

Netzwerkanforderungen dexa VPN Router

Netzwerkanforderungen — Standortvernetzung über dexa VPN-Router

Gültig für die von der Dexa Solutions GmbH bereitgestellten Standort-Router zur standortübergreifenden Vernetzung der Safe Fire House Komponenten

Gilt, wenn das VPN-Netzwerk für eine Multistandort-Lösung von dexa betrieben werden soll

Vor Inbetriebnahme der Komponenten die Betriebsanleitung lesen

Diese Anleitung ist Teil des Produktes. Die 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

Die in dieser Anleitung enthaltenen Angaben und Abbildungen entsprechen dem Stand der Auslieferung. Änderungen der Technik, Ausstattung und Form der Geräte gegenüber den Angaben und Abbildungen in dieser Anleitung bleiben der Dexa Solutions GmbH vorbehalten. Diese Anleitung darf weder teilweise noch vollständig vervielfältigt, verbreitet oder verwendet werden. Nur befugten Personen darf diese Anleitung zugänglich gemacht werden.

Diese Anleitung einschließlich aller ihrer Teile ist urheberrechtlich geschützt. Jede Verwendung außerhalb der Grenzen des Urheberrechts ist ohne die Zustimmung der Dexa Solutions GmbH nicht zulässig.

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. Für die standortübergreifende Vernetzung stellen wir Ihnen einen vorkonfigurierten Router bereit, der die Verbindung zu unserem zentralen VPN-Hub eigenständig aufbaut und betreibt.

Als Kunde stellen Sie hierfür Teile Ihrer IT-Infrastruktur zur Verfügung, insbesondere einen Netzwerkanschluss mit Internetzugang je Standort. 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 an Ihrer Internetanbindung oder Firewall vornehmen, keine Haftung übernehmen.

Damit die Zusammenarbeit gelingt, endet jede Inbetriebnahme mit einem umfangreichen Funktionstest, der dokumentiert wird.

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 nach Art. 32 DSGVO, um sicherzustellen, dass Ihre Daten während der Fernwartung sicher und geschützt bleiben. Der Fernwartungszugriff erfolgt ausschließlich über verschlüsselte, mehrfach authentifizierte Verbindungen.

3. Datenerhebung und -verarbeitung: Während der Fernwartung sowie im Rahmen des zentralen Service-Logbuchs werden technische Informationen, Fehlerprotokolle sowie Standort- und Anlagendaten (Bezeichnung des Standortes, Anschrift der Anlage, technische Kennwerte) verarbeitet. Namen, Privatanschriften oder Telefonnummern natürlicher Personen werden hierbei nicht erhoben. Die vorgenannten Daten werden ausschließlich für Support-, Überwachungs- und Produktverbesserungszwecke verwendet und nicht an sonstige Dritte weitergegeben, es sei denn, dies ist gesetzlich vorgeschrieben oder wird von Ihnen autorisiert.

4. Weitere Informationen und Ihre Rechte: Die vorstehend beschriebene Verarbeitung erfolgt in Übereinstimmung mit der Datenschutz-Grundverordnung (DSGVO). Die für Ihr System maßgeblichen Rechtsgrundlagen, Speicherdauern und eingesetzten Auftragsverarbeiter sowie Ihre Betroffenenrechte ergeben sich aus den mit Ihnen getroffenen vertraglichen Datenschutzvereinbarungen, insbesondere dem Auftragsverarbeitungsvertrag nach Art. 28 DSGVO. Bei Fragen zum Datenschutz wenden Sie sich bitte an unseren Ansprechpartner für den Datenschutz über die am Ende dieser Anleitung genannten Kontaktdaten.

2. Hinweis zur Verbindung

Zur Vernetzung mehrerer Standorte stellt dexa an jedem Standort einen vorkonfigurierten Router bereit. Dieser Router baut selbstständig eine verschlüsselte Verbindung (WireGuard) zu unserem zentralen VPN-Hub (**hub.dexa.gmbh**) auf. Über diese Verbindung werden alle Standorte zu einem gemeinsamen Netzwerksegment zusammengeschlossen, sodass Zentrale und Repeater standortübergreifend so kommunizieren, als befänden sie sich im selben lokalen Netz.

Die eigentliche Fachkommunikation (u. a. der Multicast-Verkehr zwischen Zentrale und Repeatern) läuft **vollständig innerhalb dieses verschlüsselten Tunnels**. Sie stellt dadurch **keine gesonderten Anforderungen an Ihre Firewall** — es genügt, dem Router den Verbindungsaufbau zum VPN-Hub zu ermöglichen.

Die Rauchmelder und Sensoren kommunizieren per Funk (868 MHz) mit Zentrale und Repeater und stellen keine Anforderung an Ihr Netzwerk.

2.1 Anforderungen an die Internetanbindung (WAN) je Standort

- **Anschluss:** Eine funktionierende Internetverbindung (Kabel/DSL/Glasfaser, LTE/5G oder Satellit/Starlink) mit RJ45-Übergabe an den dexa-Router.
- **IP-Adresse:** Es genügt eine normale, auch private bzw. „CGNAT“-Adresse (wie sie z. B. bei LTE- oder Satellitenanschlüssen üblich ist). Eine öffentliche oder feste IP-Adresse ist **nicht** erforderlich.
- **Verbindungsaufbau:** ausschließlich **ausgehend**. Der Router ruft den VPN-Hub von sich aus und hält die Verbindung dauerhaft aufrecht. **Eingehende Portfreigaben oder Portweiterleitungen sind nicht notwendig.**
- **Übertragungsrate / Bandbreite:** gering. Die Fachkommunikation ist datensparsam; die Anbindung funktioniert zuverlässig auch über Mobilfunk oder Satellit.

2.2 Einsatz hinter einer Firewall

Betreiben Sie den dexa-Router hinter Ihrer eigenen Firewall, stellen Sie bitte sicher, dass die in der folgenden Tabelle genannten Ziele, Ports und Protokolle **ausgehend** erreichbar sind, um eine reibungslose Funktion zu gewährleisten.

Unser System benötigt keine eingehenden Portfreigaben in Ihrer Firewall!

Verbindung	Protokoll/Port	Ziel	Zweck
dexa-Router ? VPN-Hub	WireGuard (udp/51820)	hub.dexa.gmbh (188.64.62.229)	Aufbau des verschlüsselten Standort-Tunnels. Die gesamte weitere Kommunikation (Standortkopplung, Multicast-Fachverkehr, Fernwartung des Routers) läuft gekapselt hierüber.
dexa-Router ? DNS-Server	udp/53, tcp/53	Provider-DNS oder interner DNS-Server	Namensauflösung von hub.dexa.gmbh
dexa-Router ? Zeitserver	NTP (udp/123)	0-3.de.pool.ntp.org	Synchronisation von Datum und Uhrzeit
dexa-Router ? Internet-Erreichbarkeit	ICMP (Echo/Ping)	8.8.8.8	Konnektivitätsprüfung (WatchDog)

Hinweis zur gesamten Fachkommunikation: Sämtlicher Verkehr zwischen den Standorten sowie die Fernwartung des Routers werden **innerhalb** der WireGuard-Verbindung übertragen. Über die oben genannte Zeile „dexa-Router ? VPN-Hub“ hinaus sind hierfür **keine weiteren Firewall-Freigaben** erforderlich.

Hinweis zu MTU / kleinen Paketgrößen: Der Router verarbeitet die Paketgrößen des Tunnels selbstständig; auch Anbindungen mit reduzierter MTU (z. B. LTE, Starlink, PPPoE) werden unterstützt. Ein Eingriff Ihrerseits ist nicht erforderlich.

Hinweis zur Internet-Erreichbarkeit: Die Zentrale bzw. der Router prüft die Internetverbindung per ICMP-Echo (Ping) an **8.8.8.8**. Sollte ausgehender ICMP-Verkehr in Ihrer Firewall nicht zulässig sein, kann diese Prüfung auf Wunsch deaktiviert werden. Bitte sprechen Sie uns in diesem Fall an.

Hinweis zum Zeitserver: **0-3.de.pool.ntp.org** verweist auf einen öffentlichen Zeitserver-Pool mit wechselnden IP-Adressen. Erlauben Sie hierfür den ausgehenden NTP-Verkehr (udp/123) oder hinterlegen

Sie einen festen Zeitserver.

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
