Netzwerk und Schnittstellen

- Netzwerkanforderungen
- Anleitung Schnittstelle Alamos
- Anleitung Schnittstelle DIVERA 24/7
- Anleitung Schnittstelle Feuer Software
- Anleitung Schnittstelle FF-Agent
- Anleitung Schnittstelle GroupAlarm
- Anleitung Schnittstelle FirePlan
- Anleitung Alarmanruf

Netzwerkanforderungen

Gültig für die PoE-Zentrale, PoE-Repeater und das PoE Display

Vor Inbetriebnahme der Komponenten die Betriebsanleitung lesen

Diese Anleitung ist Teil des Produktes. Das Nichtbeachtung der Vorgaben dieser Anleitung kann eine Beeinträchtigung der Funktion oder die Beschädigung des Gerätes, anderer Sachwerte sowie Personenschäden zur Folge haben.

- Vor jeder Inbetriebnahme sind die entsprechenden Kapitel dieser Anleitung zu lesen und die enthaltenen Sicherheitshinweise zu beachten.
- Die Anleitung ist an jeden nachfolgenden Benutzer zu übergeben.
- Fragen und Hinweise bitte als Serviceticket stellen. Einen Link dazu finden Sie am Ende dieser Anleitung.

Urheberrecht

Dexa Solutionst GmbH Möhnestraße 2
59519 Möhnesee

1. Einleitung

1.1 Rollenverteilung und Haftung

Die Dexa Solutions GmbH nimmt im Projekt die Rolle des Systemintegrators ein. Wir konzipieren den Lösungsansatz und setzen ihn nach Ihren Vorgaben um. Dabei kommen verschiedene technische Komponenten von namhaften Hard- und Softwareanbietern sowie eigens entwickelte Hard- und Software zum Einsatz. Wir sind nicht Hersteller aller zum Einsatz kommenden Komponenten und übernehmen daher nicht die Produkthaftung der Fremdhersteller, außer für von uns durchgeführte Modifikationen. Diese obliegt weiterhin, genau wie die Gewährleistung und Garantie, dem Hersteller der jeweiligen Komponente. Auf Seiten der Software haften wir in vollem Umfang für die eigens entwickelten Softwareteile, naturgemäß jedoch nicht für die Softwareteile von Drittanbietern.

Unsere Anlage orientiert sich an ausgewählten technischen Anforderungen der VDE 0833-1 (allgemeiner Teil). Es werden teilweise VdS- bzw. EN 54-zertifizierte Rauchmelder eingesetzt, teilweise nicht zertifizierte Rauchsensoren. Die Anlage erfüllt daher ausdrücklich nicht die Anforderungen an bauordnungsrechtlich geforderte Brandmeldeanlagen nach VDE 0833-2/DIN 14675, wie sie insbesondere in Sonderbauten (z. B. Schulen, Krankenhäuser, Beherbergungsbetriebe) verlangt werden.

In Fahrzeugen sowie in Gebäuden oder Räumen, für die keine bauordnungsrechtliche Pflicht zur Installation einer Brandmeldeanlage nach VDE 0833-2/DIN 14675 besteht, kann die Anlage eingesetzt werden. Sofern die Integration in ein Brandschutzkonzept erfolgt, kann die Anlage als ergänzende technische Maßnahme zur

Verbesserung der Früherkennung und Alarmierung berücksichtigt werden, ohne eine bauordnungsrechtlich geforderte Brandmeldeanlage zu ersetzen.

Als Kunde stellen Sie Teile Ihrer IT-Infrastruktur, zum Beispiel einen Netzwerkanschluss mit Internetzugang, WLAN oder Eingangsschnittstellen zu Alarmsystemen bzw. Gebäudetechnik oder Brandmeldeanlage zur Verfügung. Diese muss am Tag der Inbetriebnahme gemäß der abgesprochenen Anforderungen vorbereitet sein. Für das nachhaltige Funktionieren dieser Infrastruktur tragen Sie als Kunde die Verantwortung. Für ein langfristiges Funktionieren können wir, etwa wenn Sie künftig Änderungen vornehmen, keine Haftung übernehmen.

Manche Alarmsysteme, wie zum Beispiel Alamos, werden lokal durch den Kunden gehostet. Hier trägt dieser die Verantwortung für das Funktionieren der bereitgestellten Schnittstelle. Andere Systeme, wie zum Beispiel Divera24/7, sind Cloud-basiert. Hier wird die Schnittstelle direkt vom Hersteller betrieben. Wir können für den Fall, dass dieser Änderungen vornimmt und dadurch Funktionseinschränkungen auftreten, keine Haftung übernehmen. Unsere Systeme sind aber darauf ausgelegt, in diesem unwahrscheinlichen Fall nachträglich mit nur geringem Aufwand, z.B. per Fernwartung, angepasst zu werden. Die Zusage zur Anbindung von individuellen und wunschgemäßen Schnittstellen, die durch uns noch nicht entwickelt sind, erfolgt unverbindlich und im Rahmen der Verhältnismäßigkeit. Dies gilt ebenso für den Einsatz von besonderen Hardwarekomponenten.

Damit die Zusammenarbeit gelingt und der Verbau der Innenraumüberwachungssysteme zu einem nachweislichen Erfolg wird, endet jede Inbetriebnahme mit einem umfangreichen Funktionstest, der dokumentiert wird. Darüber hinaus kann jeder Melder bzw. Sensor zu jeder Zeit eigenständig getestet und somit die Funktionssicherheit überprüft werden. Den Einsatzkräften wird dies ausdrücklich als Probealarm angezeigt, sodass es nicht zu Missverständnissen kommt.

Sofern der Anschluss an eine vorhandene Brandmeldeanlage gewünscht ist, wird dieser in der Regel durch das Schalten eines potenzialfreien Eingangskontaktes realisiert. Dieser muss Ihrerseits, bzw. durch den Servicetechniker der Wartungsfirma der Brandmeldeanlage, bereitgestellt werden. In der Nähe des Kontaktes muss im fünf Meter Abstand eine 230V Steckdose vorhanden sein. Für den Anschluss unseres Schaltaktors an Ihre Brandmeldeanlage gelten die gültigen Aufschaltbedingungen Ihrer zuständigen Brandschutzbehörde. Diese geben in der Regel vor, dass Sie nur nach DIN 14675 bzw. EN 54 zertifizierte Komponenten, also Teile anderer Brandmeldeanlagen, anschließen dürfen. Naturgemäß ist dies bei unserem System nicht der Fall, da es für die Überwachung von Innenräumen der Fahrzeuge kein technisches Regelwerk gibt. In den allermeisten Fällen lässt sich ein Anschluss unseres Systems an Ihre BMA aber trotzdem realisieren, da fast alle behördlichen Aufschaltbedingungen eine Öffnungsklausel haben, die besagt, dass die zuständige Behörde im Rahmen Ihrer Genehmigung von den vorangestellten Anforderungen abweichen kann. Sie müssen daher, sofern Ihre Brandmeldeanlage bei einer Feuerwehr Leitstelle aufgeschaltet ist, vor der Inbetriebnahme eine entsprechende Genehmigung einholen. Die Verantwortung hierfür liegt beim Auftraggeber.

1.2 Hinweise zum Datenschutz

Bitte beachten Sie die folgenden Informationen bezüglich des Datenschutzes in Verbindung mit der Fernwartungsfunktion sowie unseres online Service-Logbuchs, die in unserem System enthalten ist:

1. Zweck der Fernwartung: Die Fernwartungsfunktion ermöglicht es unserem technischen Support Team, auf Ihr System zuzugreifen, um Wartungs- und Supportdienste zu erbringen, Updates durchzuführen und Probleme zu diagnostizieren und zu beheben. Dies geschieht auf freiwilliger Basis. Die Fernwartungsfunktion ist standardmäßig immer aktiv. Wünschen Sie dies nicht, müssen Sie uns darauf schriftlich hinweisen.

2. Datenschutz und Sicherheit: Wir nehmen den Schutz Ihrer Daten ernst und ergreifen angemessene technische und organisatorische Maßnahmen, um sicherzustellen, dass Ihre Daten während der Fernwartung sicher und geschützt bleiben. Jeglicher Zugriff auf Ihr System erfolgt unter Einhaltung geltender Datenschutzgesetze und unserer strengen IT-Sicherheitsregeln. Es werden ausschließlich verschlüsselte Verbindungen mit starken Passwörtern und Multi-Faktor Authentifikation verwendet.

3. Datenerhebung und -verarbeitung: Während der Fernwartung können bestimmte Daten Ihres Systems erfasst und verarbeitet werden, einschließlich technischer Informationen und Fehlerprotokolle. Diese Daten werden ausschließlich für Supportzwecke und zur Verbesserung unserer Produkte verwendet und werden nicht an Dritte weitergegeben, es sei denn, dies ist gesetzlich vorgeschrieben oder wird von Ihnen autorisiert. Es werden bei der Fernwartung und dem Service-Log keine personenbezogenen Daten erhoben, daher findet die Datenschutz Grundverordnung keine Anwendung.

4. Zentrales Service-Logbuch: Zusätzlich zu den oben genannten Informationen möchten wir darauf hinweisen, dass Anlagendaten in ein zentrales Service-Logbuch geschrieben werden. Diese Daten dienen der Überwachung und Optimierung der Systemleistung und -zuverlässigkeit und werden gemäß den geltenden Datenschutzbestimmungen verarbeitet.

5. Akzeptanz der Bestimmungen: Indem Sie dieses technische System erwerben und die Fernwartungsfunktion nutzen, erklären Sie sich mit den oben genannten Datenschutzbestimmungen sowie der Verarbeitung Ihrer Anlagendaten in unserem zentralen Service-Logbuch einverstanden.

---

2. Hinweis zur Verbindung

Die Zentrale und der Repeater müssen sich im gleichen Netzwerksegment befinden und über einen Internetzugang verfügen.

2.1 Netzwerkanforderungen für Einzelstandort

- **Anschluss**: RJ45 mit PoE
- **PoE Protokoll**: 802.3af/at – 2003
- **Übertragungsrate**: 10/100/1000 Mbps

2.2 Zusätzliche Netzwerkanforderungen für Multistandort

Wenn das System standortübergreifend eingesetzt werden soll, bedarf es einer Vernetzung der Standorte im selben Netzwerk. Dies kann über VPN-Systeme wie WireGuard, Zerotier, IPSec, o.ä. erfolgen. Alternativ auch über ein VXLAN / VLAN. Hierfür sind folgende Anforderungen zwingend erforderlich:

- **Netzwerktyp**: Layer-II-Verbindung als "echtes" Multicast oder alternativ Layer-III-Verbindung (Unicast) mit Routing der Multicast-Pakete.
- **Kommunikationsart**: Multicast
- **Architektur**: Am besten gleicher IP-Adressbereich, gleiches Subnetz, sonst feste Routings

Die Multicast-Gruppe über die kommuniziert wird ist 224.0.0.120. Es ist aber sinnvoll den gesamten Multicast (udp) Verkehr zwischen den Repeatern und der Zentrale zu erlauben. Zusätzlich wird hierfür die Ports 9292 (tcp), 43439 (tcp) und 43438 (udp) genutzt. Die gesamte Kommunikation läuft im VPN-Netzwerk ab.

Freigaben in das Internet sind für die Verbindung zwischen Zentrale und Repeater nicht notwendig, außer Sie nutzen ZeroTier als Relay-Dienst.

Der Multicast-Verkehr kann über folgenden Befehl (Linux) eingesehen werden:

```
tcpdump -i eth0 -n 'udp and dst 224.0.0.120'
```

Bitte eth0 ggf. durch das verwendete Interface ersetzen.

Achten Sie bei der Gestaltung der Netzwerkarchitektur in Ihren VPN-Routern oder Firewalls auf sauberes Bridging der Interfaces, sodass keine Loops entstehen. Multicast Pakete gehen "wild" über alle Interfaces, je nach Routing und Bridging. Lassen sich Loops nicht vermeiden, aktivieren Sie Beschränkungen, wie das z.B. Spanning Tree Protocoll (STP) und Multicast-Begrenzungen (z.B. bei Zerotier).

Falls Sie Fragen zur Umsetzung haben, sprechen Sie uns an. Gerne bieten wir Ihnen die Vernetzung Ihrer Standorte als zusätzliche Leistung in einem Vorprojekt an.

2.3 Einsatz hinter einer Firewall

Beim Betrieb der PoE-Zentrale hinter einer Firewall ist zu beachten, dass Endpunkte gemäß folgender Tabelle sowie Ports erreichbar sind. Es wird hier anhand von Divera24/7 lediglich ein Beispiel für eine Alarmschnittstelle gegeben. Für die Erreichbarkeit weiterer Alarmdienste und Schnittstellen sind die Dokumentationen der jeweiligen Anbieter zu konsultieren. Bitte sprechen Sie uns an, falls Sie Unterstützung benötigen.

Bitte stellen Sie sicher, dass alle genannten Ports und Protokolle in Ihrer Firewall freigegeben sind, um eine reibungslose Funktionalität der PoE-Zentrale und angeschlossener Geräte zu gewährleisten.

Unser System benötigt keine eingehende Portfreigaben in Ihrer Firewall!

Verbindung	Protokoll/Port	Ziel	Zweck
PoE-Zentrale ? PoE-Repeater	Multicast (udp) / 43438 (udp)	local network	Für die Kommunikation zwischen der Zentrale und den Repeatern
	(tcp/9292 und tcp/43439)	local network	
PoE-Zentrale ? Mailserver	SMTP (tcp/465)	*.alfahosting-server.de	Für den Versand von Statusmails
		*.safefirehouse.com	
PoE-Zentrale ? Service-Plattform	HTTPS (tcp/443)	*.airtable.com	Für die Überwachung der Komponenten und der Schnittstellen
	FTP (tcp/21)	*.alfahosting-server.de	Upload von Telemetriedaten
PoE-Zentrale ? Service-Connector	HTTPS (tcp/443)	*.tailscale.com	Für die Wartung der Zentrale
	WireGuard (udp/41641)	*.tailscale.com	
	STUN (udp/3478)	*.tailscale.com	
PoE-Zentrale ? Zeitserver	NTP (udp/123)	*.pool.ntp.org	Synchronisation von Datum und Uhrzeit

Verbindung	Protokoll/Port	Ziel	Zweck
PoE-Zentrale ? DNS-Server	DNS/TCP (udp/53, tcp/53)	interner DNS-Server (local network)	DNS-Namensauflösung
PoE-Zentrale ? Beispiel Alarmierungsschnittstellen		Beispiele:	Für die Alarmierung zu den genutzten Alarmierungsprodukten
	HTTP/HTTPS (tcp/83/443)	localhost bzw. local network	Beispiel Alamos
	HTTPS (tcp/443)	app.divera247.com	Beispiel Divera24/47
PoE-Display ? Poe-Zentrale	HTTP und TCL	local network	Lokale Kommunikation mit Frontend

3. Weitere Informationen und Technische Daten

- Weitere Informationen finden Sie in unserer Knowledge Base https://docs.dexa.gmbh/books/faq

4. Kontaktdaten und Serviceticket

- Ein Serviceticket können Sie durch scannen des QR-Codes auf Ihrer PoE-Zentrale/PoE-Repeater erstellen.
- Alternativ finden Sie unser Ticketsystem auch hier: https://dexa.gmbh/serviceticket

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

Telefon: +49 2924 496 937 0

E-Mail: info@dexa.gmbh

Kontakt als QR Code für Ihr Mobiltelefon:

Anleitung Schnittstelle Alamos

Bild

Hardware Stand: 1.1
Anleitung Stand: 1.6

Vor Inbetriebnahme der Komponenten die Betriebsanleitung lesen

Diese Anleitung ist Teil des Produktes. Das Nichtbeachten der Vorgaben dieser Anleitung kann eine Beeinträchtigung der Funktion oder die Beschädigung des Gerätes, anderer Sachwerte sowie Personenschäden zur Folge haben.

- Vor jeder Inbetriebnahme sind die entsprechenden Kapitel dieser Anleitung zu lesen und die enthaltenen Sicherheitshinweise zu beachten.
- Die Anleitung ist an jeden nachfolgenden Benutzer zu übergeben.
- Fragen und Hinweise bitte als Serviceticket stellen. Einen Link dazu finden Sie am Ende dieser Anleitung.

Urheberrecht

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

---

1. Einleitung

1.1 Rollenverteilung und Haftung

Die Dexa Solutions GmbH nimmt im Projekt die Rolle des Systemintegrators ein. Wir konzipieren den Lösungsansatz und setzen ihn nach Ihren Vorgaben um. Dabei kommen verschiedene technische Komponenten von namhaften Hard- und Softwareanbietern sowie eigens entwickelte Hard- und Software zum Einsatz. Wir sind nicht Hersteller aller zum Einsatz kommenden Komponenten und übernehmen daher nicht die Produkthaftung der Fremdhersteller, außer für von uns durchgeführte Modifikationen. Diese obliegt weiterhin, genau wie die Gewährleistung und Garantie, dem Hersteller der jeweiligen Komponente. Auf Seiten der Software haften wir in vollem Umfang für die eigens entwickelten Softwareteile, naturgemäß jedoch nicht für die Softwareteile von Drittanbietern.

Unsere Anlage orientiert sich an ausgewählten technischen Anforderungen der VDE 0833-1 (allgemeiner Teil). Es werden teilweise VdS- bzw. EN 54-zertifizierte Rauchmelder eingesetzt, teilweise nicht zertifizierte Rauchsensoren. Die Anlage erfüllt daher ausdrücklich nicht die Anforderungen an bauordnungsrechtlich

geforderte Brandmeldeanlagen nach VDE 0833-2/DIN 14675, wie sie insbesondere in Sonderbauten (z. B. Schulen, Krankenhäuser, Beherbergungsbetriebe) verlangt werden.

In Fahrzeugen sowie in Gebäuden oder Räumen, für die keine bauordnungsrechtliche Pflicht zur Installation einer Brandmeldeanlage nach VDE 0833-2/DIN 14675 besteht, kann die Anlage eingesetzt werden. Sofern die Integration in ein Brandschutzkonzept erfolgt, kann die Anlage als ergänzende technische Maßnahme zur Verbesserung der Früherkennung und Alarmierung berücksichtigt werden, ohne eine bauordnungsrechtlich geforderte Brandmeldeanlage zu ersetzen.

Als Kunde stellen Sie Teile Ihrer IT-Infrastruktur, zum Beispiel einen Netzwerkanschluss mit Internetzugang, WLAN oder Eingangsschnittstellen zu Alarmsystemen bzw. Gebäudetechnik oder Brandmeldeanlage zur Verfügung. Diese muss am Tag der Inbetriebnahme gemäß der abgesprochenen Anforderungen vorbereitet sein. Für das nachhaltige Funktionieren dieser Infrastruktur tragen Sie als Kunde die Verantwortung. Für ein langfristiges Funktionieren können wir, etwa wenn Sie künftig Änderungen vornehmen, keine Haftung übernehmen.

Manche Alarmsysteme, wie zum Beispiel Alamos, werden lokal durch den Kunden gehostet. Hier trägt dieser die Verantwortung für das Funktionieren der bereitgestellten Schnittstelle. Andere Systeme, wie zum Beispiel Divera24/7, sind Cloud-basiert. Hier wird die Schnittstelle direkt vom Hersteller betrieben. Wir können für den Fall, dass dieser Änderungen vornimmt und dadurch Funktionseinschränkungen auftreten, keine Haftung übernehmen. Unsere Systeme sind aber darauf ausgelegt, in diesem unwahrscheinlichen Fall nachträglich mit nur geringem Aufwand, z.B. per Fernwartung, angepasst zu werden. Die Zusage zur Anbindung von individuellen und wunschgemäßen Schnittstellen, die durch uns noch nicht entwickelt sind, erfolgt unverbindlich und im Rahmen der Verhältnismäßigkeit. Dies gilt ebenso für den Einsatz von besonderen Hardwarekomponenten.

Damit die Zusammenarbeit gelingt und der Verbau der Innenraumüberwachungssysteme zu einem nachweislichen Erfolg wird, endet jede Inbetriebnahme mit einem umfangreichen Funktionstest, der dokumentiert wird. Darüber hinaus kann jeder Melder bzw. Sensor zu jeder Zeit eigenständig getestet und somit die Funktionssicherheit überprüft werden. Den Einsatzkräften wird dies ausdrücklich als Probealarm angezeigt, sodass es nicht zu Missverständnissen kommt.

Sofern der Anschluss an eine vorhandene Brandmeldeanlage gewünscht ist, wird dieser in der Regel durch das Schalten eines potenzialfreien Eingangskontaktes realisiert. Dieser muss Ihrerseits, bzw. durch den Servicetechniker der Wartungsfirma der Brandmeldeanlage, bereitgestellt werden. In der Nähe des Kontaktes muss im fünf Meter Abstand eine 230V Steckdose vorhanden sein. Für den Anschluss unseres Schaltaktors an Ihre Brandmeldeanlage gelten die gültigen Aufschaltbedingungen Ihrer zuständigen Brandschutzbehörde. Diese geben in der Regel vor, dass Sie nur nach DIN 14675 bzw. EN 54 zertifizierte Komponenten, also Teile anderer Brandmeldeanlagen, anschließen dürfen. Naturgemäß ist dies bei unserem System nicht der Fall, da es für die Überwachung von Innenräumen der Fahrzeuge kein technisches Regelwerk gibt. In den allermeisten Fällen lässt sich ein Anschluss unseres Systems an Ihre BMA aber trotzdem realisieren, da fast alle behördlichen Aufschaltbedingungen eine Öffnungsklausel haben, die besagt, dass die zuständige Behörde im Rahmen Ihrer Genehmigung von den vorangestellten Anforderungen abweichen kann. Sie müssen daher, sofern Ihre Brandmeldeanlage bei einer Feuerwehr Leitstelle aufgeschaltet ist, vor der Inbetriebnahme eine entsprechende Genehmigung einholen. Die Verantwortung hierfür liegt beim Auftraggeber.

1.2 Hinweise zum Datenschutz

Bitte beachten Sie die folgenden Informationen bezüglich des Datenschutzes in Verbindung mit der Fernwartungsfunktion sowie unseres online Service-Logbuchs, die in unserem System enthalten ist:

1. Zweck der Fernwartung: Die Fernwartungsfunktion ermöglicht es unserem technischen Support Team, auf Ihr System zuzugreifen, um Wartungs- und Supportdienste zu erbringen, Updates durchzuführen und Probleme zu diagnostizieren und zu beheben. Dies geschieht auf freiwilliger Basis. Die Fernwartungsfunktion ist standardmäßig immer aktiv. Wünschen Sie dies nicht, müssen Sie uns darauf schriftlich hinweisen.

2. Datenschutz und Sicherheit: Wir nehmen den Schutz Ihrer Daten ernst und ergreifen angemessene technische und organisatorische Maßnahmen, um sicherzustellen, dass Ihre Daten während der Fernwartung sicher und geschützt bleiben. Jeglicher Zugriff auf Ihr System erfolgt unter Einhaltung geltender Datenschutzgesetze und unserer strengen IT-Sicherheitsregeln. Es werden ausschließlich verschlüsselte Verbindungen mit starken Passwörtern und Multi-Faktor Authentifikation verwendet.

3. Datenerhebung und -verarbeitung: Während der Fernwartung können bestimmte Daten Ihres Systems erfasst und verarbeitet werden, einschließlich technischer Informationen und Fehlerprotokolle. Diese Daten werden ausschließlich für Supportzwecke und zur Verbesserung unserer Produkte verwendet und werden nicht an Dritte weitergegeben, es sei denn, dies ist gesetzlich vorgeschrieben oder wird von Ihnen autorisiert. Es werden bei der Fernwartung und dem Service-Log keine personenbezogenen Daten erhoben, daher findet die Datenschutz Grundverordnung keine Anwendung.

4. Zentrales Service-Logbuch: Zusätzlich zu den oben genannten Informationen möchten wir darauf hinweisen, dass Anlagendaten in ein zentrales Service-Logbuch geschrieben werden. Diese Daten dienen der Überwachung und Optimierung der Systemleistung und -zuverlässigkeit und werden gemäß den geltenden Datenschutzbestimmungen verarbeitet.

5. Akzeptanz der Bestimmungen: Indem Sie dieses technische System erwerben und die Fernwartungsfunktion nutzen, erklären Sie sich mit den oben genannten Datenschutzbestimmungen sowie der Verarbeitung Ihrer Anlagendaten in unserem zentralen Service-Logbuch einverstanden.

---

2. Konfiguration

Um Alamos zu konfigurieren, rufen Sie die Verwaltungsoberfläche Ihrer Einheit auf. Dies funktioniert entweder über die IP Ihres Alamos Server oder über einen DNS Eintrag. Beispiel: https://192.168.189.205:83 oder https://alamos.musterstadt.de

Wir benötigen diese URL als Alarm-Adresse.

Folgende Informationen benötigen wir:

- Schnittstelle zu dem Alamosserver. Das kann entweder eine IP mit einem Port sein oder ein DNS Eintrag mit Port. Ähnlich wie bei dem Aufruf der Verwaltungsoberfläche.
- Gültiger Absender der Schnittstelle
- Gruppenname/Einheit für Alarm pro Standort
- Gruppenname/Einheit für Test pro Standort (wenn gewünscht)

2.1 Alarmeingang anlegen

- Klicken Sie im linken Menü auf "Administration" und dann auf "Alarmeingang"

Bild

- Klicken Sie oben rechts auf den Button "+Alarmeingang hinzufügen"
- Tragen Sie einen Namen für die Schnittstelle ein und wählen Sie in dem Drop-Down-Menü "Externe Schnittstelle" aus. Klicken Sie auf "Hinzufügen"

Bild

2.2 Externe Schnittstelle Konfigurieren

- Klicken Sie auf die soeben erstellte Schnittstelle
- Konfigurieren Sie unter dem Reiter "Einstellungen" die Kommunikationseinstellungen folgendermaßen (Beispiel):
    - TCP/IP aktivieren
    - Port vergeben z.B. 83 **diesen Port benötigen wir**
    - Version Datenformat **muss** v2 sein
    - Geben Sie einen individuellen "Gültigen Absender" ein **Diesen benötigen wir**

Bild

- Unter dem Reiter "Alarmierung" finden Sie Ihre Gruppen/Einheiten
    - Die Namen der Einheitenkennungen, die bei einer Alarmierung durch uns über Alamos alarmiert werden sollen, **benötigen wir** pro Standort (grauer Text)
    - Sollten Sie für diese Alarmierung eine spezielle Gruppe/Einheit wünschen, muss diese zuvor in den "Einheiten" erstellt werden

Bild

- Unter dem Reiter "HTTP" muss folgendes konfiguriert werden:
    - Setzen Sie den Haken bei "HTTP Post"
    - Setzen Sie den Haken bei "GET Parameter im UTF-8 Format"

Bild

- Klicken Sie auf Speichern
- Klicken Sie zum Schluss auf den Button "Starten" / "Neustarten"

Bild

2.3 Freigabe der Schnittstelle oder Erreichbarmachen aus einem anderen Standort heraus

- In der Regel müssen wir zur Alarmierung auf die Schnittstelle von einem externen Standort zugreifen, es sei denn der Server sowie unsere Zetrale befindet sich im selben internen IP-Netzwerk. Bitte teilen Sie uns in diesem Fall die Alarm-URL bzw. IP mit, die aus dem Internet heraus erreichbar ist. Hierzu gehört auch der Port, der für den Zugriff aus dem Internet bei der Portfreigabe vergeben wurde. Dies kann der gleiche Port sein wie intern, aber auch ein anderer. Oft wird zum Beispiel für intern der Port 83 und für extern der SSL-Port 443 verwendet. Dies kann Ihre IT-Abteilung festlegen.
- Um das Ansprechen der Schnittstelle aus einem anderen Standort hinaus zu ermöglichen, können auch VPN Lösungen zum Einsatz kommen. Bitte tragen Sie dafür sorge, dass uns auch in diesem Fall die Schnittstellen-URL bzw. IP sowie der passende Port mitgeteilt wird.

---

3. Probealarm

Bei selbst gehosteten System wird ein wöchentlicher Probealarm ausgeführt. Der Zeitpunkt hierfür ist individuell abstimmbar. Der Probealarm kann über ein Pattern an eine Whitelist oder Blacklist gemappt werden.

3.1 Regel

Bild

- Blacklist: Wenn "SFH-PROBE" im Alarmtext steht, dann Ablauf abbrechen, sonst aPager als "Alarm" ansteuern"
- Whitelist: Wenn "SFH-PROBE" im Alarmtext steht, dann aPager als "Info-Alarm", sonst Ablauf abbrechen.

---

4. Alarmüberlauf

Ist ein Alamos-interner Alarmüberlauf gewünscht, kann dieser direkt und ohne weitere Schnittstellendaten konfiguriert werden. Dieser kann genutzt werden, um beispielsweise bei fehlender positiver Rückmeldung der alarmierten Alarmgruppe(n) nach einem konfigurierten Zeitraum erneut oder andere Alarmgruppen zu alarmieren.

4.1 Ausgangssituation

- Die Einheit (hier "Rauchmelder Alarm") besitzt den Alarmablauf "aPager PRO"

Bild

- In diesem muss die Checkbox "Rückmeldeübersicht erlauben" aktiv gesetzt sein
- Für die Übersichtlichkeit des Alarmablaufes empfehlen wir einen Kommentar der Ablaufstufe (hier "Alarmierung")

Bild

4.2 Rückmeldeübersicht

- Als zweites Plugin und Nachfolger des Plugins "aPagerPRO" wird das Plugin "Rückmeldeübersicht" hinzugefügt
- Dazu über die Suchfunktion rechts im Fenster das Plugin suchen und hinzufügen

Bild

- Konfiguration:
  - Wartezeit: 1
  - Zeiteinheit: Minuten
  - Checkbox "Alarmablauf fortsetzen {...}" aktivieren
  - Für die Übersichtlichkeit des Alarmablaufes empfehlen wir einen Kommentar der Ablaufstufe (hier "1 Minute")

Bild

4.3 Rückmelde-Regeln

- Als drittes Plugin und Nachfolger des Plugins "Rückmeldeübersicht" wird das Plugin "Rückmelde-Regeln" hinzugefügt
- Dazu über die Suchfunktion rechts im Fenster das Plugin suchen und hinzufügen

Bild

- Konfiguration:
  - Wartezeit: 1
  - Zeiteinheit: Minuten
  - Checkbox "Alarmablauf fortsetzen {...}" aktivieren
  - Für die Übersichtlichkeit des Alarmablaufes empfehlen wir einen Kommentar der Ablaufstufe (hier "Rückmeldestatus erfassen")

Bild

4.4 Nachalarmierung

- Als viertes Plugin und Nachfolger des Plugins "Rückmelde-Regeln" wird das Plugin "aPagerPRO" hinzugefügt
- Dazu über die Suchfunktion rechts im Fenster das Plugin suchen und hinzufügen
- Alamos wird den Ablauf Gelb markieren und einen Hinweis ausgeben. Dieser kann ignoriert werden, da es in diesem Fall hierfür benötigt wird
- Konfiguration:
  - nach eigener Anforderung
  - Für die Übersichtlichkeit des Alarmablaufes empfehlen wir einen Kommentar der Ablaufstufe (hier "Nachalarmieren")

Bild

4.5 Alarmablaufbeschreibung

Ablaufbeschreibung für den **oben konfigurierten** Fall:

Wird über diese Einheit alarmiert, so wird der Rückmeldestatus nach 60 Sekunden erfasst und ausgewertet. Wurde mindestens 1 positive (Komme) Rückmeldung ermittelt, wird der weitere Ablauf abgebrochen. Sollte keine positive (Komme) Rückmeldung ermittelt werden können, wird über den im vierten Plugin konfigurierten Alarmierungsweg erneut alarmiert.

Falls Sie Fragen zur Umsetzung haben, sprechen Sie uns an.

---

5. Weitere Informationen und Technische Daten

- Weitere Informationen finden Sie in unserer Knowledge Base https://docs.dexa.gmbh/books/faq

---

6. Kontaktdaten und Serviceticket

- Ein Serviceticket können Sie durch Scannen des QR-Codes auf Ihrer PoE-Zentrale bzw. PoE-Repeater erstellen.
- Alternativ finden Sie unser Ticketsystem auch hier: https://dexa.gmbh/serviceticket

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

Telefon: +49 2924 496 937 0

E-Mail: info@dexa.gmbh

Kontakt als QR Code für Ihr Mobiltelefon:

Anleitung Schnittstelle DIVERA 24/7

Bild

Hardware Stand: 1.1
Anleitung Stand: 1.4

Vor Inbetriebnahme der Komponenten die Betriebsanleitung lesen

Diese Anleitung ist Teil des Produktes. Das Nichtbeachtung der Vorgaben dieser Anleitung kann eine Beeinträchtigung der Funktion oder die Beschädigung des Gerätes, anderer Sachwerte sowie Personenschäden zur Folge haben.

- Vor jeder Inbetriebnahme sind die entsprechenden Kapitel dieser Anleitung zu lesen und die enthaltenen Sicherheitshinweise zu beachten.
- Die Anleitung ist an jeden nachfolgenden Benutzer zu übergeben.
- Fragen und Hinweise bitte als Serviceticket stellen. Einen Link dazu finden Sie am Ende dieser Anleitung.

Urheberrecht

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

---

1. Einleitung

1.1 Rollenverteilung und Haftung

Die Dexa Solutions GmbH nimmt im Projekt die Rolle des Systemintegrators ein. Wir konzipieren den Lösungsansatz und setzen ihn nach Ihren Vorgaben um. Dabei kommen verschiedene technische Komponenten von namhaften Hard- und Softwareanbietern sowie eigens entwickelte Hard- und Software zum Einsatz. Wir sind nicht Hersteller aller zum Einsatz kommenden Komponenten und übernehmen daher nicht die Produkthaftung der Fremdhersteller, außer für von uns durchgeführte Modifikationen. Diese obliegt weiterhin, genau wie die Gewährleistung und Garantie, dem Hersteller der jeweiligen Komponente. Auf Seiten der Software haften wir in vollem Umfang für die eigens entwickelten Softwareteile, naturgemäß jedoch nicht für die Softwareteile von Drittanbietern.

Unsere Anlage orientiert sich an ausgewählten technischen Anforderungen der VDE 0833-1 (allgemeiner Teil). Es werden teilweise VdS- bzw. EN 54-zertifizierte Rauchmelder eingesetzt, teilweise nicht zertifizierte Rauchsensoren. Die Anlage erfüllt daher ausdrücklich nicht die Anforderungen an bauordnungsrechtlich

geforderte Brandmeldeanlagen nach VDE 0833-2/DIN 14675, wie sie insbesondere in Sonderbauten (z. B. Schulen, Krankenhäuser, Beherbergungsbetriebe) verlangt werden.

In Fahrzeugen sowie in Gebäuden oder Räumen, für die keine bauordnungsrechtliche Pflicht zur Installation einer Brandmeldeanlage nach VDE 0833-2/DIN 14675 besteht, kann die Anlage eingesetzt werden. Sofern die Integration in ein Brandschutzkonzept erfolgt, kann die Anlage als ergänzende technische Maßnahme zur Verbesserung der Früherkennung und Alarmierung berücksichtigt werden, ohne eine bauordnungsrechtlich geforderte Brandmeldeanlage zu ersetzen.

Als Kunde stellen Sie Teile Ihrer IT-Infrastruktur, zum Beispiel einen Netzwerkanschluss mit Internetzugang, WLAN oder Eingangsschnittstellen zu Alarmsystemen bzw. Gebäudetechnik oder Brandmeldeanlage zur Verfügung. Diese muss am Tag der Inbetriebnahme gemäß der abgesprochenen Anforderungen vorbereitet sein. Für das nachhaltige Funktionieren dieser Infrastruktur tragen Sie als Kunde die Verantwortung. Für ein langfristiges Funktionieren können wir, etwa wenn Sie künftig Änderungen vornehmen, keine Haftung übernehmen.

Manche Alarmsysteme, wie zum Beispiel Alamos, werden lokal durch den Kunden gehostet. Hier trägt dieser die Verantwortung für das Funktionieren der bereitgestellten Schnittstelle. Andere Systeme, wie zum Beispiel DIVERA 24/7, sind Cloud-basiert. Hier wird die Schnittstelle direkt vom Hersteller betrieben. Wir können für den Fall, dass dieser Änderungen vornimmt und dadurch Funktionseinschränkungen auftreten, keine Haftung übernehmen. Unsere Systeme sind aber darauf ausgelegt, in diesem unwahrscheinlichen Fall nachträglich mit nur geringem Aufwand, z.B. per Fernwartung, angepasst zu werden. Die Zusage zur Anbindung von individuellen und wunschgemäßen Schnittstellen, die durch uns noch nicht entwickelt sind, erfolgt unverbindlich und im Rahmen der Verhältnismäßigkeit. Dies gilt ebenso für den Einsatz von besonderen Hardwarekomponenten.

Damit die Zusammenarbeit gelingt und der Verbau der Innenraumüberwachungssysteme zu einem nachweislichen Erfolg wird, endet jede Inbetriebnahme mit einem umfangreichen Funktionstest, der dokumentiert wird. Darüber hinaus kann jeder Melder bzw. Sensor zu jeder Zeit eigenständig getestet und somit die Funktionssicherheit überprüft werden. Den Einsatzkräften wird dies ausdrücklich als Probealarm angezeigt, sodass es nicht zu Missverständnissen kommt.

Sofern der Anschluss an eine vorhandene Brandmeldeanlage gewünscht ist, wird dieser in der Regel durch das Schalten eines potenzialfreien Eingangskontaktes realisiert. Dieser muss Ihrerseits, bzw. durch den Servicetechniker der Wartungsfirma der Brandmeldeanlage, bereitgestellt werden. In der Nähe des Kontaktes muss im fünf Meter Abstand eine 230V Steckdose vorhanden sein. Für den Anschluss unseres Schaltaktors an Ihre Brandmeldeanlage gelten die gültigen Aufschaltbedingungen Ihrer zuständigen Brandschutzbehörde. Diese geben in der Regel vor, dass Sie nur nach DIN 14675 bzw. EN 54 zertifizierte Komponenten, also Teile anderer Brandmeldeanlagen, anschließen dürfen. Naturgemäß ist dies bei unserem System nicht der Fall, da es für die Überwachung von Innenräumen der Fahrzeuge kein technisches Regelwerk gibt. In den allermeisten Fällen lässt sich ein Anschluss unseres Systems an Ihre Brandmeldeanlage aber trotzdem realisieren, da fast alle behördlichen Aufschaltbedingungen eine Öffnungsklausel haben, die besagt, dass die zuständige Behörde im Rahmen Ihrer Genehmigung von den vorangestellten Anforderungen abweichen kann. Sie müssen daher, sofern Ihre Brandmeldeanlage bei einer Feuerwehr Leitstelle aufgeschaltet ist, vor der Inbetriebnahme eine entsprechende Genehmigung einholen. Die Verantwortung hierfür liegt beim Auftraggeber.

1.2 Hinweise zum Datenschutz

Bitte beachten Sie die folgenden Informationen bezüglich des Datenschutzes in Verbindung mit der Fernwartungsfunktion sowie unseres online Service-Logbuchs, die in unserem System enthalten ist:

1. Zweck der Fernwartung: Die Fernwartungsfunktion ermöglicht es unserem technischen Support Team, auf Ihr System zuzugreifen, um Wartungs- und Supportdienste zu erbringen, Updates durchzuführen und Probleme zu diagnostizieren und zu beheben. Dies geschieht auf freiwilliger Basis. Die Fernwartungsfunktion ist standardmäßig immer aktiv. Wünschen Sie dies nicht, müssen Sie uns darauf schriftlich hinweisen.

2. Datenschutz und Sicherheit: Wir nehmen den Schutz Ihrer Daten ernst und ergreifen angemessene technische und organisatorische Maßnahmen, um sicherzustellen, dass Ihre Daten während der Fernwartung sicher und geschützt bleiben. Jeglicher Zugriff auf Ihr System erfolgt unter Einhaltung geltender Datenschutzgesetze und unserer strengen IT-Sicherheitsregeln. Es werden ausschließlich verschlüsselte Verbindungen mit starken Passwörtern und Multi-Faktor Authentifikation verwendet.

3. Datenerhebung und -verarbeitung: Während der Fernwartung können bestimmte Daten Ihres Systems erfasst und verarbeitet werden, einschließlich technischer Informationen und Fehlerprotokolle. Diese Daten werden ausschließlich für Supportzwecke und zur Verbesserung unserer Produkte verwendet und werden nicht an Dritte weitergegeben, es sei denn, dies ist gesetzlich vorgeschrieben oder wird von Ihnen autorisiert. Es werden bei der Fernwartung und dem Service-Log keine personenbezogenen Daten erhoben, daher findet die Datenschutz Grundverordnung keine Anwendung.

4. Zentrales Service-Logbuch: Zusätzlich zu den oben genannten Informationen möchten wir darauf hinweisen, dass Anlagendaten in ein zentrales Service-Logbuch geschrieben werden. Diese Daten dienen der Überwachung und Optimierung der Systemleistung und -zuverlässigkeit und werden gemäß den geltenden Datenschutzbestimmungen verarbeitet.

5. Akzeptanz der Bestimmungen: Indem Sie dieses technische System erwerben und die Fernwartungsfunktion nutzen, erklären Sie sich mit den oben genannten Datenschutzbestimmungen sowie der Verarbeitung Ihrer Anlagendaten in unserem zentralen Service-Logbuch einverstanden.

---

2. Konfiguration

Um DIVERA 24/7 zu konfigurieren rufen Sie die Verwaltungsoberfläche Ihrer Einheit auf.

https://app.divera247.com/login.html

Folgende Informationen werden benötigt:

- Access-Key
- Gruppenname für Alarm pro Standort
- Gruppenname für Test pro Standort (wenn gewünscht)

2.1 Access-Key anzeigen

- Gilt für die "Free" und die "Alarm"-Version
- Klicken Sie auf "Verwaltung"
- Dann auf "Schnittstellen" im Bereich "Einstellungen"
- Im Abschitt "Autorisierung" wird Ihnen der Access-Key angezeigt. Mit einem Klick auf das Auge Symbol neben dem Key wird dieser auch in Klartext dargestellt. **Diesen benötigen wir**

Bild

2.2 Gruppen Anlegen

- Gilt für die "Free" und die "Alarm"-Version

- Klicken Sie auf "Verwaltung"
- Dann auf "Gruppen" im Bereich "Personal"
- Oben rechts auf den Button "+Gruppe"
- Hier geben Sie eine eindeutige Bezeichnungen für die Gruppenkonfiguration ein. Es wird jeweils eine Gruppe pro Standort benötigt. In dem Beispiel wird der Zusatz "A" für Alarm und der Zusatz "T" für Test verwendet. Beispiel Siehe Bild. **Den Namen der Gruppe benötigen wir**
- Die Gerade erstellten Gruppen müssen nun noch den Benutzern, die eine Alarmierung erhalten sollen, zugewiesen werden.

Bild

2.3 Zusätzlicher Alarmierungswege SMS / Anruf

- Gilt für die "Free" und die "Alarm"-Version
- Wenn SMS und / oder Anruf gewünscht ist, weisen wir darauf hin, dass in den Benutzereinstellungen deren Benutzer, die in der Gruppe hinzugefügt sind, die Checkboxen für SMS / Sprach-Anruf aktiviert werden müssen. Siehe Beispiel für einen Nutzer.

Bild

2.4 Alarmüberlauf

Soll ein Alarmüberlauf auf dieselbe Schnittstelle konfiguriert werden, benötigen wir folgende Informationen:

- **ID des Rückmeldestatus, der den Alarmüberlauf abbricht.** (Standardwert: Geringster Wert (z.B.: "5 Min")). Diesen finden Sie unter:
  - Klicken Sie auf "Verwaltung"
  - Im Bereich "Einstellungen" auf "Setup"
  - Reiter "Status"
  - Unter der Spalte "Aktion" auf den Button des Status klicken und "Bearbeiten" auswählen
  - Die ID finden Sie als numerischen Wert (5 Ziffern) am Ende der URL. Im folgendem Beispiel "98998"

Bild

- **Reaktionszeit in Sekunden** (Standardwert: 60 Sekunden)
- **Gruppenname der Gruppe, auf welche beim Überlauf alarmiert werden soll**
  - siehe Punkt 2.2

2.5 Einstellungen in der Pro Version

Sollten Sie die Pro-Version von DIVERA nutzen, sind die Einstellungen analog zu den zuvor beschriebenen Punkten in der Free der Alarm-Version vorzunehmen. Sie finden diese allerdings jeweils auf der Ebene Ihrer Untereinheit.

Es gibt zwei Möglichkeiten:

1. Sie nehmen alle Einstellungen in der (Unter-)Einheit vor und teilen uns die jeweiligen Auth-Keys sowie Gruppenbezeichnungen dort mit.

2. Sie setzen Sie Einstellungen in Ihrer Zentraleinheit, dann müssen Sie uns nur den zentralen Auth-Key sowie die Gruppenbenennungen mitteilen. Es ist darauf zu achten, diese nach unten hin als RIC weitergeroutet sind.

Wir empfehlen die Nutzung von einem AuthKey und einer Alarmgruppe pro Standort anstatt des zentralen Vererbens, da dies nachvollziehbarer und sicherer zu administrieren ist. Falls Sie zeingend die Variante 2 umsetzen wollen, sprechen Sie und bitte an.

---

3. Weitere Informationen und Technische Daten

- Weitere Informationen finden Sie in unserer Knowledge Base https://docs.dexa.gmbh/books/faq

---

4. Kontaktdaten und Serviceticket

- Ein Serviceticket können Sie durch Scannen des QR-Codes auf Ihrer PoE-Zentrale bzw. PoE-Repeater erstellen.
- Alternativ finden Sie unser Ticketsystem auch hier: https://dexa.gmbh/serviceticket

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

Telefon: +49 2924 496 937 0

E-Mail: info@dexa.gmbh

Kontakt als QR Code für Ihr Mobiltelefon:

Anleitung Schnittstelle Feuer Software

Bild

Hardware Stand: 1.1
Anleitung Stand: 1.3

Vor Inbetriebnahme der Komponenten die Betriebsanleitung lesen

Diese Anleitung ist Teil des Produktes. Das Nichtbeachtung der Vorgaben dieser Anleitung kann eine Beeinträchtigung der Funktion oder die Beschädigung des Gerätes, anderer Sachwerte sowie Personenschäden zur Folge haben.

- Vor jeder Inbetriebnahme sind die entsprechenden Kapitel dieser Anleitung zu lesen und die enthaltenen Sicherheitshinweise zu beachten.
- Die Anleitung ist an jeden nachfolgenden Benutzer zu übergeben.
- Fragen und Hinweise bitte als Serviceticket stellen. Einen Link dazu finden Sie am Ende dieser Anleitung.

Urheberrecht

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

---

1. Einleitung

1.1 Rollenverteilung und Haftung

Die Dexa Solutions GmbH nimmt im Projekt die Rolle des Systemintegrators ein. Wir konzipieren den Lösungsansatz und setzen ihn nach Ihren Vorgaben um. Dabei kommen verschiedene technische Komponenten von namhaften Hard- und Softwareanbietern sowie eigens entwickelte Hard- und Software zum Einsatz. Wir sind nicht Hersteller aller zum Einsatz kommenden Komponenten und übernehmen daher nicht die Produkthaftung der Fremdhersteller, außer für von uns durchgeführte Modifikationen. Diese obliegt weiterhin, genau wie die Gewährleistung und Garantie, dem Hersteller der jeweiligen Komponente. Auf Seiten der Software haften wir in vollem Umfang für die eigens entwickelten Softwareteile, naturgemäß jedoch nicht für die Softwareteile von Drittanbietern.

Unsere Anlage orientiert sich an ausgewählten technischen Anforderungen der VDE 0833-1 (allgemeiner Teil). Es werden teilweise VdS- bzw. EN 54-zertifizierte Rauchmelder eingesetzt, teilweise nicht zertifizierte Rauchsensoren. Die Anlage erfüllt daher ausdrücklich nicht die Anforderungen an bauordnungsrechtlich

geforderte Brandmeldeanlagen nach VDE 0833-2/DIN 14675, wie sie insbesondere in Sonderbauten (z. B. Schulen, Krankenhäuser, Beherbergungsbetriebe) verlangt werden.

In Fahrzeugen sowie in Gebäuden oder Räumen, für die keine bauordnungsrechtliche Pflicht zur Installation einer Brandmeldeanlage nach VDE 0833-2/DIN 14675 besteht, kann die Anlage eingesetzt werden. Sofern die Integration in ein Brandschutzkonzept erfolgt, kann die Anlage als ergänzende technische Maßnahme zur Verbesserung der Früherkennung und Alarmierung berücksichtigt werden, ohne eine bauordnungsrechtlich geforderte Brandmeldeanlage zu ersetzen.

Als Kunde stellen Sie Teile Ihrer IT-Infrastruktur, zum Beispiel einen Netzwerkanschluss mit Internetzugang, WLAN oder Eingangsschnittstellen zu Alarmsystemen bzw. Gebäudetechnik oder Brandmeldeanlage zur Verfügung. Diese muss am Tag der Inbetriebnahme gemäß der abgesprochenen Anforderungen vorbereitet sein. Für das nachhaltige Funktionieren dieser Infrastruktur tragen Sie als Kunde die Verantwortung. Für ein langfristiges Funktionieren können wir, etwa wenn Sie künftig Änderungen vornehmen, keine Haftung übernehmen.

Manche Alarmsysteme, wie zum Beispiel Alamos, werden lokal durch den Kunden gehostet. Hier trägt dieser die Verantwortung für das Funktionieren der bereitgestellten Schnittstelle. Andere Systeme, wie zum Beispiel Divera24/7, sind Cloud-basiert. Hier wird die Schnittstelle direkt vom Hersteller betrieben. Wir können für den Fall, dass dieser Änderungen vornimmt und dadurch Funktionseinschränkungen auftreten, keine Haftung übernehmen. Unsere Systeme sind aber darauf ausgelegt, in diesem unwahrscheinlichen Fall nachträglich mit nur geringem Aufwand, z.B. per Fernwartung, angepasst zu werden. Die Zusage zur Anbindung von individuellen und wunschgemäßen Schnittstellen, die durch uns noch nicht entwickelt sind, erfolgt unverbindlich und im Rahmen der Verhältnismäßigkeit. Dies gilt ebenso für den Einsatz von besonderen Hardwarekomponenten.

Damit die Zusammenarbeit gelingt und der Verbau der Innenraumüberwachungssysteme zu einem nachweislichen Erfolg wird, endet jede Inbetriebnahme mit einem umfangreichen Funktionstest, der dokumentiert wird. Darüber hinaus kann jeder Melder bzw. Sensor zu jeder Zeit eigenständig getestet und somit die Funktionssicherheit überprüft werden. Den Einsatzkräften wird dies ausdrücklich als Probealarm angezeigt, sodass es nicht zu Missverständnissen kommt.

Sofern der Anschluss an eine vorhandene Brandmeldeanlage gewünscht ist, wird dieser in der Regel durch das Schalten eines potenzialfreien Eingangskontaktes realisiert. Dieser muss Ihrerseits, bzw. durch den Servicetechniker der Wartungsfirma der Brandmeldeanlage, bereitgestellt werden. In der Nähe des Kontaktes muss im fünf Meter Abstand eine 230V Steckdose vorhanden sein. Für den Anschluss unseres Schaltaktors an Ihre Brandmeldeanlage gelten die gültigen Aufschaltbedingungen Ihrer zuständigen Brandschutzbehörde. Diese geben in der Regel vor, dass Sie nur nach DIN 14675 bzw. EN 54 zertifizierte Komponenten, also Teile anderer Brandmeldeanlagen, anschließen dürfen. Naturgemäß ist dies bei unserem System nicht der Fall, da es für die Überwachung von Innenräumen der Fahrzeuge kein technisches Regelwerk gibt. In den allermeisten Fällen lässt sich ein Anschluss unseres Systems an Ihre BMA aber trotzdem realisieren, da fast alle behördlichen Aufschaltbedingungen eine Öffnungsklausel haben, die besagt, dass die zuständige Behörde im Rahmen Ihrer Genehmigung von den vorangestellten Anforderungen abweichen kann. Sie müssen daher, sofern Ihre Brandmeldeanlage bei einer Feuerwehr Leitstelle aufgeschaltet ist, vor der Inbetriebnahme eine entsprechende Genehmigung einholen. Die Verantwortung hierfür liegt beim Auftraggeber.

1.2 Hinweise zum Datenschutz

Bitte beachten Sie die folgenden Informationen bezüglich des Datenschutzes in Verbindung mit der Fernwartungsfunktion sowie unseres online Service-Logbuchs, die in unserem System enthalten ist:

1. Zweck der Fernwartung: Die Fernwartungsfunktion ermöglicht es unserem technischen Support Team, auf Ihr System zuzugreifen, um Wartungs- und Supportdienste zu erbringen, Updates durchzuführen und Probleme zu diagnostizieren und zu beheben. Dies geschieht auf freiwilliger Basis. Die Fernwartungsfunktion ist standardmäßig immer aktiv. Wünschen Sie dies nicht, müssen Sie uns darauf schriftlich hinweisen.

2. Datenschutz und Sicherheit: Wir nehmen den Schutz Ihrer Daten ernst und ergreifen angemessene technische und organisatorische Maßnahmen, um sicherzustellen, dass Ihre Daten während der Fernwartung sicher und geschützt bleiben. Jeglicher Zugriff auf Ihr System erfolgt unter Einhaltung geltender Datenschutzgesetze und unserer strengen IT-Sicherheitsregeln. Es werden ausschließlich verschlüsselte Verbindungen mit starken Passwörtern und Multi-Faktor Authentifikation verwendet.

3. Datenerhebung und -verarbeitung: Während der Fernwartung können bestimmte Daten Ihres Systems erfasst und verarbeitet werden, einschließlich technischer Informationen und Fehlerprotokolle. Diese Daten werden ausschließlich für Supportzwecke und zur Verbesserung unserer Produkte verwendet und werden nicht an Dritte weitergegeben, es sei denn, dies ist gesetzlich vorgeschrieben oder wird von Ihnen autorisiert. Es werden bei der Fernwartung und dem Service-Log keine personenbezogenen Daten erhoben, daher findet die Datenschutz Grundverordnung keine Anwendung.

4. Zentrales Service-Logbuch: Zusätzlich zu den oben genannten Informationen möchten wir darauf hinweisen, dass Anlagendaten in ein zentrales Service-Logbuch geschrieben werden. Diese Daten dienen der Überwachung und Optimierung der Systemleistung und -zuverlässigkeit und werden gemäß den geltenden Datenschutzbestimmungen verarbeitet.

5. Akzeptanz der Bestimmungen: Indem Sie dieses technische System erwerben und die Fernwartungsfunktion nutzen, erklären Sie sich mit den oben genannten Datenschutzbestimmungen sowie der Verarbeitung Ihrer Anlagendaten in unserem zentralen Service-Logbuch einverstanden.

---

2. Konfiguration

Um Feuer Software zu konfigurieren rufen Sie die Verwaltungsoberfläche Ihrer Einheit auf.

https://connect.feuersoftware.com/

Folgende Informationen werden benötigt:

- Authentifizierungsschlüssel
- Alarmgruppenname für Alarm pro Standort
- Alarmgruppenname für Test pro Standort (wenn gewünscht)

2.1 Authentifizierungsschlüssel anzeigen

- Klicken Sie auf "Schnittstellen"
- Dann auf "Öffentliche Connect-Schnittstelle"
- Im Abschnitt "Authentifizierungsschlüssel" wird Ihnen der Authentifizierungsschlüssel angezeigt. **Diesen benötigen wir**

Bild

2.2 Alarmgruppen

- Klicken Sie auf "Alarm"
- Dann auf "Alarmgruppen"

- Hier geben Sie einen eindeutigen Namen für die Gruppenkonfiguration ein. Es wird jeweils ein Alarmgruppenname je Standort benötigt. In dem Beispiel wird der Zusatz "A" für Alarm und der Zusatz "T" für Test verwendet. Beispiel siehe Beispielbild.

  Den Namen der Alarmgruppe benötigen wir

- Die gerade erstellten Alarmgruppen müssen nun noch den Benutzern, die eine Alarmierung erhalten sollen, zugewiesen werden.

Bild

---

3. Weitere Informationen und Technische Daten

- Weitere Informationen finden Sie in unserer Knowledge Base https://docs.dexa.gmbh/books/faq

---

4. Kontaktdaten und Serviceticket

- Ein Serviceticket können Sie durch Scannen des QR-Codes auf Ihrer PoE-Zentrale bzw. PoE-Repeater erstellen.
- Alternativ finden Sie unser Ticketsystem auch hier: https://dexa.gmbh/serviceticket

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

Telefon: +49 2924 496 937 0

E-Mail: info@dexa.gmbh

Kontakt als QR Code für Ihr Mobiltelefon:

Anleitung Schnittstelle FF-Agent

Hardware Stand: 1.1
Anleitung Stand: 1.0

Vor Inbetriebnahme der Komponenten die Betriebsanleitung lesen

Diese Anleitung ist Teil des Produktes. Das Nichtbeachtung der Vorgaben dieser Anleitung kann eine Beeinträchtigung der Funktion oder die Beschädigung des Gerätes, anderer Sachwerte sowie Personenschäden zur Folge haben.

- Vor jeder Inbetriebnahme sind die entsprechenden Kapitel dieser Anleitung zu lesen und die enthaltenen Sicherheitshinweise zu beachten.
- Die Anleitung ist an jeden nachfolgenden Benutzer zu übergeben.
- Fragen und Hinweise bitte als Serviceticket stellen. Einen Link dazu finden Sie am Ende dieser Anleitung.

Urheberrecht

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

1. Einleitung

1.1 Rollenverteilung und Haftung

Die Dexa Solutions GmbH nimmt im Projekt die Rolle des Systemintegrators ein. Wir konzipieren den Lösungsansatz und setzen ihn nach Ihren Vorgaben um. Dabei kommen verschiedene technische Komponenten von namhaften Hard- und Softwareanbietern sowie eigens entwickelte Hard- und Software zum Einsatz. Wir sind nicht Hersteller aller zum Einsatz kommenden Komponenten und übernehmen daher nicht die Produkthaftung der Fremdhersteller, außer für von uns durchgeführte Modifikationen. Diese obliegt weiterhin, genau wie die Gewährleistung und Garantie, dem Hersteller der jeweiligen Komponente. Auf Seiten der Software haften wir in vollem Umfang für die eigens entwickelten Softwareteile, naturgemäß jedoch nicht für die Softwareteile von Drittanbietern.

Unsere Anlage orientiert sich an ausgewählten technischen Anforderungen der VDE 0833-1 (allgemeiner Teil). Es werden teilweise VdS- bzw. EN 54-zertifizierte Rauchmelder eingesetzt, teilweise nicht zertifizierte Rauchsensoren. Die Anlage erfüllt daher ausdrücklich nicht die Anforderungen an bauordnungsrechtlich geforderte Brandmeldeanlagen nach VDE 0833-2/DIN 14675, wie sie insbesondere in Sonderbauten (z. B. Schulen, Krankenhäuser, Beherbergungsbetriebe) verlangt werden.

In Fahrzeugen sowie in Gebäuden oder Räumen, für die keine bauordnungsrechtliche Pflicht zur Installation einer Brandmeldeanlage nach VDE 0833-2/DIN 14675 besteht, kann die Anlage eingesetzt werden. Sofern die Integration in ein Brandschutzkonzept erfolgt, kann die Anlage als ergänzende technische Maßnahme zur Verbesserung der Früherkennung und Alarmierung berücksichtigt werden, ohne eine bauordnungsrechtlich geforderte Brandmeldeanlage zu ersetzen.

Als Kunde stellen Sie Teile Ihrer IT-Infrastruktur, zum Beispiel einen Netzwerkanschluss mit Internetzugang, WLAN oder Eingangsschnittstellen zu Alarmsystemen bzw. Gebäudetechnik oder Brandmeldeanlage zur Verfügung. Diese muss am Tag der Inbetriebnahme gemäß der abgesprochenen Anforderungen vorbereitet sein. Für das nachhaltige Funktionieren dieser Infrastruktur tragen Sie als Kunde die Verantwortung. Für ein langfristiges Funktionieren können wir, etwa wenn Sie künftig Änderungen vornehmen, keine Haftung übernehmen.

Manche Alarmsysteme, wie zum Beispiel Alamos, werden lokal durch den Kunden gehostet. Hier trägt dieser die Verantwortung für das Funktionieren der bereitgestellten Schnittstelle. Andere Systeme, wie zum Beispiel Divera24/7, sind Cloud-basiert. Hier wird die Schnittstelle direkt vom Hersteller betrieben. Wir können für den Fall, dass dieser Änderungen vornimmt und dadurch Funktionseinschränkungen auftreten, keine Haftung übernehmen. Unsere Systeme sind aber darauf ausgelegt, in diesem unwahrscheinlichen Fall nachträglich mit nur geringem Aufwand, z.B. per Fernwartung, angepasst zu werden. Die Zusage zur Anbindung von individuellen und wunschgemäßen Schnittstellen, die durch uns noch nicht entwickelt sind, erfolgt unverbindlich und im Rahmen der Verhältnismäßigkeit. Dies gilt ebenso für den Einsatz von besonderen Hardwarekomponenten.

Damit die Zusammenarbeit gelingt und der Verbau der Innenraumüberwachungssysteme zu einem nachweislichen Erfolg wird, endet jede Inbetriebnahme mit einem umfangreichen Funktionstest, der dokumentiert wird. Darüber hinaus kann jeder Melder bzw. Sensor zu jeder Zeit eigenständig getestet und somit die Funktionssicherheit überprüft werden. Den Einsatzkräften wird dies ausdrücklich als Probealarm angezeigt, sodass es nicht zu Missverständnissen kommt.

Sofern der Anschluss an eine vorhandene Brandmeldeanlage gewünscht ist, wird dieser in der Regel durch das Schalten eines potenzialfreien Eingangskontaktes realisiert. Dieser muss Ihrerseits, bzw. durch den Servicetechniker der Wartungsfirma der Brandmeldeanlage, bereitgestellt werden. In der Nähe des Kontaktes muss im fünf Meter Abstand eine 230V Steckdose vorhanden sein. Für den Anschluss unseres Schaltaktors

an Ihre Brandmeldeanlage gelten die gültigen Aufschaltbedingungen Ihrer zuständigen Brandschutzbehörde. Diese geben in der Regel vor, dass Sie nur nach DIN 14675 bzw. EN 54 zertifizierte Komponenten, also Teile anderer Brandmeldeanlagen, anschließen dürfen. Naturgemäß ist dies bei unserem System nicht der Fall, da es für die Überwachung von Innenräumen der Fahrzeuge kein technisches Regelwerk gibt. In den allermeisten Fällen lässt sich ein Anschluss unseres Systems an Ihre BMA aber trotzdem realisieren, da fast alle behördlichen Aufschaltbedingungen eine Öffnungsklausel haben, die besagt, dass die zuständige Behörde im Rahmen Ihrer Genehmigung von den vorangestellten Anforderungen abweichen kann. Sie müssen daher, sofern Ihre Brandmeldeanlage bei einer Feuerwehr Leitstelle aufgeschaltet ist, vor der Inbetriebnahme eine entsprechende Genehmigung einholen. Die Verantwortung hierfür liegt beim Auftraggeber.

1.2 Hinweise zum Datenschutz

Bitte beachten Sie die folgenden Informationen bezüglich des Datenschutzes in Verbindung mit der Fernwartungsfunktion sowie unseres online Service-Logbuchs, die in unserem System enthalten ist:

1. Zweck der Fernwartung: Die Fernwartungsfunktion ermöglicht es unserem technischen Support Team, auf Ihr System zuzugreifen, um Wartungs- und Supportdienste zu erbringen, Updates durchzuführen und Probleme zu diagnostizieren und zu beheben. Dies geschieht auf freiwilliger Basis. Die Fernwartungsfunktion ist standardmäßig immer aktiv. Wünschen Sie dies nicht, müssen Sie uns darauf schriftlich hinweisen.

2. Datenschutz und Sicherheit: Wir nehmen den Schutz Ihrer Daten ernst und ergreifen angemessene technische und organisatorische Maßnahmen, um sicherzustellen, dass Ihre Daten während der Fernwartung sicher und geschützt bleiben. Jeglicher Zugriff auf Ihr System erfolgt unter Einhaltung geltender Datenschutzgesetze und unserer strengen IT-Sicherheitsregeln. Es werden ausschließlich verschlüsselte Verbindungen mit starken Passwörtern und Multi-Faktor Authentifikation verwendet.

3. Datenerhebung und -verarbeitung: Während der Fernwartung können bestimmte Daten Ihres Systems erfasst und verarbeitet werden, einschließlich technischer Informationen und Fehlerprotokolle. Diese Daten werden ausschließlich für Supportzwecke und zur Verbesserung unserer Produkte verwendet und werden nicht an Dritte weitergegeben, es sei denn, dies ist gesetzlich vorgeschrieben oder wird von Ihnen autorisiert. Es werden bei der Fernwartung und dem Service-Log keine personenbezogenen Daten erhoben, daher findet die Datenschutz Grundverordnung keine Anwendung.

4. Zentrales Service-Logbuch: Zusätzlich zu den oben genannten Informationen möchten wir darauf hinweisen, dass Anlagendaten in ein zentrales Service-Logbuch geschrieben werden. Diese Daten dienen der Überwachung und Optimierung der Systemleistung und -zuverlässigkeit und werden gemäß den geltenden Datenschutzbestimmungen verarbeitet.

5. Akzeptanz der Bestimmungen: Indem Sie dieses technische System erwerben und die Fernwartungsfunktion nutzen, erklären Sie sich mit den oben genannten Datenschutzbestimmungen sowie der Verarbeitung Ihrer Anlagendaten in unserem zentralen Service-Logbuch einverstanden.

---

2. Konfiguration

Um FF-Agent zu konfigurieren rufen Sie die Verwaltungsoberfläche Ihrer Einheit auf.

https://ff-agent.com/app/login/

Folgende Informationen werden benötigt:

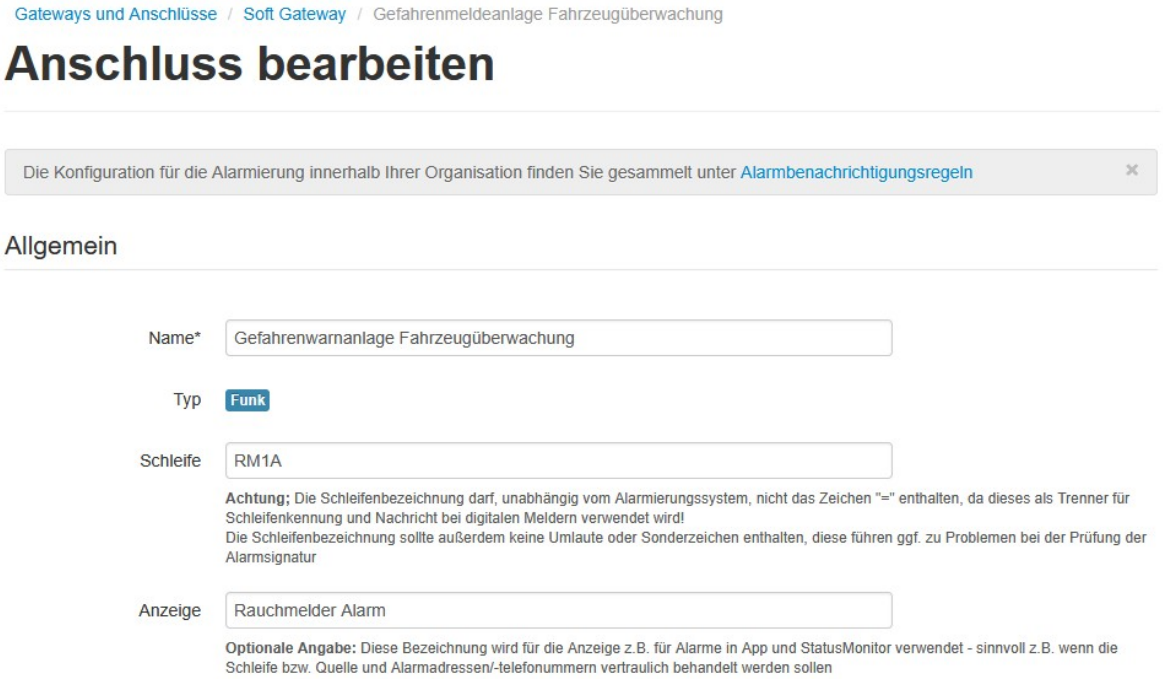
- Source-ID
- Authentifizierungsschlüssel (AccessToken)
- Schleifenbezeichnung des Anschlusses für den Alarm pro Standort

2.1 Source-ID und Authentifizierungsschlüssel

- die Source-ID erhalten Sie auf Anfrage von FF-Agent
- den Authentifizierungsschlüssel (AccessToken) erhalten Sie auf Anfrage von FF-Agent

2.2 Schleife

- Im Abschnitt **"Admin" -> "Gatways und Anschlüsse -> Softgateways -> Bearbeiten -> [Anschluss wählen] -> Bearbeiten -> Feld "Schleife"** wird die Schleifenbezeichnung angezeigt. **Diese benötigen wir**



3. Weitere Informationen und Technische Daten

- Weitere Informationen finden Sie in unserer Knowledge Base https://docs.dexa.gmbh/books/faq

4. Kontaktdaten und Serviceticket

- Ein Serviceticket können Sie durch Scannen des QR-Codes auf Ihrer PoE-Zentrale bzw. PoE-Repeater erstellen.
- Alternativ finden Sie unser Ticketsystem auch hier: https://dexa.gmbh/serviceticket

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

Telefon: +49 2924 496 937 0

E-Mail: info@dexa.gmbh

Kontakt als QR Code für Ihr Mobiltelefon:

Anleitung Schnittstelle GroupAlarm

Hardware Stand: 1.1
Anleitung Stand: 1.1

Vor Inbetriebnahme der Komponenten die Betriebsanleitung lesen

Diese Anleitung ist Teil des Produktes. Das Nichtbeachtung der Vorgaben dieser Anleitung kann eine Beeinträchtigung der Funktion oder die Beschädigung des Gerätes, anderer Sachwerte sowie Personenschäden zur Folge haben.

- Vor jeder Inbetriebnahme sind die entsprechenden Kapitel dieser Anleitung zu lesen und die enthaltenen Sicherheitshinweise zu beachten.
- Die Anleitung ist an jeden nachfolgenden Benutzer zu übergeben.
- Fragen und Hinweise bitte als Serviceticket stellen. Einen Link dazu finden Sie am Ende dieser Anleitung.

Urheberrecht

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

---

1. Einleitung

1.1 Rollenverteilung und Haftung

Die Dexa Solutions GmbH nimmt im Projekt die Rolle des Systemintegrators ein. Wir konzipieren den Lösungsansatz und setzen ihn nach Ihren Vorgaben um. Dabei kommen verschiedene technische Komponenten von namhaften Hard- und Softwareanbietern sowie eigens entwickelte Hard- und Software zum Einsatz. Wir sind nicht Hersteller aller zum Einsatz kommenden Komponenten und übernehmen daher nicht die Produkthaftung der Fremdhersteller, außer für von uns durchgeführte Modifikationen. Diese obliegt weiterhin, genau wie die Gewährleistung und Garantie, dem Hersteller der jeweiligen Komponente. Auf Seiten der Software haften wir in vollem Umfang für die eigens entwickelten Softwareteile, naturgemäß jedoch nicht für die Softwareteile von Drittanbietern.

Unsere Anlage orientiert sich an ausgewählten technischen Anforderungen der VDE 0833-1 (allgemeiner Teil). Es werden teilweise VdS- bzw. EN 54-zertifizierte Rauchmelder eingesetzt, teilweise nicht zertifizierte Rauchsensoren. Die Anlage erfüllt daher ausdrücklich nicht die Anforderungen an bauordnungsrechtlich geforderte Brandmeldeanlagen nach VDE 0833-2/DIN 14675, wie sie insbesondere in Sonderbauten (z. B. Schulen, Krankenhäuser, Beherbergungsbetriebe) verlangt werden.

In Fahrzeugen sowie in Gebäuden oder Räumen, für die keine bauordnungsrechtliche Pflicht zur Installation einer Brandmeldeanlage nach VDE 0833-2/DIN 14675 besteht, kann die Anlage eingesetzt werden. Sofern die Integration in ein Brandschutzkonzept erfolgt, kann die Anlage als ergänzende technische Maßnahme zur Verbesserung der Früherkennung und Alarmierung berücksichtigt werden, ohne eine bauordnungsrechtlich geforderte Brandmeldeanlage zu ersetzen.

Als Kunde stellen Sie Teile Ihrer IT-Infrastruktur, zum Beispiel einen Netzwerkanschluss mit Internetzugang, WLAN oder Eingangsschnittstellen zu Alarmsystemen bzw. Gebäudetechnik oder Brandmeldeanlage zur Verfügung. Diese muss am Tag der Inbetriebnahme gemäß der abgesprochenen Anforderungen vorbereitet sein. Für das nachhaltige Funktionieren dieser Infrastruktur tragen Sie als Kunde die Verantwortung. Für ein langfristiges Funktionieren können wir, etwa wenn Sie künftig Änderungen vornehmen, keine Haftung übernehmen.

Manche Alarmsysteme, wie zum Beispiel Alamos, werden lokal durch den Kunden gehostet. Hier trägt dieser die Verantwortung für das Funktionieren der bereitgestellten Schnittstelle. Andere Systeme, wie zum Beispiel Divera24/7, sind Cloud-basiert. Hier wird die Schnittstelle direkt vom Hersteller betrieben. Wir können für den Fall, dass dieser Änderungen vornimmt und dadurch Funktionseinschränkungen auftreten, keine Haftung übernehmen. Unsere Systeme sind aber darauf ausgelegt, in diesem unwahrscheinlichen Fall nachträglich mit nur geringem Aufwand, z.B. per Fernwartung, angepasst zu werden. Die Zusage zur Anbindung von individuellen und wunschgemäßen Schnittstellen, die durch uns noch nicht entwickelt sind, erfolgt unverbindlich und im Rahmen der Verhältnismäßigkeit. Dies gilt ebenso für den Einsatz von besonderen Hardwarekomponenten.

Damit die Zusammenarbeit gelingt und der Verbau der Innenraumüberwachungssysteme zu einem nachweislichen Erfolg wird, endet jede Inbetriebnahme mit einem umfangreichen Funktionstest, der dokumentiert wird. Darüber hinaus kann jeder Melder bzw. Sensor zu jeder Zeit eigenständig getestet und somit die Funktionssicherheit überprüft werden. Den Einsatzkräften wird dies ausdrücklich als Probealarm angezeigt, sodass es nicht zu Missverständnissen kommt.

Sofern der Anschluss an eine vorhandene Brandmeldeanlage gewünscht ist, wird dieser in der Regel durch das Schalten eines potenzialfreien Eingangskontaktes realisiert. Dieser muss Ihrerseits, bzw. durch den Servicetechniker der Wartungsfirma der Brandmeldeanlage, bereitgestellt werden. In der Nähe des Kontaktes muss im fünf Meter Abstand eine 230V Steckdose vorhanden sein. Für den Anschluss unseres Schaltaktors an Ihre Brandmeldeanlage gelten die gültigen Aufschaltbedingungen Ihrer zuständigen Brandschutzbehörde. Diese geben in der Regel vor, dass Sie nur nach DIN 14675 bzw. EN 54 zertifizierte Komponenten, also Teile

anderer Brandmeldeanlagen, anschließen dürfen. Naturgemäß ist dies bei unserem System nicht der Fall, da es für die Überwachung von Innenräumen der Fahrzeuge kein technisches Regelwerk gibt. In den allermeisten Fällen lässt sich ein Anschluss unseres Systems an Ihre BMA aber trotzdem realisieren, da fast alle behördlichen Aufschaltbedingungen eine Öffnungsklausel haben, die besagt, dass die zuständige Behörde im Rahmen Ihrer Genehmigung von den vorangestellten Anforderungen abweichen kann. Sie müssen daher, sofern Ihre Brandmeldeanlage bei einer Feuerwehr Leitstelle aufgeschaltet ist, vor der Inbetriebnahme eine entsprechende Genehmigung einholen. Die Verantwortung hierfür liegt beim Auftraggeber.

1.2 Hinweise zum Datenschutz

Bitte beachten Sie die folgenden Informationen bezüglich des Datenschutzes in Verbindung mit der Fernwartungsfunktion sowie unseres online Service-Logbuchs, die in unserem System enthalten ist:

1. Zweck der Fernwartung: Die Fernwartungsfunktion ermöglicht es unserem technischen Support Team, auf Ihr System zuzugreifen, um Wartungs- und Supportdienste zu erbringen, Updates durchzuführen und Probleme zu diagnostizieren und zu beheben. Dies geschieht auf freiwilliger Basis. Die Fernwartungsfunktion ist standardmäßig immer aktiv. Wünschen Sie dies nicht, müssen Sie uns darauf schriftlich hinweisen.

2. Datenschutz und Sicherheit: Wir nehmen den Schutz Ihrer Daten ernst und ergreifen angemessene technische und organisatorische Maßnahmen, um sicherzustellen, dass Ihre Daten während der Fernwartung sicher und geschützt bleiben. Jeglicher Zugriff auf Ihr System erfolgt unter Einhaltung geltender Datenschutzgesetze und unserer strengen IT-Sicherheitsregeln. Es werden ausschließlich verschlüsselte Verbindungen mit starken Passwörtern und Multi-Faktor Authentifikation verwendet.

3. Datenerhebung und -verarbeitung: Während der Fernwartung können bestimmte Daten Ihres Systems erfasst und verarbeitet werden, einschließlich technischer Informationen und Fehlerprotokolle. Diese Daten werden ausschließlich für Supportzwecke und zur Verbesserung unserer Produkte verwendet und werden nicht an Dritte weitergegeben, es sei denn, dies ist gesetzlich vorgeschrieben oder wird von Ihnen autorisiert. Es werden bei der Fernwartung und dem Service-Log keine personenbezogenen Daten erhoben, daher findet die Datenschutz Grundverordnung keine Anwendung.

4. Zentrales Service-Logbuch: Zusätzlich zu den oben genannten Informationen möchten wir darauf hinweisen, dass Anlagendaten in ein zentrales Service-Logbuch geschrieben werden. Diese Daten dienen der Überwachung und Optimierung der Systemleistung und -zuverlässigkeit und werden gemäß den geltenden Datenschutzbestimmungen verarbeitet.

5. Akzeptanz der Bestimmungen: Indem Sie dieses technische System erwerben und die Fernwartungsfunktion nutzen, erklären Sie sich mit den oben genannten Datenschutzbestimmungen sowie der Verarbeitung Ihrer Anlagendaten in unserem zentralen Service-Logbuch einverstanden.

---

2. Konfiguration

Um FF-Agent zu konfigurieren rufen Sie die Verwaltungsoberfläche Ihrer Einheit auf.

https://www.groupalarm.com

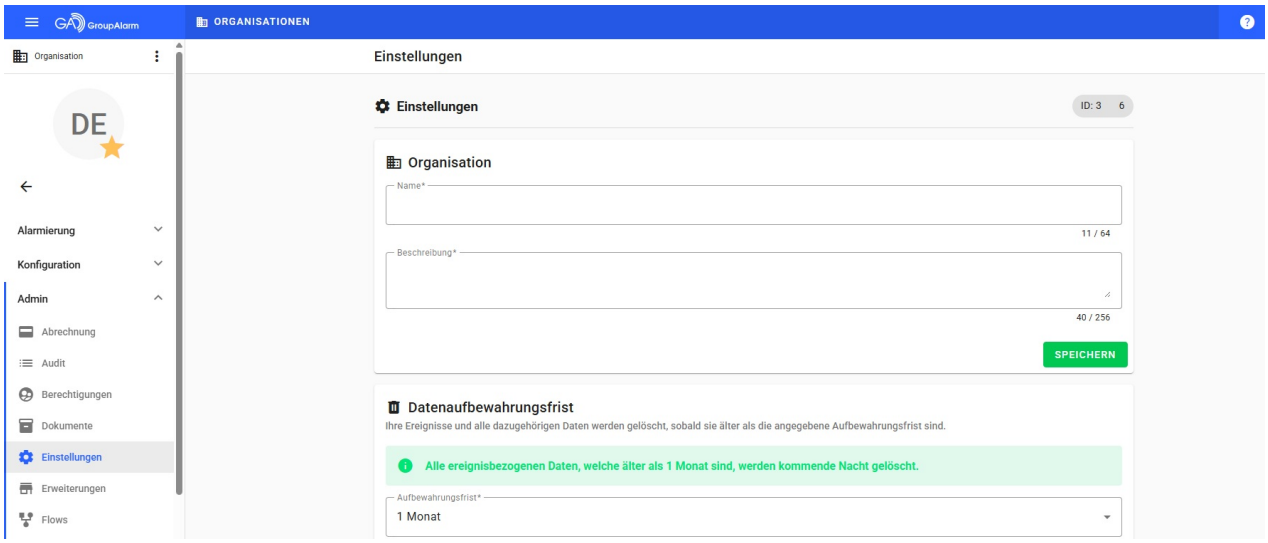
Folgende Informationen werden benötigt:

- Organisations-ID
- API-Schlüssel

- Externer Bezeichner pro Standort

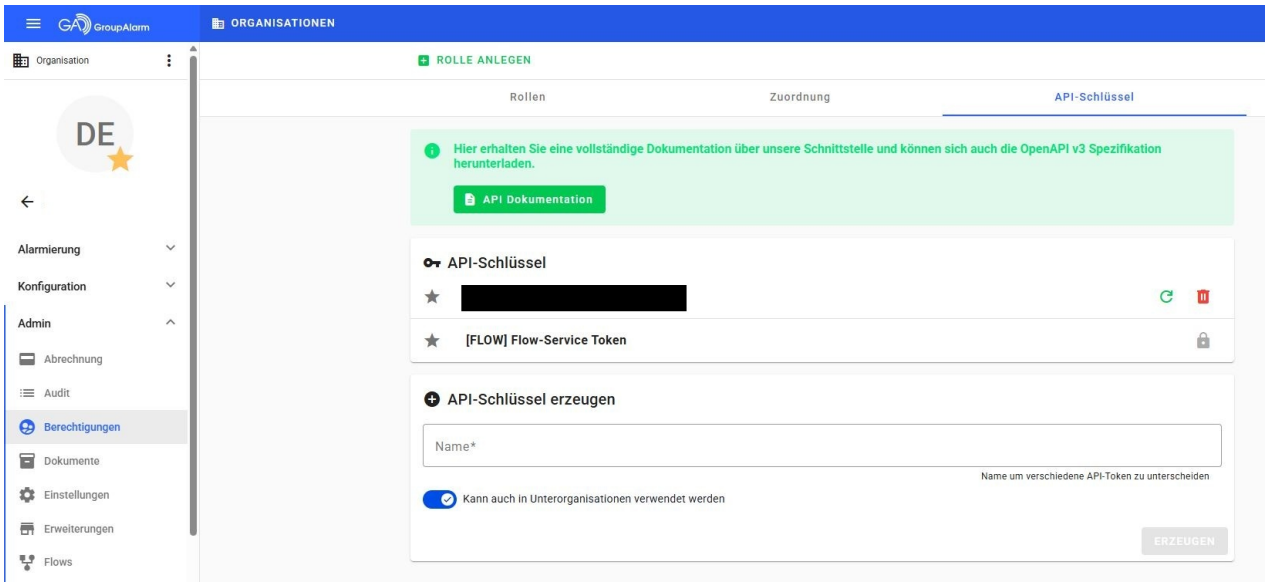
2.1 Organisations-ID

- die Organisations-ID ist zu finden unter **Admin -> Einstellungen**
- oben rechts ist die **ID: xxxxx** auslesbar



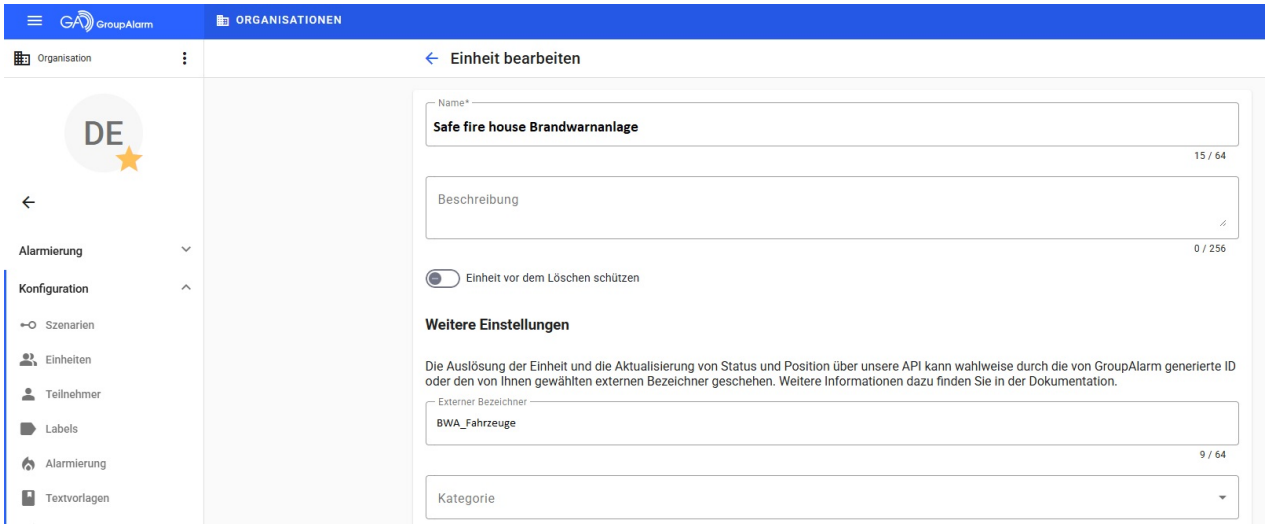
2.2 API-Key

- unter **Admin -> Berechtigungen** können Sie einen API-Schlüssel erzeugen
- **Für jede Applikation, welche einen API-Zugriff benötigt, sollte ein separater Schlüssel erzeugt werden! So kann jeder Client bei Bedarf vom System getrennt werden, ohne das andere Systeme mit API-Zugriff betroffen sind!**
- **Wichtig!** Setzen Sie die Option "Kann auch in Unterorganisationen verwendet werden", wenn sie mit Unterorganisationen arbeiten!



2.3 Externer Bezeichner

- unter **Konfiguration -> Einheiten -> Einheit bearbeiten** im Abschnitt "Weitere Einstellungen" finden Sie den Externen Bezeichner



3. Weitere Informationen und Technische Daten

- Weitere Informationen finden Sie in unserer Knowledge Base https://docs.dexa.gmbh/books/faq

4. Kontaktdaten und Serviceticket

- Ein Serviceticket können Sie durch Scannen des QR-Codes auf Ihrer PoE-Zentrale bzw. PoE-Repeater erstellen.
- Alternativ finden Sie unser Ticketsystem auch hier: https://dexa.gmbh/serviceticket

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

Telefon: +49 2924 496 937 0

E-Mail: info@dexa.gmbh

Kontakt als QR Code für Ihr Mobiltelefon:

Anleitung Schnittstelle FirePlan

Hardware Stand: 1.1
Anleitung Stand: 1.0

Vor Inbetriebnahme der Komponenten die Betriebsanleitung lesen

Diese Anleitung ist Teil des Produktes. Das Nichtbeachtung der Vorgaben dieser Anleitung kann eine Beeinträchtigung der Funktion oder die Beschädigung des Gerätes, anderer Sachwerte sowie Personenschäden zur Folge haben.

- Vor jeder Inbetriebnahme sind die entsprechenden Kapitel dieser Anleitung zu lesen und die enthaltenen Sicherheitshinweise zu beachten.
- Die Anleitung ist an jeden nachfolgenden Benutzer zu übergeben.
- Fragen und Hinweise bitte als Serviceticket stellen. Einen Link dazu finden Sie am Ende dieser Anleitung.

Urheberrecht

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

---

1. Einleitung

1.1 Rollenverteilung und Haftung

Die Dexa Solutions GmbH nimmt im Projekt die Rolle des Systemintegrators ein. Wir konzipieren den Lösungsansatz und setzen ihn nach Ihren Vorgaben um. Dabei kommen verschiedene technische Komponenten von namhaften Hard- und Softwareanbietern sowie eigens entwickelte Hard- und Software zum Einsatz. Wir sind nicht Hersteller aller zum Einsatz kommenden Komponenten und übernehmen daher nicht die Produkthaftung der Fremdhersteller, außer für von uns durchgeführte Modifikationen. Diese obliegt weiterhin, genau wie die Gewährleistung und Garantie, dem Hersteller der jeweiligen Komponente. Auf Seiten der Software haften wir in vollem Umfang für die eigens entwickelten Softwareteile, naturgemäß jedoch nicht für die Softwareteile von Drittanbietern.

Unsere Anlage orientiert sich an ausgewählten technischen Anforderungen der VDE 0833-1 (allgemeiner Teil). Es werden teilweise VdS- bzw. EN 54-zertifizierte Rauchmelder eingesetzt, teilweise nicht zertifizierte Rauchsensoren. Die Anlage erfüllt daher ausdrücklich nicht die Anforderungen an bauordnungsrechtlich geforderte Brandmeldeanlagen nach VDE 0833-2/DIN 14675, wie sie insbesondere in Sonderbauten (z. B. Schulen, Krankenhäuser, Beherbergungsbetriebe) verlangt werden.

In Fahrzeugen sowie in Gebäuden oder Räumen, für die keine bauordnungsrechtliche Pflicht zur Installation einer Brandmeldeanlage nach VDE 0833-2/DIN 14675 besteht, kann die Anlage eingesetzt werden. Sofern die Integration in ein Brandschutzkonzept erfolgt, kann die Anlage als ergänzende technische Maßnahme zur Verbesserung der Früherkennung und Alarmierung berücksichtigt werden, ohne eine bauordnungsrechtlich geforderte Brandmeldeanlage zu ersetzen.

Als Kunde stellen Sie Teile Ihrer IT-Infrastruktur, zum Beispiel einen Netzwerkanschluss mit Internetzugang, WLAN oder Eingangsschnittstellen zu Alarmsystemen bzw. Gebäudetechnik oder Brandmeldeanlage zur Verfügung. Diese muss am Tag der Inbetriebnahme gemäß der abgesprochenen Anforderungen vorbereitet sein. Für das nachhaltige Funktionieren dieser Infrastruktur tragen Sie als Kunde die Verantwortung. Für ein langfristiges Funktionieren können wir, etwa wenn Sie künftig Änderungen vornehmen, keine Haftung übernehmen.

Manche Alarmsysteme, wie zum Beispiel Alamos, werden lokal durch den Kunden gehostet. Hier trägt dieser die Verantwortung für das Funktionieren der bereitgestellten Schnittstelle. Andere Systeme, wie zum Beispiel Divera24/7, sind Cloud-basiert. Hier wird die Schnittstelle direkt vom Hersteller betrieben. Wir können für den Fall, dass dieser Änderungen vornimmt und dadurch Funktionseinschränkungen auftreten, keine Haftung übernehmen. Unsere Systeme sind aber darauf ausgelegt, in diesem unwahrscheinlichen Fall nachträglich mit nur geringem Aufwand, z.B. per Fernwartung, angepasst zu werden. Die Zusage zur Anbindung von individuellen und wunschgemäßen Schnittstellen, die durch uns noch nicht entwickelt sind, erfolgt unverbindlich und im Rahmen der Verhältnismäßigkeit. Dies gilt ebenso für den Einsatz von besonderen Hardwarekomponenten.

Damit die Zusammenarbeit gelingt und der Verbau der Innenraumüberwachungssysteme zu einem nachweislichen Erfolg wird, endet jede Inbetriebnahme mit einem umfangreichen Funktionstest, der dokumentiert wird. Darüber hinaus kann jeder Melder bzw. Sensor zu jeder Zeit eigenständig getestet und somit die Funktionssicherheit überprüft werden. Den Einsatzkräften wird dies ausdrücklich als Probealarm angezeigt, sodass es nicht zu Missverständnissen kommt.

Sofern der Anschluss an eine vorhandene Brandmeldeanlage gewünscht ist, wird dieser in der Regel durch das Schalten eines potenzialfreien Eingangskontaktes realisiert. Dieser muss Ihrerseits, bzw. durch den Servicetechniker der Wartungsfirma der Brandmeldeanlage, bereitgestellt werden. In der Nähe des Kontaktes muss im fünf Meter Abstand eine 230V Steckdose vorhanden sein. Für den Anschluss unseres Schaltaktors an Ihre Brandmeldeanlage gelten die gültigen Aufschaltbedingungen Ihrer zuständigen Brandschutzbehörde. Diese geben in der Regel vor, dass Sie nur nach DIN 14675 bzw. EN 54 zertifizierte Komponenten, also Teile anderer Brandmeldeanlagen, anschließen dürfen. Naturgemäß ist dies bei unserem System nicht der Fall, da es für die Überwachung von Innenräumen der Fahrzeuge kein technisches Regelwerk gibt. In den allermeisten Fällen lässt sich ein Anschluss unseres Systems an Ihre BMA aber trotzdem realisieren, da fast alle behördlichen Aufschaltbedingungen eine Öffnungsklausel haben, die besagt, dass die zuständige Behörde im Rahmen Ihrer Genehmigung von den vorangestellten Anforderungen abweichen kann. Sie müssen daher, sofern Ihre Brandmeldeanlage bei einer Feuerwehr Leitstelle aufgeschaltet ist, vor der Inbetriebnahme eine entsprechende Genehmigung einholen. Die Verantwortung hierfür liegt beim Auftraggeber.

1.2 Hinweise zum Datenschutz

Bitte beachten Sie die folgenden Informationen bezüglich des Datenschutzes in Verbindung mit der Fernwartungsfunktion sowie unseres online Service-Logbuchs, die in unserem System enthalten ist:

1. Zweck der Fernwartung: Die Fernwartungsfunktion ermöglicht es unserem technischen Support Team, auf Ihr System zuzugreifen, um Wartungs- und Supportdienste zu erbringen, Updates durchzuführen und Probleme zu diagnostizieren und zu beheben. Dies geschieht auf freiwilliger Basis. Die Fernwartungsfunktion ist standardmäßig immer aktiv. Wünschen Sie dies nicht, müssen Sie uns darauf schriftlich hinweisen.

2. Datenschutz und Sicherheit: Wir nehmen den Schutz Ihrer Daten ernst und ergreifen angemessene technische und organisatorische Maßnahmen, um sicherzustellen, dass Ihre Daten während der Fernwartung sicher und geschützt bleiben. Jeglicher Zugriff auf Ihr System erfolgt unter Einhaltung geltender Datenschutzgesetze und unserer strengen IT-Sicherheitsregeln. Es werden ausschließlich verschlüsselte Verbindungen mit starken Passwörtern und Multi-Faktor Authentifikation verwendet.

3. Datenerhebung und -verarbeitung: Während der Fernwartung können bestimmte Daten Ihres Systems erfasst und verarbeitet werden, einschließlich technischer Informationen und Fehlerprotokolle. Diese Daten werden ausschließlich für Supportzwecke und zur Verbesserung unserer Produkte verwendet und werden nicht an Dritte weitergegeben, es sei denn, dies ist gesetzlich vorgeschrieben oder wird von Ihnen autorisiert. Es werden bei der Fernwartung und dem Service-Log keine personenbezogenen Daten erhoben, daher findet die Datenschutz Grundverordnung keine Anwendung.

4. Zentrales Service-Logbuch: Zusätzlich zu den oben genannten Informationen möchten wir darauf hinweisen, dass Anlagendaten in ein zentrales Service-Logbuch geschrieben werden. Diese Daten dienen der Überwachung und Optimierung der Systemleistung und -zuverlässigkeit und werden gemäß den geltenden Datenschutzbestimmungen verarbeitet.

5. Akzeptanz der Bestimmungen: Indem Sie dieses technische System erwerben und die Fernwartungsfunktion nutzen, erklären Sie sich mit den oben genannten Datenschutzbestimmungen sowie der Verarbeitung Ihrer Anlagendaten in unserem zentralen Service-Logbuch einverstanden.

---

2. Benötigte Daten

Folgende Informationen werden benötigt:

- API-Key
- RIC
- SubRIC (default: "A")

2.1 Schnittstelle hinzufügen

- Legen Sie in fireplan.desktop uns als **externe Schnittstelle** an

2.2 API-Key

- Generieren Sie in fireplan.desktop einen **API-Key** - dieser wird von uns für die Alarmierung benötigt
- **Für jede Applikation, welche einen API-Zugriff benötigt, sollte ein separater Schlüssel erzeugt werden! So kann jeder Client bei Bedarf vom System getrennt werden, ohne das andere Systeme mit API-Zugriff betroffen sind!**

2.3 RIC & SubRIC

- unter **WEITERE STAMMDATEN** sind die RICs zu finden
- teilen Sie uns diejenige mit, die für die Alarmierung übertragen werden soll

2.4 Alarmüberlauf

Soll ein Alarmüberlauf auf dieselbe Schnittstelle konfiguriert werden, benötigen wir folgende Informationen:

- Nach wie vielen Sekunden / Minuten sollen Rückmeldungen geprüft werden?
- Welche maximale Rückmeldezeit gilt als Abbruchkriterium der Eskalationsstufe?
- Mit welcher RIC soll die nächste Eskalationsstufe alarmieren?

---

3. Weitere Informationen und Technische Daten

- Weitere Informationen finden Sie in unserer Knowledge Base https://docs.dexa.gmbh/books/faq

---

4. Kontaktdaten und Serviceticket

- Ein Serviceticket können Sie durch Scannen des QR-Codes auf Ihrer PoE-Zentrale bzw. PoE-Repeater erstellen.
- Alternativ finden Sie unser Ticketsystem auch hier: https://dexa.gmbh/serviceticket

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

Telefon: +49 2924 496 937 0

E-Mail: info@dexa.gmbh

Kontakt als QR Code für Ihr Mobiltelefon:

Anleitung Alarmanruf

Anleitung Stand: 1.1

Vor Nutzung des Systems diese Anleitung lesen

Diese Anleitung ist Teil des Produktes. Das Nichtbeachten der Vorgaben dieser Anleitung kann eine Beeinträchtigung der Funktion zur Folge haben.

- Vor der ersten Nutzung sind die entsprechenden Kapitel dieser Anleitung zu lesen.
- Die Anleitung ist an jeden nachfolgenden Benutzer zu übergeben.
- Fragen und Hinweise bitte als Serviceticket stellen. Einen Link dazu finden Sie am Ende dieser Anleitung.

Urheberrecht

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

---

1. Einleitung

1.1 Was ist das Alarmanruf-System?

Wenn ein Rauchmelder in Ihrer Anlage auslöst, werden automatisch Telefonanrufe an hinterlegte Rufnummern gestartet. Eine Computerstimme informiert Sie über den Alarm und fordert Sie zur Bestätigung auf.

---

2. Ablauf eines Alarmanrufs

2.1 Rauchmelder löst aus

Ihre Brandmeldeanlage erkennt den Alarm und startet automatisch die Anrufkette.

2.2 Anruf auf Ihrem Telefon

Sie erhalten einen Anruf von einer Ihnen zugewiesenen Rufnummer. Diese Nummer sollten Sie in Ihrem Telefon speichern, damit Sie den Alarmanruf sofort erkennen.

2.3 Sprachansage

Nach Annahme des Anrufs hören Sie eine automatische Ansage, z.B.:

„Achtung Alarmanruf. Rauchmelder im Erdgeschoss Flur hat ausgelöst. Drücken Sie die 1 um den Alarm zu bestätigen."

2.4 Bestätigung mit Taste 1

- **Drücken Sie die Taste 1** auf Ihrem Telefon, um den Alarm zu bestätigen
- Die anderen Personen in der Runde werden **trotzdem noch angerufen** – erst nach der Runde wird ausgewertet
- Sie sind nun verantwortlich, den Alarm vor Ort zu prüfen

2.5 Keine Bestätigung?

Wenn Sie:

- den Anruf nicht annehmen
- keine Taste drücken
- eine andere Taste als 1 drücken

...wird Ihr Anruf als **„nicht bestätigt"** gewertet. Die **nächsten Personen werden weiter angerufen**. Erst nach Abschluss der Runde wird ausgewertet, ob mindestens eine Person bestätigt hat.

---

3. Anrufkette

3.1 So läuft eine Runde ab

In jeder Runde werden **alle hinterlegten Personen** nacheinander angerufen:

Runde 1: Person 1 → Person 2 → Person 3 → ... → Auswertung

Wichtig: Auch wenn Person 1 bereits bestätigt hat, werden Person 2 und 3 trotzdem noch angerufen. So ist sichergestellt, dass alle Verantwortlichen informiert sind.

3.2 Auswertung nach jeder Runde

Nach Abschluss einer Runde wird geprüft:

- Hat **mindestens eine Person** mit Taste 1 bestätigt? ? **Fertig**, keine weitere Runde
- Hat **niemand** bestätigt? ? **Nächste Runde** startet

3.3 Mehrere Runden möglich

Falls in Runde 1 niemand bestätigt, werden bis zu **5 Runden** durchgeführt:

Runde 1: Alle anrufen → Niemand bestätigt → Runde 2
Runde 2: Alle anrufen → Niemand bestätigt → Runde 3
...
Runde 5: Alle anrufen → Finale Auswertung

---

4. Wichtige Hinweise

4.1 Bitte beachten Sie

- **Rufnummer speichern:** Speichern Sie die Alarmanruf-Nummer in Ihrem Telefon als „Alarmanruf" oder „Brandmeldung"
- **Anruf annehmen:** Nehmen Sie Anrufe von dieser Nummer immer an – auch nachts
- **Taste 1 drücken:** Bestätigen Sie den Alarm, wenn Sie sich darum kümmern können
- **Alle werden informiert:** Auch nach Ihrer Bestätigung werden die anderen Personen noch angerufen
- **Vor Ort prüfen:** Nach Bestätigung: Überprüfen Sie die Situation vor Ort
- **Nicht bestätigen wenn verhindert:** Wenn Sie nicht reagieren können, legen Sie auf – die nächste Person wird angerufen

4.2 Zeitfenster

- Ein Anruf klingelt ca. **30-60 Sekunden**
- Danach wird die nächste Nummer angerufen
- Die Ansage dauert ca. **10-15 Sekunden** – warten Sie bis zum Ende

4.3 Mobiltelefon-Tipps

- Stellen Sie sicher, dass Ihr Telefon nicht auf „Nicht stören" steht
- Die Alarmnummer sollte auch nachts durchkommen (ggf. als Favorit/Ausnahme einstellen)
- Bei schlechtem Empfang kann der Anruf fehlschlagen – stellen Sie eine Ersatznummer bereit

---

5. Häufige Fragen

5.1 Was passiert, wenn niemand den Alarm bestätigt?

Es werden bis zu **5 Runden** durchgeführt. In jeder Runde werden alle hinterlegten Nummern angerufen. Bestätigt nach 5 Runden immer noch niemand, wird dies protokolliert. Je nach Konfiguration Ihrer Anlage können weitere Maßnahmen ausgelöst werden (z.B. Alarmierung der Feuerwehr).

5.2 Kann ich den Anruf zurückrufen?

Nein, ein Rückruf ist nicht möglich. Alarmanrufe werden nur automatisch bei einem Ereignis ausgelöst.

5.3 Was bedeutet es, wenn ich Taste 1 drücke?

Sie bestätigen, dass Sie den Alarm zur Kenntnis genommen haben und sich darum kümmern. **Wichtig:** Die anderen Personen in der Liste werden trotzdem noch angerufen, damit alle informiert sind. Erst nach Abschluss der Runde wird keine weitere Runde gestartet.

5.4 Ich habe aus Versehen aufgelegt – was nun?

Die nächste Person in der Liste wird angerufen. In der Auswertung nach der Runde wird Ihr Anruf als "keine Bestätigung" gewertet. Falls Sie sich dennoch um den Alarm kümmern möchten, koordinieren Sie sich mit den anderen Verantwortlichen.

5.5 Werden die Anrufe protokolliert?

Ja, alle Alarmanrufe werden mit Zeitstempel, angerufener Nummer und Ergebnis (bestätigt/keine Antwort) protokolliert.

---

6. Ihre Alarmanruf-Konfiguration

- **Absender-Rufnummer:** *(wird von Dexa mitgeteilt)*
- **Maximale Runden:** 5
- **Versuche pro Nummer/Runde:** 2
- **Wartezeit zwischen Anrufen:** ca. 10 Sekunden
- **Maximale Anrufdauer:** ca. 2 Minuten

---

7. Kontaktdaten und Serviceticket

- Ein Serviceticket können Sie durch Scannen des QR-Codes auf Ihrer PoE-Zentrale bzw. PoE-Repeater erstellen.
- Alternativ finden Sie unser Ticketsystem auch hier: https://dexa.gmbh/serviceticket

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

Telefon: +49 2924 496 937 0
E-Mail: info@safefirehouse.de

Kontakt als QR Code für Ihr Mobiltelefon:

Stand: Januar 2026