



### **Hekatron Brandschutz**

Hekatron Vertriebs GmbH

Brühlmatten 9

79295 Sulzburg

Deutschland

Tel: +49 7634 500-8004

hotline@hekatron.de

hekatron-brandschutz.de

Ein Unternehmen der Securitas Gruppe Schweiz

7002783 · V5.0 · de · 05/2023

Technische Änderungen vorbehalten.

