EWS Anleitungen

Betriebs- und Bedienungsanleitungen zum Einbruchwarnsystem (EWS)

- Betriebsanleitung Ihrer Einbruchwarnsystem-Anlage

Betriebsanleitung Ihrer Einbruchwarnsystem-Anlage

Betriebsanleitung für das Einbruchwarnsystem (EWS) der dexa group

Anleitung Stand: 2.0
Software Stand: EWS-Broker 1.x auf Safe Fire House Plattform

Diese Anleitung richtet sich an Betreiber, Bediener und technisch Verantwortliche einer Einbruchwarnsystem-Anlage. Sie beschreibt den Aufbau der Anlage, die Inbetriebnahme, die vollständige Konfiguration, den täglichen Betrieb und das Verhalten im Alarmfall. Die abgebildeten Oberflächen stammen aus einer Musteranlage; Bezeichnungen, Kameraanzahl und Einstellungen Ihrer Anlage können abweichen.

---

1. Sicherheitshinweise

> **Wichtig:** Das Einbruchwarnsystem ist keine Einbruchmeldeanlage im Sinne der DIN VDE 0833-3 und ersetzt keine behördlich oder versicherungsseitig geforderte Einbruchmeldeanlage. Es dient der Früherkennung unberechtigten Zutritts und der schnellen Alarmierung mit Bildbeweis.

- Betreiben Sie die Anlage nur in dem Zustand, der bei der Abnahme dokumentiert wurde. Änderungen an Kameras, Switch, Zentrale und Netzwerk sind ausschließlich durch die Dexa Solutions GmbH oder in Abstimmung mit ihr vorzunehmen.
- Das Einbruchwarnsystem verarbeitet personenbezogene Daten in Form von Bildaufnahmen. Der Betreiber ist verantwortlich für die datenschutzrechtliche Zulässigkeit, insbesondere für die Hinweisbeschilderung und die Information von Personal und Besuchern. Näheres in Kapitel 14.
- Bewahren Sie PINs und NFC-Token sicher auf und geben Sie sie nicht an Dritte weiter. Nach drei Fehlversuchen wird der jeweilige Benutzer für fünf Minuten gesperrt.
- Eine scharfe Anlage löst bei erkannten Personen Sirene und Strahler aus, sofern kein stiller Alarm konfiguriert ist. Betreten Sie den überwachten Bereich nur nach dem Unscharfschalten.
- Arbeiten an Kameras, Switch oder Netzwerk führen Sie ausschließlich im Wartungsmodus oder bei unscharfer Anlage durch.
- Bei kombiniertem Betrieb mit dem Brandwarnsystem Safe Fire House hat ein Brandalarm stets Vorrang vor einem Einbruchalarm.

---

2. Systemübersicht

2.1 Grundlegende Beschreibung

Das Einbruchwarnsystem überwacht Außen- und Innenbereiche von Gebäuden über IP-Kameras mit eingebauter KI-Personenerkennung. Die Kameras klassifizieren selbstständig, ob eine erkannte Bewegung von einem Menschen stammt. Tiere, Fahrzeuge, Schatten, Regen und Insekten lösen keinen Alarm aus.

Erkennt eine Kamera eine Person im überwachten Bereich, startet die Alarmkette: Nach einer einstellbaren Voralarmzeit werden Sirene und Strahler aktiviert, ein Beweisbild gespeichert und alle konfigurierten Alarmschnittstellen benachrichtigt. Empfänger sehen das Beweisbild über einen zeitlich begrenzten Link ohne Anmeldung und können den Alarm quittieren.

Das Einbruchwarnsystem läuft auf derselben Zentrale wie das Brandwarnsystem Safe Fire House. Beide Systeme können gemeinsam auf einer Anlage betrieben werden und nutzen dieselbe Weboberfläche, dasselbe Bediengerät und dieselben Alarmschnittstellen.

2.2 Datenschutzprinzip: Kameras stromlos im Ruhezustand

Im **unscharfen Zustand sind alle Kameras physisch vom Strom getrennt**. Die Kameras werden über Power over Ethernet (PoE) versorgt; die Zentrale schaltet die betreffenden Ports am Switch ab. In diesem Zustand gibt es kein Bild, keinen Stream und keine Aufzeichnung.

Erst beim Scharfschalten werden die Ports aktiviert. Die Kameras starten, werden von der Zentrale neu konfiguriert und beginnen mit der Überwachung. Beim Unscharfschalten werden sie wieder stromlos.

Damit ist im Normalbetrieb – Personal anwesend, Anlage unscharf – eine Überwachung technisch ausgeschlossen, nicht nur per Software abgeschaltet. Zugleich lässt sich an stromlosen Kameras nichts manipulieren; beim Scharfschalten werden die Erkennungsfunktionen ohnehin frisch konfiguriert.

2.3 Anlagenzustände

Zustand	Anzeige	Bedeutung
Unscharf	grün	Kameras stromlos, keine Überwachung. Normalzustand bei Anwesenheit.
Scharfschaltung	blau	Verzögerung läuft (Standard 180 Sekunden). Zeit, das Gebäude zu verlassen. Kameras starten.
Scharf	rot	Kameras aktiv, Überwachung läuft. Erkannte Personen lösen die Alarmkette aus.
Voralarm	rot, Signalton	Eine Kamera hat eine Person erkannt. Berechtigte können den Alarm noch per PIN unterdrücken.
Alarm	rot, Vollbild	Sirene, Strahler und Alarmschnittstellen sind aktiv.
Wartungsmodus	–	Kameras eingeschaltet, Erkennung blockiert. Nur für Justage und Konfiguration.

Der aktuelle Zustand wird in der Kopfzeile jeder Ansicht angezeigt, beispielsweise **EINBRUCHWARNSYSTEM SCHARF**. Ist ein Bediengerät mit LED-Leiste installiert, leuchtet diese im scharfen Zustand rot und im unscharfen Zustand grün.

2.4 Ablauf beim Scharfschalten (technisch)

1. Berechtigung des Benutzers wird geprüft (PIN oder NFC, Rolle).
2. Die Scharfschalt-Verzögerung läuft mit Signaltönen am Bediengerät.
3. Nach Ablauf schaltet die Zentrale die Kameraports am Switch ein.
4. Die Zentrale wartet, bis jede Kamera erreichbar ist (Zeitüberschreitung 90 Sekunden).
5. Für jede Kamera werden Szenenprofil, Erkennungsfunktionen und die Meldeadresse zur Zentrale geprüft und angewendet.
6. Die Anlage meldet **scharf**. Ab jetzt lösen erkannte Personen die Alarmkette aus.

Wird eine Kamera in Schritt 4 nicht erreichbar, bricht die Scharfschaltung mit einer Fehlermeldung ab. Die übrigen Kameras werden wieder stromlos geschaltet.

---

3. Komponenten

3.1 Übersicht

Komponente	Bezeichnung	Funktion
Zentrale	DXO-SFH-CU-B-02 (Standard) oder DXO-SFH-CU-P-01 (Pro)	Steuerung, Auswertung, Alarmschnittstellen, Weboberfläche
KI-Kamera	DXO-IDS-CM-XX-01	8-Megapixel-Netzwerkkamera mit Personenerkennung, Infrarot-Nachtsicht und Weißlicht-Strahler
Kamerasockel	DXO-IDS-CM-XX-01-EC	Anschlussgehäuse zur Wand- oder Deckenmontage
PoE-Switch klein	***REDACTED*** hEX PoE	Bis zu 5 Kameras; kompakte Bauform für einzelne Gebäude
PoE-Switch groß	***REDACTED*** CRS328-24P-4S+RM	Bis zu 15 Kameras; 19-Zoll-Rack, 500 Watt PoE-Leistung, für größere Liegenschaften
Bediengerät	DXO-SFH-DP-F-01 (Aufbau) oder DXO-SFH-DP-B-01 (Einbau)	Touchdisplay zur Anzeige und Bedienung, NFC-Leser, LED-Leiste
Alarmsirene	DXO-SFH-AS-XX-01	Optische und akustische Alarmierung bis 100 dB, für den Außenbereich geeignet
Schaltkontakt	DXO-SFH-SC-1-01 (1-fach) oder DXO-SFH-SC-4-01 (4-fach)	Potenzialfreier Kontakt zur Ansteuerung von Türöffnern, Schließanlagen, Toren oder Beleuchtung
Lizenz	DXO-IDS-LIC-ID-16	Freischaltung des Einbruchwarnsystems, gestaffelt nach Kameraanzahl

3.2 Zentrale

Die Zentrale betreibt den EWS-Dienst, die Streaming- und Korrelationslogik sowie die Alarmschnittstellen. Sie steuert den Switch, empfängt die Ereignisse der Kameras, speichert Beweisbilder und stellt die Weboberfläche bereit. Die Standard-Zentrale wird an der Wand montiert und über PoE versorgt; die Pro-Zentrale ist ein 19-Zoll-Server mit unterbrechungsfreier Stromversorgung für Multistandort-Installationen.

3.3 KI-Kamera

Die Kameras erkennen Personen direkt im Gerät. Erkennungsarten sind:

Erkennung	Beschreibung
Bereichserkennung	Eine Person betritt eine definierte Fläche im Bild
Linienüberschreitung	Eine Person überschreitet eine definierte Linie in eine oder beide Richtungen
Zonen-Eintritt und -Austritt	Eine Person betritt oder verlässt eine definierte Zone
Manipulationserkennung	Kamera wird verdeckt, verdreht oder das Bild verändert sich grundlegend

Die Erkennungsbereiche werden bei der Inbetriebnahme je Kamera festgelegt. Tag-, Dämmerungs- und Nachtprofil werden automatisch nach Sonnenstand umgeschaltet; je Profil sind Belichtung, Gegenlichtkompensation und Infrarot-Beleuchtung hinterlegt.

Pro Kamera lässt sich einstellen, ob im Alarmfall Weißlicht-Strahler und Sirene ausgelöst werden oder ob ein **stiller Alarm** erfolgt, bei dem ausschließlich die Alarmschnittstellen benachrichtigt werden. Der Strahler dient zugleich der Abschreckung und der Ausleuchtung des Beweisbilds.

3.4 PoE-Switch

Der Switch wird in zwei Varianten ausgeliefert:

Variante	Modell	Kameras	Bauform	Einsatz
klein	***REDACTED*** hEX PoE	bis zu 5	kompakt, Wand- oder Hutschienenmontage	Feuerwehrhaus, Gerätehaus, einzelnes Gebäude
groß	***REDACTED*** CRS328-24P-4S+RM	bis zu 15	19-Zoll, 1 Höheneinheit, 500 Watt PoE-Leistung	Liegenschaften mit mehreren Gebäuden, Bauhöfe, Rechenzentrumsumgebung

Beide Varianten werden ab Werk mit der dexa-Konfiguration ausgeliefert und verhalten sich gegenüber der Zentrale identisch. Die Wahl richtet sich nach der Anzahl der Kameras und den Gegebenheiten am Standort; ein späterer Wechsel von klein auf groß ist möglich.

Der Switch ist das zentrale Bindeglied. Er versorgt Kameras, Bediengerät und gegebenenfalls Zentrale mit Strom und Netzwerk. Die Zentrale schaltet die Kameraports beim Scharf- und Unscharfschalten ein und aus. Über die Adresstabelle des Switches erkennt die Zentrale außerdem, ob am Kameraport ein fremdes Gerät angeschlossen oder die Verkabelung verändert wurde (Port-Mismatch-Erkennung).

Die Zuordnung Kamera ? Switch-Port wird bei der Inbetriebnahme festgelegt und darf danach nicht mehr verändert werden.

3.5 Bediengerät

Das Bediengerät ist ein Touchdisplay mit integriertem NFC-Leser und seitlicher LED-Leiste. Es zeigt dauerhaft den Anlagenzustand und dient zum Scharf- und Unscharfschalten per PIN oder NFC-Token. Es wird über das Netzwerkkabel mit Strom versorgt und läuft im Kiosk-Modus, das heißt, es zeigt ausschließlich die Oberfläche der Anlage.

In Kombination mit dem Schaltkontakt übernimmt das Bediengerät zusätzlich die Türfreigabe: Beim Unscharfschalten öffnet die Tür, beim Scharfschalten wird verriegelt.

3.6 Alarmsirene

Die Sirene signalisiert Einbruchalarme optisch über LED und akustisch mit bis zu 100 dB. Sie ist für den Außenbereich geeignet, wird über eine Solarzelle mit Pufferakku versorgt und bei Bedarf über einen Micro-USB-Port nachgeladen; die Anbindung erfolgt per Funk. Bei stillem Alarm bleibt sie stumm.

---

4. Planung

4.1 Zu überwachende Bereiche

Legen Sie vor der Installation fest, welche Bereiche überwacht werden sollen und welche ausdrücklich nicht. Typische Bereiche sind Fahrzeughallen, Lagerräume, Zugänge, Hofflächen und Stellplätze. Öffentlicher Raum, Nachbargrundstücke und Bereiche, in denen sich Personen berechtigt aufhalten, während die Anlage scharf ist, dürfen nicht im Erkennungsbereich liegen.

Je Kamera wird ein Erkennungsbereich definiert. Nur Personen in diesem Bereich lösen einen Alarm aus; der übrige Bildausschnitt wird ignoriert.

4.2 Kamerapositionen

- Montagehöhe 2,5 bis 4 Meter, Blickrichtung leicht nach unten
- Personen sollen den Erkennungsbereich frontal oder seitlich durchqueren, nicht direkt auf die Kamera zulaufen
- Keine direkte Sicht auf starke Lichtquellen (Sonne, Scheinwerfer, Leuchtreklame)
- Keine bewegten Objekte im Bereich (Fahnen, Äste, Vorhänge)
- Der Weißlicht-Strahler soll den Erkennungsbereich ausleuchten können
- Ein Bereich sollte von zwei Kameras erfasst werden, wenn eine Bestätigung durch Mehrfacherkennung gewünscht ist

4.3 Netzwerkanforderungen

Anforderung	Wert
Netzwerkanschluss	Ein freier RJ45-Anschluss für den Switch am Standort
Internetzugang	Ausgehende HTTPS-Verbindungen für Alarmschnittstellen; keine eingehenden Verbindungen erforderlich
Adressvergabe	DHCP im Standortnetz oder feste Adressen in Abstimmung mit Ihrer IT
Verkabelung	Cat.5e oder besser, maximal 100 Meter je Strecke
Switch-Variante	Bis zu 5 Kameras: Switch klein (hEX PoE). Bis zu 15 Kameras: Switch groß (CRS328, 19-Zoll, 500 Watt). Die Variante wird bei der Planung festgelegt
PoE-Leistung	Etwa 12 Watt je Kamera, etwa 15 Watt für das Bediengerät; das Leistungsbudget wird bei der Planung gegen die Switch-Variante geprüft
Zeitsynchronisation	NTP über das Internet oder einen lokalen Zeitserver

Kameras, Bediengerät und Zentrale müssen im selben Netzsegment liegen oder erreichbar geroutet sein. Eine Trennung der Kameras in ein eigenes Netzsegment ist möglich und empfohlen.

4.4 Stromversorgung

Zentrale, Kameras und Bediengerät werden über PoE versorgt. Der Switch benötigt einen 230-V-Anschluss; die große Variante wird im 19-Zoll-Rack montiert und sollte an einer unterbrechungsfreien Stromversorgung hängen. Für Multistandort-Installationen und die Pro-Zentrale ist eine unterbrechungsfreie Stromversorgung enthalten beziehungsweise vorzusehen.

4.5 Alarmierungswege

Klären Sie vor der Inbetriebnahme, welche Alarmschnittstellen genutzt werden und wer im Alarmfall benachrichtigt wird. Für DIVERA 24/7, Alamos und GroupAlarm benötigen wir die Zugangsdaten beziehungsweise Schlüssel Ihres Kontos; für E-Mail den Postausgangsserver oder die Freigabe unseres Versandservers.

---

5. Montage und Verkabelung

5.1 Zentrale

Die Standard-Zentrale wird an der Wand in einem trockenen Innenraum montiert, vorzugsweise im Technik- oder Netzwerkraum. Sie wird über ein Netzwerkkabel mit dem Switch verbunden und darüber versorgt. Die Pro-Zentrale wird im 19-Zoll-Rack eingebaut.

5.2 Switch

Der Switch wird nahe der Zentrale montiert und an das Standortnetz angeschlossen (Uplink). Die Kameraports werden fest zugewiesen und beschriftet.

Switch klein (hEX PoE): kompaktes Gehäuse, Montage an der Wand oder auf einer Hutschiene im Netzwerk- oder Technikschrank. Bis zu 5 Kameras.

Switch groß (CRS328-24P-4S+RM): 19-Zoll-Gehäuse mit einer Höheneinheit, Einbau in ein Rack. Bis zu 15 Kameras; die übrigen Ports stehen für Bediengerät, Zentrale und weitere Komponenten zur Verfügung.

Die konkrete Portbelegung Ihrer Anlage steht in der Anlagendokumentation, die Sie bei der Abnahme erhalten. Beispiel:

Port	Gerät
Uplink	Standortnetz
Port A	Zentrale
Port B	Bediengerät
Port C bis …	Kamera 1 bis Kamera n

> **Wichtig:** Die Portbelegung ist Bestandteil der Anlagenkonfiguration. Kameras dürfen nach der Inbetriebnahme nicht umgesteckt werden. Die Anlage erkennt Abweichungen und meldet sie als Störung.

5.3 Kameras

1. Kamerasockel an der geplanten Position montieren; Netzwerkkabel durch den Sockel führen.
2. Kamera auf den Sockel setzen und Netzwerkkabel anschließen.
3. Kamera grob auf den Erkennungsbereich ausrichten. Die Feinjustage erfolgt bei der Inbetriebnahme mit Live-Bild.
4. Netzwerkkabel am zugewiesenen Switch-Port anschließen und Port beschriften.

Die Kameras sind für den Außenbereich geeignet. Achten Sie auf tropfwassergeschützte Kabelführung und ziehen Sie die Sockelverschraubung erst nach der Feinjustage fest.

5.4 Bediengerät

Das Bediengerät wird im Eingangsbereich montiert, so dass es beim Betreten und Verlassen des Gebäudes erreichbar ist. Es wird über ein Netzwerkkabel am Switch angeschlossen und darüber versorgt. Die Aufbauvariante wird an der Wand oder auf einem Tischständer montiert, die Einbauvariante in ein Wandpanel oder einen Schaltschrank.

5.5 Sirene

Die Sirene wird an einer von außen sichtbaren, schwer erreichbaren Stelle montiert, beispielsweise an der Fassade unter dem Dachüberstand. Bei Solarbetrieb ist eine Ausrichtung mit Tageslicht erforderlich. Die

Funkanbindung an die Zentrale wird bei der Inbetriebnahme eingemessen.

5.6 Schaltkontakt

Der Schaltkontakt wird in der Nähe des anzusteuernden Geräts montiert und über PoE versorgt. Der potenzialfreie Kontakt wird gemäß den Vorgaben des jeweiligen Türöffners, Motorschlosses oder Tores angeschlossen. Der elektrische Anschluss erfolgt durch eine Elektrofachkraft.

---

6. Inbetriebnahme

Die Inbetriebnahme erfolgt durch die Dexa Solutions GmbH oder in ihrer Anleitung. Die folgenden Schritte beschreiben den vollständigen Ablauf, damit Sie den Aufbau nachvollziehen und einzelne Schritte, beispielsweise das Anlegen von Benutzern, selbst durchführen können.

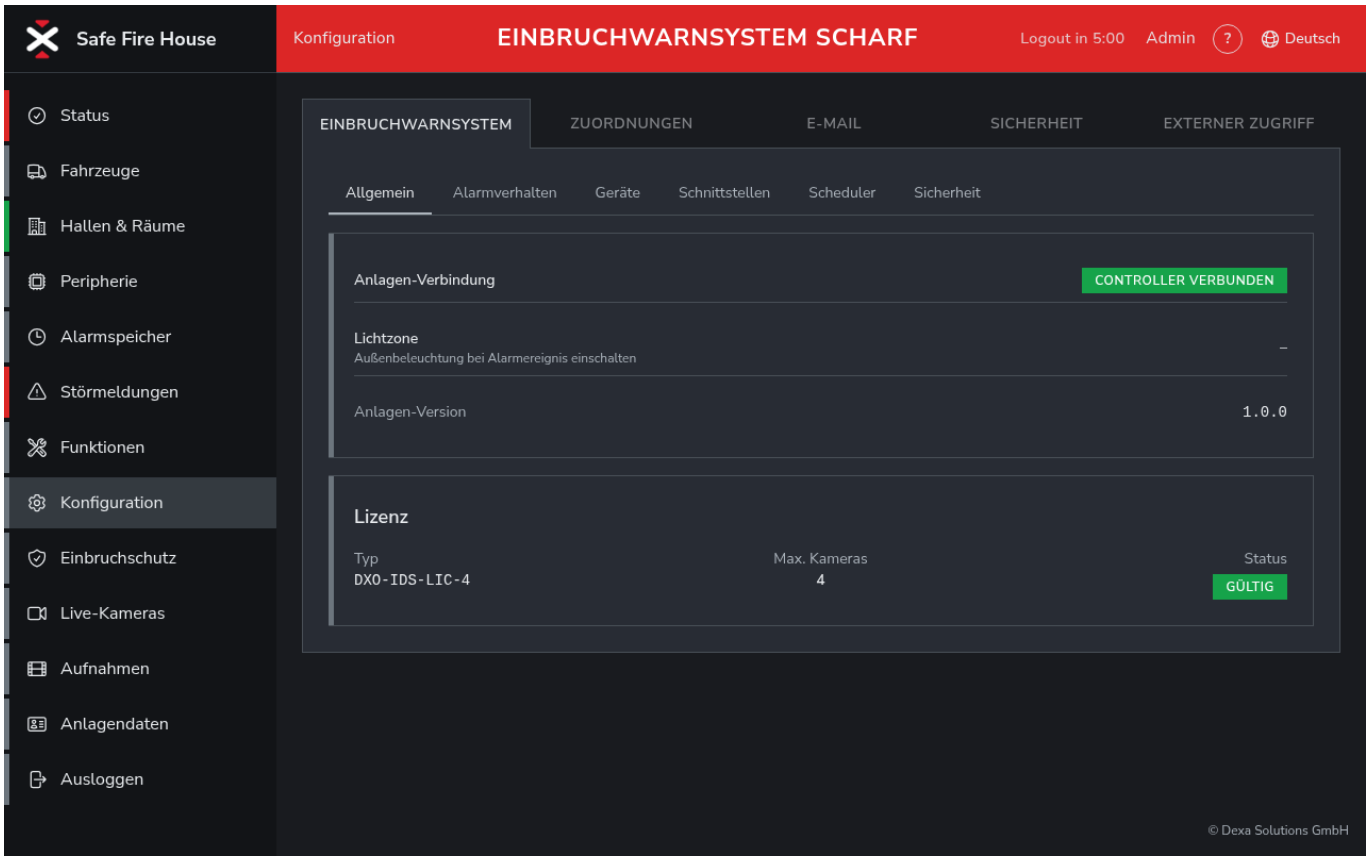
6.1 Ablauf im Überblick

1. Lizenz einspielen und Anlagen-Verbindung prüfen
2. Switch einrichten und Ports zuordnen
3. Kameras einbinden (One-Click-Konfiguration)
4. Erkennungsbereiche und Szenenprofile je Kamera festlegen
5. Alarmverhalten einstellen
6. Alarmschnittstellen einrichten und testen
7. Benutzer, Rollen und NFC-Token anlegen
8. Bediengerät einrichten
9. Türsteuerung einrichten (optional)
10. Abnahme mit Testalarm und Übergabe

6.2 Lizenz und Anlagen-Verbindung

Das Einbruchwarnsystem ist ein lizenzpflichtiges Modul. Die Lizenz ist an die Hardware der Zentrale gebunden und legt die maximale Kameraanzahl fest. Ohne gültige Lizenz startet der EWS-Dienst nicht.

Den Lizenzstatus sehen Sie unter **Konfiguration ? Einbruchwarnsystem ? Allgemein**: Lizenztyp, maximale Kameraanzahl und Status **GÜLTIG**. Dort wird auch die **Anlagen-Verbindung** angezeigt; **CONTROLLER VERBUNDEN** bestätigt, dass der EWS-Dienst läuft und mit der Zentrale kommuniziert.



Die Lizenzdatei wird bei der Inbetriebnahme durch die Dexa Solutions GmbH eingespielt. Bei einem Tausch der Zentrale ist eine neue Lizenz erforderlich.

6.3 Switch einrichten

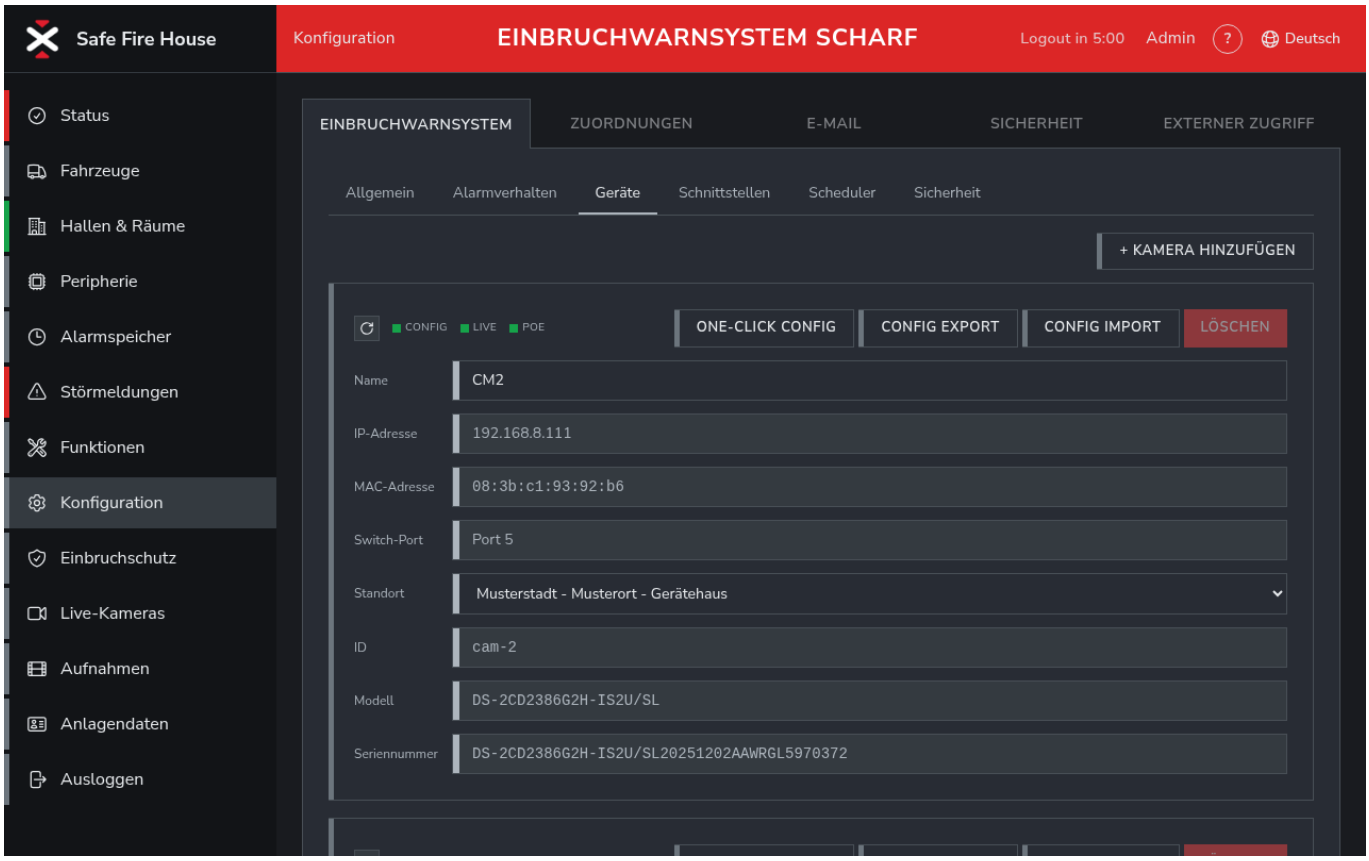
Der Switch wird über einen Einrichtungsassistenten eingebunden:

1. **Switch suchen** – die Zentrale sucht im Netzwerk nach dem Switch und zeigt Adresse, Bezeichnung und Hardwareadresse an.
2. **Bestätigen** – prüfen, ob es der richtige Switch ist.
3. **Zugangsdaten** – Benutzer und Passwort des Switches eintragen und die Verbindung testen.
4. **Portzuordnung** – festlegen, an welchem Port welche Kamera angeschlossen ist.
5. **Speichern** – der Switch ist registriert.

Die Zentrale prüft die Verbindung zum Switch fortlaufend. Bei Ausfall wird eine Störung gemeldet; ein Scharfschalten ist dann nicht möglich, da die Kameras nicht eingeschaltet werden könnten.

6.4 Kameras einbinden

Kameras werden unter **Konfiguration ? Einbruchwarnsystem ? Geräte** verwaltet.



Neue Kamera hinzufügen:

1. Kamera am zugewiesenen Switch-Port anschließen und die Anlage in den **Wartungsmodus** versetzen, damit der Port bestromt wird.
2. **+ KAMERA HINZUFÜGEN** wählen. Die Zentrale sucht im Netzwerk nach neuen Kameras und listet sie mit Modell und Seriennummer auf.
3. Die gewünschte Kamera auswählen und **ONE-CLICK CONFIG** ausführen. Die Zentrale richtet die Kamera vollständig ein:
    - Vergabe des Kamerapasswords (wird verschlüsselt in der Zentrale hinterlegt)
    - Aktivierung der Erkennungsfunktionen und der Manipulationserkennung
    - Eintragen der Meldeadresse, an die die Kamera Ereignisse sendet
    - Anwenden des Szenenprofils
    - Bindung an den Switch-Port
4. Der Kamera einen sprechenden Namen und einen Standort zuweisen, beispielsweise „Fahrzeughalle Tor 1".

Die Kamera erscheint anschließend in der Liste mit Name, IP-Adresse, Switch-Port, Standort, Modell und Seriennummer. Die Spalte **Konfiguriert** zeigt, dass die Einrichtung vollständig ist.

Funktionen je Kamera:

Schaltfläche	Funktion
CONFIG	Konfigurationsstand der Kamera anzeigen und mit dem Soll abgleichen
LIVE	Live-Bild der Kamera anzeigen (nur bei bestromter Kamera)

Schaltfläche	Funktion
POE	Stromversorgung des Kameraports schalten, zum Beispiel für einen Neustart
ONE-CLICK CONFIG	Konfiguration erneut vollständig anwenden, zum Beispiel nach einem Kameratausch
CONFIG EXPORT / IMPORT	Kamerakonfiguration sichern und wiederherstellen
LÖSCHEN	Kamera aus der Anlage entfernen

> **Hinweis:** Kameras sollten ausschließlich in Abstimmung mit der Dexa Solutions GmbH hinzugefügt, getauscht oder entfernt werden. Bei einem Tausch wird die Portbindung geprüft, die Konfiguration neu angewendet und der Erkennungsbereich neu eingemessen.

6.5 Erkennungsbereiche und Szenenprofile

Nach der Einbindung wird je Kamera der Erkennungsbereich festgelegt. Dazu wird die Anlage in den Wartungsmodus versetzt, das Live-Bild geöffnet und der Bereich im Bild eingezeichnet, in dem Personen einen Alarm auslösen sollen. Zusätzlich können Linien definiert werden, deren Überschreiten einen Alarm auslöst, beispielsweise entlang einer Grundstücksgrenze oder eines Tores.

Je Kamera wird ein **Szenenprofil** gewählt, das zur Umgebung passt:

Profil	Einsatz
Fahrzeughalle	Innenräume mit Kunstlicht, hohe Kontraste durch Tore
Außenbereich	Hof, Stellplätze, Fassaden; wechselndes Tageslicht
Flur	Innenräume mit gleichmäßigem Licht, kurze Distanzen

Jedes Profil enthält Einstellungen für Tag, Dämmerung und Nacht (Belichtung, Gegenlichtkompensation, Infrarot-Beleuchtung). Die Umschaltung erfolgt automatisch nach Sonnenstand, siehe Kapitel 11.5.

Abschließend wird die Erkennung geprüft: Eine Person durchquert im Wartungsmodus den Erkennungsbereich, die Zentrale zeigt das Ereignis an. Personen außerhalb des Bereichs dürfen kein Ereignis erzeugen.

6.6 Bediengerät einrichten

Das Bediengerät wird per PoE am Switch angeschlossen und bezieht seine Adresse automatisch. Es startet im Kiosk-Modus direkt mit der Oberfläche der Anlage. Bei der Inbetriebnahme werden hinterlegt:

- die Adresse der Zentrale als Startseite
- die Freigabe des NFC-Lesers für die Anmeldung
- die Verbindung zur LED-Leiste, damit der Anlagenzustand farbig angezeigt wird

Prüfung: Ein Testscan mit einem NFC-Token wird in der Oberfläche erkannt; beim Scharfschalten leuchtet die LED-Leiste rot, beim Unscharfschalten grün.

6.7 Abnahme

Die Inbetriebnahme endet mit einer dokumentierten Abnahme:

1. Alle Kameras werden als erreichbar und konfiguriert angezeigt.
2. Scharfschalten mit Verzögerung; alle Kameras kommen innerhalb von 90 Sekunden online.

3. Testperson durchquert jeden Erkennungsbereich; jede Kamera löst aus.
4. Voralarm wird per PIN unterdrückt – Prüfung der Unterdrückung.
5. Voralarm läuft ab – Prüfung von Sirene, Strahler, Beweisbild, Alarmschnittstellen und Beweisbild-Link.
6. Quittierung am Bediengerät und über eine Schnittstelle.
7. Unscharfschalten per PIN und per NFC; Kameras werden stromlos.
8. Türsteuerung: Tür öffnet beim Unscharfschalten, verriegelt beim Scharfschalten (sofern eingerichtet).
9. Übergabe der Anlagendokumentation mit Portbelegung, Kameraliste, Erkennungsbereichen, Benutzerliste und Schnittstellenkonfiguration.

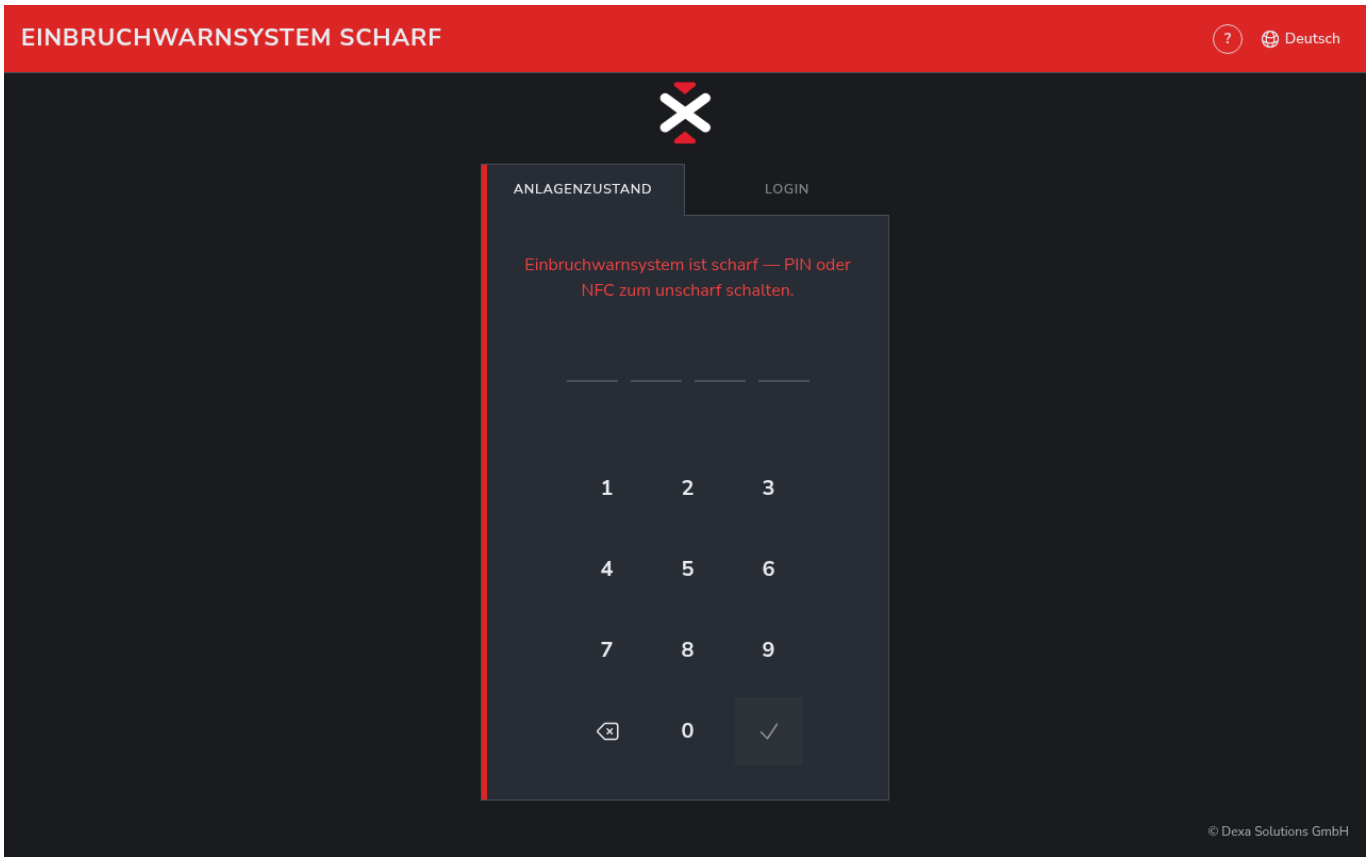
Sie erhalten die Projektdokumentation im Anschluss per E-Mail.

---

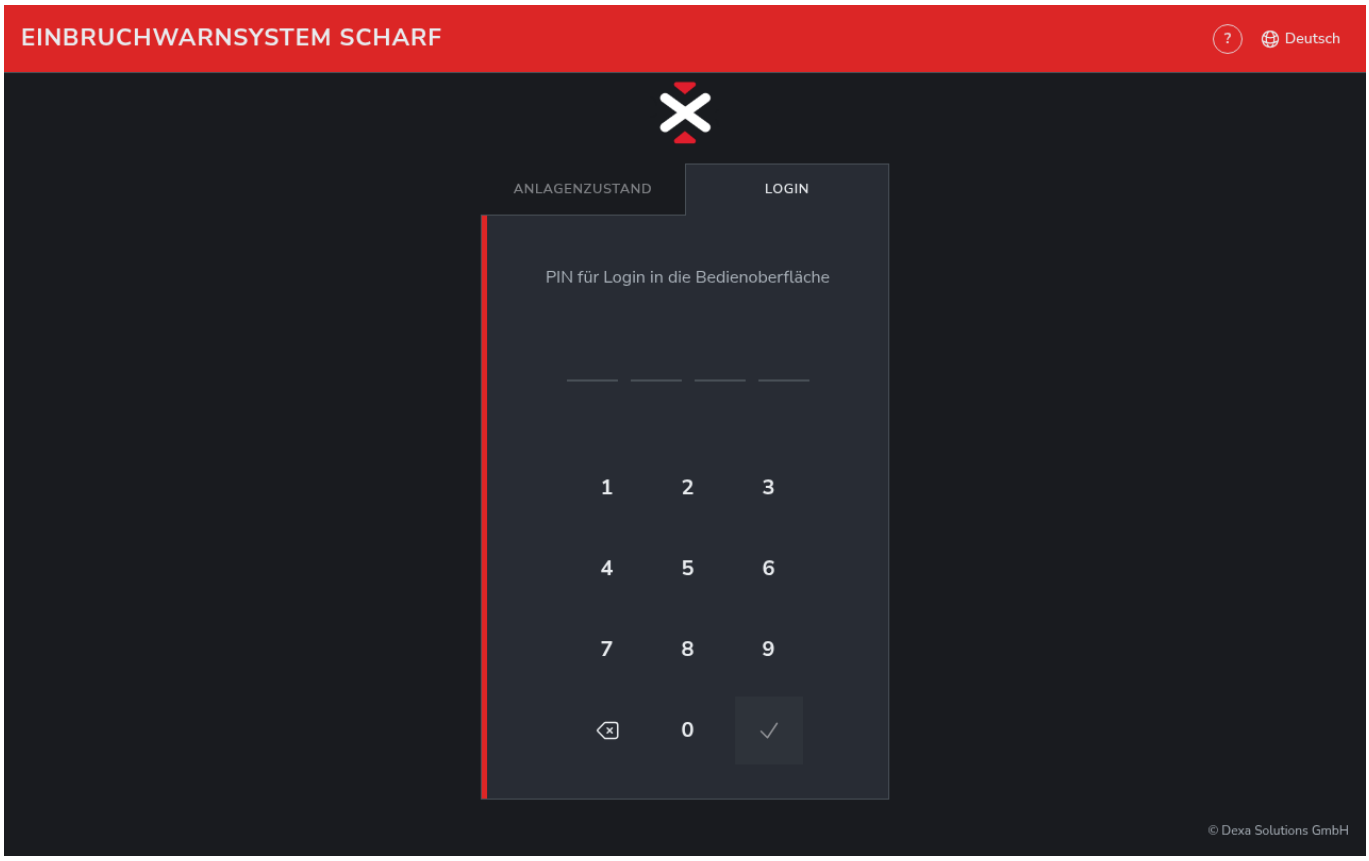
7. Anmelden und Benutzerrollen

7.1 Anmelden am Bediengerät

Das Bediengerät zeigt im Ruhezustand die Ansicht **Anlagenzustand**. Sie sehen den aktuellen Zustand der Anlage und den Ziffernblock. Von hier aus schalten Sie die Anlage scharf oder unscharf.



Für alle weiteren Funktionen – Live-Ansicht, Aufnahmen, Alarmspeicher, Konfiguration – melden Sie sich über den Reiter **LOGIN** an.



Anmeldung per PIN: Tippen Sie Ihre vierstellige persönliche PIN auf dem Ziffernblock ein. Nach der vierten Ziffer werden Sie automatisch angemeldet.

Anmeldung per NFC: Halten Sie Ihren NFC-Token an den Leser des Bediengeräts. Bei gültigem Token werden Sie sofort angemeldet.

Nach erfolgreicher Anmeldung öffnet sich die Ansicht **Status**. Nach fünf Minuten ohne Eingabe werden Sie automatisch abgemeldet; die verbleibende Zeit wird in der Kopfzeile angezeigt. Über **Ausloggen** in der Navigation melden Sie sich sofort ab.

> **Hinweis:** Nach drei falschen PIN-Eingaben wird der Benutzer für fünf Minuten gesperrt. Warten Sie die Sperrzeit ab, bevor Sie es erneut versuchen.

7.2 Anmelden von einem anderen Gerät

Die Oberfläche erreichen Sie auch von einem PC, Tablet oder Smartphone im Standortnetz über die Adresse der Zentrale. Die Anmeldung erfolgt ebenfalls per PIN. Für den Zugriff von außerhalb des Standortnetzes sprechen Sie uns an; er wird über eine gesicherte Verbindung eingerichtet.

7.3 Benutzerrollen

Rolle	Berechtigung
Benutzer	Anlage scharf- und unscharfschalten, Voralarm unterdrücken, Alarme quittieren, Live-Ansicht und Aufnahmen einsehen
Verwalter	zusätzlich: Alarmverhalten, Schnittstellen, Benutzer, Rollen und NFC-Token verwalten, Wartungsmodus
REDACTED	Vollzugriff einschließlich Kamera-, Switch- und Systemkonfiguration

Jeder Benutzer hat eine eigene vierstellige PIN und kann bis zu fünf NFC-Token zugewiesen bekommen. Rollen und ihre Rechte können unter **Konfiguration ? Sicherheit ? Rollenverwaltung** angepasst werden.

8. Scharf- und Unscharfschalten

8.1 Scharfschalten

1. Stellen Sie sicher, dass sich keine Personen mehr im überwachten Bereich aufhalten.
2. Melden Sie sich am Bediengerät per PIN oder NFC an.
3. Tippen Sie auf **Anlage scharfschalten** und bestätigen Sie den Dialog.
4. Die Verzögerung startet. Ein Banner zeigt die verbleibende Zeit an (Standard 180 Sekunden). Verlassen Sie in dieser Zeit das Gebäude. Über **Abbrechen** stoppen Sie den Vorgang jederzeit.
5. Nach Ablauf der Verzögerung ist die Anlage **scharf**. Die Kameras werden mit Strom versorgt, starten und beginnen mit der Überwachung.

> **Hinweis:** Nach Ablauf der Verzögerung benötigen die Kameras etwa 30 bis 60 Sekunden, bis sie vollständig betriebsbereit sind. Erst dann werden Personen erkannt.

Ist ein Schaltkontakt zur Türsteuerung eingerichtet, wird die Tür beim Scharfschalten verriegelt.

8.2 Unscharfschalten

Die Anlage kann auf drei Wegen unscharf geschaltet werden:

Methode	Vorgehen
NFC-Token	Token an den Leser halten und den Dialog mit **Unscharf** bestätigen
PIN	Persönliche PIN auf dem Ziffernblock der Ansicht Anlagenzustand eingeben
PIN + Anlagen-PIN	Wenn vom Verwalter aktiviert: nach der persönlichen PIN zusätzlich die Anlagen-PIN eingeben

Beim Unscharfschalten werden die Kameras sofort stromlos geschaltet. Ist ein Schaltkontakt eingerichtet, wird die Tür freigegeben.

Die zusätzliche Anlagen-PIN ist eine optionale zweite Sicherheitsstufe, beispielsweise wenn viele Personen Zugang zum Bediengerät haben.

8.3 Scharfschaltung schlägt fehl

Kann eine Kamera nach dem Einschalten nicht erreicht werden, bricht die Scharfschaltung ab und die Anlage meldet die betroffene Kamera. Prüfen Sie in der Ansicht **Einbruchschutz**, welche Kamera fehlt, und kontrollieren Sie Netzwerkkabel und Switch-Port. Lässt sich die Störung nicht beheben, eröffnen Sie ein Serviceticket. Ein Scharfschalten mit fehlender Kamera ist nicht vorgesehen, damit keine unbemerkte Überwachungslücke entsteht.

9. Verhalten im Alarmfall

9.1 Ablauf der Alarmkette

```
1  ERKENNUNG       Kamera erkennt Person im Erkennungsbereich
                 ↓
2  VORALARM        Zeitfenster (Standard 30 Sekunden), in dem ein
berechtigter
                Benutzer den Alarm per PIN unterdrücken kann
                 ↓
3  ALARM           Beweisbild wird gespeichert
                Sirene und Strahler (außer bei stillem Alarm)
                Vollbildanzeige auf allen Bediengeräten
                Mehrfacherkennung durch weitere Kameras wird
zusammengefasst
                 ↓
4  BENACHRICHTIGUNG  Alle aktiven Alarmschnittstellen werden gleichzeitig
                angesprochen, mit Beweisbild oder Link zum Beweisbild
                 ↓
5  QUITTIERUNG     Bestätigung am Bediengerät oder über eine Schnittstelle;
                wird an alle unterstützenden Schnittstellen weitergegeben
```

9.2 Voralarm

Im Voralarm piept das Bediengerät und die auslösende Kamera wird rot dargestellt. Wenn Sie den Alarm selbst ausgelöst haben – beispielsweise weil Sie bei scharfer Anlage durch den Erfassungsbereich gegangen sind – geben Sie im Voralarm-Dialog Ihre PIN ein. Der Alarm wird unterdrückt und keine Schnittstelle benachrichtigt. Der Vorgang wird protokolliert.

Die Voralarmdauer ist unter **Konfiguration ? Alarmverhalten** einstellbar (0 bis 300 Sekunden). Ein Wert von 0 löst sofort den Alarm aus.

9.3 Alarm

Nach Ablauf des Voralarms wechselt die Oberfläche auf allen Bediengeräten in die **Vollbild-Alarmanzeige**. Sie zeigt die auslösende Kamera, den Zeitpunkt und das Beweisbild. Andere Ansichten sind während des Alarms gesperrt.

Sofern für die Kamera kein stiller Alarm eingestellt ist, werden Sirene und Weißlicht-Strahler aktiviert. Der Alarm bleibt mindestens 10 Sekunden aktiv.

Erkennen mehrere Kameras innerhalb von 30 Sekunden eine Person, fasst die Zentrale die Ereignisse zu einem Alarm zusammen. Die Schnittstellen erhalten eine Meldung mit allen beteiligten Kameras statt mehrerer Einzelmeldungen.

9.4 Beweisbild

Zu jedem Alarm wird ein Beweisbild gespeichert. Die Alarmschnittstellen erhalten – je nach Schnittstelle – das Bild als Anhang oder einen Kurzlink, über den Empfänger das Bild **ohne Anmeldung** ansehen können.

Der Link ist **15 Minuten gültig** und wird danach automatisch ungültig. Das Bild selbst wird nach der konfigurierten Aufbewahrungsfrist gelöscht.

9.5 Quittieren und Sirene stoppen

- **Sirene stoppen** beendet ausschließlich die akustische Signalisierung. Der Alarm bleibt bestehen, bis er quittiert wird.
- **Quittieren** beendet den Alarm. Die Quittierung wird an alle Schnittstellen weitergeleitet, die dies unterstützen (DIVERA 24/7, GroupAlarm).

Nach dem Alarm folgt eine Nachlaufzeit von 15 Sekunden, in der die Quittierung möglich ist; danach kehrt die Anlage in den scharfen Zustand zurück. Nicht quittierte Alarme bleiben im **Alarmspeicher** als offen markiert.

9.6 Verhalten der Empfänger

Empfänger einer Alarmmeldung sollten:

1. Das Beweisbild über den Link oder Anhang prüfen.
2. Bei erkennbarem Einbruch die Polizei verständigen und den Alarm über die Schnittstelle quittieren, damit weitere Empfänger informiert sind.
3. Bei erkennbarem Fehlalarm den Alarm quittieren und den Vorfall zur Prüfung des Erkennungsbereichs melden.
4. Das Gebäude nicht allein betreten, solange ein Einbruch nicht ausgeschlossen ist.

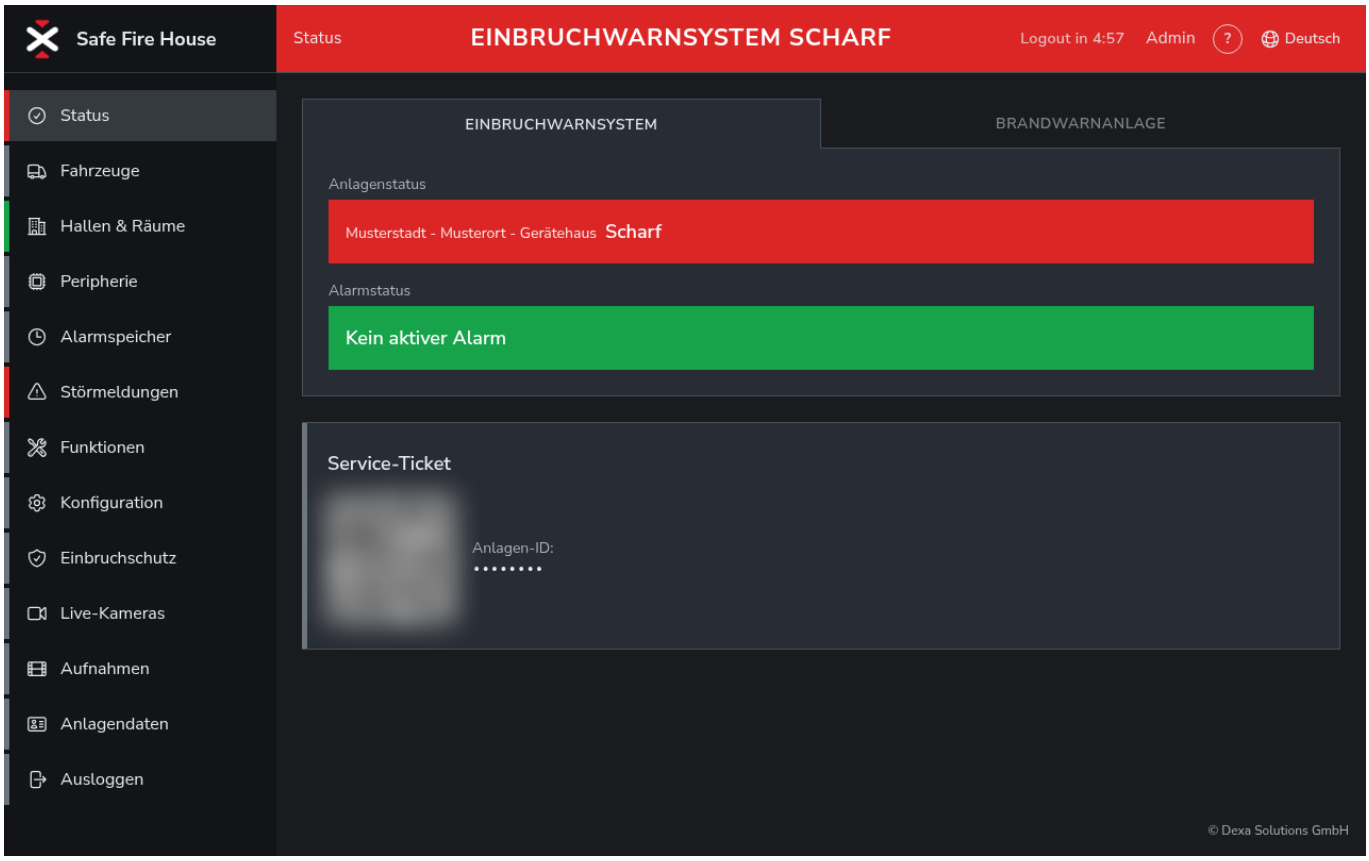
---

10. Die Weboberfläche im Betrieb

Nach der Anmeldung steht die vollständige Oberfläche der Zentrale zur Verfügung. Die linke Navigation führt zu allen Bereichen; die für das Einbruchwarnsystem relevanten sind **Einbruchschutz**, **Live-Kameras**, **Aufnahmen**, **Alarmspeicher** und **Konfiguration**. Bei kombiniertem Betrieb finden Sie daneben die Bereiche des Brandwarnsystems (Fahrzeuge, Hallen & Räume, Peripherie, Störmeldungen).

10.1 Status

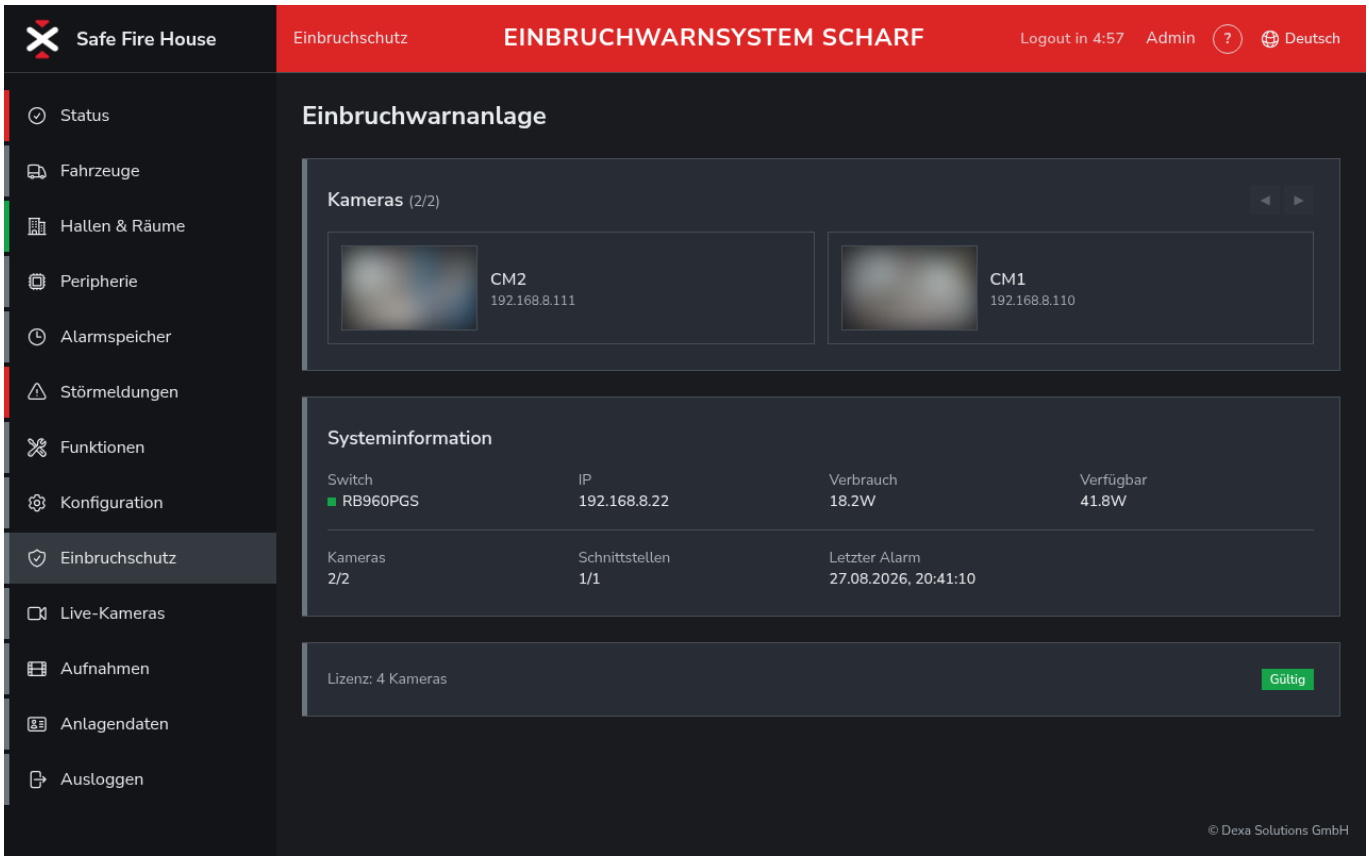
Die Ansicht **Status** zeigt den Anlagenzustand, den Alarmstatus und die Anlagen-ID. Über die Anlagen-ID eröffnen Sie ein Serviceticket; sie wird beim Kontakt mit dem Service benötigt.



10.2 Einbruchschutz

Die Ansicht **Einbruchschutz** ist die Übersicht des Einbruchwarnsystems:

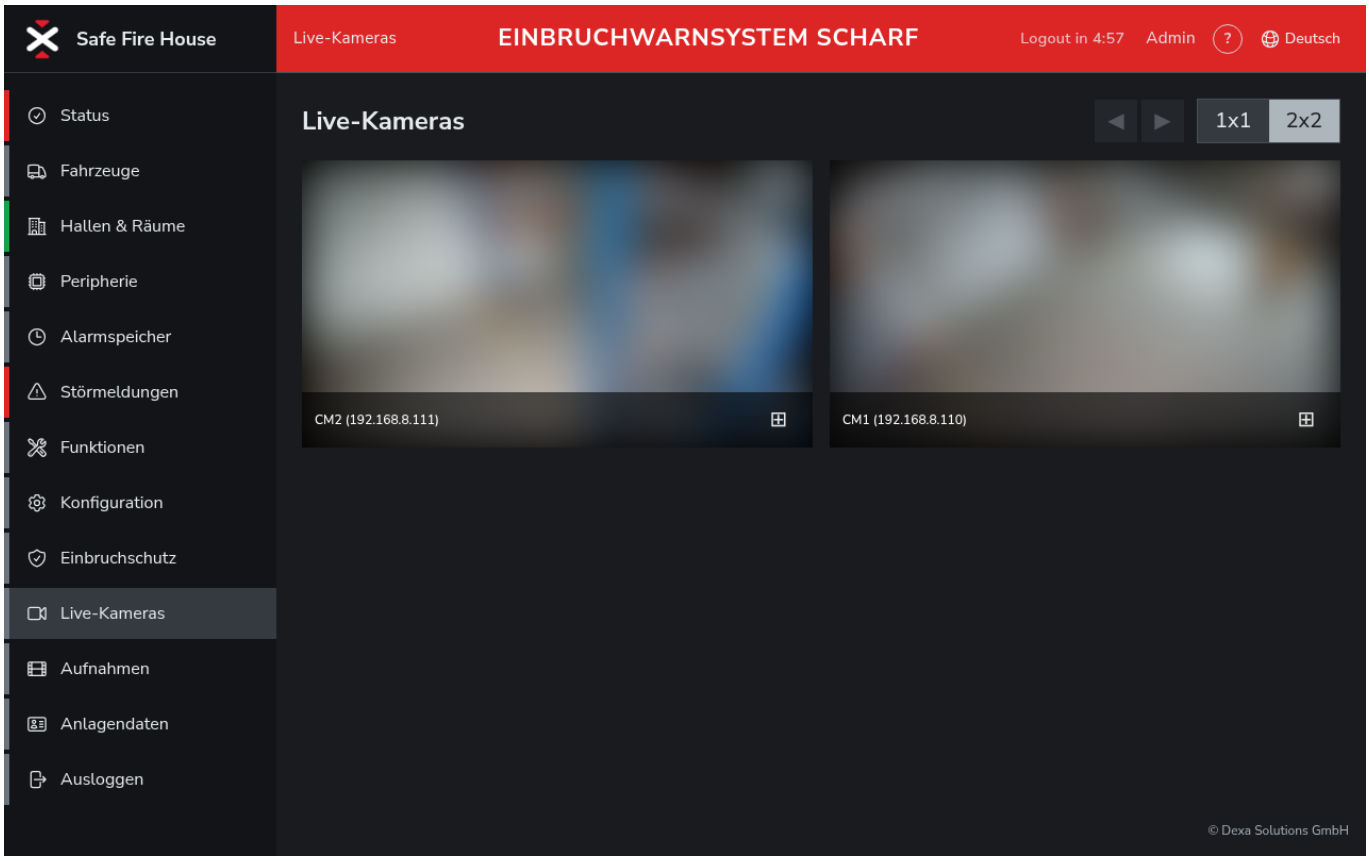
- **Einbruchwarnanlage** – aktueller Zustand und Schaltfläche zum Scharf- beziehungsweise Unscharfschalten
- **Kameras** – alle eingerichteten Kameras mit Name, Adresse und Erreichbarkeit; die Anzahl in Klammern zeigt, wie viele Kameras derzeit online sind
- **Systeminformation** – Switch, Leistungsaufnahme der Kameras, verfügbare PoE-Leistung, Anzahl aktiver Schnittstellen, Zeitpunkt des letzten Alarms und Lizenzstatus



Prüfen Sie hier bei jedem Scharfschalten, ob alle Kameras online sind. Eine Kamera, die im scharfen Zustand dauerhaft als nicht erreichbar angezeigt wird, ist eine Störung.

10.3 Live-Kameras

Die Ansicht **Live-Kameras** zeigt die Kamerabilder in Echtzeit. Über **1x1** sehen Sie eine Kamera groß, über **2x2** bis zu vier Kameras gleichzeitig. Bei mehr als vier Kameras blättern Sie mit den Pfeiltasten. Das Symbol an jeder Kachel öffnet die Kamera im Vollbild.



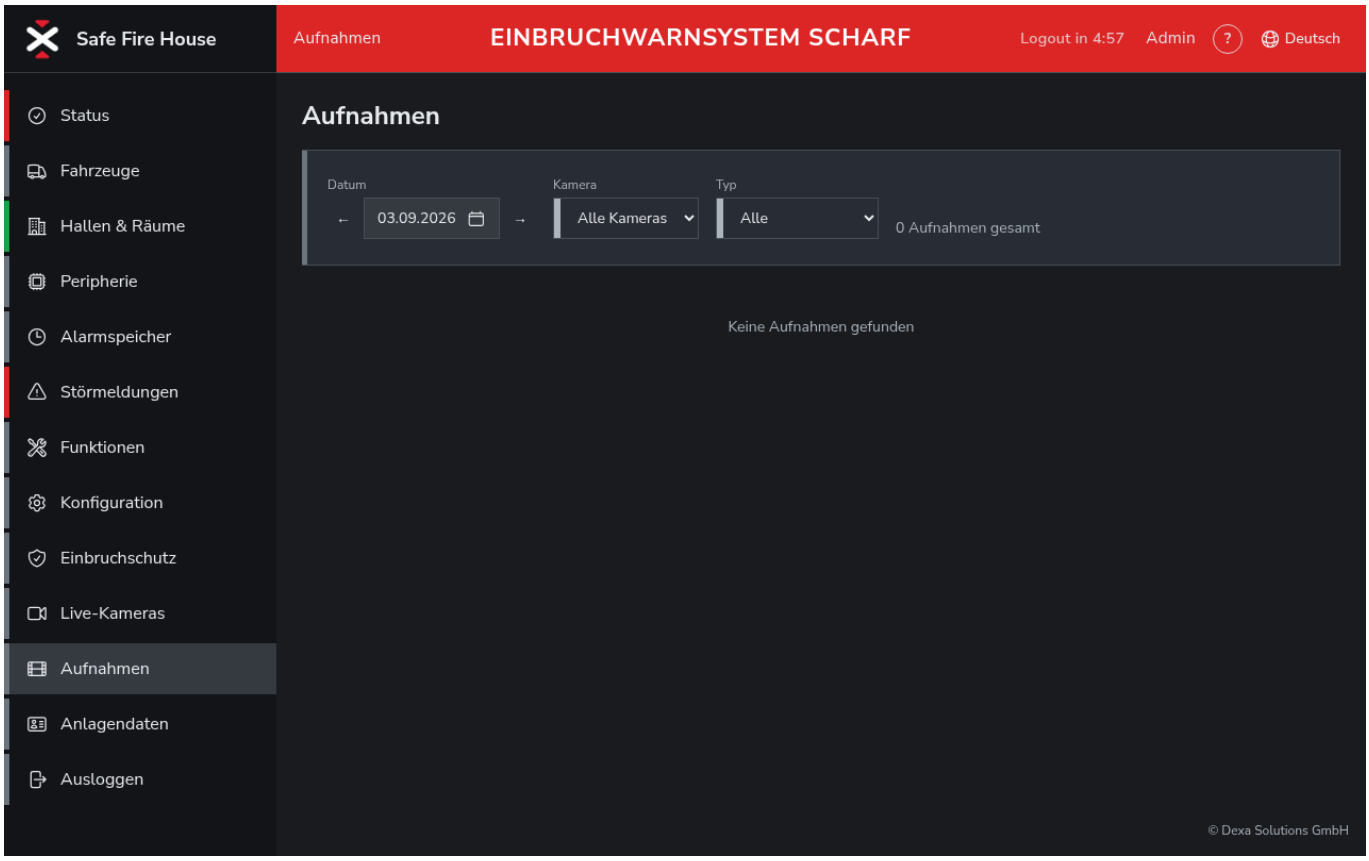
> **Hinweis:** Live-Bilder sind nur verfügbar, wenn die Anlage scharf ist oder sich im Wartungsmodus befindet. Im unscharfen Zustand sind die Kameras stromlos und liefern kein Bild.

10.4 Aufnahmen

Die Ansicht **Aufnahmen** listet alle gespeicherten Bilder und Aufzeichnungen. Filtern Sie nach **Datum**, **Kamera** und **Typ**:

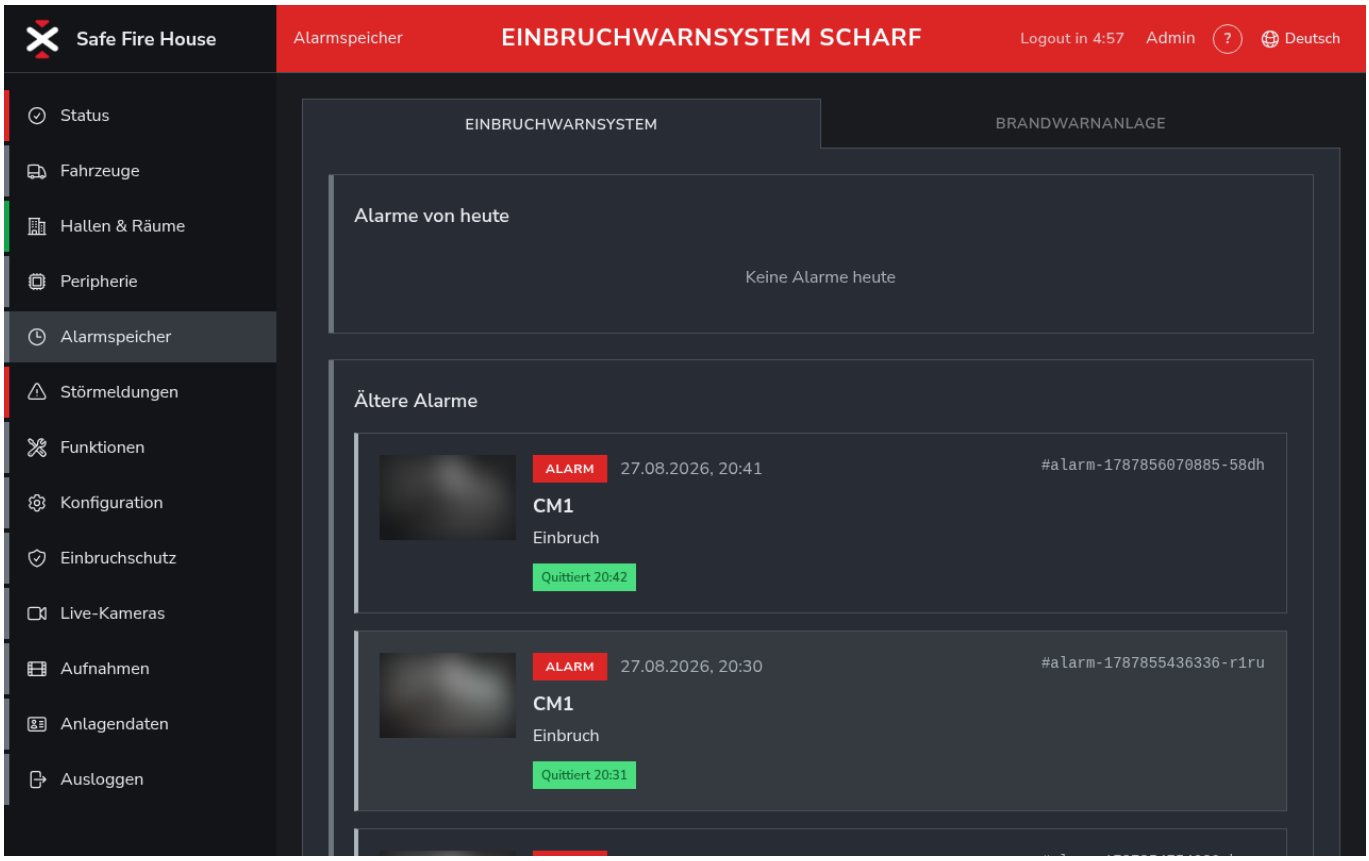
Typ	Inhalt
Snapshots	Beweisbilder aus Alarmen und Ereignissen
Daueraufnahme	Fortlaufende Aufzeichnung, sofern für die Kamera aktiviert
Event	Kurze Aufzeichnungen rund um ein Ereignis

Ein Klick auf ein Vorschaubild öffnet die Vollansicht. Die Aufbewahrungsfrist ist einstellbar (1 bis 180 Tage, Standard 30 Tage); ältere Aufnahmen werden automatisch gelöscht.



10.5 Alarmspeicher

Der **Alarmspeicher** zeigt alle Alarme mit Zeitpunkt, auslösender Kamera, Beweisbild und Quittierungsstatus – getrennt nach **Alarme von heute** und **Ältere Alarme**. Noch nicht quittierte Alarme stehen oben. Bei kombiniertem Betrieb erscheinen hier auch die Alarme des Brandwarnsystems.



11. Konfiguration

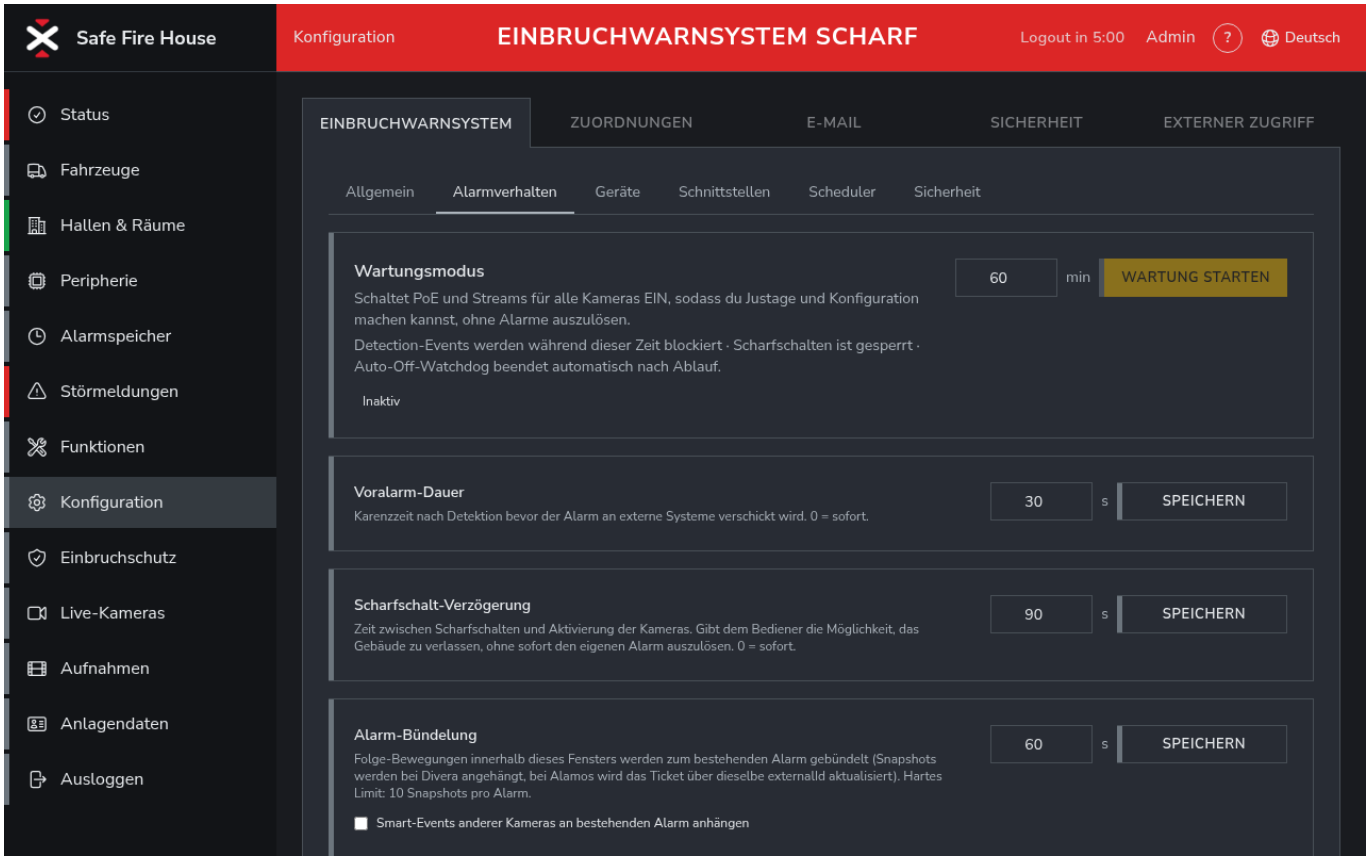
Die Konfiguration erreichen Sie über **Konfiguration** in der Navigation. Die Einstellungen des Einbruchwarnsystems liegen unter **EINBRUCHWARNSYSTEM** und sind in Reiter gegliedert: **Allgemein**, **Alarmverhalten**, **Geräte**, **Schnittstellen**, **Scheduler** und **Sicherheit**. Die weiteren Bereiche **ZUORDNUNGEN**, **E-MAIL**, **SICHERHEIT** und **EXTERNER ZUGRIFF** gelten anlagenweit.

Änderungen erfordern die Rolle Verwalter oder ***REDACTED***. Jede Änderung wird im Audit-Log mit Benutzer und Zeitpunkt protokolliert.

11.1 Allgemein

Einstellung	Bedeutung
Anlagen-Verbindung	Zeigt, ob der EWS-Dienst läuft: **CONTROLLER VERBUNDEN**
Lichtzone	Zuordnung einer Beleuchtung, die bei einem Alarmereignis eingeschaltet wird (beispielsweise Außenbeleuchtung über einen Schaltkontakt)
Anlagen-Version	Softwarestand des EWS-Dienstes
Lizenz	Lizenztyp, maximale Kameraanzahl, Status

11.2 Alarmverhalten



Einstellung	Bereich	Empfehlung
Voralarm-Dauer	0 bis 300 Sekunden	30 Sekunden; länger, wenn Berechtigte häufig den Bereich betreten
Scharfschalt-Verzögerung	0 bis 600 Sekunden	180 Sekunden; an die Zeit bis zum Verlassen des Gebäudes anpassen
Stiller Alarm (global)	ein / aus	aus; einzelne Kameras können abweichend eingestellt werden
Anlagen-PIN	ein / aus, vierstellig	ein, wenn viele Personen Zugang zum Bediengerät haben
Aufbewahrung Aufnahmen	1 bis 180 Tage	30 Tage; mit dem Datenschutzbeauftragten abstimmen
Wartungsmodus	ein / aus	nur für Arbeiten an der Anlage

Wartungsmodus: Schaltet die Stromversorgung und die Streams aller Kameras ein, ohne dass Ereignisse verarbeitet werden. Damit lassen sich Kameras ausrichten, Erkennungsbereiche einstellen und Konfigurationen prüfen, ohne Alarme auszulösen. Während des Wartungsmodus ist das Scharfschalten gesperrt. Ein Wächter beendet den Modus automatisch nach Ablauf einer Frist, damit die Anlage nicht versehentlich ungeschützt bleibt.

11.3 Geräte

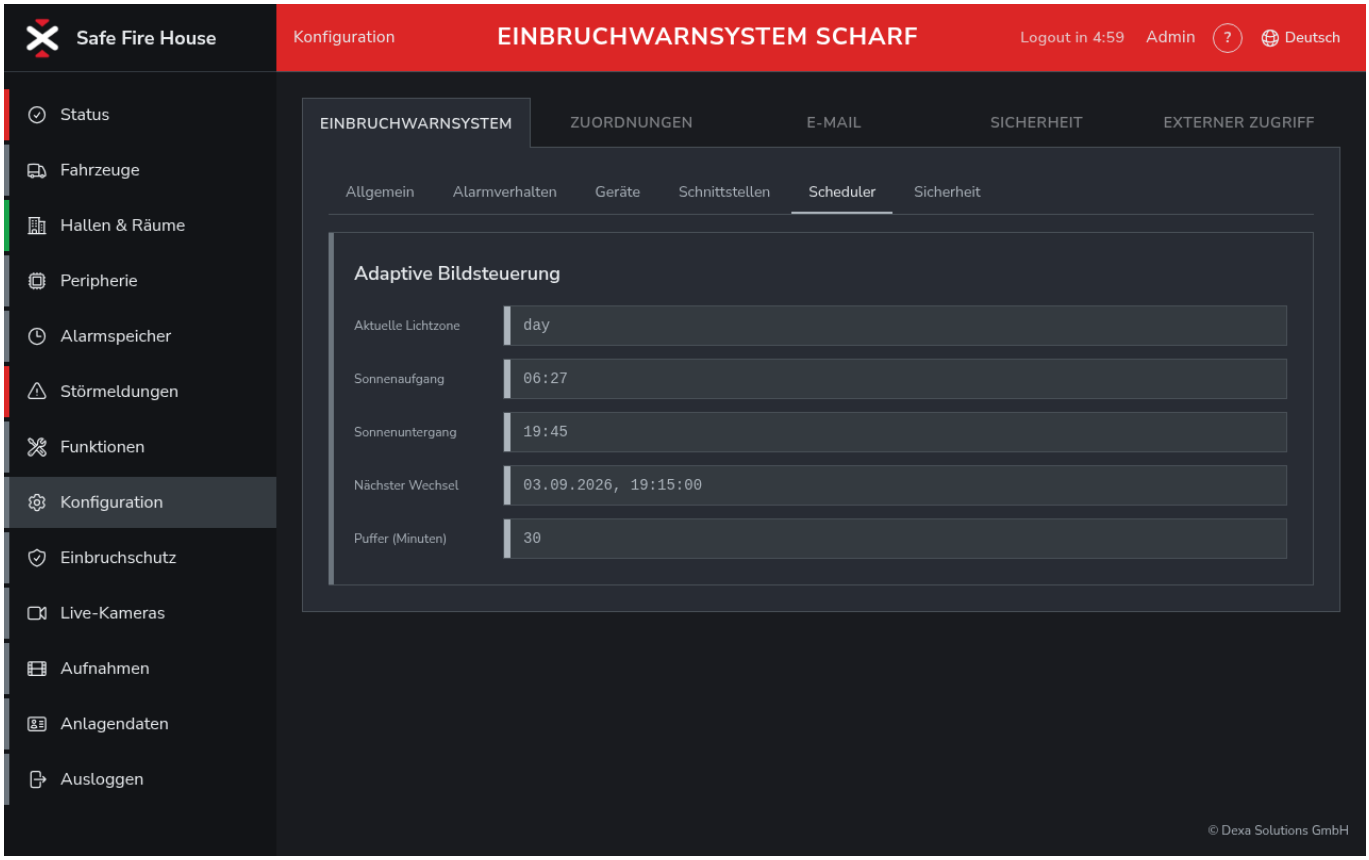
Der Reiter **Geräte** listet alle Kameras mit Name, IP-Adresse, MAC-Adresse, Switch-Port, Standort, ID, Modell und Seriennummer. Die Funktionen je Kamera sind in Kapitel 6.4 beschrieben.

Zusätzlich wird hier die Verbindung zum Bediengerät hinterlegt (**Display / SICP-Verbindung**), damit die LED-Leiste den Anlagenzustand anzeigen kann.

11.4 Schnittstellen

Der Reiter **Schnittstellen** zeigt alle verfügbaren Alarmschnittstellen mit Status und Funktionsumfang. Die Einrichtung ist in Kapitel 12 beschrieben.

11.5 Scheduler: Adaptive Bildsteuerung

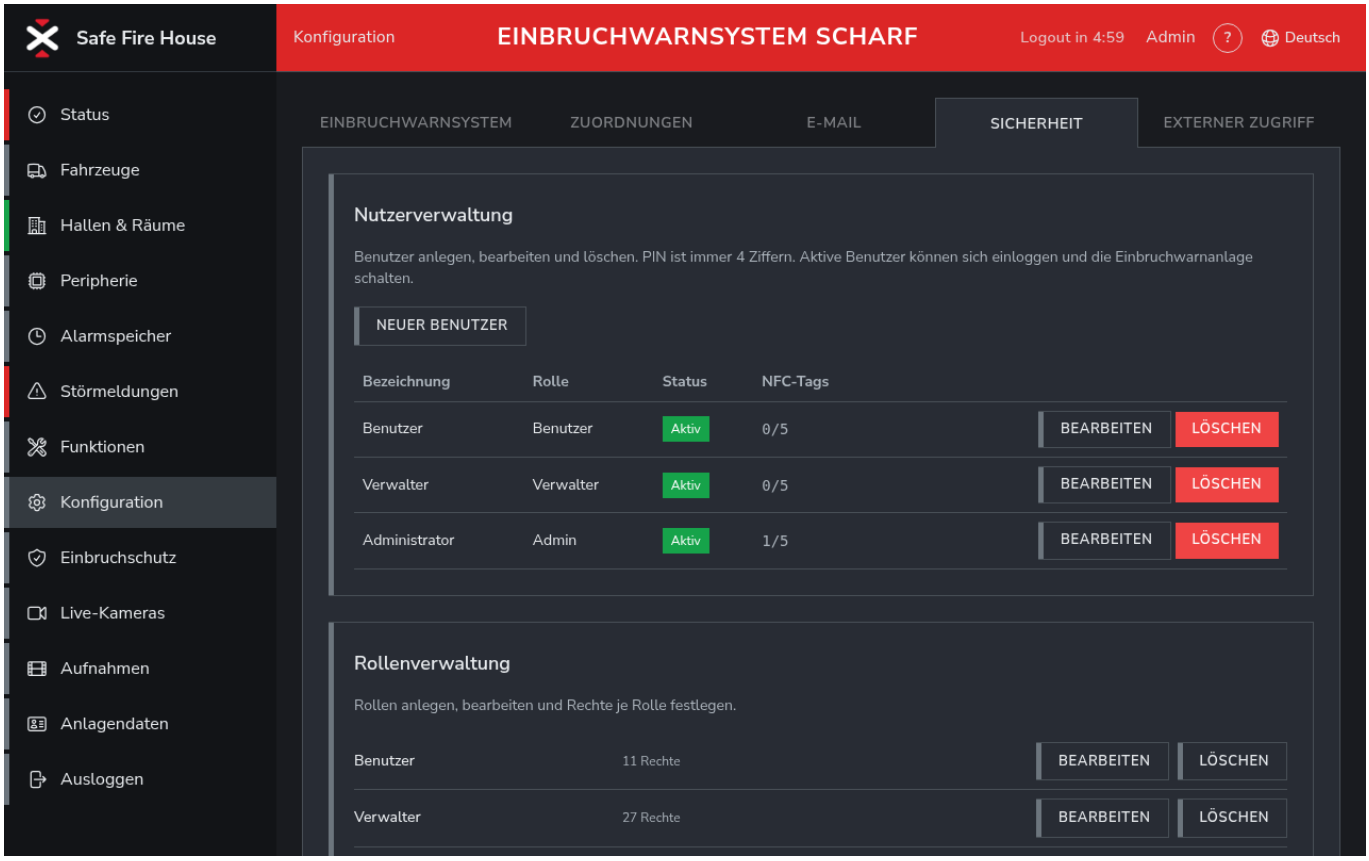


Die Kameras arbeiten mit drei Lichtzonen – Tag, Dämmerung und Nacht – und wechseln die Bildeinstellungen automatisch. Der Reiter zeigt die aktuelle Lichtzone, den berechneten Sonnenauf- und -untergang für den Standort und den nächsten Wechsel.

Einstellung	Bedeutung
Aktuelle Lichtzone	Tag, Dämmerung oder Nacht
Sonnenaufgang / Sonnenuntergang	Berechnet aus den Standortkoordinaten der Anlage
Nächster Wechsel	Zeitpunkt der nächsten Profilumschaltung
Puffer (Minuten)	Vorlauf, mit dem die Dämmerungsphase vor Sonnenuntergang beginnt beziehungsweise nach Sonnenaufgang endet

Stimmen die berechneten Zeiten nicht, prüfen Sie die Standortkoordinaten der Anlage unter **Anlagendaten**.

11.6 Sicherheit: Benutzer und Rollen



Benutzer anlegen:

1. **NEUER BENUTZER** wählen.
2. Bezeichnung eintragen (Name oder Funktion, beispielsweise „Gerätewart").
3. Rolle zuweisen: Benutzer, Verwalter oder ***REDACTED***.
4. Vierstellige PIN vergeben. Die PIN darf nicht mit anderen Benutzern übereinstimmen.
5. Status auf **Aktiv** setzen und speichern.

Benutzer bearbeiten oder deaktivieren: Über **BEARBEITEN** ändern Sie Bezeichnung, Rolle, PIN und Status. Deaktivierte Benutzer können sich nicht anmelden und die Anlage nicht schalten; ihre Einträge im Audit-Log bleiben erhalten. Über **LÖSCHEN** entfernen Sie den Benutzer vollständig.

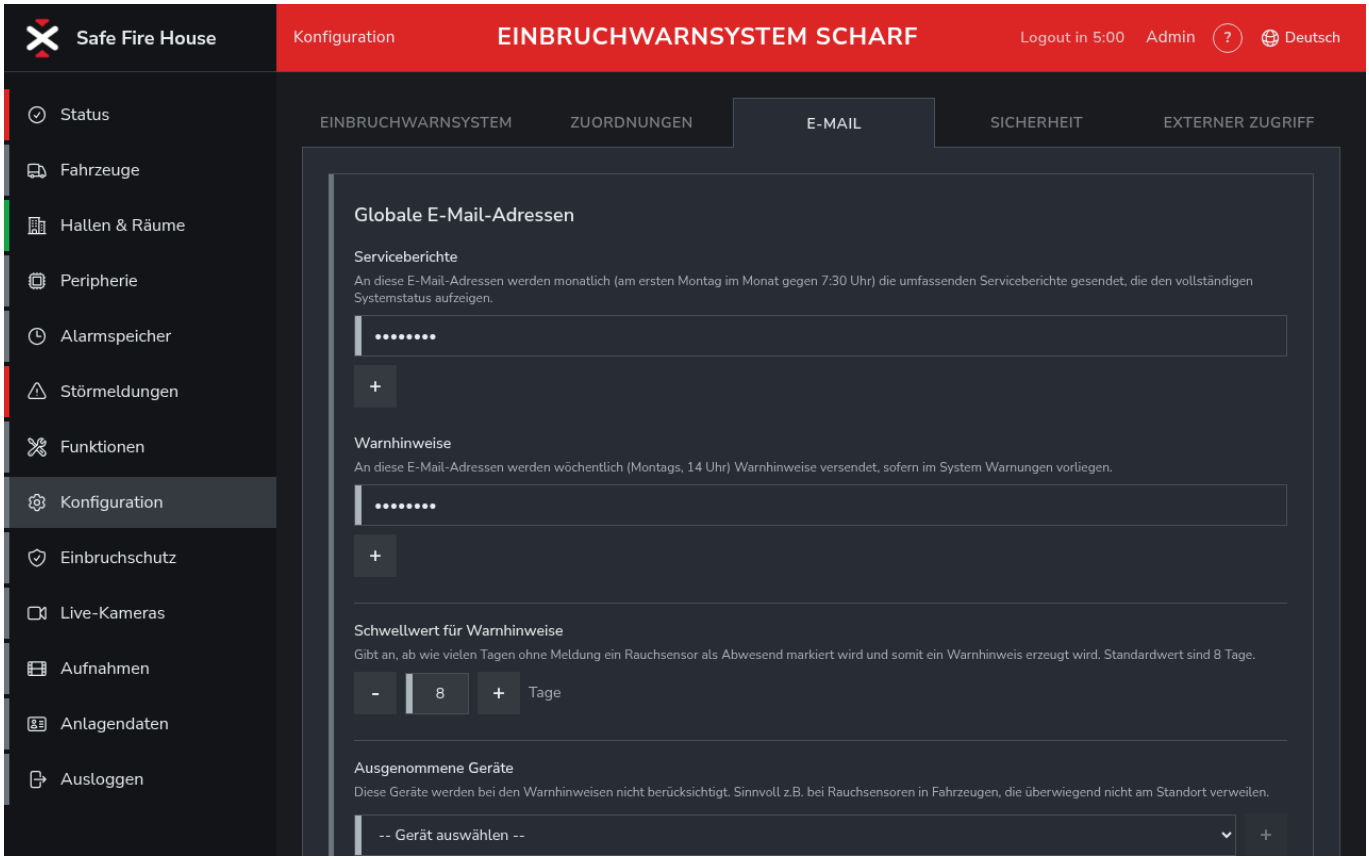
NFC-Token einlernen:

1. Benutzer über **BEARBEITEN** öffnen und **Token einlernen** wählen.
2. Den Token an den Leser des Bediengeräts halten.
3. Der Token wird dem Benutzer zugewiesen und ist sofort gültig. Bis zu fünf Token je Benutzer sind möglich, beispielsweise Erst- und Zweittoken.

Verlorene Token entfernen Sie umgehend aus der Zuordnung. Ein entfernter Token wird beim nächsten Scan abgewiesen.

Rollenverwaltung: Unter **Rollenverwaltung** sehen Sie die Rollen mit der Anzahl ihrer Rechte und können Rechte je Rolle anpassen, beispielsweise ob Benutzer Aufnahmen einsehen dürfen. Die Standardrollen sollten nur in Abstimmung mit uns verändert werden.

11.7 E-Mail: Serviceberichte und Warnhinweise



Unter **E-MAIL** hinterlegen Sie Empfänger für die automatischen Berichte der Anlage:

Bericht	Versand	Inhalt
Servicebericht	monatlich, am ersten Montag gegen 7:30 Uhr	Vollständiger Systemstatus aller Komponenten
Warnhinweise	wöchentlich, montags um 14 Uhr	Störungen und Auffälligkeiten, sofern vorhanden

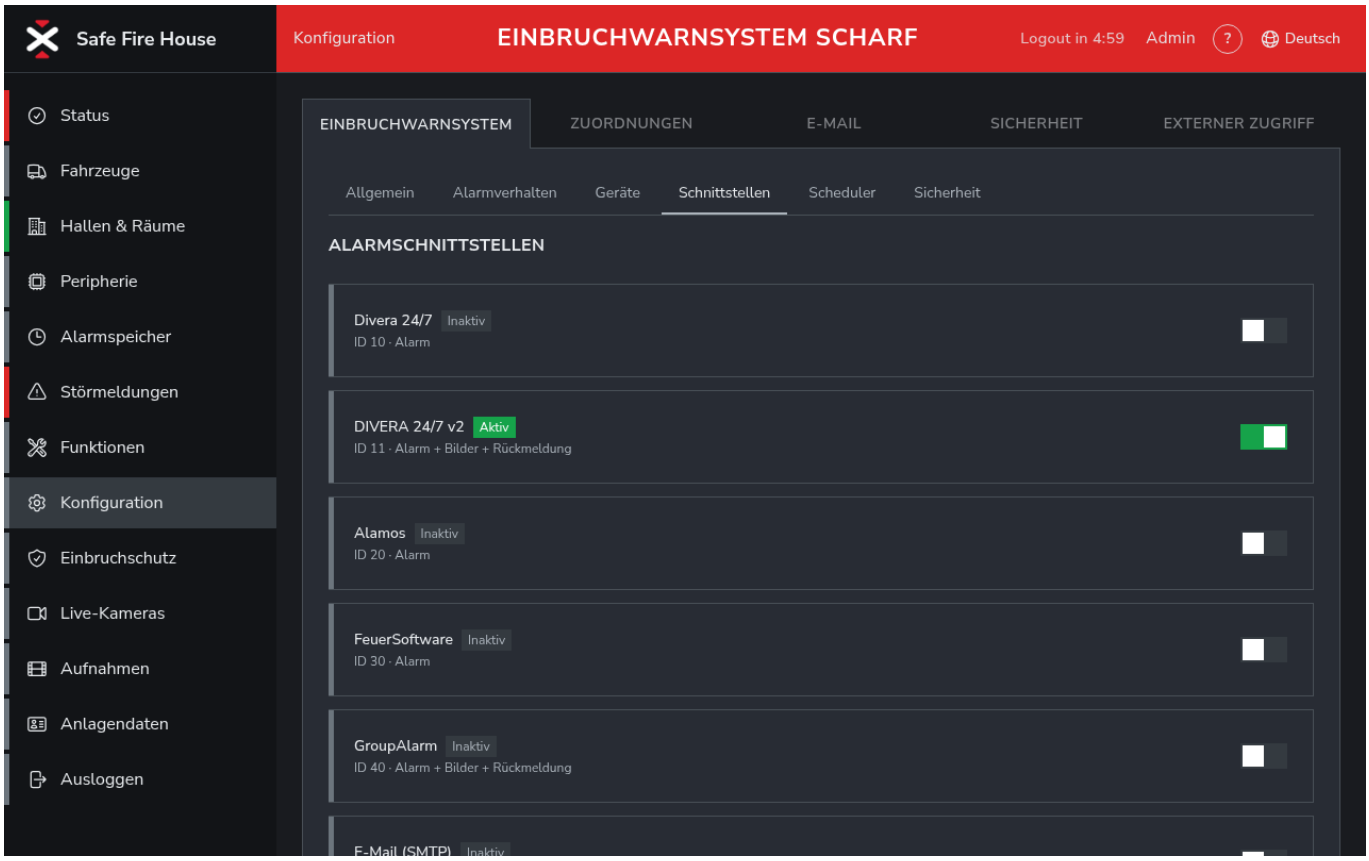
Über **+** fügen Sie Adressen hinzu. Tragen Sie mindestens eine Adresse ein, die regelmäßig gelesen wird.

11.8 Externer Zugriff

Unter **EXTERNER ZUGRIFF** werden Verbindungen für die Fernwartung und den Zugriff von außerhalb des Standortnetzes verwaltet. Änderungen hier erfolgen ausschließlich durch die Dexa Solutions GmbH.

12. Schnittstellen einrichten

Alle aktiven Schnittstellen werden bei jedem Alarm gleichzeitig benachrichtigt. Eine fehlgeschlagene Zustellung blockiert die übrigen nicht; sie wird nach 10, 30 und 60 Sekunden sowie nach 5 Minuten wiederholt, bevor sie aufgegeben wird.



Schnittstelle	Beweisbild	Quittierung aus der App
DIVERA 24/7 v2	als Anhang	ja
Alamos FE2 / aPager Pro	als Link im Alarmtext	nein
GroupAlarm	als Anhang	ja
E-Mail (SMTP)	als Anhang	nein

Weitere Leitstellen- und Alarmierungssysteme lassen sich über die dexa-Plattform anbinden. Sprechen Sie uns an.

12.1 DIVERA 24/7

1. Im Reiter **Schnittstellen** den Eintrag **DIVERA 24/7 v2** öffnen.
2. **Adresse** belassen (Standard: Alarmschnittstelle von DIVERA 24/7).
3. **Zugangsschlüssel** aus Ihrem DIVERA-Konto eintragen (Verwaltung ? Schnittstellen).
4. **Empfänger** festlegen: Gruppe oder Alarmierungsschema, beispielsweise „Einbruchalarm".
5. Schnittstelle **aktivieren**.
6. **Test-Alarm** auslösen und prüfen, ob die Meldung mit Beweisbild in DIVERA ankommt.

Quittierungen aus DIVERA werden an die Anlage zurückgemeldet und beenden den Alarm.

12.2 Alamos FE2 / aPager Pro

1. Eintrag **Alamos** öffnen.
2. **Adresse** Ihres Alamos-Servers eintragen. Der Server muss Meldungen aus dem Standortnetz beziehungsweise aus dem Internet annehmen; die Freigabe richten Sie mit Ihrem Alamos-

Betreuer ein.
3. **Authentifizierung** gemäß Alamos-Konfiguration eintragen.
4. Schnittstelle **aktivieren** und **Test-Alarm** auslösen.

Das Beweisbild wird als Link im Alarmtext übertragen. Empfänger öffnen den Link auf dem Smartphone.

12.3 GroupAlarm

1. Eintrag **GroupAlarm** öffnen.
2. **API-Token** aus Ihrer GroupAlarm-Organisation eintragen.
3. **Empfänger** (Alarmierungsszenario oder Einheit) festlegen.
4. Schnittstelle **aktivieren** und **Test-Alarm** auslösen.

Quittierungen aus GroupAlarm werden an die Anlage zurückgemeldet.

12.4 E-Mail

1. Eintrag **E-Mail** öffnen.
2. Postausgangsserver, Port, Verschlüsselung und Zugangsdaten eintragen – oder den Versandserver der Dexa Solutions GmbH nutzen.
3. **Empfänger** eintragen; mehrere Adressen durch Komma trennen.
4. Schnittstelle **aktivieren** und **Test-Alarm** auslösen.

Das Beweisbild wird als Anhang übertragen. Eine Quittierung per E-Mail ist nicht möglich.

12.5 Test-Alarm

Jede Schnittstelle bietet einen **Test-Alarm**. Er versendet eine als Test gekennzeichnete Meldung mit einem Beispielbild an die konfigurierten Empfänger, ohne Sirene und Strahler auszulösen. Führen Sie nach jeder Änderung an einer Schnittstelle einen Test-Alarm durch und informieren Sie die Empfänger vorab.

---

13. Türsteuerung und Schließanlagen

Das Einbruchwarnsystem kann beim Scharf- und Unscharfschalten eine Tür, ein Tor oder eine Schließanlage ansteuern. Beim Unscharfschalten wird die Tür freigegeben, beim Scharfschalten verriegelt – ein Vorgang am Bediengerät, kein Medienbruch.

13.1 Potenzialfreier Schaltkontakt (universell)

Der SFH Schaltkontakt (DXO-SFH-SC-1-01 einfach, DXO-SFH-SC-4-01 vierfach) schaltet beim Scharf- und Unscharfschalten einen potenzialfreien Kontakt. Damit lässt sich praktisch jede elektrische Türöffnung, jedes Motorschloss, jedes Tor und jedes Relais ansteuern – herstellerunabhängig. Der Schaltkontakt wird bei der Inbetriebnahme der Anlage zugeordnet; die Schaltlogik (Impuls oder Dauerkontakt) wird an das angesteuerte Gerät angepasst.

Über weitere Kontakte des vierfachen Schaltkontakts lassen sich zusätzlich Außenbeleuchtung oder Rolltore bei Alarm ansteuern (siehe **Lichtzone** in Kapitel 11.1).

13.2 Integrierte Schließsysteme

Neben dem Schaltkontakt bestehen Integrationen für gängige Zutrittssysteme:

- **ABUS** – professionelle Schließzylinder und Zutrittskontrolle

- **Salto** – Zutrittslösungen für Gebäude und Liegenschaften
- **dormakaba** – Schließanlagen und digitale Zylinder
- **ASSA ABLOY** – Zutrittssysteme und Aperio-Komponenten
- **Nuki, SwitchBot** und weitere Consumer-Systeme

Die Einrichtung erfolgt bei der Inbetriebnahme in Abstimmung mit dem Betreuer Ihrer Schließanlage.

13.3 NFC-Token als Schlüssel

Die NFC-Token der Anlage sind herstellerunabhängige Token. Sie dienen der Anmeldung und dem Schalten der Anlage; über die Türsteuerung wirken sie zugleich als Schlüssel. Verlorene Token werden in der Benutzerverwaltung entfernt und sind damit sofort ungültig – ohne Zylindertausch.

---

14. Datenschutz

Das Einbruchwarnsystem verarbeitet personenbezogene Daten in Form von Bildaufnahmen. Die Anlage ist so ausgelegt, dass diese Verarbeitung auf das Notwendige beschränkt bleibt:

- **Kameras nur bei scharfer Anlage aktiv** – im unscharfen Zustand physisch stromlos, keine Aufzeichnung möglich
- **Erkennungsbereiche** – nur der definierte Bereich löst aus; öffentlicher Raum wird ausgespart
- **Beweisbild-Links nur 15 Minuten gültig** – danach automatisch ungültig
- **Automatische Löschung** aller Aufnahmen nach der konfigurierten Frist
- **Zugriffsschutz** über PIN, NFC-Token, Rollen und Audit-Log

14.1 Pflichten des Betreibers

Als Betreiber sind Sie Verantwortlicher im Sinne der DSGVO. Dazu gehören:

- Festlegung der Rechtsgrundlage (in der Regel berechtigtes Interesse am Schutz des Eigentums)
- Hinweisbeschilderung an den Zugängen zum überwachten Bereich mit Angabe des Verantwortlichen
- Information von Personal, Mitgliedern und Besuchern
- Abstimmung mit Personal- oder Betriebsrat, sofern vorhanden
- Aufnahme in das Verzeichnis der Verarbeitungstätigkeiten
- Festlegung der Aufbewahrungsfrist; 30 Tage sind ein üblicher Wert

Die Dexa Solutions GmbH stellt einen **Auftragsverarbeitungsvertrag nach Art. 28 DSGVO** sowie eine **Erklärung zur Datenschutzkonformität** bereit; beide finden Sie im Buch „Datenschutz". Für die Fernwartung wird der Zugriff auf Bilddaten im Vertrag geregelt.

14.2 Auskunft und Löschung

Betroffene können Auskunft über gespeicherte Aufnahmen verlangen. Über die Ansicht **Aufnahmen** lassen sich Aufnahmen nach Datum und Kamera filtern und einzeln löschen. Das Audit-Log dokumentiert Zugriffe und Löschungen.

---

15. Wartung

Die Anlage ist im laufenden Betrieb **wartungsfrei**. Kameras, Switch und Zentrale überwachen sich gegenseitig; Störungen werden in der Oberfläche, in den wöchentlichen Warnhinweisen und über die Schnittstellen gemeldet.

Wir empfehlen:

- **Monatlich:** Sichtkontrolle der Kameras auf Verschmutzung, Spinnweben und Ausrichtung. Objektive bei Bedarf mit einem weichen, trockenen Tuch reinigen. Kontrolle des monatlichen Serviceberichts.
- **Bei jedem Scharfschalten:** Beobachten, ob alle Kameras in der Ansicht **Einbruchschutz** als erreichbar angezeigt werden.
- **Halbjährlich:** Benutzerliste prüfen; ausgeschiedene Personen deaktivieren, verlorene Token entfernen.
- **Jährlich:** Funktionstest der Alarmkette in Abstimmung mit uns – Erkennung, Sirene, Strahler und Schnittstellen. Prüfung der Zugangsschlüssel der Schnittstellen auf Gültigkeit.

Ein optionaler Wartungsvertrag umfasst die Fernüberwachung der Anlage rund um die Uhr, die Prüfung der Serviceberichte durch uns und eine jährliche Prüfung vor Ort.

> **Wartungsmodus:** Für Arbeiten an Kameras oder Netzwerk versetzen Sie die Anlage in den Wartungsmodus (Konfiguration ? Alarmverhalten). Die Kameras sind dann eingeschaltet, lösen aber keinen Alarm aus. Beenden Sie den Wartungsmodus nach Abschluss der Arbeiten.

15.1 Kameratausch

Ein Kameratausch erfolgt durch uns oder nach unserer Anleitung: neue Kamera am selben Switch-Port anschließen, unter **Geräte** die alte Kamera löschen, die neue Kamera hinzufügen und per **ONE-CLICK CONFIG** einrichten, anschließend Erkennungsbereich und Ausrichtung im Wartungsmodus prüfen.

15.2 Softwareaktualisierung

Aktualisierungen der Zentrale werden durch die Dexa Solutions GmbH im Rahmen der Fernwartung eingespielt und vorab angekündigt. Während der Aktualisierung ist die Anlage kurzzeitig nicht scharfschaltbar.

---

16. Fehleranalyse

Beobachtung	Mögliche Ursache	Maßnahme
Anlage lässt sich nicht scharfschalten	Wartungsmodus aktiv	Wartungsmodus unter Konfiguration ? Alarmverhalten beenden
Anlage lässt sich nicht scharfschalten	Kamera nicht erreichbar	Ansicht Einbruchschutz prüfen; Netzwerkkabel und Switch-Port kontrollieren; Kamera über POE neu starten
Anlage lässt sich nicht scharfschalten	Switch nicht erreichbar	Stromversorgung und Uplink des Switches prüfen; Serviceticket eröffnen
Scharfschaltung bricht nach 90 Sekunden ab	Kamera startet nicht	Kamera über POE aus- und einschalten; bleibt sie offline, Serviceticket eröffnen
Kamera wird als nicht erreichbar angezeigt	Anlage unscharf	Normalzustand: Kameras sind stromlos

Beobachtung	Mögliche Ursache	Maßnahme
Kein Live-Bild	Anlage unscharf	Live-Bilder nur bei scharfer Anlage oder im Wartungsmodus
PIN wird nicht angenommen	Benutzer gesperrt oder deaktiviert	Fünf Minuten warten; Verwalter prüft Benutzerstatus
NFC-Token wird nicht erkannt	Token nicht eingelernt, entfernt oder Leser des Bediengeräts gestört	Verwalter lernt den Token neu ein; Bediengerät neu starten
Fehlalarm durch Tiere, Fahrzeuge oder Licht	Erkennungsbereich ungünstig oder Szenenprofil unpassend	Serviceticket eröffnen; Erkennungsbereich oder Profil wird angepasst
Häufige Manipulationsmeldungen	Kamera verschmutzt, Spinnweben, Lichtwechsel	Objektiv reinigen; bleibt es, Serviceticket eröffnen
Alarm, aber keine Benachrichtigung	Schnittstelle inaktiv oder Zugangsschlüssel abgelaufen	Reiter Schnittstellen prüfen, Test-Alarm auslösen; Zustellung wird automatisch wiederholt
Beweisbild-Link funktioniert nicht	Link älter als 15 Minuten	Bild im Alarmspeicher der Anlage ansehen
Meldung „Port-Mismatch"	Kamera umgesteckt oder fremdes Gerät am Kameraport	Verkabelung auf den dokumentierten Stand zurückführen
Anzeige „Lizenz ungültig"	Lizenz abgelaufen oder Zentrale getauscht	Serviceticket eröffnen
LED-Leiste am Bediengerät zeigt keinen Zustand	Verbindung zum Bediengerät unterbrochen	Bediengerät neu starten; Adresse unter Geräte prüfen
Sonnenauf-/-untergang falsch	Standortkoordinaten fehlen	Koordinaten unter Anlagendaten prüfen

Lässt sich eine Störung nicht beheben, eröffnen Sie ein Serviceticket über die Anlagen-ID in der Ansicht **Status** oder wenden Sie sich an unseren Service.

17. Technische Daten

Parameter	Wert
Erkennung	KI-Personenerkennung in der Kamera: Bereich, Linie, Zone, Manipulation
Kamera	8 Megapixel, Infrarot-Nachtsicht, Weißlicht-Strahler
Maximale Kameras	Switch klein: 5 · Switch groß: 15 · Lizenz gestaffelt bis 16
PoE-Switch	klein: ***REDACTED*** hEX PoE · groß: ***REDACTED*** CRS328-24P-4S+RM (19-Zoll, 1 HE, 500 Watt)
Stromversorgung Kameras	PoE nach IEEE 802.3af/at, im unscharfen Zustand abgeschaltet
Switch-Steuerung	Verschlüsselt, Reaktionszeit unter 100 Millisekunden
Kamerastart beim Scharfschalten	30 bis 60 Sekunden, Zeitüberschreitung 90 Sekunden
Voralarm	0 bis 300 Sekunden, Standard 30
Scharfschalt-Verzögerung	0 bis 600 Sekunden, Standard 180
Mehrfacherkennung	Zusammenfassung innerhalb von 30 Sekunden
Live-Ansicht	1x1 oder 2x2, nur bei scharfer Anlage oder im Wartungsmodus
Beweisbild-Link	15 Minuten gültig, ohne Anmeldung abrufbar
Aufbewahrung	1 bis 180 Tage, Standard 30 Tage

Parameter	Wert
Speicher	bis 10 GB je Anlage, älteste Aufnahmen werden zuerst gelöscht
Alarmschnittstellen	DIVERA 24/7, Alamos FE2 / aPager Pro, GroupAlarm, E-Mail; weitere über die dexa-Plattform
Wiederholung fehlgeschlagener Zustellungen	nach 10 s, 30 s, 60 s und 5 min
Authentifizierung	PIN (4 Ziffern), NFC-Token (bis 5 je Benutzer), optionale Anlagen-PIN, 3 Fehlversuche = 5 Minuten Sperre
Automatische Abmeldung	nach 5 Minuten ohne Eingabe
Berichte	Servicebericht monatlich, Warnhinweise wöchentlich
Sirene	bis 100 dB, IP44, Solarbetrieb mit Pufferakku, Nachladen über Micro-USB
Lizenz	an die Zentrale gebunden
Plattform	Safe Fire House Zentrale DXO-SFH-CU-B-02 oder DXO-SFH-CU-P-01

18. Kontakt

Ein Serviceticket eröffnen Sie am schnellsten über die Anlagen-ID in der Ansicht **Status** Ihrer Anlage.

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee
Telefon: +49 2924 496 937-0
E-Mail: info@dexa.gmbh

Stand: 2026-09