Besonders. Sicher.

SECURITON

Technische Information für Betreiber

Securiton Remote – Mobile Benachrichtigung und Live-Support in Echtzeit

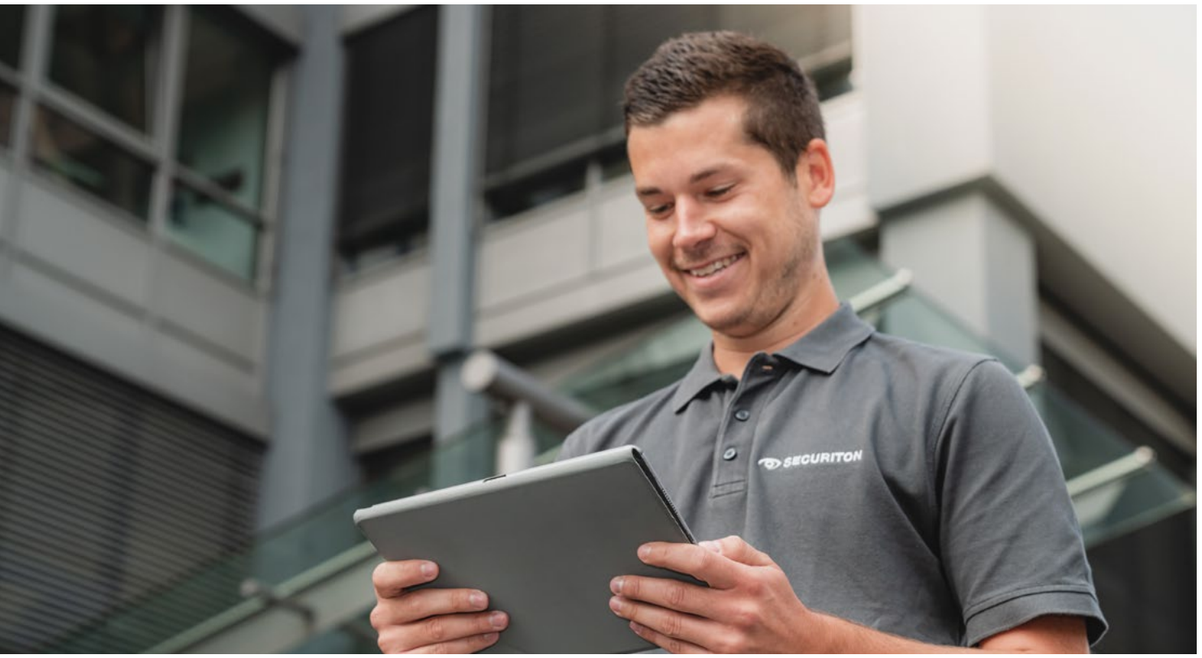
Live-Support in Echtzeit

Securiton Remote ist der perfekt zugeschnittene Dienst für den Fernzugriff auf die Brandmelderzentrale SecuriFire – sowohl für Ihren Facherrichter, als auch für Sie als Betreiber oder Eigentümer.

Während Ihr Errichter aus der Ferne auf die Programmierung der Zentrale zugreifen kann, um Ihnen im Alarm- oder Störungsfall schnell und unkompliziert zu helfen, werden Sie bzw. der von Ihnen definierte Personenkreis über Push-Benachrichtigungen in der App über Meldungen der Zentrale informiert. In Echtzeit können Sie über die App SecuriFire MobileControl direkt einen Blick in die Zentrale werfen und notwendige Maßnahmen einleiten.

Welche Vorteile bietet Ihnen der Remote-Zugriff?

- **Echtzeit-Informationen** zu Alarmen und sonstigen Ereignissen via **Push-Benachrichtigung**
- **Verkürzte Laufwege** und somit **schnellere Interventionen**
- Kurzfristige **Bedienung** der BMA **durch die eigene Haustechnik** z. B. bei Umbau- oder Malerarbeiten
- **Live-Support und schnelle Störungsbeseitigung** (Fernanalyse – und Störungsbehebung) ohne Anfahrtskosten Ihres Errichters
  - Ausfahlzeiten, Täuschungs- oder Falschalarme und Betriebsunterbrechungen reduzieren und vermeiden
  - **Kosteneffizienter Einsatz vor Ort** dank Vorabanalyse
- **Zentrale**, standortübergreifende **Liegenschaftsbetreuung**
- **Ereignisspeicherung** auch bei Offline-Status: **Historie** im Nachhinein **abrufbar**



Immer auf dem aktuellen Stand – unter höchsten Sicherheitsaspekten

Zugang für Sie als Betreiber [1)]

SecuriFire MobileControl

- Anzeigen
- Bedienen
- **Benachrichtigen**

Ihre Vorteile

- **Echtzeit-Information** aller betreuter Anlagen via Push-Benachrichtungen bei Störungen und Alarmen
- Schnelles Ableiten gezielter Maßnahmen

Zugang für Ihren Errichter

SecuriFire Studio RemoteAccess

- Anzeigen
- Bedienen
- **Analysieren**
- **Programmieren**

Ihre Vorteile

- **Sofortige Unterstützung** durch Ihren Errichter
- **Schnellstmögliche Analyse** und Fehlerbehebung **aus der Ferne**

Securiton Remote Service

Geschützter Zugriff

- Einrichtung, Adminstration und Verbindung von mobilen Endgeräten über https Verschlüsselung
- Sie definieren den Benutzerkreis und vergeben Zugriffsrechte
- Zusätzliche Absicherung durch die Freigabe in der BMZ vor Ort (je nach Tätigkeit)

Brandmelderzentrale

Lokale Verbindung

Dongle

Zugriff auf BMZ-Bedienfeld (VirtualMIC) über kundeneigene Netzwerkverbindung

SecuriFire MobileControl

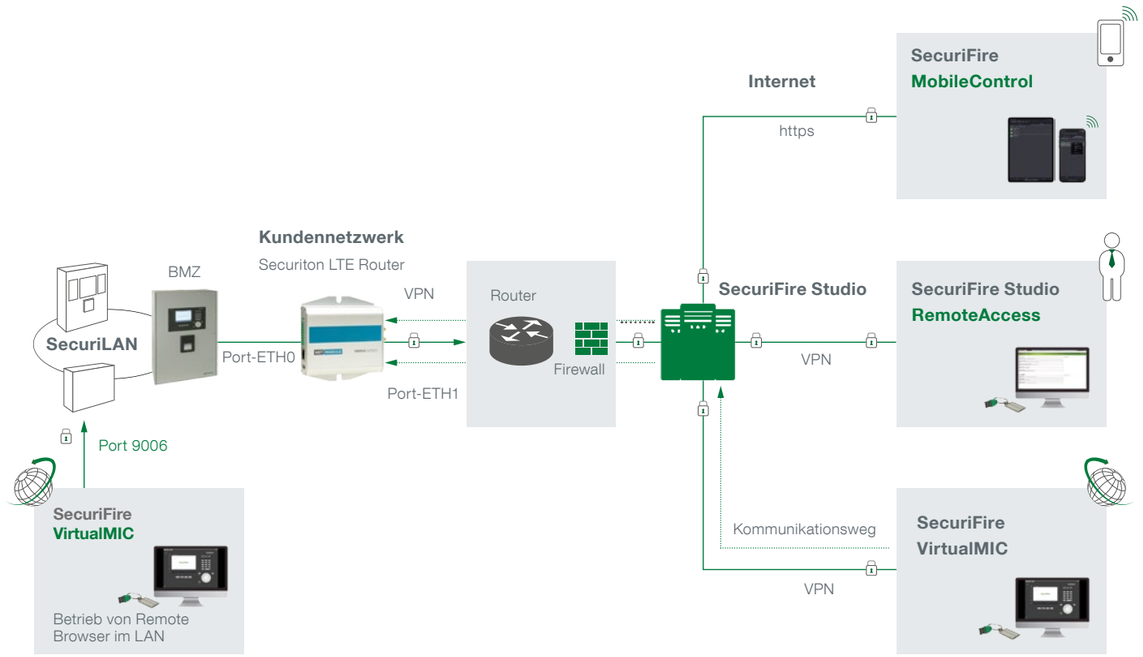
Laden im App Store

JETZT BEI Google Play

1) U. a. Brandschutzbeauftragte, Facility-Management, Werksfeuerwehren

BETREIBER-INFORMATION

Systemanforderungen für LAN-Router im Kundennetzwerk



Securiton Remote Dienst

Wie gewährleistet Securiton Deutschland einen sicheren Fernzugriff?

Der Remote Dienst (remote.securiton.de) zur Vermittlung von Datenströmen und Verwaltung von Benutzer- und Gerätedaten wird vollständig von Securiton Deutschland zur Verfügung gestellt, sodass kein Zugriff Dritter möglich ist. Die IP-Datenströme der Kunden werden transparent durchgeleitet – jeder Schritt unterliegt höchsten Sicherheitsanforderungen:

- **Einrichtung und Administration** des Remote Dienstes über das Internet für gesicherte bidirektionale Verbindungen zwischen sicherheitstechnischen Einrichtungen (z. B. Brandmelderzentrale) und unterschiedlichen User-Interfaces (z. B. Smartphone oder PC)
- 2048-Bit-verschlüsselte Anbindung der Brandmelderzentrale über speziell vorkonfigurierte Securiton **VPN-Router mit integrierter Firewall**
- Authentifizierung über **x509-Zertifikate** zur Sicherheit gegenüber dem Fremdnetz (Internet)
- Verbindungsaufbau erfolgt ausschließlich vom Router zum Remote Dienst: **ständig stehende und überwachte Verbindung** zu den sicherheitstechnischen Einrichtungen (z. B. Brandmelderzentrale)
- Verbindung von mobilen Endgeräten zum Remote Dienst über **https-Verschlüsselung**
- **Mehrstufiges, individuell abgestimmtes Sicherheitskonzept** (nach DIN VDE 0833-1) mit verschiedenen Identifizierungsschritten und –möglichkeiten
- **Zugriffsrechte** auf einen bestimmten Benutzerkreis eingrenzbar (über Benutzerverwaltung der Brandmelderzentrale)
  - Je Benutzer kann ein Passwort für den Zugriff und ein Code für die Bedienung vergeben werden
  - Je nach Tätigkeit ist vorab eine Freigabe an der BMZ vor Ort erforderlich
  - Aktivierung einer geografischen Zugriffs-Einschränkung (z. B. nur auf dem Betriebsgelände) möglich

Über welchen Server werden die Daten verwaltet?

Securiton Deuschland ist ein Unternehmen der Securitas Gruppe, Schweiz – eine familiengeführte Unternehmensgruppe, die seit 1907 im Dienste der Sicherheit tätig ist. Der Remote Dienst wird über unsere eigenen **georedundanten Rechenzentren** vertrieben und ist somit unabhängig von Fremdprovidern und Dienstleistern. Die Rechenzentren entsprechen der **aktuell höchsten Sicherheitsstufe Tier-4** und weisen damit eine **Höchstverfügbarkeit von 99,99 %** auf, was eine maximale Auswahllzeit von lediglich 0,8 Stunden pro Jahr bedeutet. Die SecuriCloud ist ISO27001 zertifiziert. Die Server werden nebst umfassender Sicherheitstechnik vor Ort, sogar vom eigenem **Sicherheitspersonal** der Securitas Gruppe Schweiz bewacht, um physische Manipulation oder Diebstahl zu verhindern.

Wie wird der Datenaustausch abgesichert?

Der **Router** bietet mit seiner **integrierten Firewall** und **regelmäßigen Sicherheitsupdates** Sicherheit gegenüber dem Fremdnetz (Internet). Der Datenaustausch zwischen Router und Cloud wird auf ein Minimum reduziert, um möglichst wenig Angriffsfläche zu bieten. Er wird zwischen Fremdnetz und dem internen Netzwerk mit der Brandmelderzentrale angeschlossen. Wird die Brandmelderzentrale im Kundennetzwerk betrieben, sind folgende Ports an der Firewall freizugeben:

Port	Zweck	Ziel
UDP Port 500/4500 (IPSec)	Betrieb VPN-Router im Kundennetzwerk	IP 185.161.103.206

Wie erfolgt die IP-Adressvergabe?

Die IP-Adresse für das interne Netzwerk aus Netzklasse C ist im Router bereits vorkonfiguriert, für die Brandmelderzentrale muss diese programmiert werden. Die IP-Adresse für den VPN-Tunnel aus Netzklasse A, mit der der Router später über den Fernzugriff angesprochen wird, ist im Router ebenfalls vorkonfiguriert. Für das Kundennetzwerk (Internetzugang) kann eine IP-Adresse aus Netzklasse B oder C vergeben werden, bei Nutzung einer Klasse C Adresse darf diese nicht identisch mit der IP-Adresse des internen Netzwerks sein. Nachfolgend ein Anwendungsbeispiel:

Geräte	Router-Ports	IP-Adressen intern
BMZ (TZ 1 bis 16)	ETH0 (LAN)	10.112.168.1 bis 10.112.168.16
Securiton LAN-Router		10.112.168.254 [1]
Kundennetzwerk	ETH4 (WAN)	DHCP Client (enabled)

[1] von Securiton Deutschland projektbezogen voreingestellt, diese dürfen bei Anwendung im Kundennetzwerk nicht anderweitig vergeben sein.

Welche Hard- und Softwarevoraussetzungen muss die SecuriFire Brandmelderzentrale erfüllen?

An den Securiton Remote Dienst können sämtliche Zentralen der Systemfamilie SecuriFire ab Hardware-Plattform ≥ B5/B6/B7 sowie Software-Version ≥ SRP 2.3 angebunden werden. Diese verfügen über eine LAN-Schnittstelle (Onboard oder eigene Baugruppe) sowie das Internet Protokoll (IP).

Besonders. Sicher.

SECURITON

Securiton Deutschland

Alarm- und Sicherheitssysteme
Unternehmenszentrale: Von-Drais-Straße 33 | 77855 Achern | DE
www.securiton.de | willkommen@securiton.de

Ein Unternehmen der Securitas Gruppe Schweiz

BMS Remote 03.24