AX PRO

Benutzerhandbuch

Rechtliche Informationen

Über dieses Benutzerhandbuch

Das Handbuch enthält Anweisungen zur Verwendung und Verwaltung des Produkts. Bilder, Diagramme, Skizzen und alle anderen Informationen im Folgenden dienen nur der Beschreibung und Erklärung. Die im Handbuch enthaltenen Informationen können sich ohne Vorankündigung aufgrund von Firmware-Upgrades oder aus anderen Gründen ändern. Die neueste Version dieses Handbuchs finden Sie auf der Hikvision-Website (***https://www.hikvision.com/***).
Bitte verwenden Sie dieses Handbuch mit der Anleitung und Unterstützung von Fachleuten, die in der Unterstützung des Produkts geschult sind.

Warenzeichen

HIKVISION und andere Marken und Logos von Hikvision sind das Eigentum von Hikvision in verschiedenen Rechtsordnungen.
Andere erwähnte Marken und Logos sind Eigentum ihrer jeweiligen Inhaber.

Haftungsausschluss

DIESES HANDBUCH UND DAS BESCHRIEBENE PRODUKT MIT SEINER HARDWARE, SOFTWARE UND FIRMWARE WERDEN IM GRÖSSTMÖGLICHEN GESETZLICH ZULÄSSIGEN UMFANG "WIE BESEHEN" UND "MIT ALLEN FEHLERN UND IRRTÜMERN" ZUR VERFÜGUNG GESTELLT. HIKVISION GIBT KEINE GARANTIEN, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF, MARKTGÄNGIGKEIT, ZUFRIEDENSTELLENDE QUALITÄT ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK. DIE NUTZUNG DER MATERIALIEN ERFOLGT AUF IHR EIGENES RISIKO. HIKVISION HAFTET IN KEINEM FALL FÜR BESONDERE, FOLGE-, BEILÄUFIG ENTSTANDENE ODER INDIREKTE SCHÄDEN, EINSCHLIESSLICH SCHÄDEN DURCH ENTGANGENE GEWINNE, BETRIEBSUNTERBRECHUNGEN, VERLUST VON DATEN, SYSTEMKORRUPTION ODER VERLUST DER DOKUMENTATION, SEI ES AUFGRUND EINER VERTRAGSVERLETZUNG ODER AUS UNERLAUBTER HANDLUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT), DER PRODUKTHAFTUNG ODER ANDERWEITIG, IN VERBINDUNG MIT DER NUTZUNG DER MATERIALIEN, AUCH WENN HIKVISION ÜBER DIE MÖGLICHKEIT EINES DERARTIGEN SCHADENS ODER VERLUSTES INFORMIERT WURDE.
SIE ERKENNEN AN, DASS DIE NATUR DES INTERNETS INHÄRENTE SICHERHEITSRISIKEN MIT SICH BRINGT, UND HIKVISION ÜBERNIMMT KEINE VERANTWORTUNG FÜR ANORMALEN BETRIEB, DATENSCHUTZVERLETZUNGEN ODER ANDERE SCHÄDEN, DIE DURCH CYBERANGRIFFE, HACKER-ANGRIFFE, VIRENINSPEKTIONEN ODER ANDERE INTERNET-SICHERHEITSRISIKEN ENTSTEHEN; HIKVISION WIRD JEDOCH BEI BEDARF RECHTZEITIG TECHNISCHE UNTERSTÜTZUNG LEISTEN.
6.4 SIE WILLIGEN EIN, BEI DER NUTZUNG DER MATERIALIEN ALLE GELTENDEN GESETZE ZU ERFÜLLEN UND SIE TRAGEN DIE ALLEINIGE VERANTWORTUNG FÜR DIE SICHERSTELLUNG, DASS IHRE NUTZUNG DEM GELTENDEN RECHT ENTSPRICHT. SIE SIND VOR ALLEM DAFÜR VERANTWORTLICH, DIE MATERIALIEN IN EINER WEISE ZU NUTZEN, DIE NICHT DIE RECHTE DRITTER VERLETZT, INSBESONDERE DIE ÖFFENTLICHKEITSRECHTE, RECHTE AN GEISTIGEM EIGENTUM ODER

DATENSCHUTZRECHTE UND SONSTIGE RECHTE ZUM SCHUTZ VON PERSÖNLICHKEITSRECHTEN. SIE DÜRFEN DIE MATERIALIEN NICHT FÜR VERBOTENE ENDVERWENDUNGEN NUTZEN; DIES SCHLIESST DIE ENTWICKLUNG ODER HERSTELLUNG VON MASSENVERNICHTUNGSWAFFEN, DIE ENTWICKLUNG ODER HERSTELLUNG VON CHEMISCHEN ODER BIOLOGISCHEN WAFFEN, ALLE AKTIVITÄTEN IN VERBINDUNG MIT NUKLEAREN SPRENGSTOFFEN ODER UNSICHEREN KERNBRENNSTOFFKREISLÄUFEN ODER ZUGUNSTEN VON MENSCHENRECHTSVERLETZUNGEN EIN. IM FALLE VON KONFLIKTEN ZWISCHEN DIESEM HANDBUCH UND DEM ANWENDBAREN RECHT IST DAS LETZTERE MASSGEBEND.

Symbol Konventionen

Die in diesem Dokument enthaltenen Symbole sind wie folgt definiert:

Symbol	Beschreibung
Gefahr	Weist auf eine gefährliche Situation hin, die, wenn sie nicht vermieden wird, zum Tod oder zu schweren Verletzungen führen wird oder führen könnte.
Vorsicht	Weist auf eine potenziell gefährliche Situation hin, die, wenn sie nicht vermieden wird, zu Geräteschäden, Datenverlust, Leistungseinbußen oder unerwarteten Ergebnissen führen könnte.
Hinweis	Bietet zusätzliche Informationen, um wichtige Punkte des Haupttextes hervorzuheben oder zu ergänzen.

Rechtliche Informationen

EN 50131-1:2006+A1:2009+A2:2017

EN 50131-3:2009

EN 50131-6:2017

EN 50131-5-3:2017

EN 50131-10: 2014

EN 50136-2: 2013

Sicherheitsklasse (SG): 2

Umweltklasse (EC): II

DP2

Von Telefication zertifiziert

Hinweis Die EN50131-Konformitätskennzeichnung sollte entfernt werden, wenn nicht-konforme Konfigurationen verwendet werden.

EU-Konformitätserklärung

CE	Dieses Produkt und - falls zutreffend - auch das mitgelieferte Zubehör sind mit "CE" gekennzeichnet und entsprechen somit den geltenden harmonisierten europäischen Normen, die unter der EMV-Richtlinie 2014/30/EU, der RE-Richtlinie 2014/53/EU, der RoHS-Richtlinie 2011/65/EU aufgeführt sind.
	2012/19/EU (WEEE-Richtlinie): Produkte, die mit diesem Symbol gekennzeichnet sind, dürfen in der Europäischen Union nicht als unsortierter Hausmüll entsorgt werden. Um ein ordnungsgemäßes Recycling zu gewährleisten, geben Sie dieses Produkt beim Kauf eines gleichwertigen Neugerätes an Ihren örtlichen Lieferanten zurück oder entsorgen Sie es an den dafür vorgesehenen Sammelstellen. Weitere Informationen finden Sie unter: www.recyclethis.info
	2006/66/EC (Batterierichtlinie): Dieses Produkt enthält eine Batterie, die in der Europäischen Union nicht als unsortierter Hausmüll entsorgt werden kann. Spezifische Informationen zur Batterie finden Sie in der Produktdokumentation. Die Batterie ist mit diesem Symbol gekennzeichnet, das Schriftzüge zur Angabe von Cadmium (Cd), Blei (Pb) oder Quecksilber (Hg) enthalten kann. Geben Sie den Akku zum ordnungsgemäßen Recycling an Ihren Lieferanten oder an eine ausgewiesene Sammelstelle zurück. Weitere Informationen finden Sie unter: www.recyclethis.info

	Warnung Dies ist ein Produkt der Klasse A. In einer häuslichen Umgebung kann dieses Produkt Funkstörungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Maßnahmen zu ergreifen.
	FCC Informationen Bitte beachten Sie, dass Änderungen oder Modifikationen, die nicht ausdrücklich von der für die Einhaltung der Vorschriften verantwortlichen Partei genehmigt wurden, die Berechtigung des Benutzers zum Betrieb des Geräts aufheben können. FCC Konform: Dieses Gerät wurde getestet und entspricht den Grenzwerten für ein digitales Gerät der Klasse B gemäß Teil 15 der FCC-Vorschriften. Diese Grenzwerte sind so ausgelegt, dass sie einen angemessenen Schutz gegen schädliche Störungen in einer Wohnanlage bieten. Dieses Gerät erzeugt, verwendet und kann Hochfrequenzenergie ausstrahlen und kann, wenn es nicht in Übereinstimmung mit den Anweisungen installiert und verwendet wird, schädliche Störungen des Funkverkehrs verursachen. Es gibt jedoch keine Garantie, dass in einer bestimmten Installation keine Störungen auftreten. Wenn dieses Gerät schädliche Störungen des Radio- oder Fernsehempfangs verursacht, was durch Ein- und Ausschalten des Geräts festgestellt werden kann, sollte der Benutzer versuchen, die Störung durch eine oder mehrere der folgenden Maßnahmen zu beheben: –Richten Sie die Empfangsantenne neu aus oder positionieren Sie um. –Vergrößern Sie den Abstand zwischen Gerät und Empfänger. –Schließen Sie das Gerät an eine Steckdose an, die sich von der Steckdose unterscheidet, an die der Empfänger angeschlossen ist. –Wenden Sie sich an den Händler oder einen erfahrenen Radio-/TV-Techniker. Dieses Gerät sollte mit einem Mindestabstand von 20 cm zwischen dem Heizkörper und Ihrem Körper installiert und betrieben werden. FCC-Bedingungen Dieses Gerät entspricht Teil 15 der FCC-Vorschriften. Der Betrieb unterliegt den folgenden zwei Bedingungen:

	1. Dieses Gerät darf keine schädlichen Interferenzen verursachen. 2. Dieses Gerät muss alle empfangenen Interferenzen akzeptieren, einschließlich Interferenzen, die einen unerwünschten Betrieb verursachen können.

Inhalt

Kapitel 1 Einführung

1.1 Systembeschreibung

AX PRO ist eine funkbasierte Einbruchmeldeanlage zum Schutz von Räumlichkeiten, das für den ordnungsgemäßen Schutz vor Einbruchalarm erforderlich ist. Das System unterstützt LAN/Wi-Fi als primären Übertragungsweg und GPRS/3G/4G LTE als sekundären Übertragungsweg. Das System ist sowohl für private als auch gewerbliche Applikationen geeignet.

- Innovative Tri-X 2-Wege-Wireless-Technologie.
- Bidirektionale Funkübertragung mit AES 128-Bit Verschlüsselung
- Das Frequenzsprung-Spreizspektrum (Frequenz-Hopping Spread Spectrum, FHSS) wird verwendet, um Interferenzen zu vermeiden und die Code-Division Multiple Access (CDMA)-Kommunikation zu ermöglichen.
- Sprachausgabe bei Alarmmeldung, Systemstatus, Betriebsaufforderung usw.
- Konfiguration über Web Client, App und Cloud
- Alarmierung via Push Benachrichtigung oder Telefonanruf
- Zeigt Livebilder von Geräten an Hik-Connect angeschlossen und versendet Alarmvideoclips per E-Mail, Hik-ProConnect und Hik-Connect an.
- Sendet Alarmberichte an Leitstellen
- Unterstützt SIA DC-09 und Contact ID
- 4.520 mAh Lithium-Notstrombatterie mit 12 Stunden Standby-Dauer.

Bestellung

Modell	Beschreibung
DS-PWA64-L-WE	Unterstützt Ethernet/Wi-Fi und GPRS
DS-PWA96-M-WE	Unterstützt Ethernet/Wi-Fi, 3G/4G LTE und IC-Karte

1.2 Spezifikation

		AX PRO	
		AX PRO L	**AX PRO M**
Kapazität	Bereiche	16	32
	Zonen	Bis zu 64	Bis zu 96
	Ausgänge		
	Transponder-Lesegerät	Bis zu 8	Bis zu 8
	Tastenfelder		
	Signalgeber	4	6
	Repeater	2	4
	Fernbedienung	32	48
	Transponder	32	48
	Lesegerät integriert	×	√
Benutzer	Errichter	1	1
	Administrator	1	1
	Normale Benutzer	30	46
Funk	Funk-Frequenz	868 MHz (865 MHz für Funk PIR Kamera Bewegungsmelder)	
	Funk-Typ	2-Wege Funk-Technologie (bidirektional)	
	Funk-Sicherheit	Frequency Hopping, 128 Bit-AES Verschlüsselung	
Features	Sprachausgaben	√	√
	Sprache der Sprachausgabe	Englisch, Italienisch, Spanisch, Französisch, Russisch, Portugiesisch, Deutsch, Polnisch	
	Web Client	√	√
	Diagnose	√	√
	SMS-Benachrichtigung	√	√
	Sprachanrufbenachrichtigung	√	√
	Ereignisprotokoll	5.000 einschließlich 1.000 obligatorisch[a]	
	Funk PIR Kamera Bewegungsmelder	√	√
	IVaaS-Speicherung	×	4 Clips @ 7 Sekunden
Kommunikations-schnittstelle	Ethernet-Anschluss	10/100 Mbps self-adaptive	
	Wi-Fi	802.11b/g/n (2,4 GHz)	
	GPRS	√	×
	3G/4G LTE	×	√
	SIM-Steckplatz	Einzel	Dual
Leitstellen-Alarmierung	ATS-Kategorie[a]	DP2	
	Primärer Übertragungsweg	LAN/Wi-Fi	
	Sekundärer Übertragungsweg	GPRS oder 3G/4G LTE	

	Bestätigungsvorgang[a]	Pass-through	
	Protokolle	SIA-DC09[b], ISUP 5.0	
Cloud	Hik-ProConnect	√	√
	Hik-Connect	√	√
Automatisierung	Relais-Modul	√	√
	Relais-Modul	√	√
	Funksteckdose	√	√
Spannungsversorgung	PS Typ[c]	Typ A	
	Netzeingang	~ 100-240V 50/60Hz 0.3A(Max)	
	Batteriekapazität[d]	4.520 mAh	
	Notstromversorgun[g]	Bis zu 12 Stunden	
	Batterietyp	Integrierter Lithium-Ionen-Akku Polymer-Batterie Modell: 765965	
	Stromverbrauch	Bei Alarm: 340 mA Ohne Alarm: 405 mA	
	Stromverbrauch bei Batterienutzung	340 mA	
	Aufladezeit	4 Stunden bis 80 %	
	Niederspannungsmeldung	3,55 V	
Dienstleistung	Keine vom Benutzer zu wartenden Teile enthalten		
Umweltanforderungen	Betriebstemperatur	-10°C bis 50°C - 10℃ to＋40℃ (Zertifizierte Temperatur)	
	Relative Luftfeuchtigkeit	10 % bis 90 % (nicht kondensierend)	
Größe und Gewicht	Abmessungen (B×H×T)	170,0 mm x 170,0 mm x 38,6 mm	
	Gewicht	557,5 g	
Zertifizierungen	EN 50131	SG 2 EG II	
	CE	√	
	RoHS/Reach/WEEE	√	

a

Gemäß den in EN 50131-1:2006+A1:2009+A2:2017 definierten Anforderungen
Das AX Pro Funkbedienteil übernimmt den Pass-Through-Modus des Bestätigungsvorgangs. Sowohl die positive als auch die negative Bestätigung vom Empfänger des Empfangszentrums werden gespeichert.

Beschreibung des Ereignisprotokolls

Positive Bestätigung	ARC hochgeladen
Negative Bestätigung	Leitstellen-Kommunikation fehlgeschlagen

b	Die AX PRO Einbruchmeldeanlage ist mit SIA IP Reporting (UDP/TCP-2013) gemäß ANSI/SIA DC-09-2013 kompatibel: Internet Protokoll-Ereignisbericht. Die Einbruchmeldeanlage unterstützt Tokens (Protokolle) von **ADM-CID** und **SIA-DCS** definiert in SIA DC-07-2001.04. Vor dem Versenden wird dem Tokennamen ein „*“ am Anfang hinzugefügt (***ADM-CID** und ***SIA-DCS**, bevor die Daten verschlüsselt versendet werden. AES-128, AES-192 und AES-256 werden alle unterstützt.
c	Gemäß EN 50131-1:2006+A1:2009+A2:2017, 9.1 Typen von Netzteilen
d	Nennwert. Die tatsächliche Kapazität kann leicht variieren. Die tatsächliche Batteriekapazität für jedes einzelne Gerät kann leicht über oder unter der nominalen Batteriekapazität liegen. Das Entfernen des Akkus kann das Gerät beschädigen. Wenden Sie sich zum Austausch oder zur Reparatur der Batterie an Ihren Errichter.
e	In dem Zustand, in dem Wi-Fi, GPRS/3G/4G LTE, Leitstelle (Abfrage-Intervall: 1.800 s) verbunden sind, 8 Eingänge und 1 Bedienteil eingelernt sind und Cloud-Dienst aufgerufen wird.

Hinweis

ISUP5.0: ein Datenschutz-Internetprotokoll, das für den Zugriff auf die Drittanbieterplattform verwendet wird und das Hochladen von Alarmberichten, das AX PRO-Management und das Hochladen von Kurzvideos unterstützt.
Die Priorisierung der Meldungen und der Indikationen sind gleichwertig. AX-PRO lädt Meldungen hoch und signalisiert synchron.

Hinweis

Standard DC-09 Prüfplan:
ADM-CID: Die Datenpräsentationsmethode von DC-09 ist CID, die nicht verschlüsselt ist und nur zum Hochladen von Alarmberichten dient.
*ADC-CID: Die Datenpräsentationsmethode von DC-09 ist CID, die verschlüsselt ist und nur zum Hochladen von Alarmberichten dient.
SIA-DCS: Die Datenpräsentationsmethode von DC-09 ist DCS (auch als SIA-Protokoll bezeichnet), das nicht verschlüsselt ist und nur zum Hochladen von Alarmberichten dient.
*SIA-DCS: Die Datenpräsentationsmethode von DC-09 ist DCS (auch als SIA-Protokoll bezeichnet), das verschlüsselt ist und nur zum Hochladen von Alarmberichten dient.

RSSI Anweisung für Peripheriegeräte

In Bezug auf EN 50131-5-3 4.2.2 Anforderung der Störfestigkeit gegen Dämpfung.

Signalstärke	RSSI-Wert	Indikation	Anmerkung
Stark	>120	Grün	OK für Installation
Mittel	81 bis 120	Gelb	OK für Installation
Schwach	60 bis 80	Rot	Installation nicht empfohlen, kann aber funktionieren
Ungültig	0 bis 59	Rot (blinkt)	Nicht OK zu installieren, kann nicht normal funktionieren

Hinweis

Installieren Sie Peripheriegeräte nur, wenn die Signalstärke über 80 liegt. Um ein viel besseres System zu erhalten, installieren Sie bei 120 und höher.

AX PRO Benachrichtigungsoptionen

Die AX PRO Einbruchmeldeanlage ist für die unten aufgeführten Meldeanforderungen zusammen mit den erforderlichen Signalgebern geeignet

Benachrichtigungsausrüstung	I&HAS Stufe 2		
	Optionen		
	C	E	F
Selbstversorgt hörbare WD	2	1	Optional:
ATS	DP1	Optional:	DP2

1.3 Aussehen

Vorderseite

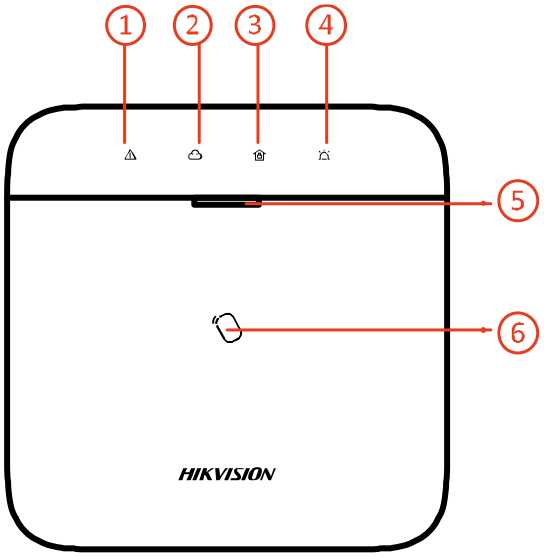


Tabelle 1 - 2 Beschreibung der Vorderseite

Nr.	Name	Beschreibung
1	Warnanzeige	Dauerhaft orange: Im Status unscharf zeigt die LED einen Alarm (z.B. Sabotagealarm) und Fehler (z.B. Verbindungsfehler) an. Hinweis ● Die Anzeige oder die Sprachbenachrichtigungen reagieren nicht auf Vorgänge, die von Benutzern der Stufe1 durchgeführt werden. Benachrichtigungen werden nur ausgegeben, wenn ein Benutzer der Stufe 1 einen gültigen Transponder oder eine Fernbedienung verwendet. ● Das Gerät gibt detaillierte Alarm- oder Fehlerinformationen aus, während ein autorisierter Benutzer das System unscharf schaltet.
2	Verbindungsanzeige	Dauerhaft grün: Die Zentrale ist mit einem Hik-Connect-Konto verbunden Aus: Die Zentrale ist nicht mit einem Hik-Connect-Konto verbunden
3	Anzeige für	Dauerhaft blau für 5Sekunden: Scharfgeschalten

Nr.	Name	Beschreibung
	Scharf/Unscharf	Blinkt zweimal grün: Unscharfgeschalten Hinweis Wenn die Funktion **Scharfschalte LED** aktivieren, leuchtet die LED dauerhaft blau, wenn die Anlage scharfgeschalten ist, und leuchtet nicht, wenn sie unscharfgeschalten ist. Die Funktion entspricht nicht der EN-Norm.
4	Anzeige für Alarm	Rot blinkend: Alarm aufgetreten Dauerhaft rot: Sabotagealarm Aus: Kein Alarm
5	Stromanzeige	Dauerhaft grünt: Einschalten Aus: Ausschalten
6	Transponder Lesebereich	Hinweis Funktionen variieren je nach Modell.

Komponente und Schnittstelle

Entfernen Sie die hintere Abdeckung, auf der Rückseite befinden sich einige Schnittstellen.

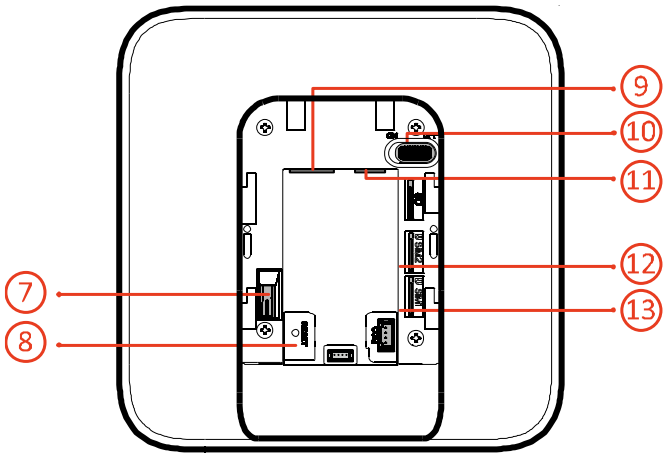


Tabelle 1 - 3 Beschreibung der Rückseite

Anzahl	Beschreibung
7	Sabotagekontakt
8	Reset-Taste

Anzahl	Beschreibung
	Hinweis Starten Sie das Gerät neu, die Betriebs-LED blinkt 3 Mal und halten Sie die Reset-Taste 5 Sekunden lang gedrückt. Die Sprachansage zeigt das Ausführungsergebnis an. Drücken Sie die Taste, um den STA- und Hotspot-Modus zu wechseln.
9	Stromanschluss
10	Netzschalter
11	Netzwerkschnittstelle
12	SIM-Kartensteckplatz 1 **Hinweis** Die Funktion von GPRS oder 3G/4G (funktioniert nur mit einer SIM-Karte) ist Modellabhängig.
13	SIM-Kartensteckplatz 2 **Hinweis** Die Funktion von GPRS oder 3G/4G (funktioniert nur mit einer SIM-Karte) ist Modellabhängig.

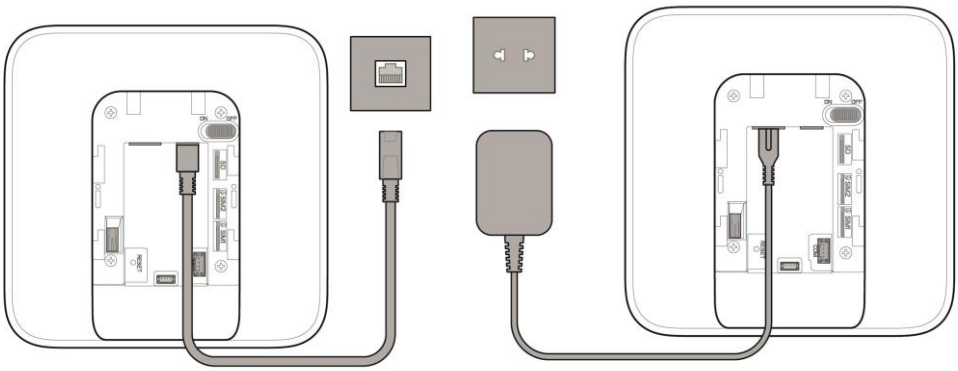
Kapitel 2 Inbetriebnahme

2.1 Initialisierung des Geräts

Während Sie das Gerät mit Hik-ProConnect initialisieren, sollte das AX Pro immer zuerst zu einem Installer-Konto hinzugefügt werden. Das Installer-Konto wird auf das Administratorkonto übertragen, nachdem alle anfänglichen Einstellungen und Tests abgeschlossen wurden. Führen Sie die folgenden Schritte aus, um das Funk Alarmsystem zu initialisieren.

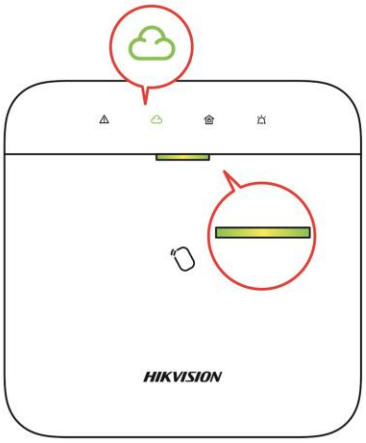
1. Stellen Sie eine Verbindung zum Netzwerk her.

Schließen Sie das Gerät an das Netzwerk an und schalten Sie das Gerät ein.



Hinweis

Während das Gerät eingeschaltet ist, leuchten die Betriebs-LED und die Verbindungs-LED grün.



2. Einen Standort erstellen

Öffnen Sie Hik-ProConnect und melden Sie sich mit dem Installer-Konto an.

Ein Standort ist der Ort, an dem das Alarmsystem eingesetzt wird. Erstellen Sie einen Standort, zu dem das Gerät mit dem Standortnamen und der Adresse hinzugefügt werden kann. Der Eigentümer vom Standort wäre ein Endbenutzer, der normalerweise als Administrator betrachtet wird.

3. Gerät hinzufügen

Öffnen Sie den Standort. Tippen Sie auf **Gerät hinzufügen** und scannen Sie den QR-Code auf dem Etikett des Gerätes.

Die Systemsteuerung wird dem vom Installer-Konto erstellten und verwalteten Standort hinzugefügt, was auch bedeutet, dass das Installer-Konto im Panel erstellt wurde.

Das Installationsprogramm kann nun die Konfiguration und Tests der Zentrale vor der Bereitstellung von durchführen. Sowohl der Hik-ProConnect-Dienst als auch der lokale WebClient können mit dem Hik-ProConnect-Installationskonto angemeldet werden.

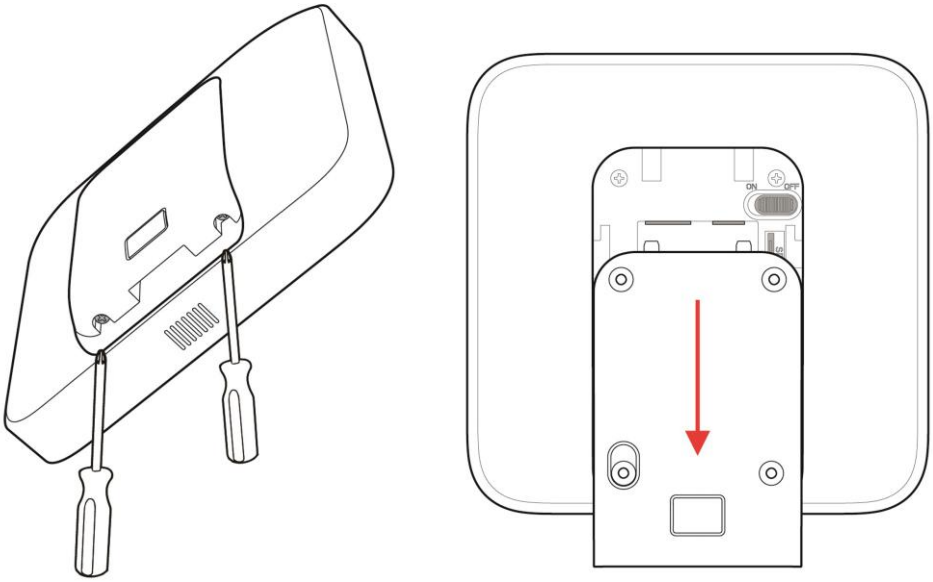
Hinweis

Während Sie das Gerät mit Hik-Connect initialisieren, müssen Sie nicht zuerst einen Standort erstellen. Laden Sie die App herunter, melden Sie sich an und fügen Sie das Gerät durch Scannen des QR-Codes hinzu oder geben Sie die Seriennummer des Geräts ein.

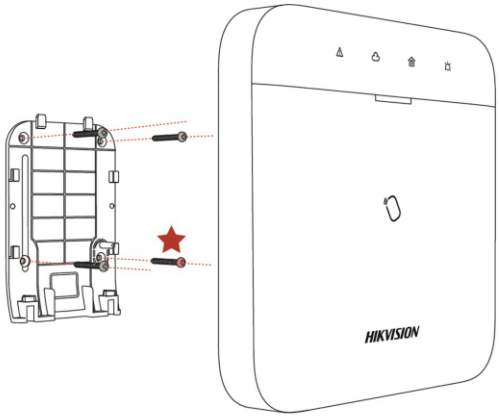
2.2 Installieren des Geräts

Vorgehensweise

1. Lösen Sie die Schraube an der hinteren Abdeckung. Schieben Sie die hintere Abdeckung nach unten, um sie zu entfernen.



2. Befestigen Sie die hintere Abdeckung mit den mitgelieferten Schrauben an der vorgesehenen Position. Befestigen Sie die hintere Abdeckung und ziehen Sie die Schraube fest, um die Installation abzuschließen.



Hinweis

- Roter Stern: SICHERUNGSSCHRAUBE. Es ist zwingend erforderlich, den Sabotagekontakt zu sichern.
- Es sind keine Anpassungen erforderlich.
- Nur zur Verwendung in den überwachten Räumlichkeiten.

Hinweis

Überprüfen Sie die Funk-Signalstärke vor dem Anschluss und der Installation von weiteren Funkkomponenten. Sie können die Funk-Signalstärke auf der Anzeige der Funkkomponenten sehen.

Kapitel 3 Benutzerverwaltung

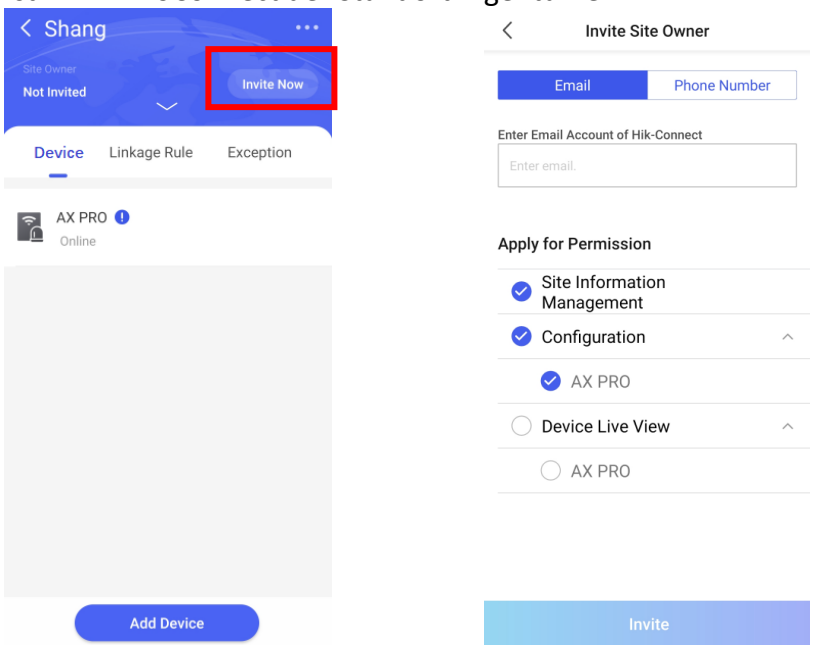
3.1 Benutzerverwaltung

Hinweis

- Die Benutzer können nur in der APP erstellt werden.
- Die Länge vom Benutzername kann 1 bis 27 Zeichen und vom Passwort kann 8 bis 16 Zeichen lang sein (Webclient und APP-Benutzer).

3.1.1 Den Administrator einladen

Der Administrator ist in Hik-ProConnect der Standort-Eigentümer.



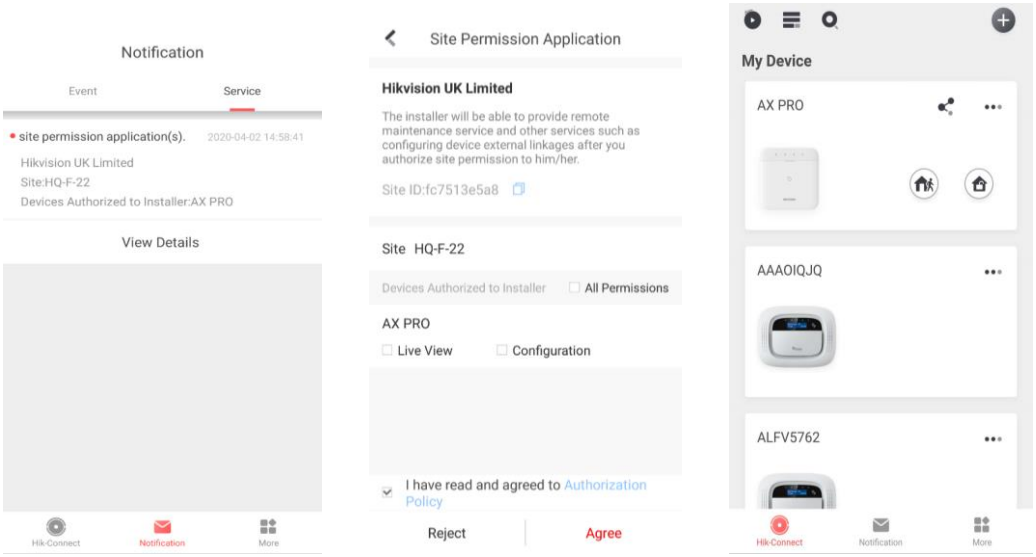
Nach Abschluss der Erstkonfiguration muss der Errichter den Standort-Eigentümer einladen und die Berechtigung der Standort-Verwaltung und Gerätekonfiguration übertragen. Das Administratorkonto ist ein Endbenutzerkonto im Hik-Connect-Dienst.

Klicken Sie auf die Schaltfläche „Jetzt einladen“ und geben Sie das E-Mail-Konto oder Telefonnummer ein, um den Standort an den Administrator zu übertragen. Gleichzeitig wird der Errichter die Berechtigungen des Standort-Eigentümers anfragen, z.B. Konfiguration und Verwaltung.

Öffnen Sie die Hik-Connect-App und melden Sie sich mit dem Administratorkonto an. Die Errichter Anfrage wird auf der Benachrichtigungsseite angezeigt. Öffnen Sie die Benachrichtigungsdetails, um die Errichter Anfrage zu akzeptieren und die Berechtigungen zu übertragen. Das Bedienteil und

andere Geräte am Standort werden in Ihrer Geräteliste angezeigt.

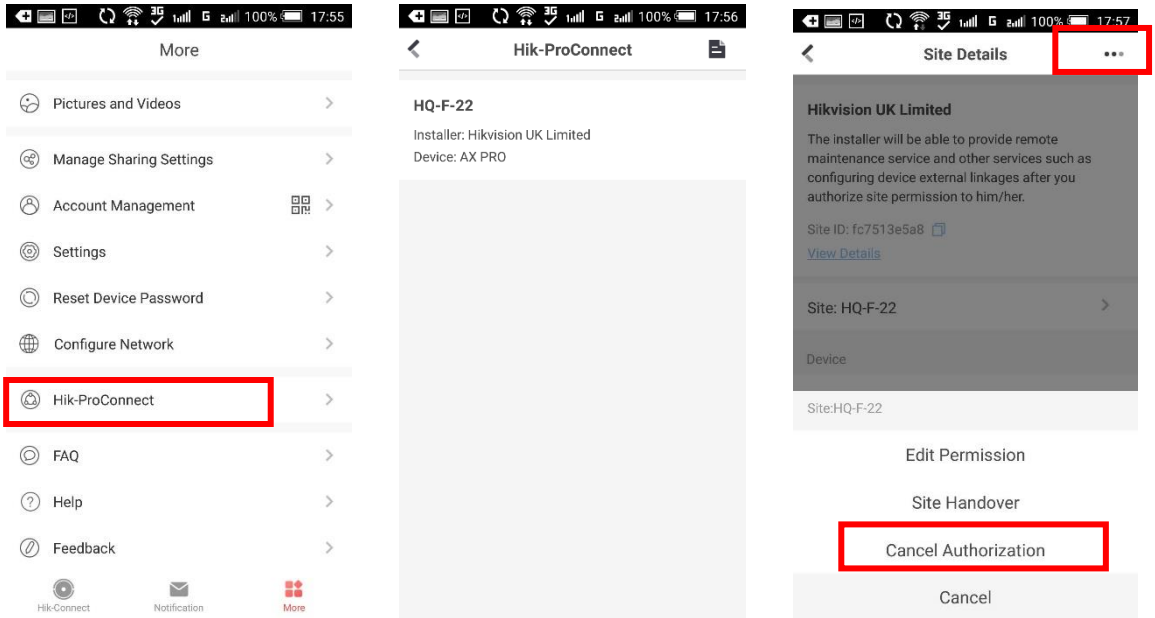
Das Administratorkonto wird der Zentral hinzugefügt, das zur Anmeldung bei der Hik-Connect-App und dem lokalen Webclient verwendet werden kann.



3.1.2 Errichter Zugriff auf das System unterbrechen

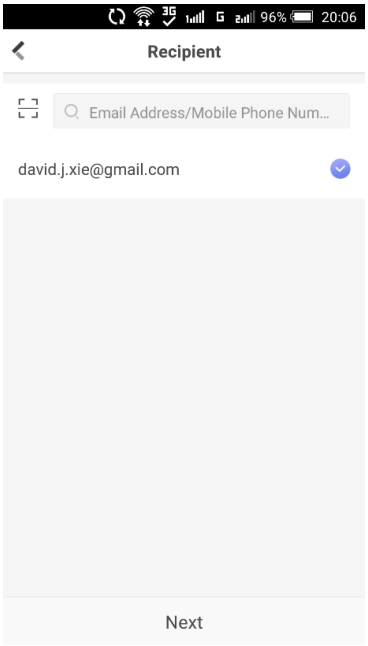
Der Administrator kann die Zugriffsberechtigung des Errichters aufheben.

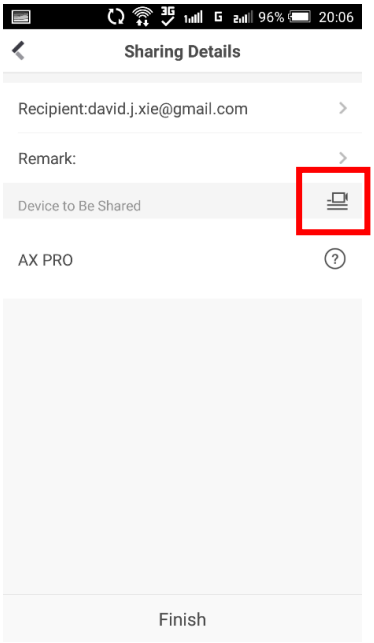
1. Wählen Sie Seite **Weitere Informationen** und tippen Sie auf **Hik-ProConnect**. Alle vom Hik-ProConnect-Dienst verwalteten Standorte sind auf der Seite aufgeführt.
2. Tippen Sie auf die Optionsschaltfläche in der oberen rechten Ecke der Seite und tippen Sie auf **Autorisierung abbrechen**.
3. Bestätigen Sie den Vorgang und die Autorisierung des Errichters wird aufgehoben. Sobald die Autorisierung aufgehoben wurde, muss der Errichter diese erneut anfragen.



3.1.3 Hinzufügen eines Benutzers

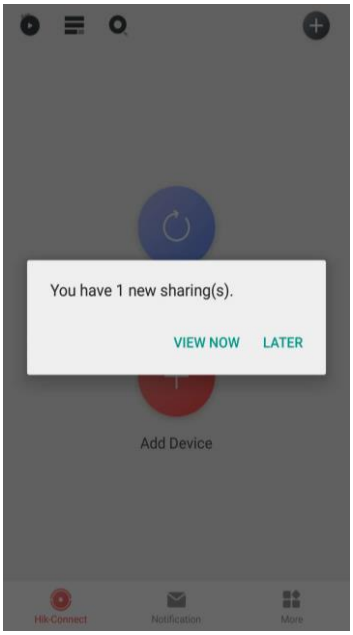
Der Administrator kann das Gerät für andere Benutzer freigeben.

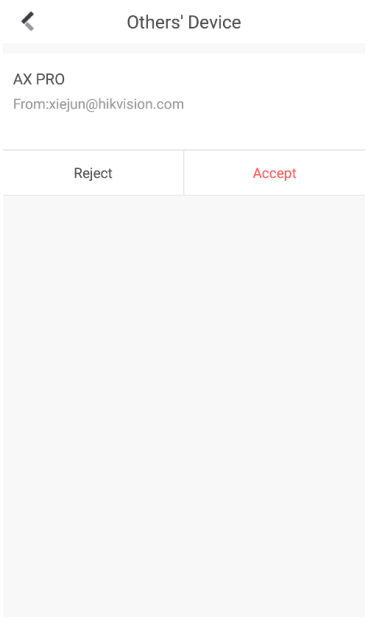


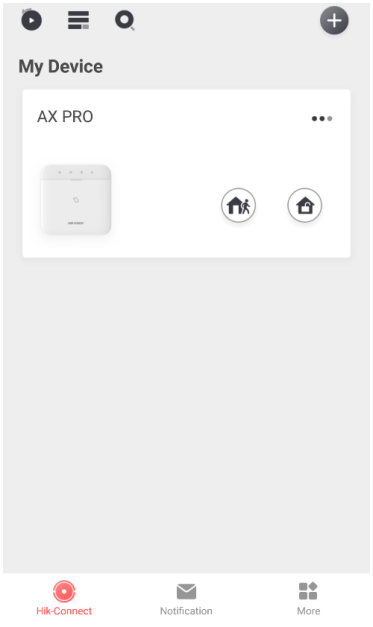


1. Tippen Sie auf (Freigabetaste) in der Geräteliste.
2. Öffnen Sie das Hik-Connect-Konto des Benutzers.

   Der Administrator kann auch auswählen, welches Gerät freigegeben werden soll.







Eine Benachrichtigung wird an das Konto des Benutzers gesendet. Dieser kann die Nachricht in der Hik-Connect App lesen.

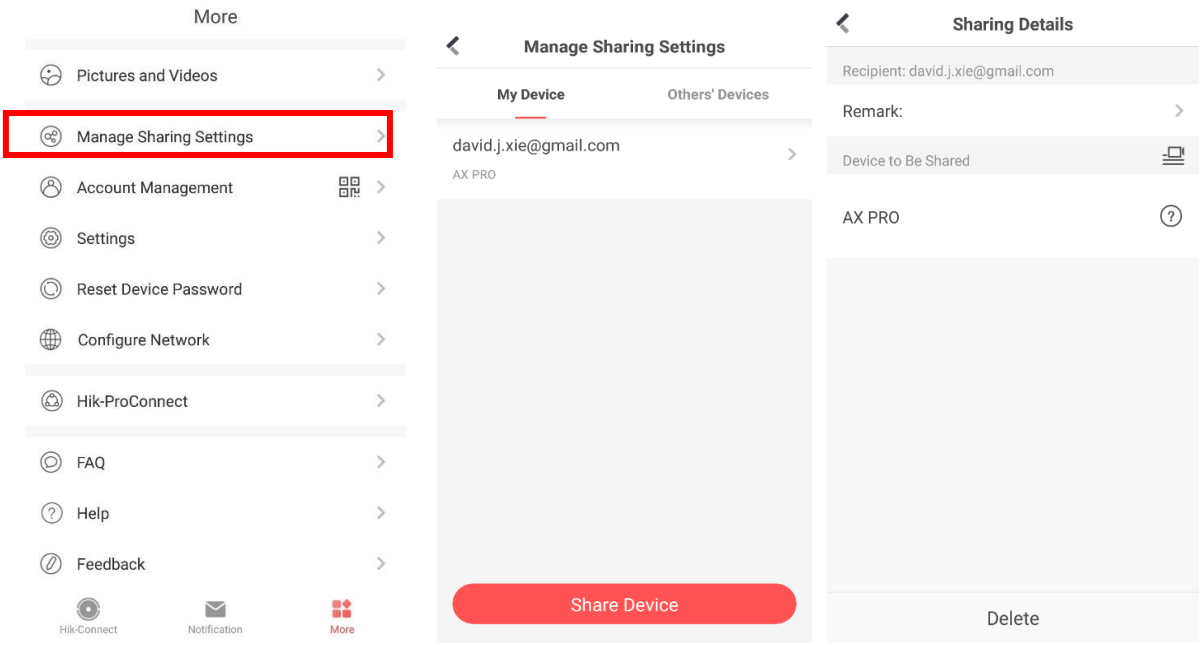
3. Nehmen Sie die Einladung an und das Gerät wird in der Geräteliste aufgeführt.

Das Benutzerkonto wird der Zentrale hinzugefügt, das zur Anmeldung bei der Hik-Connect-App und dem lokalen WebClient verwendet werden kann.

3.1.4 Löschen eines Benutzers

Der Administrator kann einen Benutzer löschen.

1. Wählen Sie die Seite **Weitere Informationen** und tippen Sie auf **Freigabeeinstellungen**.
2. Löschen Sie den ausgewählten Benutzers oder entfernen Sie ihn vom Gerät.



3.2 Zugriffseinträge

Der Errichter und der Benutzer werden verschiedene Zugriffsebenen zugewiesen, die Systemfunktionen definieren, die ein einzelner Benutzer ausführen kann. Für verschiedene Benutzerrollen mit einer bestimmten Zugriffsebene werden verschiedene Benutzereinträge bereitgestellt.

Zugriffseinträge für Errichter (Zugriffsebene 3)

- **Hik-ProConnect Dienst**
  Hik-ProConnect ist ein Service für Errichter, der zur Fernverwaltung der Alarmsysteme von Kunden an verschiedenen Standorten verwendet wird. Einbruchmeldeanlagen können einem Errichter-Konto im Hik-ProConnect Dienst hinzugefügt und anhand Standorten verwaltet werden.

- **Lokaler Webclient**
  Rufen Sie die IP-Adresse des Geräts auf. Nutzen Sie für die Suche im Netzwerk das SADP-Tool.

Der Errichter kann sich mit dem Hik-ProConnect Servicekonto anmelden, nachdem die Anlage hinzugefügt wurde.

- **Veraltete Einträge**
  Bedienteil-PIN Codes und -Transponder können auch dem Errichter auf einer bestimmten Zugriffsebene zugewiesen werden, um wesentliche Vorgänge auszuführen.

Zugriffseinträge für Administrator und Benutzer (Zugriffsebene 2)

- **Hik-Connect Dienst**
  Endbenutzer können den Hik-Connect Dienst verwenden, um auf die Geräte zuzugreifen und sie zu verwalten.
- **Lokaler Webclient**
  Sobald die Zentrale dem Endbenutzerkonto im Hik-Connect Dienst hinzugefügt wurde, kann das Hik-Connect-Konto zur Anmeldung verwendet werden.
- **Veraltete Einträge**
  Bedienteil-PIN Codes und -Transponder können auch dem Endbenutzer auf einer bestimmten Zugriffsebene zugewiesen werden, um wesentliche Vorgänge auszuführen.

Kapitel 4 Konfiguration

4.1.Einrichtung mit Hik-ProConnect

4.1.1 Verwendung der Hik-ProConnect App

Der Errichter kann AX PRO mit dem Hik-ProConnect konfigurieren, z.B. Aktivierung, Geräteregistrierung usw.

Hik-ProConnect herunterladen und anmelden

Laden Sie die Hik-ProConnect App herunter und melden Sie sich mit Ihrem Konto an.

Vorgehensweise

1. Laden Sie die Hik-ProConnect App herunter.
2. Optional: Registrieren Sie ein neues Konto, wenn Sie die Hik-ProConnect App zum ersten Mal verwenden.

Hinweis

- Weitere Informationen finden Sie unter *Benutzerhandbuch der Hik-ProConnect App*.
- Sie benötigen einen Einladungscode für die Registrierung. Bitte wenden Sie sich an den technischen Support.

3. Führen Sie dies aus und melden Sie bei der App an.

AX PRO Zentrale der App hinzufügen

Fügen Sie als erstes AX PRO zur App hinzu.

Vorgehensweise

1. Schalten Sie die AX PRO Zentrale ein.
2. Erstellen oder suchen Sie einen Standort.
   – Um einen Standort zu erstellen tippen Sie auf **+**, geben Sie den Standortnamen, die Zeitzone und die Adresse ein und tippen Sie auf **OK**.
   – Geben Sie den Namen des Standorts in den Suchbereich ein und tippen Sie auf **Suchsymbol** zum durchsuchen.
3. Tippen Sie auf **Gerät hinzufügen**.
   – Tippen Sie auf **QR-Code scannen**. Scannen Sie den QR-Code auf der AX PRO Zentrale.

Hinweis

Normalerweise ist der QR-Code auf das Etikett auf der Rückseite des AX PRO Zentrale aufgedruckt.

Tippen Sie auf **Manuell hinzufügen**. Geben Sie die Seriennummer und den Verifizierungscode des Geräts ein, um das Gerät hinzuzufügen.

4. Aktivieren Sie das **Gerät**.

Funkkomponenten der AX PRO Zentrale hinzufügen

Peripheriegeräte der AX PRO Zentrale hinzufügen.

Vorgehensweise

1. Wählen Sie einen Standort aus.
2. Wählen Sie eine AX PRO Zentrale aus.
3. Tippen Sie auf das **+** Symbol.
   - Tippen Sie auf **QR-Code scannen**. Scannen Sie den QR-Code auf der Funkkomponente.
   - Tippen Sie auf **Manuell hinzufügen**. Geben Sie die Seriennummer und den Verifizierungscode des Geräts ein, um das Gerät hinzuzufügen.

Benutzerverwaltung

Die Errichter (Benutzer von Hik-ProConnect) können Benutzer verwalten. Wenn Sie der Administrator sind, können Sie Benutzer hinzufügen, bearbeiten und löschen und den neu hinzugefügten Benutzern unterschiedliche Berechtigungen zuweisen. Wenn Sie ein Errichter sind, können Sie nur Benutzer hinzufügen und löschen.

Vorgehensweise

Hinweis

Es gibt vier Benutzertypen für AX PRO, einschließlich Administrator (oder Eigentümer), Benutzer, Errichter und Hersteller. Verschiedene Benutzertypen haben unterschiedliche Berechtigungen für den Zugriff auf die Funktionalität des AX PRO Systems.

1. Wählen Sie den Standort und das AX PRO System aus und melden Sie sich an.
2. Tippen Sie auf **Weiter**, um den Benutzer einzuladen.

Hinweis

Der Empfänger muss die Einladung annehmen.

3. Tippen Sie auf → **Benutzerverwaltung** → **Benutzer**.
4. Tippen Sie auf einen Benutzer, um die Seite „Benutzerverwaltung“ aufzurufen.
5. Optional: Führen Sie bei Bedarf die folgenden Schritte durch.

Benutzerberechtigung	Sie können auf den Benutzer in der Benutzerliste tippen und dann auf **Symbol bearbeiten** um die Berechtigungen festzulegen. **Hinweis** Nur der Administrator kann einen solchen Vorgang ausführen.
Verknüpfte Bereiche festlegen	Wenn der Benutzer ein Benutzer ist, tippen Sie auf den Benutzer in der Benutzerliste und dann auf **Verknüpfte Bereiche**, um den Benutzer verknüpften Bereiche zuzuweisen. **Hinweis** Nur der Administrator kann einen solchen Vorgang ausführen.
Bedienteil Pin Code bearbeiten	Wenn der Benutzer ein Administrator, ein Errichter oder ein Hersteller ist, können Sie auf den Benutzer in der Benutzerliste tippen und dann auf **Bedienteil Pin Code bearbeiten**, um den Pin Code für den Benutzer festzulegen.
Überfall PIN bearbeiten	Wenn der Benutzer ein Administrator ist, können Sie auf den Benutzer in der Benutzerliste tippen und dann auf **Überfall PIN bearbeiten**, um den Überfall PIN für den Benutzer festzulegen. **Hinweis** Wenn Sie gezwungen werden die Alarmanlage unscharf zu schalten, sollten Sie den Überfall PIN verwenden, um einen stillen Alarm auszulösen.

Hinweis

- Konfigurationselemente und Benutzerberechtigungen variieren je nach Benutzertyp.
- Sie können verknüpfte Transponder und Fernbedienungen des Benutzers anzeigen, haben jedoch keine Berechtigung diese zu konfigurieren.

Beispiel

Geben Sie ein Beispiel ein, das die aktuelle Aufgabe veranschaulicht (optional).

Was als nächstes zu tun ist

Geben Sie die Aufgaben ein, die der Benutzer nach Abschluss dieser Aufgabe ausführen soll (optional).

Transponder Verwaltung

Nach dem Hinzufügen von Transponder zum AX PRO System können Sie den Transponder vorhalten, um bestimmte oder alle Bereiche scharf/unscharf zu schalten und Alarme zu löschen.

Hinweis

Die Transponder ID/PIN ist eine 32-Bit-lange Ganzzahl, daraus ergeben sich 42.949.672.956 Varianten.

Vorgehensweise

1. Wählen Sie den Standort, wählen Sie das AX PRO System und melden Sie sich an.
2. Tippen Sie auf → **Benutzerverwaltung** → **Transponder** um die Seite „Transponder-Verwaltung“ aufzurufen.
3. Tippen Sie auf **+** um einen Transponder hinzuzufügen.
4. Wenn Sie die Sprachaufforderung „Transponder vorhalten“ hören, sollten Sie den Transponder der AX PRO Zentrale vorhalten.
   - Wenn ein Signalton ertönt, wurde der Transponder erkannt.
   - Der Transponder wird auf der Transponder-Seite angezeigt.
5. Optional: Tippen Sie auf einen Transponder, um die Einstellungsseite aufzurufen.
6. Tippen Sie auf **Symbol bearbeiten**, um den Transponder-Namen zu bearbeiten.

Hinweis

- Wenn Sie sich als Errichter anmelden, überspringen Sie diesen Schritt. Nur Administratoren können den Namen von Transponder bearbeiten.
- Der Name sollte 1 bis 32 Zeichen enthalten.

7. **Transponder aktivieren**...
8. Wählen Sie einen verknüpften Benutzer aus.
9 Wählen Sie den Transponder-Typ aus

Hinweis

Verschiedene verknüpfte Benutzer haben unterschiedliche Transponder-Berechtigungen.

Benutzer Transponder

Sie können durch vorhalten des Transponders das System scharf-/unscharfschalten.

Wächterrundgang Transponder

Wenn Sie den Transponder vorhalten, lädt das System einen Datensatz hoch.

10 Optional: Tippen Sie auf **Löschen** um den Transponder zu löschen.

Systemeinstellungen

Systemkonfiguration

Sie können die Zeitzone des Geräts und die Sommerzeit einstellen.

Wählen Sie den Standort und das AX PRO System aus und melden Sie sich dann an.

Tippen Sie auf → **System** → **Konfiguration**, um die Konfigurationsseite aufzurufen.

Antippen, um eine Zeitzone auszuwählen.

Sie können die Sommerzeit aktivieren und die Sommerzeit-Bias, die Sommerzeit-Startzeit und die Sommerzeit-Endzeit einstellen.

Systemoptionen

Stellen Sie die Systemoptionen ein.

Optionen Verwaltung

Wählen Sie den Standort und das AX PRO System aus und melden Sie sich dann an. Tippen Sie auf → System → Systemoptionen → Optionsverwaltung, um die Seite aufzurufen.

Zwangs-Scharfschaltung

Wenn diese Option aktiviert ist und aktive Fehler in einer Zone vorliegen, wird die Zone automatisch Bypassed (umgangen).

Systemfehlerbericht

Wenn die Option aktiviert ist, meldet das Gerät den Systemfehler automatisch.

Sprachausgabe

Wenn die Option aktiviert ist, ist die Sprachausgabe für die AX PRO Zentrale aktiviert.

Sprachaufforderung zum Unscharfschalten und Löschen des Alarms

Wenn die Option aktiviert ist, sendet die AX PRO Zentrale alle Systemfehler vor der Unscharfschaltung und Löschen der Alarme.

Hinweis

Um die Funktion aktivieren zu können, muss zuvor die Funktion Sprachansage aktiviert sein.

Systemlautstärke

Der Lautstärke liegt zwischen 0 und 10.

Verknüpfter Sabotagealarm

Wenn die Option aktiviert ist, wird die AX PRO Zentrale bei Sabotagealarm alle akustischen Signalgeber, Bedienteile und andere verknüpfte Geräte alarmieren.

System sperren

Wenn die Option aktiviert ist, kann der Errichter die AX PRO Zentrale mit einer Taste sperren. Nach dem Sperren können Benutzer das Gerät nicht mehr bedienen und Nachrichten empfangen.

Paketverlust-Zeiten bei Kommunikationsfehlern

Wenn die Option aktiviert ist, erkennt das System den interaktiven Heartbeat zwischen Funkkomponenten und dem AX PRO System. Wenn kein Heartbeat erkannt wird, ist das Gerät offline.

Fehlerprüfung

Wählen Sie den Standort und das AX PRO System aus. Tippen Sie auf → System → Systemoptionen → Fehlerprüfung.

Netzwerkkamera- Getrennte Verbindung erkennen

Wenn die Option aktiviert ist und die verknüpfte Netzwerkkamera getrennt wird, wird ein Alarm ausgelöst.

Batterie Fehlerprüfung

Wenn die Option aktiviert ist, lädt das Gerät keine Ereignisse hoch, wenn die Batterie getrennt oder nicht geladen ist.

Netzwerk Fehlerprüfung

Wenn die Option aktiviert ist und das drahtgebundene Netzwerk getrennt ist oder andere Fehler vorliegen, wird der Alarm ausgelöst.

WLAN Fehlerprüfung

Wenn die Option aktiviert ist und die WLAN-Verbindung getrennt wird oder andere Fehler vorliegen, wird der Alarm ausgelöst.

Mobilfunknetz Fehlerprüfung

Wenn die Option aktiviert ist und das Mobilfunk-Datennetzwerk getrennt ist oder andere Fehler vorliegen, wird der Alarm ausgelöst.

Stromausfall Prüfzeit

Das System prüft den Fehler nach der konfigurierten Zeitdauer, nach dem Abschalten des Netzstroms.
Um die Norm EN 50131-3 zu erfüllen, sollte die Prüfdauer 10 Sekunden betragen.

Systemanweisungen

Wählen Sie den Standort und das AX PRO System aus und melden Sie sich dann an. Tippen Sie auf → System → Systemoptionen → Systemanweisungen.

Scharfschalten stoppen

Wenn diese Option aktiviert ist und während des Scharfschaltung ein Fehler auftritt, können Sie die Scharfschaltung manuell stoppen.

Fehlerprüfung

Das System prüft ob der Scharfschaltung Fehler vorliegen.

Scharfschalten mit Fehler

Überprüfen Sie die Fehler in der Fehlerliste und die Fehler werden bei der Scharfschaltung ignoriert.

Scharfschaltungsanzeige leuchtet

Wenn das Gerät den EN-Standard anwendet, ist die Funktion standardmäßig deaktiviert. Wenn das Gerät aktiviert ist, leuchtet die Anzeige 5 Sekunden lang durchgehend blau. Wenn die Zentrale unscharf geschalten ist, blinkt die Anzeige 5 Mal.
Wenn die Funktion aktiviert ist, und das Gerät scharf geschalten ist, leuchtet die Anzeige dauerhaft. Und wenn die Zentrale unscharf geschalten ist, ist die Anzeige aus.

Fehler beim Scharfschalten melden

Wenn das Gerät den EN-Standard anwendet, ist die Funktion standardmäßig deaktiviert. Wenn diese Option aktiviert ist, wird während des Scharfschaltung kein Fehler gemeldet.

Frühalarm

Wenn diese Option aktiviert ist und die Zone scharfgeschalten und ausgelöst wird, wird der Alarm nach der Verzögerungszeit ausgelöst.

Verzögerungszeit

Wenn die Funktion “Frühalarm“ aktiviert ist, sollten Sie die Verzögerungszeit einstellen. Der Alarm wird nach der konfigurierten Verzögerungszeit ausgelöst.

Einlernmethode

Wählen Sie den Standort und das AX PRO System aus und melden Sie sich dann an. Tippen Sie auf → System → Systemoptionen → Einlernmethode.

Tippen Sie auf Einlernmodus eingeben.

Folgen Sie den Anweisungen, um ein Gerät hinzuzufügen.

Tippen Sie auf Einlernmodus beenden.

Netzwerkkamera

Kameras zu AX PRO hinzufügen

Vorgehensweise

1. Wählen Sie den Standort und das AX PRO System aus und melden Sie sich dann an.
2. Tippen Sie auf → **IPC** → **IPC-Verwaltung**.
3. Tippen Sie auf **Hinzufügen**.
4. Geben Sie die IP-Adresse, den Port, den Benutzernamen und das Passwort der Kamera ein.
5. Tippen Sie auf **Symbol „Speichern“**.

6. Optional: Tippen Sie auf **Bearbeiten** oder **Löschen** um die ausgewählte Kamera zu bearbeiten oder zu löschen.

Videoparameter einstellen

Vorgehensweise

1. Wählen Sie den Standort und das AX PRO System aus und melden Sie sich dann an.
2. Tippen Sie auf → **IPC** → **Video Ereignis Einstellungen**.
3. Wählen Sie eine Kamera aus und stellen Sie die Videoparameter ein.

Stream Typ

Main Stream: Wird für die Aufnahme- und HD-Vorschau verwendet und verfügt über eine hohe Auflösung, Bitrate und Bildqualität.
Sub Stream: Wird für das Videostreaming und Vorschaubilder verwendet, mit niedrigerer Auflösung, Bitrate und Bildqualität.

Bitratentyp

Wählen Sie den Bitratentyp als Konstant oder Variable aus.

Auflösung

Wählen Sie die Auflösung des Videoausgangs aus.

Video Bitrate

Der höhere Wert entspricht der höheren Videoqualität, aber eine höhere Bandbreite ist erforderlich.

Zeitplan für scharf-/unscharfschalten festlegen

Stellen Sie den Zeitplan fürs scharf-/unscharfschalten ein, um eine bestimmte Zone automatisch scharf/unscharf zu schalten.

Wählen Sie den Standort und das AX PRO System aus und melden Sie sich dann an.

Tippen Sie auf → **Bereich**.

Tippen Sie auf einen Bereich in der Liste, aktivieren Sie den Bereich und wählen Sie verknüpfte Zonen aus.

Aktivieren Sie die Funktion „Automatisches Scharf-/Unscharfschalten“ und stellen Sie die Zeit für das „Automatisches Scharf-/Unscharfschalten“ schalten ein. Sie können auch die Uhrzeit für Deadline Unscharfschalten, die Eingangsverzögerungszeit, die Ausgangsverzögerungszeit, die akustische Verzögerungszeit, die Wochenendausnahme und die Feiertagausnahme einstellen.

Automatisches. Scharfschalten

Aktivieren Sie den Bereich, um den Bereich zu einem bestimmten Zeitpunkt automatisch scharf zu schalten.

Zeitpunkt für Automatisches Scharfschalten

Stellen Sie den Zeitplan fürs automatische Scharfschalten ein.

Deadline Unscharfschalten

Die Zentrale sendet eine Benachrichtigung an das Telefon oder Tablet, um den Benutzer daran zu erinnern, den Bereich unscharf zu schalten, wenn der Bereich nach einem bestimmten Zeitpunkt noch scharfgeschalten ist.

Hinweis

Sie sollten die Benachrichtigungs-Funktion der Zentrale auf dem Web Client von **Kommunikationsparameter** → **Ereigniskommunikation** bevor Sie die Funktion „Deadline Unscharfschalten“ aktivieren.

Uhrzeit für Deadline Unscharfschalten

Legen Sie den Zeitpunkt der **Deadline Unscharfschalten** fest. Bis zu diesem Zeitpunkt muss die Zentrale unscharf geschalten werden.

Wochenendausnahme

Wenn aktiviert sind die Funktionen **Automatisches Scharfschalten**, **Automatisches Unscharfschalten** und **Deadline Unscharfschalten** am Wochenende deaktiviert.

Feiertagsausnahme

Aktivieren Sie die Funktion und die Zone wird am Feiertag nicht scharf-/unscharfgeschalten. Sie sollten den Feiertagsplan nach der Aktivierung von festlegen.

Hinweis

Es können bis zu 6 Feiertagsgruppen festgelegt werden.

Kommunikation

Mobilfunknetz

Geben Sie hier eine kurze Beschreibung Ihrer Aufgabe ein (optional).

Vorgehensweise

1. Wählen Sie den Standort und das AX PRO System aus und melden Sie sich dann an.
2. Tippen Sie auf → **Kommunikation** → **Mobilfunknetz**.
3. **Mobilfunknetz** aktivieren.
4. Tippen Sie auf **Parameterkonfiguration** → **Symbol bearbeiten** und setzen Sie Parameter, einschließlich Benutzername, APN, MTU und PIN-Code.
5. Tippen Sie auf **Symbol „Speichern“**.
6. Aktivieren Sie **Datennutzungslimit**.
7. Bearbeiten **In diesem Monat verwendete Daten** und **Daten begrenzt pro Monat**.

App Push-Benachrichtigung

Wenn ein Alarm ausgelöst wird und Sie die Alarmbenachrichtigung an Ihr Telefon senden möchten, können Sie die Push-Parameter für die Benachrichtigung festlegen.

Vorgehensweise

1. Wählen Sie den Standort und das AX PRO System aus und melden Sie sich dann an.
2. Tippen Sie auf → **Kommunikation** → **App Push-Benachrichtigung**.
3. Tippen Sie auf **Telefonnummer hinzufügen** und geben Sie die Telefonnummer ein.
4. Aktivieren Sie **Telefonanruf** und **SMS-Nachricht** je nach Ihren Bedürfnissen.
5. Stellen Sie die **Anzahl der Anrufe** ein.
6. Überprüfen Sie die Benachrichtigungen.

Zonenalarm- und Sabotagealarm-Benachrichtigung

Das Gerät sendet Benachrichtigungen, wenn der Zonenalarm ausgelöst oder der Zonen Sabotagealarm ausgelöst oder wiederhergestellt wird.

Hinweis

Sie müssen die Intervallzeit für die Ereignisfilterung einstellen.

Zentrale Benachrichtigungsverwaltung

Das Gerät sendet Push-Benachrichtigungen, wenn der Benutzer das AX PRO System bedient.

Alarmbenachrichtigung bei Sabotage von Funkkomponenten

Das Gerät sendet Benachrichtigungen, wenn der Alarm einer Funkkomponente ausgelöst oder wiederhergestellt wird.

AX PRO Sabotagealarm-Benachrichtigung

Das Gerät sendet Benachrichtigungen, wenn der Sabotagealarm der Zentrale ausgelöst oder wiederhergestellt wird.

Überfall-Benachrichtigung

Das Gerät sendet Benachrichtigungen, wenn ein Überfallalarm durch Zonen, Bedienteile oder Fernbedienungen ausgelöst oder wiederhergestellt wird.

Medizinischer Notruf Benachrichtigung

Das Gerät sendet Benachrichtigungen, wenn ein medizinischer Alarm ausgelöst wird.

Gasalarm Benachrichtigung

Das Gerät sendet Benachrichtigungen, wenn ein Gasalarm ausgelöst wird.

Feueralarm Benachrichtigung

Das Gerät sendet Benachrichtigungen, wenn ein Feueralarm ausgelöst wird oder ein Benutzer die Feueralarmtaste auf dem Bedienteil drückt.

AX PRO Systemstatus-Benachrichtigung

Das Gerät sendet Push-Benachrichtigungen, wenn sich der Systemstatus ändert.

Statusbenachrichtigung des Funkmelders

Das Gerät sendet Benachrichtigungen, wenn der Status eines Funkmelders sich ändert.

Gerätestatus Benachrichtigung

Das Gerät sendet Benachrichtigungen, wenn ein Gerätestatus sich ändert.

Alarmzentrum

Sie können die Parameter der Alarmzentrale einstellen und alle Alarme werden an die konfigurierte Alarmzentrale gesendet.

Vorgehensweise

1. Wählen Sie den Standort und das AX PRO System aus und melden Sie sich dann an.
2. Tippen Sie auf → **Kommunikation** → **Alarmzentrum**.
3. Wählen Sie eine Alarmzentrale aus und aktivieren Sie diese.
4. Wählen Sie den **Protokolltyp**: **ADM-CID**, **ISUP**, **SIA-DCS**, ***SIA-DCS**, oder ***ADM-Kennzeichen** um den Upload-Modus festzulegen.

   ADM-CID oder **SIA-DCS** Sie sollten den **Leitstellentyp** als **IP** oder **Domänenname** wählen und die IP-Adresse/Domänennamen, die Portnummer, den Kontocode, die Zeitüberschreitung und das Heartbeat-Intervall eingeben.

   Hinweis

   Stellen Sie das Heartbeat Intervall zwischen 10 bis 3.888.000 Sekunden ein.

   ISUP Es müssen keine Protokollparameter eingestellt werden.
   ***SIA-DCS** oder ***ADM-CID** Sie sollten den **Leitstellentyp** als **IP** oder **Domänenname** wählen und die IP-Adresse/Domänennamen, die Portnummer, den Kontocode, das Zeitlimit für Wiederholungen, die Versuche, das Heartbeat Intervall, die arithmetische Verschlüsselung, die Passwortlänge und den geheimen Schlüssel eingeben.

   Hinweis

   Stellen Sie das Heartbeat Intervall zwischen 10 bis 3.888.000 Sekunden ein.
   Für arithmetische Verschlüsselung: Die Zentrale unterstützt die Verschlüsselung der Informationen gemäß DC-09, AES-128, AES-192 und AES-256.
   Für den geheimen Schlüssel: Wenn Sie ein verschlüsseltes Format von DC-09 verwenden, sollte bei der Konfiguration der Leitstelle ARC ein Schlüssel festgelegt werden. Der Schlüssel wird offline von der Leitstelle ausgegeben, das zur Verschlüsselung der Nachricht verwendet wird.

Gerätewartung

Sie können das Gerät neu starten.

Vorgehensweise

1. Wählen Sie den Standort und das AX PRO System aus und melden Sie sich dann an.
2. Tippen Sie auf → **Projektverwaltung** → **Gerätewartung**.

3. Tippen Sie auf **Prüfung** und dann auf **Gehtest starten** um zu testen, ob das Gerät ordnungsgemäß funktioniert oder nicht.
3. Tippen Sie auf **Wartung** → **Gerät neu starten**.
   Die AX PRO Zentrale wird neu gestartet.

Geräteverwaltung

Geben Sie hier eine kurze Beschreibung Ihres Konzepts ein (optional).

Dies ist der Anfang Ihres Konzepts.

Bereich

Sie können die Zonenparameter auf der Zonenseite einstellen.

Vorgehensweise

1. Wählen Sie den Standort und das AX PRO System aus und melden Sie sich dann an.
2. Tippen Sie auf eine Zone auf der Registerkarte **Gerät**.
3. Tippen Sie auf .
4. Tippen Sie auf Symbol **Bearbeiten**, um den Zonennamen zu ändern.
5. Wählen Sie einen Zonentyp aus.

Normal Alarm Zone

Dieser Zonentyp löst sofort ein Alarmereignis aus, wenn er aktiviert wird.

Verzögerungszone

Ausgangsverzögerung: Die Ausgangsverzögerung gibt Ihnen Zeit, den Bereich ohne Alarm auszulösen zu verlassen.
Eingangsverzögerung: Die Eingangsverzögerung gibt Ihnen Zeit, den Bereich ohne Alarm auszulösen zu betreten, um das System unscharf zu schalten.
Das System gibt die Eingangs-/Ausgangsverzögerungszeit an, wenn es Scharfgeschalten oder erneut betreten wird. Wird normalerweise in der Eingangs-/Ausgangsroute (z.B. Vordereingang/Haupteingang) verwendet wo die Scharf-/Unscharfschaltung stattfindet.

Hinweis

In **Systemoptionen** → **Zeitplan und Timer** können Sie 2 verschiedene Zeitdauern einstellen. Stellen Sie sicher, dass der Timer nicht länger als 45 Sekunden eingestellt ist, um die Norm EN50131-1 zu erfüllen.
Wenn es sich bei der Zone um eine verzögerte Zone handelt, können Sie die Parameter für die Eingangs-/Ausgangsverzögerung einstellen.

Folge Zone

Die Zone agiert als verzögerte Zone während der Eingangsverzögerung, ansonsten agiert diese als Normal Alarm Zone.

Perimeter Zone

Das System gibt sofort einen Alarm aus, wenn es ein auslösendes Ereignis nach dem

Scharfschalten erkannt wurde. Es gibt einen konfigurierbaren Intervall-Timer von 0 bis 600 Sekunden zwischen der Alarmaktivierung und der Signalisierung. Mit dieser Option können Sie den Alarm überprüfen und die Signalisierung während der Intervallzeit, im Falle eines Fehlalarms, abbrechen.
Wenn die Zone scharfgeschalten ist, können Sie die Verzögerungszeit des Peripheriealarms in **Systemoptionen** → **Zeitplan und Timer** einstellen. Sie können die Sirene auch in der Zeitverzögerung stummschalten.

24 Stunden stiller Überfall Zone

Dieser Zonen Typ ist 24 Std. aktiv und wird für Überfall verwendet, nicht für Rauch- oder Glasbruchmelder.

Überfall Zone

Die Zone ist ständig aktiviert. Dieser Zonen Typ wird normalerweise an Standorten eingesetzt, die mit Überfalltaster, Rauchmelder und Glasbruchmelder ausgestattet sind.

Feuer Zone

Diese Zone wird immer Sirenen aktivieren, wenn ein Alarm auftritt. Dieser Zonen Typ wird normalerweise in brandgefährdete Bereiche eingesetzt, die mit Rauchmeldern und Temperatursensoren ausgestattet sind.

Gas Zone

Diese Zone wird immer Sirenen aktivieren, wenn ein Alarm auftritt. Dieser Zonen Typ wird normalerweise in Bereichen verwendet, die mit Gaswarngeräten ausgestattet sind (z.B. in der Küche).

Medizinische Zone

Die Zone wird immer mit einem Signalton aktiviert, wenn ein Alarm auftritt. Dieser Zonen Typ wird normalerweise an Orten verwendet, die mit medizinischen Notruftasten ausgestattet sind.

Timeout Zone

Die Zone ist ständig aktiviert. Dieser Zonen Typ wird verwendet, um den "AKTIVEN"-Status einer Zone zu überwachen und zu melden, aber meldet und alarmiert nur, nachdem die konfigurierbare Zeit (1 bis 599 Sekunden) abgelaufen ist. Dieser Zonen Typ wird normalerweise an Orten verwendet, die mit Magnetkontakten ausgestattet sind, die einen Zugang nur für kurze Zeit (z.B. Tür zum Feuerwehrhydrant) erfordern.

Schlüssel Zone

Der verknüpfte Bereich wird nach der Auslösung scharf geschalten und nach der Wiederherstellung unscharf geschalten. Im Falle eines Sabotagealarms wird das scharf-/unscharfschalten nicht ausgeführt.

Deaktivierte Zone

Alarme werden nicht aktiviert, wenn die Zone ausgelöst oder sabotiert wurde. Sie wird in der Regel zum Deaktivieren fehlerhafter Meldern verwendet.

6. Aktivieren **Intern Scharfschaltung Bypass**, **Ton**, **Dual Alarm** oder **Stiller Alarm** entsprechend Ihren tatsächlichen Bedürfnissen.

Hinweis

- Einige Zonen unterstützen diese Funktion nicht. Siehe die aktuelle Zone, um die Funktion einzustellen.
- Verschiedene Zonentypen haben unterschiedliche Parameter.

7. Heartbeat Intervall einstellen.
8. Optional: Tippen Sie auf **Löschen**, um das Gerät zu löschen.

Tastatur

Sie können die Parameter des Bedienteils einstellen, die am AX PRO System angemeldet ist.

Vorgehensweise

1. Wählen Sie den Standort und das AX PRO System aus und melden Sie sich dann an.
2. Tippen Sie auf der Registerkarte **Gerät** auf ein Bedienteil.
3. Tippen Sie auf .
4. Tippen Sie auf das Symbol **Bearbeiten**, um den Namen des Bedienteils zu ändern.
5. Aktivieren **Fernbedienung aktivieren**.
6. Verknüpfte Benutzer auswählen.
7. Tippen Sie auf **Tasten Einstellungen**, um Funktionen für einzelne Tasten und Kombinationstasten einzustellen.
8. Optional: Tippen Sie auf **Löschen**, um das Gerät zu löschen.

Sirenen

Die Sirene wird über das Funkempfängermodul in den AX PRO eingelernt.

Vorgehensweise

1. Wählen Sie den Standort und das AX PRO System aus und melden Sie sich dann an.
2. Tippen Sie auf die Registerkarte **Geräte**, um eine Sirene auszuwählen.
3. Tippen Sie auf .
4. Tippen Sie auf das Symbol **Bearbeiten**, um den Namen des akustischen Signalgebers zu ändern.
5. Verknüpfte Zonen auswählen.
6. Stellen Sie die Dauer und die Lautstärke des Alarms ein.
7. Aktivieren Sie die Scharf/Unscharf LED, den Scharf/Unscharf Signalton, die Alarmanzeige entsprechend den tatsächlichen Anforderungen.
8. Heartbeat Intervall einstellen.
9. Optional: Tippen Sie auf **Löschen**, um das Gerät zu löschen.

4.1.2 Hik-ProConnect Portal Benutzer

Bei der AX Pro Zentrale können Sie Vorgänge wie Bereich scharf-/unscharfschalten, Löschen des Alarms, Bypass der Zone usw. durchführen und die Steuerung auf dem Portal per Fernzugriff konfigurieren. Sie können auch eine PIN anfordern (erforderlich für die Aktualisierung der

Firmware von AX Pro) und die Sprache von AX Pro wechseln.

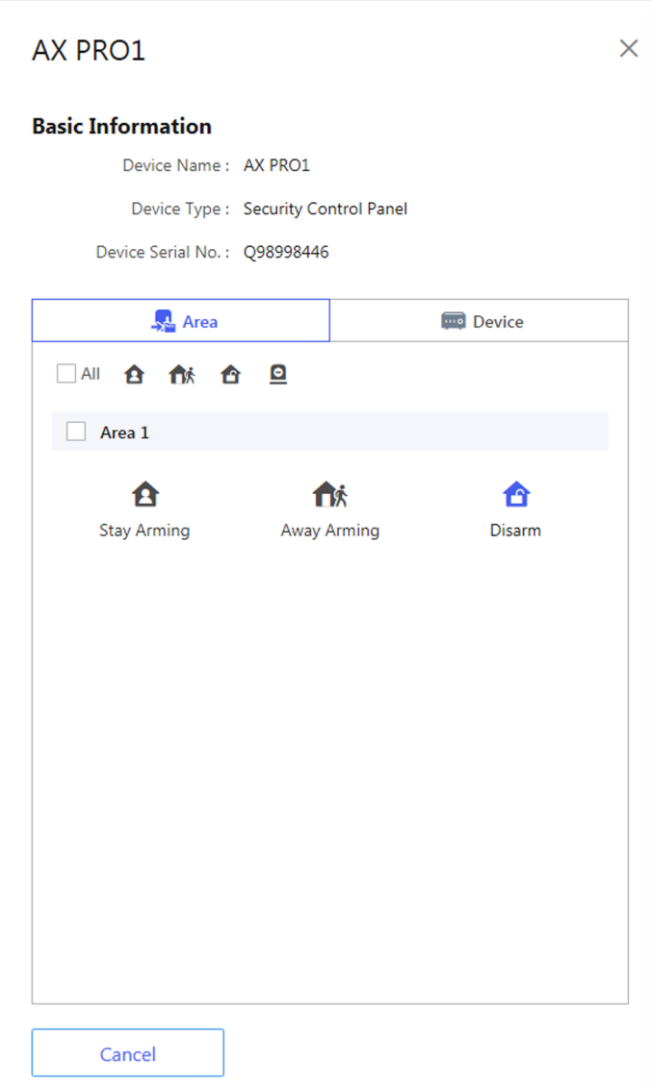
Klicken Sie auf **Standort**, um die Seite mit der Standortliste aufzurufen, und klicken Sie dann auf den Namen eines Standorts, um Details aufzurufen.

AX Pro Remote Bedienung

Klicken Sie auf die AX Pro Zentrale, um das Bedienfeld zu öffnen. Sie können die folgenden Operationen ausführen.

Tabelle 4 - 3 Betriebsbeschreibung

Bedienung	Beschreibung
Einen bestimmten Bereich intern scharfschalten	Wählen Sie den Tab **Bereich** und klicken Sie dann auf **Intern Scharfschaltung**, um den Bereich scharf zu schalten.
Abwesenheitsalarm für einen bestimmten Bereich	Wählen Sie den Tab **Bereich** und klicken Sie dann auf **Extern Scharfschalten**.
Einen bestimmten Bereich unscharfschalten	Wählen Sie den Tab **Bereich** und klicken Sie dann auf **Unscharfschalten**.
Mehrere Bereiche intern scharfschalten	Wählen Sie **Bereich** und dann die Bereiche aus.
Mehrere Bereiche im Modus Abwesend	Wählen Sie **Bereich** und dann die Bereiche aus.
Mehrere Zonen entschärfen	Wählen Sie **Bereich** und dann die Bereiche aus.
Alarme mehrerer Bereiche löschen	Wählen Sie den Tab **Bereich** und wählen Sie dann Bereiche aus und klicken Sie auf
Peripheriegerät nach Bereich filtern	Wählen Sie den Tab **Gerät** und klicken Sie dann auf und wählen Sie einen Bereich aus, um nur die Peripheriegeräte anzuzeigen, die mit dem ausgewählten Bereich verknüpft sind - oder wählen Sie **Alle**, um alle Peripheriegeräte anzuzeigen, die mit allen Bereichen verknüpft sind.
Relais steuern	Wählen Sie **Gerät** und wählen Sie dann einen Funkausgang, um die mit ihm verknüpften Sirenen anzuzeigen. Wählen Sie dann Sirenen aus, um diese zu aktivieren/deaktivieren.
Bypass Zone	Wählen Sie das **Gerät** und wählen Sie dann eine Zone (z.B. einen Melder) und aktivieren Sie **Bypass**, um die Zone zu umgehen.



AX Pro Remote Konfiguration

Sie können auf ⚙ um die Webseite der Zentrale aufzurufen, um das Gerät zu konfigurieren.

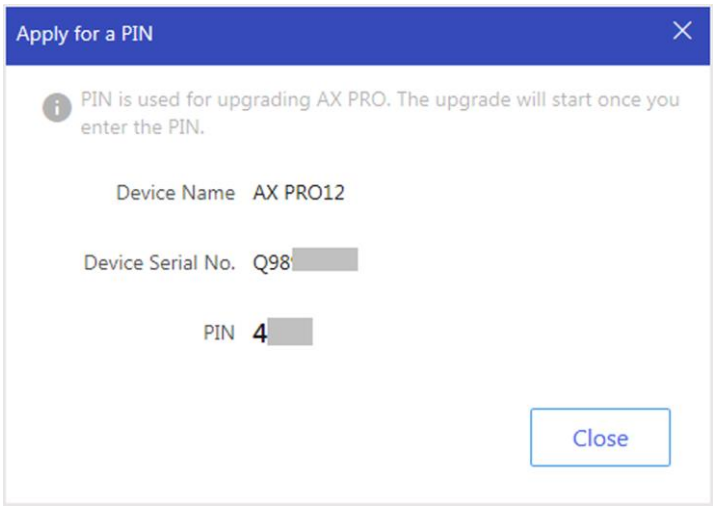
Hinweis

Weitere Informationen zur Konfiguration der Zentrale finden Sie im Benutzerhandbuch des Geräts.

Einen PIN anfordern

Sie können auf ••• klicken → 📄, um das Fenster „PIN beantragen“ zu öffnen. Anschließend

wird der PIN-Code angezeigt.

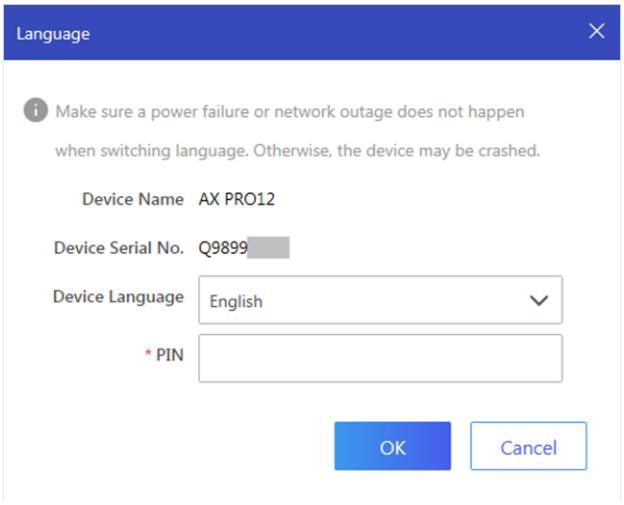


Sprache wechseln

Hinweis

Sie hätten eine PIN beantragen sollen.

Tippen Sie auf • • • → ⇆, um das Fenster für die Sprachauswahl zu öffnen und dann die Gerätesprache einzustellen und die PIN einzugeben.



4.2 Einrichtung mit Hik-Connect

Der Benutzer kann das Gerät mit via Hik-Connect steuern, z.B. den allgemeinen Scharf-/Unscharfschaltvorgang, die Benutzerverwaltung usw.

Herunterladen und Anmelden der App

Laden Sie die Hik-Connect App herunter und melden Sie sich an.

Vorgehensweise

1. Laden Sie die Hik-Connect App herunter.
2. Optional: Registrieren Sie ein neues Konto, wenn Sie die Hik-Connect App zum ersten Mal verwenden.

Hinweis

Weitere Informationen finden Sie im *Benutzerhandbuch des Hik-Connect App*.

3. Führen Sie dies aus und melden Sie bei der App an.

AX PRO Zentrale der App hinzufügen

Vor der Nutzung fügen Sie der App eine AX PRO Zentrale hinzu.

Vorgehensweise

1. Schalten Sie die AX PRO Zentrale ein.
2. Wählen Sie den Typ zum Hinzufügen aus.
   – Tippen Sie auf → **QR-Code scannen**. Scannen Sie den QR-Code auf der AX PRO Zentrale.

   Hinweis

   Normalerweise ist der QR-Code auf das Etikett auf der Rückseite des AX PRO Zentrale aufgedruckt.

Tippen Sie auf → **Manuell hinzufügen**. Geben Sie die Seriennummer des Geräts ein.
3. Tippen Sie auf , um nach Gerät zu suchen.
4. Tippen Sie auf **Hinzufügen** auf der Ergebnisseite.
5. Geben Sie den Verifizierungscode ein und tippen Sie auf **OK**.
6. Geben Sie nach Abschluss des Hinzufügens den Alias ein und tippen Sie auf **Speichern**.
7. Optional: Tippen Sie auf → **Löschen**, um das Gerät zu löschen.
8. Optional: Tippen Sie auf und tippen Sie auf das Symbol **Bearbeiten**, um den Gerätenamen zu ändern.

Funkkomponenten der AX PRO Zentrale hinzufügen

Peripheriegeräte der AX PRO Zentrale hinzufügen.

Vorgehensweise

1. Wählen Sie einen Standort aus.
2. Wählen Sie eine AX PRO Zentrale aus.
3. Tippen Sie auf und die **und mehr** Symbol.
   – Tippen Sie auf **QR-Code scannen**. Scannen Sie den QR-Code auf der Funkkomponente.

Tippen Sie auf **Manuell hinzufügen**. Geben Sie die Seriennummer und den Verifizierungscode des Geräts ein, um das Gerät hinzuzufügen.

Transponder Verwaltung

Nach dem Hinzufügen von Transponder zum AX PRO System können Sie den Transponder vorhalten, um bestimmte oder alle Bereiche scharf/unscharf zu schalten und Alarme zu löschen.

Vorgehensweise

1. Tippen Sie auf der Gerätelistenseite, wählen die AX PRO Zentrale und melden Sie sich dann (falls erforderlich) am Gerät an, um die Seite aufzurufen.
2. Tippen Sie auf → **Benutzerverwaltung** → **Transponder** um die Seite „Transponder-Verwaltung“ aufzurufen.
3. Tippen Sie auf **+** um einen Transponder hinzuzufügen.
4. Wenn Sie die Sprachaufforderung „Transponder vorhalten“ hören, sollten Sie den Transponder der AX PRO Zentrale vorhalten.
   - Wenn ein Signalton ertönt, wurde der Transponder erkannt.
   - Der Transponder wird auf der Transponder-Seite angezeigt.
5. Optional: Tippen Sie auf einen Transponder, um die Einstellungsseite aufzurufen.
6. Tippen Sie auf **Symbol bearbeiten**, um den Transponder-Namen zu bearbeiten.

Hinweis

- Wenn Sie sich als Errichter anmelden, überspringen Sie diesen Schritt. Nur Administratoren können den Namen von Transponder bearbeiten.
- Der Name sollte 1 bis 32 Zeichen enthalten.

7. **Transponder aktivieren**.
8. Wählen Sie einen verknüpften Benutzer aus.
9 Wählen Sie den Transponder-Typ aus

Hinweis

Verschiedene verknüpfte Benutzer haben unterschiedliche Transponder-Berechtigungen.

Benutzer Transponder

Sie können durch vorhalten des Transponders das System scharf-/unscharfschalten.

Wächterrundgang Transponder

Wenn Sie den Transponder vorhalten, lädt das System einen Datensatz hoch.

10. Optional: Tippen Sie auf **Löschen** um den Transponder zu löschen.

Benutzerverwaltung

Der Administrator und der Errichter können Benutzer verwalten. Wenn Sie der Administrator sind, können Sie Benutzer hinzufügen, bearbeiten und löschen und den neu hinzugefügten Benutzern unterschiedliche Berechtigungen zuweisen. Wenn Sie ein Errichter sind, können Sie nur Benutzer hinzufügen und löschen.

Vorgehensweise

Hinweis

Es gibt vier Benutzertypen für AX PRO, einschließlich Administrator (oder Eigentümer), Benutzer, Errichter (oder Setter) und Hersteller. Verschiedene Benutzertypen haben unterschiedliche Berechtigungen für den Zugriff auf die Funktionalität des AX PRO Systems.

1. Tippen Sie auf der Gerätelistenseite, wählen Sie die AX PRO Zentrale und melden Sie sich an.
2. Tippen Sie auf **Einladungssymbol**, um die Empfängerseite aufzurufen.
3. Wählen Sie einen Benutzer aus, um diesen einzuladen.
   – Scannen Sie den QR-Code, um einen Benutzer einzuladen.
   – Geben Sie die E-Mail-Adresse/Mobiltelefonnummer ein, um einen Benutzer einzuladen.
   – Wählen Sie einen Benutzer in der Liste aus.
4. Tippen Sie auf **Weiter**, um den Benutzer einzuladen.

Hinweis

Der Empfänger muss die Einladung annehmen.

5. Tippen Sie auf → **Benutzerverwaltung** → **Benutzer**.
6. Tippen Sie auf einen Benutzer, um die Seite „Benutzerverwaltung“ aufzurufen.
7. Optional: Führen Sie bei Bedarf die folgenden Schritte durch.

Benutzerberechtigung	Sie können auf den Benutzer in der Benutzerliste tippen und dann auf **Symbol bearbeiten** um die Berechtigungen festzulegen, die für den Benutzer autorisiert sind. **Hinweis** Nur der Administrator kann einen solchen Vorgang ausführen.
Verknüpfte Zone festlegen	Wenn der Benutzertyp ein Benutzer ist, tippen Sie auf den Benutzer in der Benutzerliste und dann auf **Verknüpfte Bereiche** um den mit dem Benutzer verknüpften Bereich einzustellen. **Hinweis** Nur der Administrator kann einen solchen Vorgang ausführen.

Bedienteil Pin-Code bearbeiten

Wenn der Benutzer ein Administrator, ein Errichter oder ein Hersteller ist, können Sie auf den Benutzer in der Benutzerliste tippen und dann auf **Bedienteil Pin-Code bearbeiten**, um den Pin Code für den Benutzer festzulegen.

Hinweis

Der PIN-Code muss zwischen 4 und 6 Ziffern lang sein. Keine Zahl ist unzulässig, es gibt 10.000 bis 100.000 Abweichungen und keine Begrenzung der Ziffernkombination.
Nach dem Hinzufügen eines Bedienteils können Sie im Benutzermenü einen PIN-Code hinzufügen. Wenn Sie in das Eingabefeld klicken, wird angezeigt, dass 4 oder 6-stellige Zahlen zulässig sind. Dies ist für jeden Benutzer gleich

Überfall PIN bearbeiten

Wenn der Benutzer ein Administrator ist, können Sie auf den Benutzer in der Benutzerliste tippen und dann auf **Überfall PIN bearbeiten**, um den Überfall PIN für den Benutzer festzulegen.

Hinweis

Wenn Sie gezwungen werden die Alarmanlage unscharf zu schalten, sollten Sie den Überfall PIN verwenden, um einen stillen Alarm auszulösen.

Hinweis

- Konfigurationselemente und Benutzerberechtigungen variieren je nach Benutzertyp.
- Sie können verknüpfte Transponder und Fernbedienungen des Benutzers anzeigen, haben jedoch keine Berechtigung diese zu konfigurieren.

Bypass Zone

Wenn der Bereich scharfgeschalten ist, können Sie eine bestimmte Zone wie gewünscht Bypassen (umgehen).

Bevor Sie beginnen

Verbinden Sie einen Melder mit der Zone.

Vorgehensweise

1. Tippen Sie auf der Gerätelistenseite, wählen die AX PRO Zentrale und melden Sie sich dann (falls erforderlich) am Gerät an, um die Bereichsseite aufzurufen.
2. Tippen Sie auf **Gerät**.
3. Tippen Sie auf eine Zone auf der Registerkarte Gerät.
4. Tippen Sie auf um die Einstellungsseite aufzurufen.
5. Aktivieren Sie **Zonen Bypass** und die Zone befindet sich im Bypass-Status.
   Der Melder in der Zone erkennt nichts und Sie erhalten keinen Alarm von der Zone.

Zone scharf/unscharfschalten

Schalten Sie den Bereich manuell scharf/unscharf wie gewünscht.
Tippen Sie auf der Gerätelistenseite, wählen die AX PRO Zentrale und melden Sie sich dann (falls erforderlich) am Gerät an, um die Bereichsseite aufzurufen.

Vorgänge für einen einzelnen Bereich

- **Extern Scharfschalten**: Tippen Sie auf einen beliebigen Bereich, um einen einzelnen Bereich Abwesend scharf zu schalten. Wenn alle Personen im Erfassungsbereich den Abwesenheitsmodus verlassen, schalten Sie den Abwesenheitsmodus ein, um alle Zonen im Bereich nach der definierten Verweilzeit zu aktivieren.
- **Unscharfschalten**: Tippen Sie auf das Symbol**Extern Scharfschalten** in einem beliebigen Bereich, um einen einzelnen Bereich scharf zu schalten. Im Modus „Unscharf“ werden alle Zonen im Bereich keinen Alarm auslösen, unabhängig davon, ob Alarmereignisse auftreten oder nicht.

Betrieb für alle Bereiche

- **Abwesend**: Tippen Sie auf das Symbol **Extern Scharfschalten**, um alle Bereiche extern scharf zu schalten. Wenn alle Personen den Erfassungsbereich verlassen haben, schalten Sie den Modus Abwesend ein, um alle Zonen in allen Bereichen nach der definierten Verweilzeit zu aktivieren.
- **Intern**: Tippen Sie auf das Symbol**Intern scharfschalten**, um alle Bereiche intern scharf zu schalten. Wenn die Personen im Erfassungsbereich sich aufhalten, schalten Sie intern scharf, um die Außenhautüberwachung (wie z.B. Perimeterüberwachung, Magnetkontakte, Vorhangmelder) in allen Zonen und Bereichen zu aktivieren. In der Zwischenzeit werden die Melder innerhalb des Erfassungsbereichs Bypassed (umgangen - z.B. Bewegungsmelder). Personen können sich innerhalb des Bereichs bewegen und der Alarm wird nicht ausgelöst.
- **Unscharfschalten**: Tippen Sie auf das Symbol **„Unscharfschalten“** um alle Bereiche unscharf zu schalten. Im Modus „Unscharf“ lösen alle Zonen aller Bereiche keinen Alarm aus, unabhängig davon, ob Alarmereignisse auftreten oder nicht.
- **Alarm bestätigen**: Tippen Sie auf das Symbol **Alarm löschen**, um Alarme für alle Bereiche zu löschen. Löschen Sie alle Alarme, die von allen Zonen aller Bereiche ausgelöst werden.

Alarmbenachrichtigung prüfen

Wenn ein Alarm ausgelöst wird, erhalten Sie eine Alarmbenachrichtigung. Sie können die

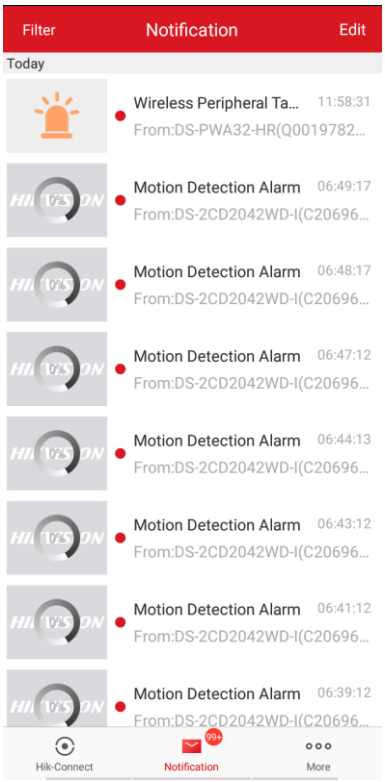
Alarminformationen in der App überprüfen.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie eine Zone mit einem Melder verknüpft haben.
- Stellen Sie sicher, dass die Zone Bypassed ist.
- Stellen Sie sicher, dass Sie nicht die Funktion Stille Zone aktiviert haben.

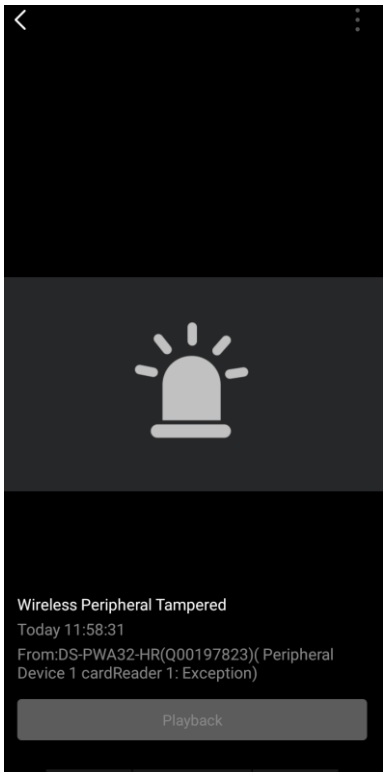
Vorgehensweise

1. Tippen Sie auf **Benachrichtigung** in der App, um die Seite aufzurufen.



Alle Alarmbenachrichtigungen werden auf der Seite „Benachrichtigung“ aufgeführt.

2. Wählen Sie einen Alarm aus und Sie können die Alarmdetails anzeigen.



3. Optional: Wenn die Zone mit einer der Kamera verknüpft ist, können Sie die Wiedergabe anzeigen, wenn der Alarm ausgelöst wird.

WLAN-Verbindung

Sie können die AX PRO Zentrale mit der App mit dem WLAN verbinden.

Vorgehensweise

1. Tippen Sie auf der Gerätelistenseite, wählen die AX PRO Zentrale und melden Sie sich dann (falls erforderlich) am Gerät an, um die Seite aufzurufen.
2. Tippen Sie auf → **Kommunikationsparameter** → **WLAN-Anschluss**.
3. Folgen Sie den Anweisungen auf der Seite und wechseln Sie die AX PRO Zentrale in den AP-Modus. Tippen Sie auf **Weiter**.
4. Wählen Sie ein stabiles WLAN für das Gerät aus, um eine Verbindung herzustellen.
5. Zurück zur Konfigurationsseite, um das WLAN-Passwort einzugeben und tippen Sie **Weiter**.
6. Tippen Sie auf **Mit einem Netzwerk verbinden** und warten Sie auf die Verbindung.
   Nach Abschluss der Verbindung fordert die AX PRO Zentrale Sie auf, den AP-Modus zu verlassen und automatisch in den STA-Modus zu wechseln.

Gerätewartung

Sie können das Gerät neu starten.

Vorgehensweise

1. Tippen Sie auf der Gerätelistenseite, wählen die AX PRO Zentrale und melden Sie sich dann (falls erforderlich) am Gerät an, um die Seite aufzurufen.
2. Tippen Sie auf → **Projektpflege** → **Gerätewartung**.
3. Tippen Sie auf **Gerät neu starten**.
   Die AX PRO Zentrale wird neu gestartet.

4.3 Einrichten mit dem Web-Client

Vorgehensweise

1. Schließen Sie das Gerät an das Netzwerk an.
2. Suchen Sie die Geräte-IP-Adresse mit Hilfe der Client- und SADP-Software.
3. Geben Sie die gesuchte IP-Adresse in die Adressleiste ein.

Hinweis

Bei Verwendung des mobilen Browsers ist die Standard-IP-Adresse 192.168.8.1.

Hinweis

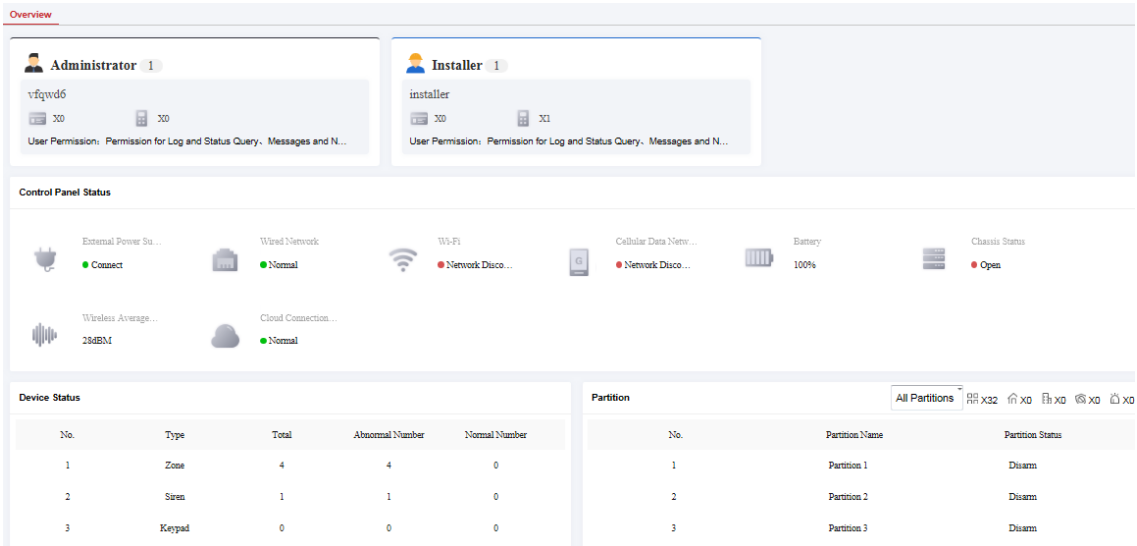
Wenn Sie das Netzwerkkabel direkt mit dem Computer verbinden, ist die Standard-IP-Adresse 192.0.0.64

4. Verwenden Sie den Benutzernamen und das Passwort, um sich anzumelden.

Hinweis

Siehe *Aktivierung* Kapitel für die Details.

Es werden der Benutzer-, Geräte- und Bereichsstatus auf der Übersichtsseite anzeigt.



4.3.1 Kommunikationseinstellungen

Kabelgebundenes Netzwerk

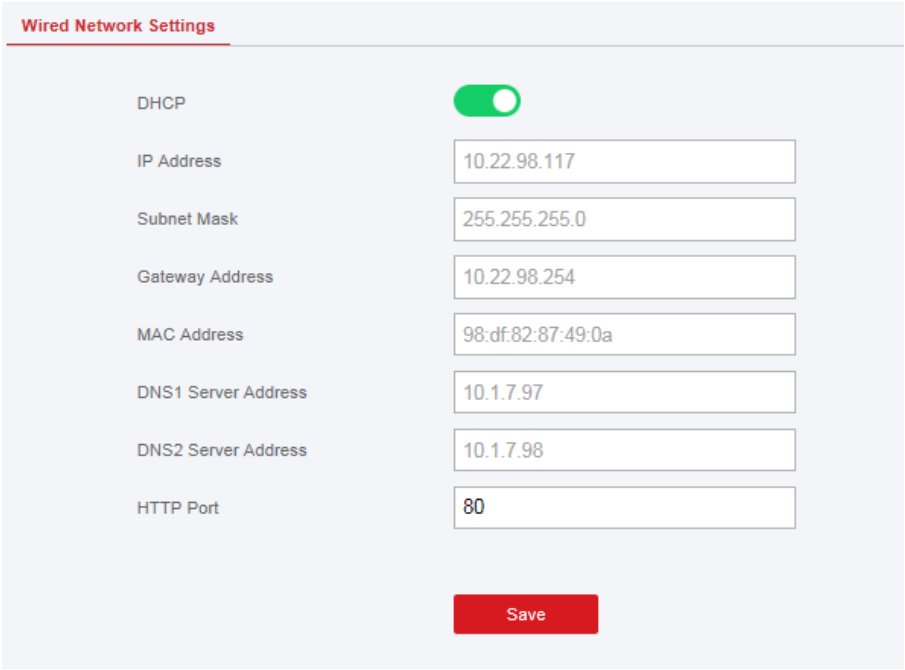
Sie können die IP-Adresse des Geräts und andere Netzwerkparameter einstellen.

Vorgehensweise

Hinweis

Die Funktionen variieren je nach Gerätemodell.

1. Wählen Sie in der Client-Software das Gerät in der **Geräteverwaltung** und klicken Sie auf oder geben Sie die IP-Adresse in die Adressleiste des Webbrowsers ein und melden Sie sich an.



2. Klicken Sie auf **Kommunikationsparameter** → **Ethernet-Anschluss**.
3. Stellen Sie die Parameter ein.

Automatische Einstellungen: Aktivieren Sie **DHCP** und stellen Sie den HTTP-Port ein. Manuelle Einstellungen: Deaktivieren Sie **DHCP** und stellen Sie **IP-Adresse**, **Subnetzmaske**, **Adresse des Gateways** und **Adresse des DNS-Servers** ein.

4. Optional: Legen Sie die korrekte DNS-Serveradresse fest, wenn das Gerät den Hik-Connect-Server über einen Domänennamen aufrufen soll.
5. Klicken Sie auf **Speichern**.

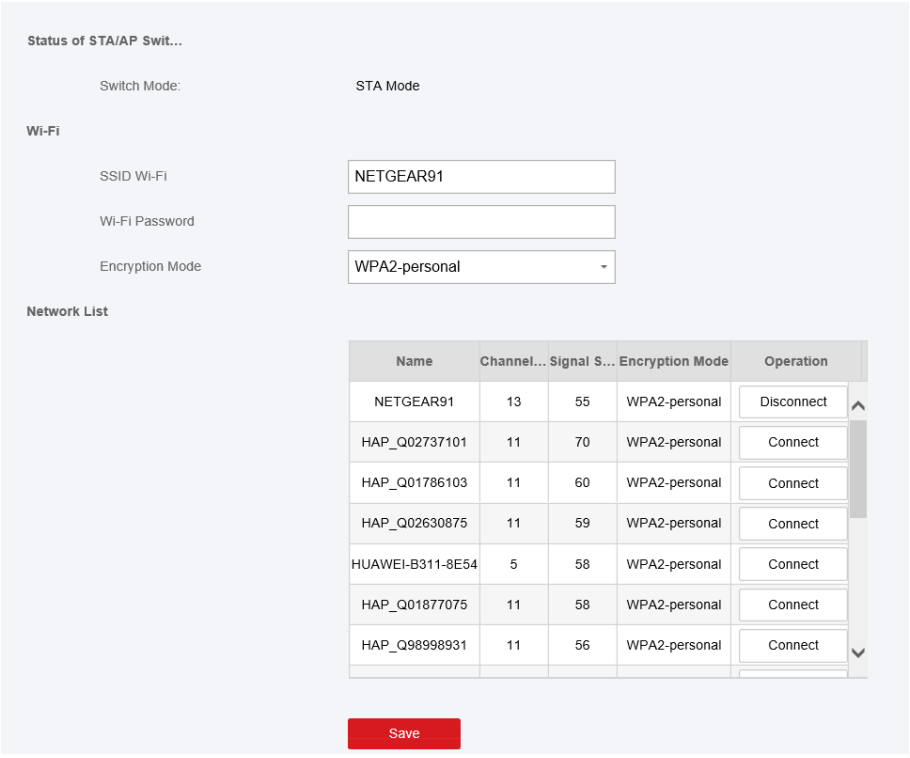
WLAN

Sie können die WLAN-Parameter einstellen, wenn sich in der Nähe eines sicheren und

glaubwürdigen WLAN-Netzwerkes befinden.

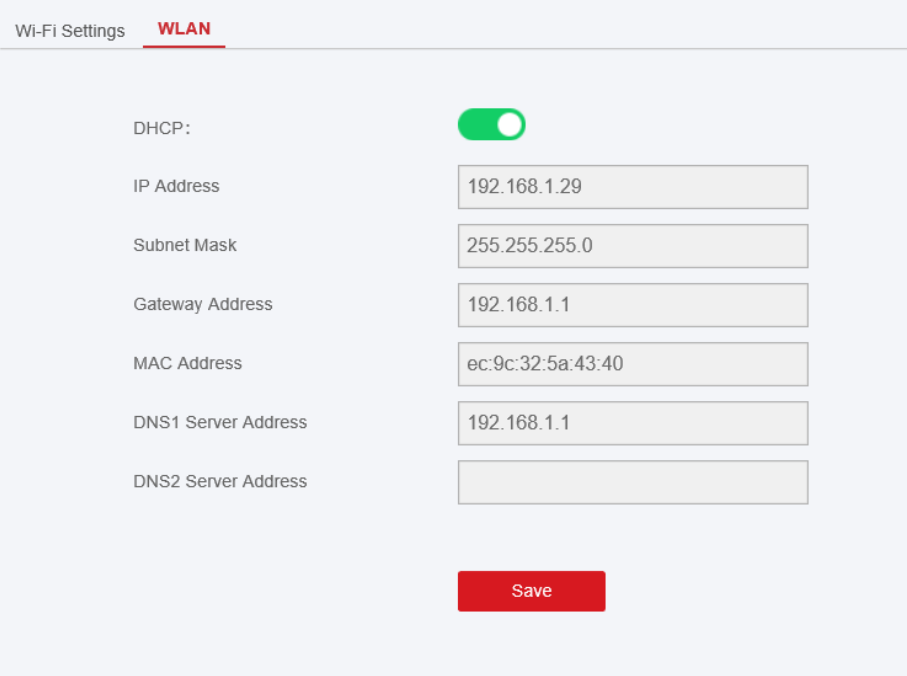
Vorgehensweise

1. Klicken Sie auf **Kommunikationsparameter → WLAN**.



2. Verbinden Sie sich mit einem WLAN.
Manuell verbinden: Geben Sie die **SSID** und **WLAN-Passwort** ein, wählen Sie **Verschlüsselungsmodus** und klicken Sie auf **Speichern**. Aus Netzwerkliste auswählen: Wählen Sie ein WLAN aus der Liste aus. Klicken Sie auf **Verbinden** und geben Sie das WLAN-Passwort ein und klicken Sie auf **Verbinden**.

2. Klicken Sie auf **WLAN**.



4. Stellen Sie die **IP-Adresse**, **Subnetzmaske**, **Adresse des Gateways** und **Adresse des DNS-Servers** ein.

Hinweis

Wenn DHCP aktiviert ist, erhält das Gerät die Netzwerk-Parameter automatisch.

5. Klicken Sie auf **Speichern**.

Mobilfunknetz

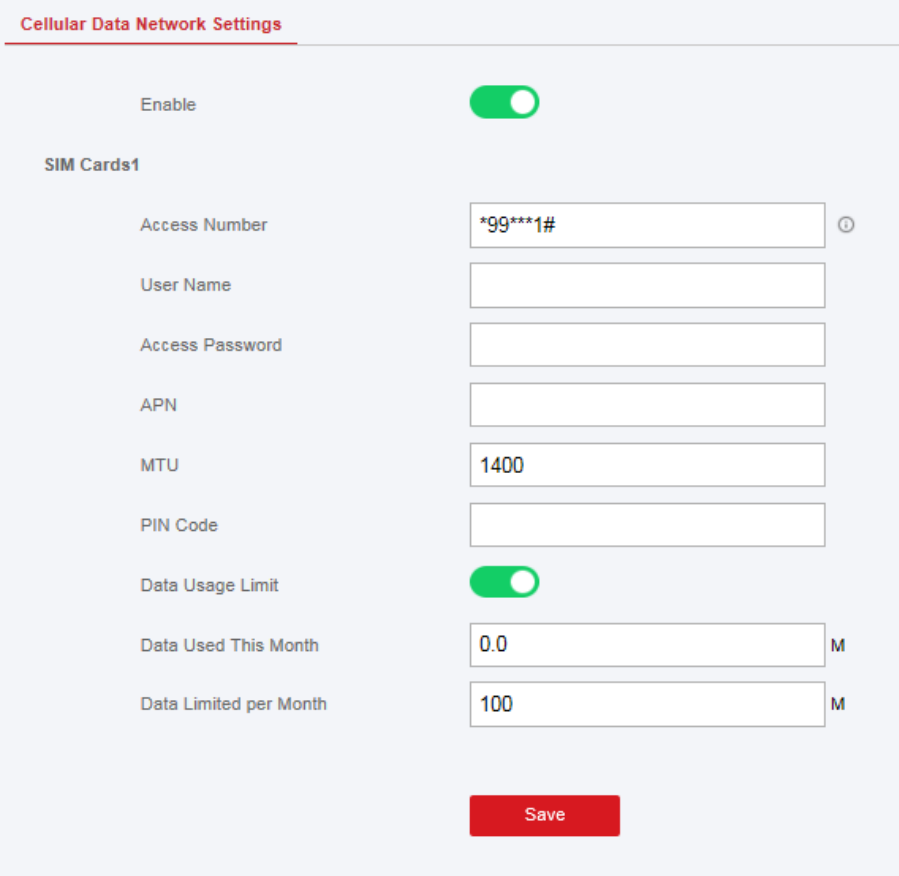
Legen Sie die Parameter des Mobilfunknetzes fest, wenn Sie eine SIM-Karte in das Gerät einsetzen. Durch die Verwendung des Mobilfunknetzes kann das Gerät Alarmbenachrichtigungen an das Alarmzentrum hochladen.

Bevor Sie beginnen

Setzen Sie eine SIM-Karte in den SIM-Kartensteckplatz des Geräts ein.

Vorgehensweise

1. Klicken Sie auf **Kommunikationsparameter** → **Mobilfunknetz**.



2. Aktivieren Sie die Funk Wahl.
3. Legen Sie die Parameter des Mobilfunk-Datennetzwerks fest.

PIN

Geben Sie die Benutzer Rufnummer an.

Hinweis

Nur bei privaten Netzwerk-SIM-Karten muss die PIN eingeben werden.

Benutzername

Fragen Sie den Netzbetreiber und geben Sie den Benutzernamen ein.

Zugangspasswort

Fragen Sie den Netzbetreiber und geben Sie das Passwort ein.

APN

Fragen Sie den Netzbetreiber und geben Sie die APN-Informationen ein.

Datennutzungslimit

Sie können die Funktion aktivieren und jeden Monat den Datenschwellenwert einstellen. Wenn die Datennutzung größer als der konfigurierte Schwellenwert ist, wird ein Alarm ausgelöst und in das Alarmzentrum und der App hochgeladen.

In diesem Monat verwendete Daten

Die verwendeten Daten werden gesammelt und in diesem Textfeld angezeigt.

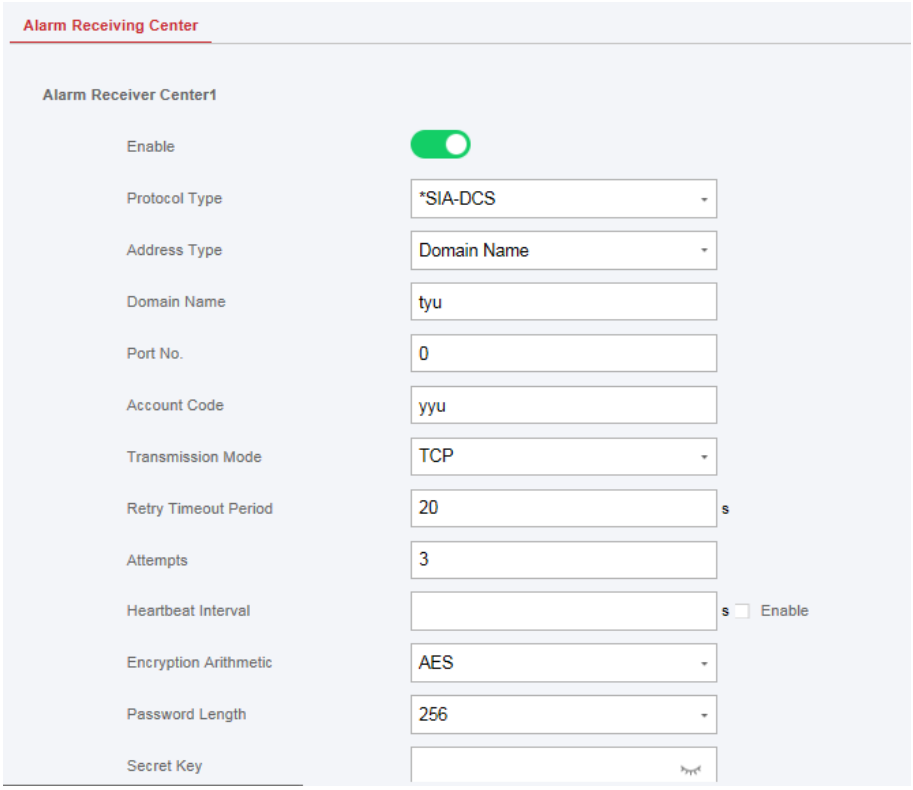
4. Klicken Sie auf **Speichern**.

Alarmzentrum

Sie können die Parameter der Alarmzentrale einstellen und alle Alarme werden an die konfigurierte Alarmzentrale gesendet.

Vorgehensweise

1. Klicken Sie auf **Kommunikationsparameter** → **Leitstelle**.



2. Wählen Sie die **Leitstelle** als **1** oder **2** für Konfiguration und aktivieren Sie die Funktion.

Hinweis

Nur wenn die Leitstelle 1 aktiviert ist, können Sie die Leitstelle 2 als **Backup** einstellen und bearbeiten.

3. Wählen Sie den **Protokolltyp**: **ADM-CID**, **ISUP**, **SIA-DCS**, ***SIA-DCS**, oder ***ADM-Kennzeichen**, um den Upload-Modus festzulegen.

Hinweis

Standard DC-09 Protokoll
ADM-CID: Die Datenpräsentationsmethode von DC-09 ist CID, die nicht verschlüsselt ist und nur zum Hochladen von Alarmberichten dient.
*ADC-CID: Die Datenpräsentationsmethode von DC-09 ist CID, die verschlüsselt ist und nur zum Hochladen von Alarmberichten dient.
SIA-DCS: Die Datenpräsentationsmethode von DC-09 ist DCS (auch als SIA-Protokoll bezeichnet), das nicht verschlüsselt ist und nur zum Hochladen von Alarmberichten dient.
*SIA-DCS: Die Datenpräsentationsmethode von DC-09 ist DCS (auch als SIA-Protokoll bezeichnet), das verschlüsselt ist und nur zum Hochladen von Alarmberichten dient.

ADM-CID oder **SIA-DCS** Sie sollten den **Leitstellentyp** als **IP** oder **Domänenname** wählen und die IP-Adresse/Domänennamen, die Portnummer, den Kontocode, die Zeitüberschreitung, die Wiederaufladezeiten und das Heartbeat Intervall eingeben.

Hinweis

Stellen Sie das Heartbeat Intervall zwischen 10 bis 3.888.000 Sekunden ein.

ISUP Es müssen keine Protokollparameter eingestellt werden.
***SIA-DCS** oder ***ADM-CID** Sie sollten den **Leitstellentyp** als **IP** oder **Domänenname** wählen und die IP-Adresse/Domänennamen, die Portnummer, den Kontocode, den Zeitlimit für Wiederholungen, die Versuche, das Heartbeat Intervall, die arithmetische Verschlüsselung, die Passwortlänge und den geheimen Schlüssel eingeben.

Hinweis

Stellen Sie das Heartbeat Intervall zwischen 10 bis 3.888.000 Sekunden ein.
Für arithmetische Verschlüsselung: Die Zentrale unterstützt die Verschlüsselung der Informationen gemäß DC-09, AES-128, AES-192 und AES-256.
Für den geheimen Schlüssel: Wenn Sie ein verschlüsseltes Format von DC-09 verwenden, sollte bei der Konfiguration der Leitstelle ein Schlüssel festgelegt werden. Der Schlüssel wird offline von der Leitstelle ausgegeben, das zur Verschlüsselung der Nachricht verwendet wird.

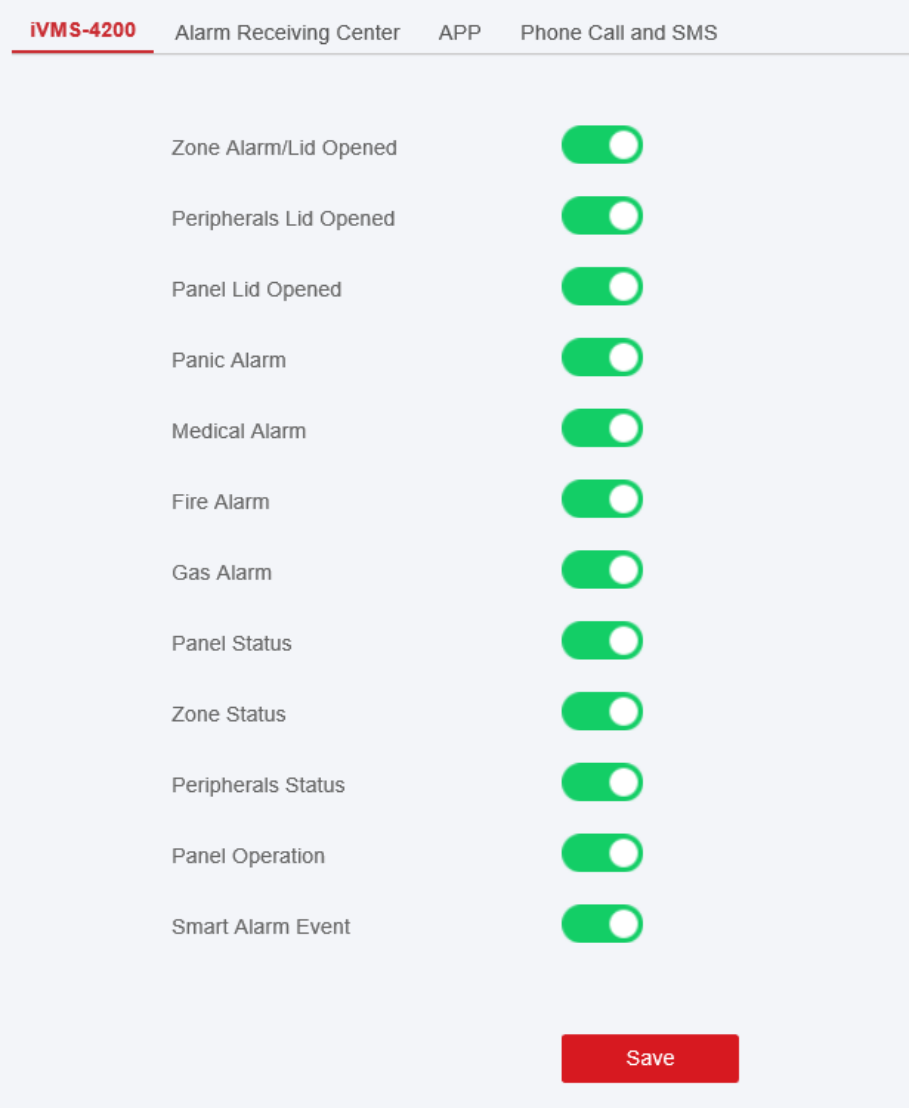
4. Klicken Sie auf **Speichern**.

Benachrichtigungs-Push

Wenn ein Alarm ausgelöst wird und Sie die Alarmbenachrichtigung an den Client, das Alarmcenter, die Cloud oder das Mobiltelefon senden möchten, können Sie die Push-Parameter für die Benachrichtigung festlegen.

Vorgehensweise

1. Klicken Sie auf **Kommunikationsparameter** → **Benachrichtigung über Ereignistypen**.



2. Aktivieren Sie die Zielbenachrichtigung.

Hinweis

Wenn Sie die Alarmbenachrichtigungen an den mobilen Client senden möchten, sollten Sie auch das **Mobiltelefonverzeichnis**, **Mobiltelefonnummer** und den **Benachrichtigungstyp** einstellen.

Hinweis

Wählen Sie für die Benachrichtigung an Leitstellen den Leitstellenindex vor den Einstellungen aus.

3. Klicken Sie auf **Speichern**.

Ergebnis

Tabelle 4-1 Benachrichtigungsoptionen

Option	Benachrichtigung
iVMS-4200	Zonenalarm und Deckel geöffnet Deckel der Funkkomponente geöffnet Sabotage-Benachrichtigung Überfallalarm-Benachrichtigung Medizinische Alarmbenachrichtigung Gasalarm-Benachrichtigung Feueralarm-Benachrichtigung Zentralen-Verwaltungsbenachrichtigung Systemstatus-Benachrichtigung Melderstatus-Benachrichtigung Statusbenachrichtigung für Funkkomponenten
Leitstelle	Leitstelle 1 & 2 Zonenalarm und Deckel geöffnet Deckel der Funkkomponente geöffnet Sabotage-Benachrichtigung Überfallalarm-Benachrichtigung Medizinische Alarmbenachrichtigung Gasalarm-Benachrichtigung Feueralarm-Benachrichtigung Zentralen-Verwaltungsbenachrichtigung Systemstatus-Benachrichtigung Melderstatus-Benachrichtigung Statusbenachrichtigung für Funkkomponenten
Cloud	Zonenalarm und Deckel geöffnet Deckel der Funkkomponente geöffnet Sabotage-Benachrichtigung Überfallalarm-Benachrichtigung Medizinische Alarmbenachrichtigung

Option	Benachrichtigung
	Gasalarm-Benachrichtigung Feueralarm-Benachrichtigung Zentralen-Verwaltungsbenachrichtigung Systemstatus-Benachrichtigung Melderstatus-Benachrichtigung Statusbenachrichtigung für Funkkomponenten
Mobiltelefon	Mobiltelefon 1 bis 8 Mobiltelefonnummer Kontrollkästchen „Benachrichtigungstyp SMS & Sprachanruf“ Zonenalarm und Deckel geöffnet (Filterzeit einstellen) Anzahl der Anrufe Deckel der Funkkomponente geöffnet Sabotage-Benachrichtigung Überfallalarm-Benachrichtigung Medizinische Alarmbenachrichtigung Gasalarm-Benachrichtigung Feueralarm-Benachrichtigung Zentralen-Verwaltungsbenachrichtigung Systemstatus-Benachrichtigung Melderstatus-Benachrichtigung Statusbenachrichtigung für Funkkomponente

Hinweis

Für Mobiltelefonbenachrichtigung:

- Sie müssen * drücken, um den Anruf zu beenden.
- Bei der Eingabe der Mobiltelefonnummer muss ein Kontrollcode hinzugefügt werden.

Cloud-Dienst

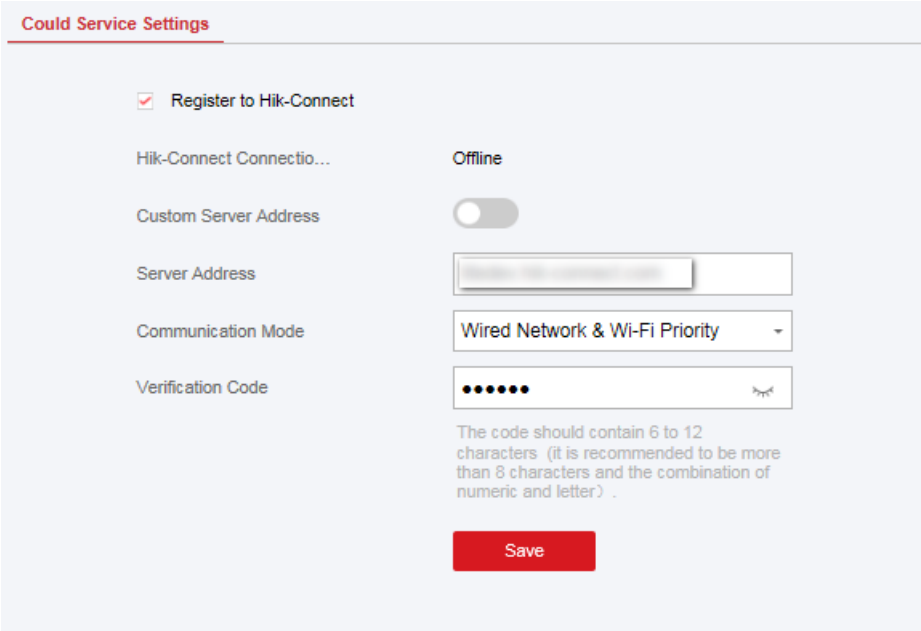
Wenn Sie das Gerät für die Remote-Konfiguration per App anmelden möchten, sollten Sie die Registrierungsparameter der App einstellen.

Bevor Sie beginnen

- Verbinden Sie das Gerät über eine kabelgebundene Verbindung, eine Einwahlverbindung oder eine WLAN-Verbindung mit dem Netzwerk.
- Legen Sie die IP-Adresse, die Subnetzmaske, das Gateway und den DNS-Server des Geräts fest.

Vorgehensweise

1. Klicken Sie auf **Kommunikationsparameter →Einstellungen für Cloud-Dienste**, um die Seite Hik-Connect Einstellungen aufzurufen.



2. Klicken Sie auf **Kommunikationsparameter → Guarding Vision Registrierung**, um die Seite „Einstellungen für Guarding Vision“ aufzurufen.
3. Wählen Sie **Bei Hik-Connect registrieren**.

Hinweis

Standardmäßig ist der Hik-Connect-Dienst des Geräts aktiviert.

Sie können den Gerätestatus auf dem Hik-Connect-Server (www.hik-connect.com) einsehen.

4. Wählen Sie **Bei Guarding Vision registrieren**.

Hinweis

Standardmäßig ist der Dienst Guarding Vision des Geräts aktiviert.

Sie können den Gerätestatus auf dem Guarding Vision-Server (www.guardingvision.com) anzeigen.

5. Aktivieren Sie **Benutzerdefinierte Serveradresse**.

   Die Serveradresse wird bereits im Textfeld Serveradresse angezeigt.
6. Wählen Sie einen Kommunikationsmodus aus der Dropdown-Liste entsprechend der tatsächlichen Gerätekommunikationsmethode aus.

   Automatisch

   Das System wählt den Kommunikationsmodus automatisch entsprechend der Reihenfolge des drahtgebundenen Netzwerks, des WLAN-Netzwerks und des Mobilfunk-Datennetzwerks aus. Nur wenn das aktuelle Netzwerk getrennt ist, stellt das Gerät eine Verbindung zu einem anderen Netzwerk her.

   Kabelgebundene Netzwerk- und WLAN-Priorität

   Die Reihenfolge der Verbindungspriorität von hoch nach niedrig ist: kabelgebundenes Netzwerk, WLAN, Mobilfunk-Datennetzwerk.

   Kabelgebunden Netzwerk und WLAN

   Das System wählt zuerst das kabelgebundene Netzwerk aus. Wenn kein kabelgebundenes Netzwerk erkannt wird, wird WLAN-Netzwerk ausgewählt.

   Mobilfunknetz

   Das System wählt nur das Mobilfunk-Datennetzwerk aus.
7. Optional: Ändern Sie das Authentifizierungspasswort.

Hinweis

- Standardmäßig wird das Authentifizierungspasswort im Textfeld angezeigt.
- Das Authentifizierungspasswort sollte 6 bis 12 Buchstaben oder Ziffern enthalten. Aus Sicherheitsgründen wird ein 8-stelliges Passwort empfohlen, das zwei oder mehr der folgenden Zeichentypen enthält: Großbuchstaben, Kleinbuchstaben und Ziffern.

8. Klicken Sie auf **Speichern**.

Benachrichtigung per E-Mail

Sie können das Alarmvideo oder -ereignis an die konfigurierte E-Mail senden.

Vorgehensweise

1. Klicken Sie auf **Kommunikation →Benachrichtigung per E-Mail** , um die Seite aufzurufen.
2. Klicken Sie auf den Block, um die Funktion zum Senden des Videoereignisses zu aktivieren.
3. Geben Sie die Informationen des Absenders ein.

Hinweis

Es wird empfohlen, Gmail und Hotmail zum Senden von E-Mails zu verwenden.

4. Geben Sie die Informationen des Empfängers ein.

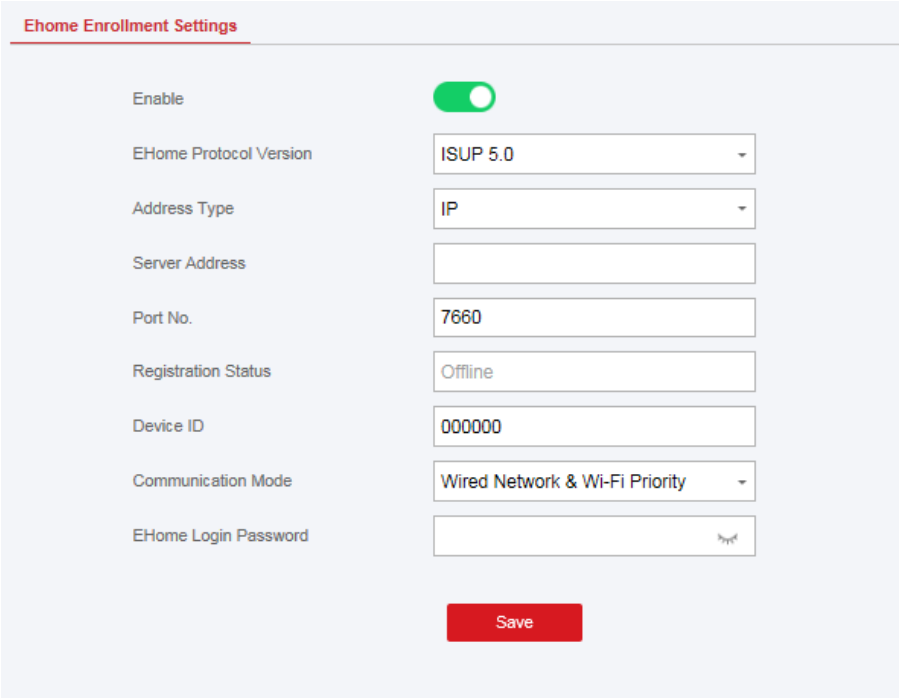
5. Klicken Sie auf **Empfängeradressen Test** und vergewissern Sie sich, dass die Adresse korrekt ist.
6. Klicken Sie auf **Speichern**.

ISUP

In diesem Abschnitt können Sie ein ISUP-Konto erstellen und die IP-Adresse/den Domänennamen und die Portnummer bearbeiten.

Vorgehensweise

1. Klicken Sie auf **Kommunikationsparameter** → **ISUP-Registrierung**, um die Seite ISUP-Einstellungen aufzurufen.



2. Schieben Sie den Schieberegler, um das ISUP-Protokoll zu aktivieren.
3. Wählen Sie den **Adressen Typ** und zwar als **IP-Adresse** oder **Domänenname**.
4. Geben Sie die IP-Adresse oder den Domänennamen entsprechend dem Adresstyp ein.
5. Geben Sie die Portnummer für das Protokoll ein.

Hinweis

Standardmäßig ist die Portnummer für ISUP 7660.

6. Legen Sie ein Konto fest, einschließlich der **Geräte-ID** und **ISUP-Anmeldepasswort**.
7. Auswählen **Kommunikationsmodus**.

Automatisch

Das System wählt den Kommunikationsmodus automatisch entsprechend der Reihenfolge des drahtgebundenen Netzwerks, des WLAN-Netzwerks und des Mobilfunk-Datennetzwerks aus. Nur wenn das aktuelle Netzwerk getrennt ist, stellt das Gerät eine Verbindung zu einem anderen Netzwerk her.

Kabelgebundene Netzwerk- und WLAN-Priorität

Die Reihenfolge der Verbindungspriorität von hoch nach niedrig ist: kabelgebundenes Netzwerk, WLAN, Mobilfunk-Datennetzwerk.

Kabelgebunden Netzwerk und WLAN

Das System wählt zuerst das drahtgebundene Netzwerk aus. Wenn kein drahtgebundenes Netzwerk erkannt wird, wird WLAN-Netzwerk ausgewählt.

Mobilfunknetz

Das System wählt nur das Mobilfunk-Datennetzwerk aus.

8. Klicken Sie auf **Speichern**.

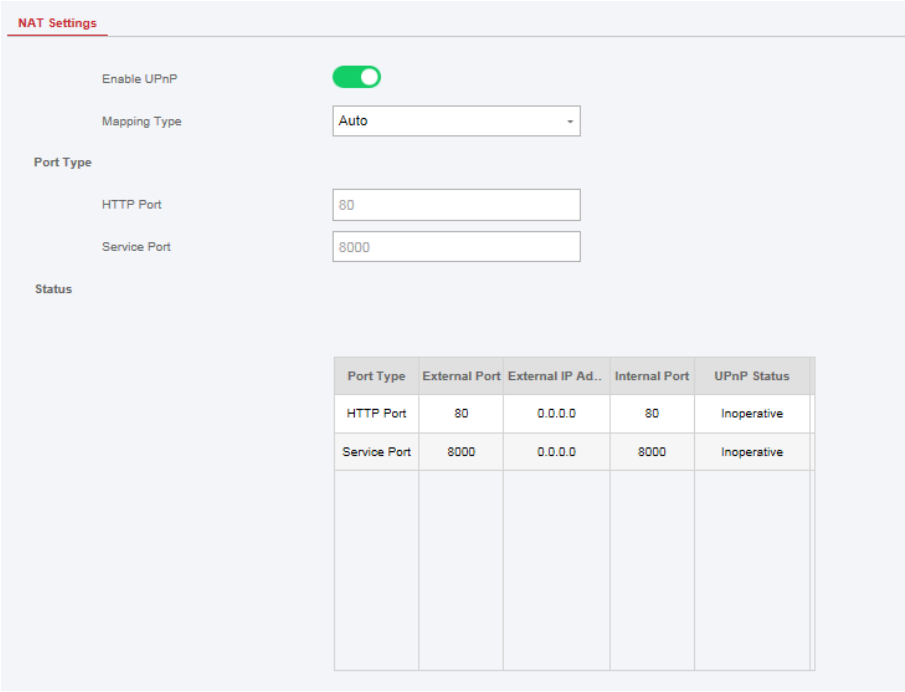
NAT

Universal Plug and Play (UPnP™) ist eine Netzwerkarchitektur, die Kompatibilität zwischen Netzwerkgeräten, Software und anderen Hardwaregeräten bietet. Mit dem UPnP-Protokoll können Geräte nahtlos verbunden werden und die Implementierung von Netzwerken in Heim- und Unternehmensumgebungen vereinfachen.

Wenn Sie die UPnP-Funktion aktivieren, müssen Sie nicht die Portzuordnung für jeden Port konfigurieren, und das Gerät ist über den Router mit dem Internet verbunden.

Vorgehensweise

1. Klicken Sie auf **Kommunikationsparameter** → **NAT**, um die Seite aufzurufen.



2. Ziehen Sie den Schieberegler, um UPnP zu aktivieren.
3. Optional: Wählen Sie den Zuordnungstyp als **Manuell**
4. Legen Sie den HTTP-Port und den Service-Port fest.
5. Klicken Sie auf **Speichern** um die Einstellungen abzuschließen

FTP

Sie können den FTP-Server so konfigurieren, um Alarmvideos zu speichern.

Vorgehensweise

1. Klicken Sie auf **Kommunikation** → **FTP**, um die Seite aufzurufen.
2. Konfigurieren der FTP-Parameter

FTP-Typ

Stellen Sie den FTP-Typ als bevorzugte oder alternative ein.

FTP-Protokoll

FTP und SFTP sind auswählbar. Die Dateien, die hochgeladen werden, werden mit dem SFTP-Protokoll verschlüsselt.

Serveradresse und -Port

Die FTP-Serveradresse und der entsprechende Port.

Benutzername und Passwort

Der FTP-Benutzer sollte die Berechtigung zum Hochladen von Bildern haben. Wenn der FTP-Server das Hochladen von Bildern durch anonyme Benutzer unterstützt, können Sie Anonym aktivieren, um Ihre Geräteinformationen während des Hochladens auszublenden.

Verzeichnisstruktur

Der Speicherpfad von Snapshots auf dem FTP-Server.

4.3.2 Geräteverwaltung

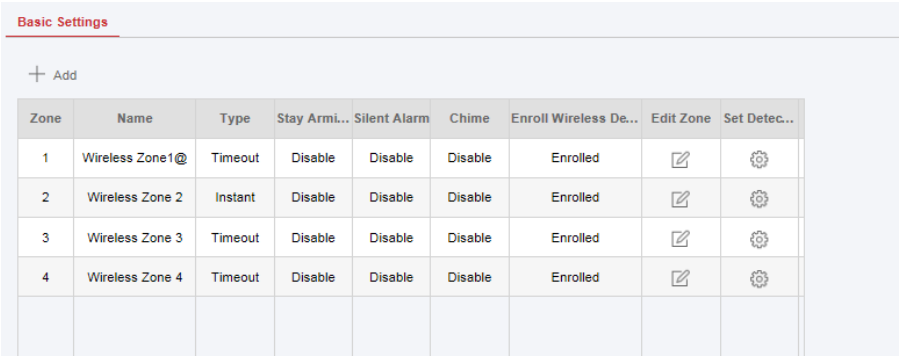
Sie können die angemeldeten Peripheriegeräte einschließlich Melder, Signalgeber, Bedienteil usw. in diesem Abschnitt verwalten.

Zone

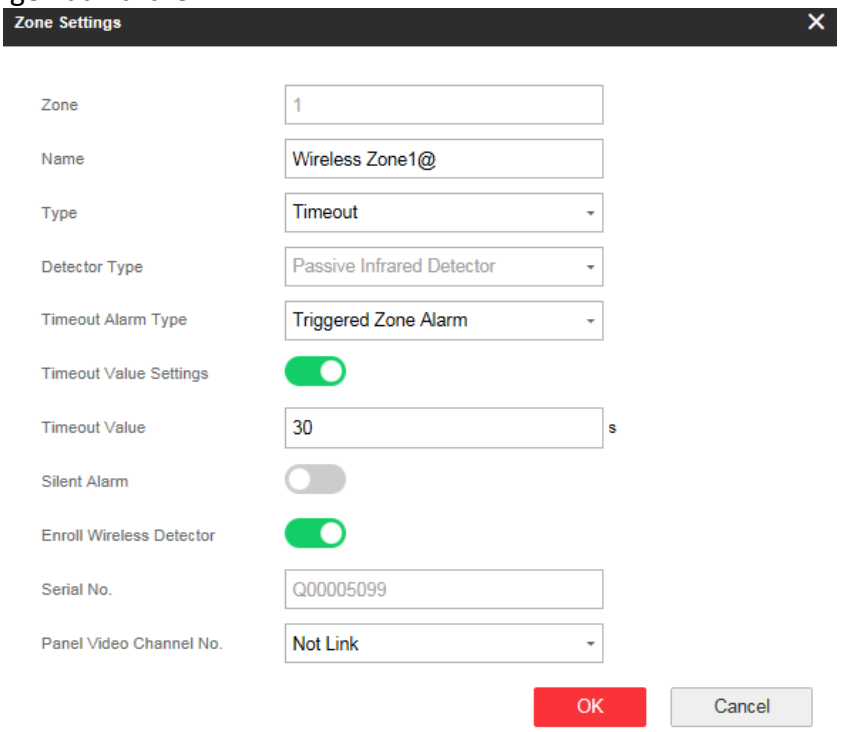
Sie können die Zonenparameter auf der Zonenseite einstellen.

Vorgehensweise

1. Klicken Sie auf **Gerät** → **Zone**, um auf die Zone-Seite zu gelangen.



2. Wählen Sie eine Zone aus und klicken Sie auf Zone bearbeiten, um die Seite Zoneneinstellungen aufzurufen.



3. Zonennamen bearbeiten.
4. Wählen Sie einen Zonen Typ aus.

Normal Alarm Zone

Dieser Zonen Typ löst sofort ein Alarmereignis aus, wenn er aktiviert wird.

Verzögerungszone

Ausgangsverzögerung: Die Ausgangsverzögerung gibt Ihnen Zeit, den Bereich ohne Alarm auszulösen zu verlassen.
Eingangsverzögerung: Die Eingangsverzögerung gibt Ihnen Zeit, den Bereich ohne Alarm auszulösen zu betreten, um das System unscharf zu schalten.
Das System gibt die Eingangs-/Ausgangsverzögerungszeit an, wenn es Scharfgeschalten oder erneut betreten wird. Wird normalerweise in der Eingangs-/Ausgangsroute (z.B. Vordereingang/Haupteingang) verwendet wo die Scharf-/Unscharfschaltung stattfindet.

Hinweis

In **Systemoptionen** → **Zeitplan und Timer** können Sie 2 verschiedene Zeitdauern einstellen. Stellen Sie sicher, dass der Timer nicht länger als 45 Sekunden eingestellt ist, um die Norm EN50131-1 zu erfüllen.

Hinweis

Sie können für intern scharfschalten die Verzögerungszeit für die Verzögerungszone einstellen.

Folge Zone

Die Zone agiert als verzögerte Zone während der Eingangsverzögerung, ansonsten agiert diese als Normal Alarm Zone.

Perimeter Zone

Das System gibt sofort einen Alarm aus, wenn es ein auslösendes Ereignis nach dem Scharfschalten erkannt wurde. Es gibt einen konfigurierbaren Intervall-Timer von 0 bis 600 Sekunden zwischen der Alarmaktivierung und der Signalisierung. Mit dieser Option können Sie den Alarm überprüfen und die Signalisierung während der Intervallzeit, im Falle eines Fehlalarms, abbrechen.
Wenn die Zone scharfgeschalten ist, können Sie die Verzögerungszeit des Peripheriealarms in **Systemoptionen** → **Zeitplan und Timer** einstellen. Sie können die Sirene auch in der Zeitverzögerung stummschalten.

Stiller Überfallalarm

Dieser Zonen Typ ist 24 Std. aktiv und wird für Überfall verwendet, nicht für Rauch- oder Glasbruchmelder.

Überfall Zone

Die Zone ist ständig aktiviert. Dieser Zonen Typ wird normalerweise an Standorten eingesetzt, die mit Überfalltaster, Rauchmelder und Glasbruchmelder ausgestattet sind.

Feuer Zone

Diese Zone wird immer Sirenen aktivieren, wenn ein Alarm auftritt. Dieser Zonen Typ wird normalerweise in brandgefährdete Bereiche eingesetzt, die mit Rauchmeldern und Temperatursensoren ausgestattet sind.

Gas Zone

Diese Zone wird immer Sirenen aktivieren, wenn ein Alarm auftritt. Dieser Zonen Typ wird normalerweise in Bereichen verwendet, die mit Gaswarngeräten ausgestattet sind (z.B. in der Küche).

Medizinische Zone

Die Zone wird immer mit einem Signalton aktiviert, wenn ein Alarm auftritt. Dieser Zonen Typ wird normalerweise an Orten verwendet, die mit medizinischen Notruftasten ausgestattet sind.

Timeout Zone

Die Zone ist ständig aktiviert. Dieser Zonen Typ wird verwendet, um den "AKTIVEN"-Status einer Zone zu überwachen und zu melden, aber meldet und alarmiert nur, nachdem die konfigurierbare Zeit (1 bis 599 Sekunden) abgelaufen ist. Dieser Zonen Typ wird

normalerweise an Orten verwendet, die mit Magnetkontakten ausgestattet sind, die einen Zugang nur für kurze Zeit (z.B. Tür zum Feuerwehrhydrant) erfordern.

Schlüsselschalterzone

Der verknüpfte Bereich wird nach der Auslösung scharf geschalten und nach der Wiederherstellung unscharf geschalten. Im Falle eines Sabotagealarms wird das scharf-/unscharfschalten nicht ausgeführt.

Hinweis

Für die Zone können zwei Auslösetypen (nach Zeiten und nach Zonenstatus) ausgewählt werden. Wenn der Zonenstatustyp ausgewählt ist, stellen Sie den Auslösevorgang ein (Scharf/Unscharfschalten).

Deaktivierte Zone

Alarme werden nicht aktiviert, wenn die Zone ausgelöst oder sabotiert wurde. Wird in der Regel zum Deaktivieren fehlerhafter Meldern verwendet.

24-Stunden-Zone

Die Zone aktiviert immer eine Sirene, wenn ein Alarm auftritt. Dieser Zonen Typ wird normalerweise in brandgefährdete Bereiche eingesetzt, die mit Rauchmeldern und Temperatursensoren ausgestattet sind.

5. Aktivieren **Bereichsübergreifender**, **Stiller Alarm usw.** entsprechend Ihren tatsächlichen Bedürfnissen.

Hinweis

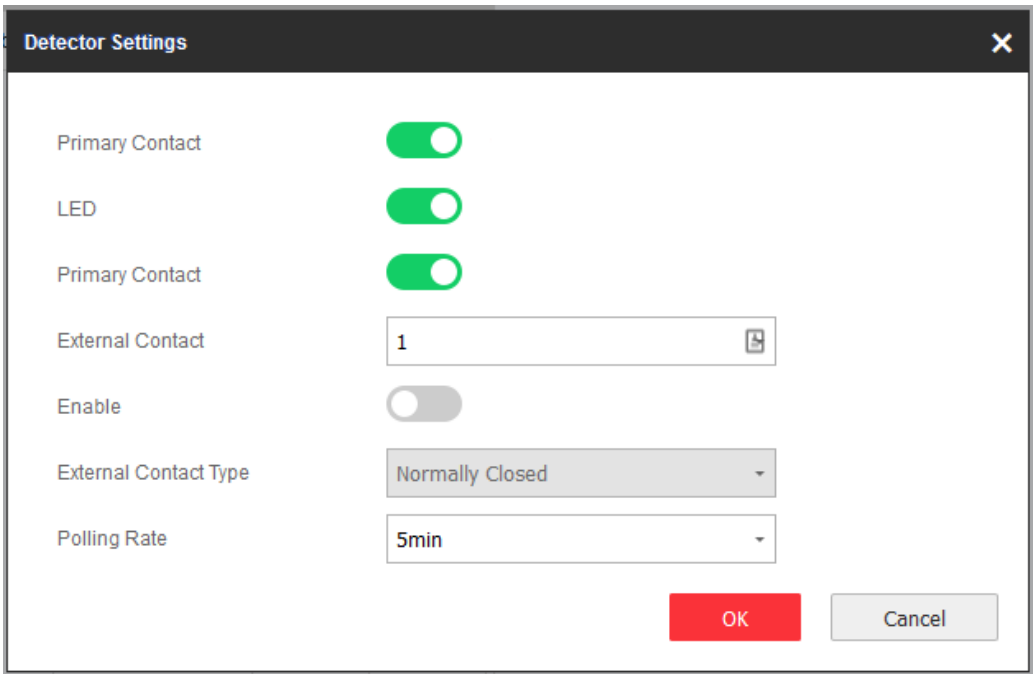
Einige Zonen unterstützen die Funktion nicht. Siehe die aktuelle Zone, um die Funktion einzustellen.

6. Stellen Sie die **Signalgeberverzögerungszeit.** Der Signalgeber wird sofort oder nach der eingestellten Zeit ausgelöst.
7. Verknüpfen Sie bei Bedarf eine Kamera mit der Zone.
8. Aktivieren Sie **Melder eingelernt**, geben Sie die Seriennummer ein und legen Sie die verknüpfte Kamera fest.
9. Klicken Sie auf **Bestätigen**.

Hinweis

Nachdem Sie die Zone eingestellt haben, können Sie **Status** → **Zone** aufrufen, um den Zonenstatus anzuzeigen.

10. Klicken Sie auf Zone bearbeiten, um die Seite Melder Einstellungen aufzurufen.



Hinweis

Die EN-Konformität erlaubt es nicht, den Kontakt zu deaktivieren.

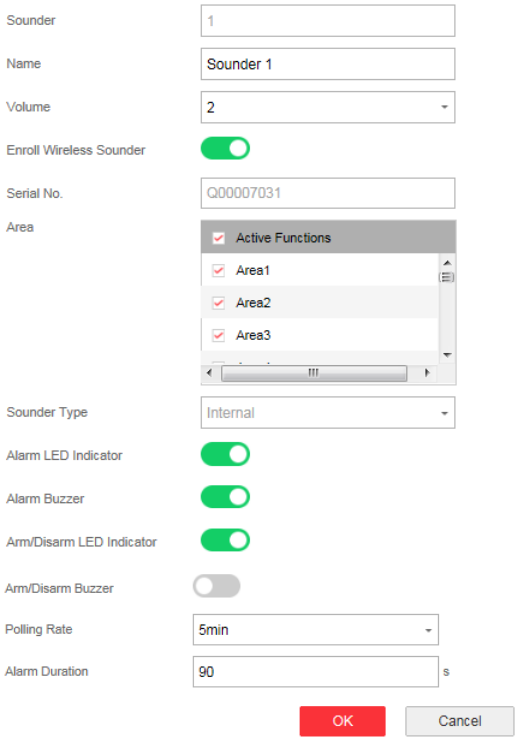
8.

Sirenen

Die Sirene wird über das Funkempfängermodul in den AX PRO eingelernt.

Vorgehensweise

1. Klicken Sie auf **Gerät** → **Signalgeber**.
2. Klicken Sie auf ⚙, um die Seite „Sirenen Einstellungen“ aufzurufen.



3. Stellen Sie den Namen des Signalgebers und die Lautstärke ein.

Hinweis

Der zur Verfügung stehende Lautstärkebereich liegt zwischen 0 und 3 (Funktion variiert je nach Gerätemodell).

5. Aktivieren Sie **Funk Sirene einlernen** und geben Sie die Seriennummer der Funk Sirene ein.
6. Wählen Sie den verknüpften Bereich aus.
7. Wählen Sie zum Aktivieren von **Alarm-LED-Anzeige**, **Alarm Signalton**, **Scharf/Unscharf LED** und **Scharf/Unscharf Signalton**.
8. Stellen Sie das **Abfrage-Intervall** und die **Alarmdauer** ein.
9. Klicken Sie auf **Bestätigen**.

Hinweis

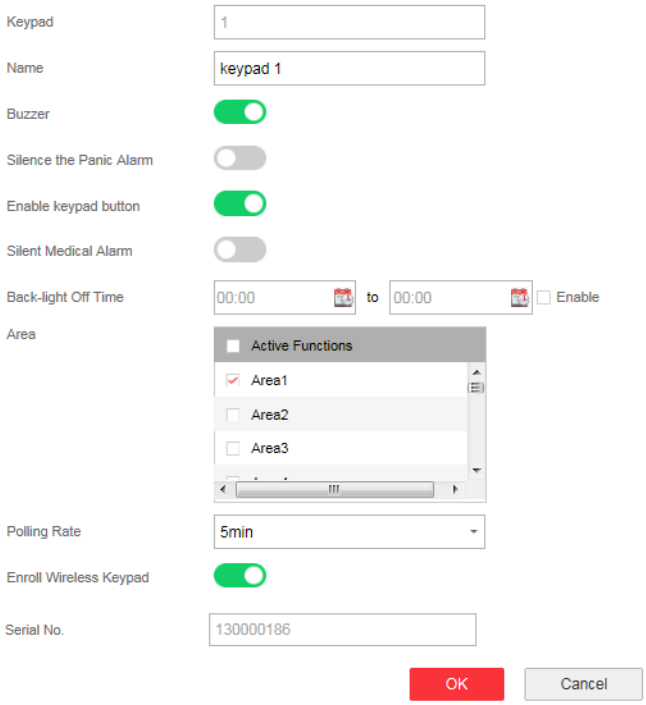
Nachdem der Signalgeber konfiguriert wurde, können Sie auf **Status** → **Signalgeber**, um den Status des Signalgebers anzuzeigen.

Bedienteil

Sie können die Parameter des Bedienteils einstellen, die am AX PRO System angemeldet ist.

Vorgehensweise

1. Klicken Sie auf **Gerät** → **Bedienteil**.
2. Klicken Sie auf ⚙ um die Seite „Bedienteil Einstellungen“ aufzurufen.



3. Geben Sie einen Namen für das Bedienteil ein.
4. Aktivieren Sie das Kontrollkästchen, um die Funktion von Signalton, Stiller Überfallalarm, Stiller Medizinischer Alarm und Bedienteil zu aktivieren.
5. Überprüfen Sie das **Aktivieren** Kontrollkästchen der Hintergrundbeleuchtungs-Aus-Zeit und stellen Sie die Dauer der Beleuchtung ein.
6. Wählen Sie den mit dem Bedienteil den verknüpften Bereich aus.
7. Aktivieren Sie **Funkbedienteil einlernen** und geben Sie die Seriennummer ein.
8. Klicken Sie auf **Bestätigen**.

Hinweis

- Nachdem das Bedienteil konfiguriert wurde, können Sie auf **Status** → **Bedienteil** aufrufen, um den Status des Bedienteils anzuzeigen.
- Sie können den Pin-Code des Bedienteils auf der Seite **Benutzerverwaltung** → **Benutzer** → **Betrieb** einstellen.

4.3.3 Zonen Einstellungen

Grundeinstellungen

Sie können Zonen mit dem ausgewählten Bereich verknüpfen.

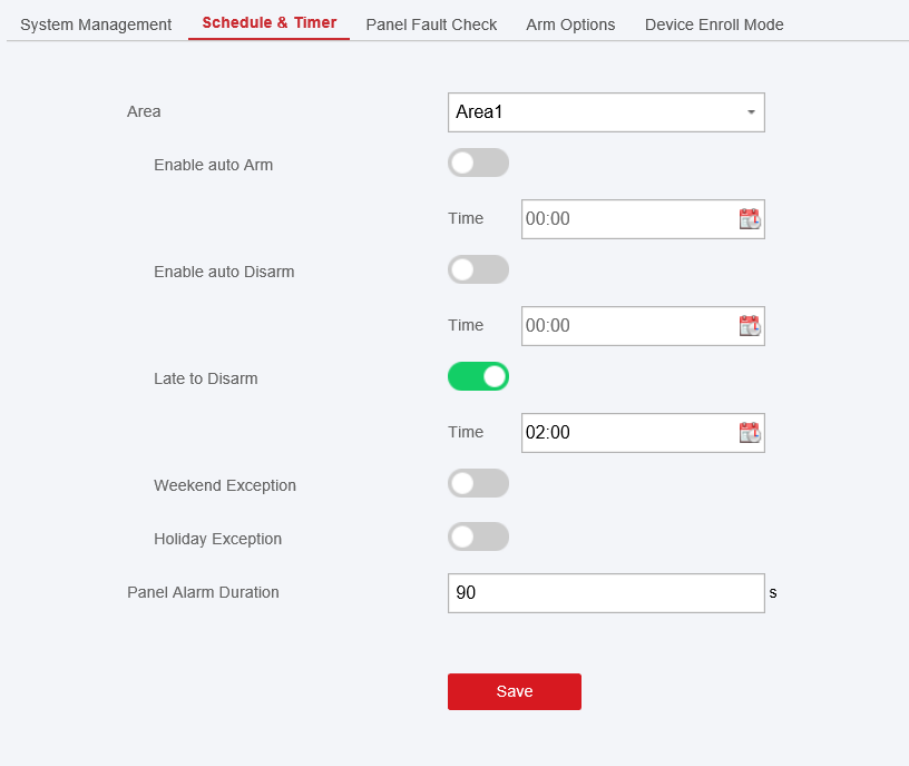
Vorgehensweise

1. Klicken Sie auf **Bereich** → **Grundeinstellungen**, um die Seite aufzurufen.

2. Wählen Sie einen Bereich aus.
3. Überprüfen Sie **Aktivieren**.
4. Aktivieren Sie das Kontrollkästchen vor der Zone, um Zonen für den Bereich auszuwählen.
5. Klicken Sie auf **Speichern**, um die Einstellungen abzuschließen.

Zeitplan- und Timer-Einstellungen

Sie können den Alarmzeitplan einstellen. Die Zone wird gemäß dem konfigurierten Zeitplan scharf-/unscharfgeschalten.



Vorgehensweise

1. Klicken Sie auf **System** → **Systemoptionen** → **Zeitplan und Timer**, um die Seite Zeitplan und Timer aufzurufen.
2. Wählen Sie einen Bereich aus.
3. Stellen Sie die folgenden Parameter entsprechend den tatsächlichen Anforderungen ein.

Automatisches Scharfschalten aktivieren

Aktivieren Sie die Funktion und stellen Sie die Startzeit die Scharfschaltung ein. Die Zone wird entsprechend der konfigurierten Zeit scharfgeschalten.

Hinweis

- Die Zeit für „Automatisches Scharfschalten“ und die Zeit für „Automatisches Unscharfschalten“ können nicht identisch sein.
- Der Signalton ertönt langsam 2 Minuten vor dem Start der automatischen Scharfschaltung und 1 Minute vor dem Start der automatischen Scharfschaltung ertönt ein schneller

Signalton.

- Sie können auf der Seite Systemoptionen auswählen, ob die Zwangs-Scharfschaltung aktiviert werden soll. Während die Funktion aktiviert ist, wird das System unabhängig vom Fehler scharfgeschalten.
- Wenn der öffentliche Bereich aktiviert ist, unterstützt der Bereich 1 die Funktion „Automatisches Scharfschalten“ nicht.

Automatisches Unscharfschalten aktivieren

Aktivieren Sie die Funktion und legen Sie die Zeit für die Unscharfschaltung fest. Die Zone wird gemäß der konfigurierten Zeit unscharfgeschalten.

Hinweis

- Der Zeitpunkt für „Automatisches Scharfschalten“ und der Zeitpunkt für „Automatisches Unscharfschalten“ können nicht identisch sein.
- Wenn der öffentliche Bereich aktiviert ist, unterstützt der Bereich 1 die Funktion „Automatisches Unscharfschalten“ nicht.

Deadline Unscharfschalten

Aktivieren Sie die Funktion und stellen Sie die Zeit ein. Wenn der Alarm nach der konfigurierten Zeit ausgelöst wird, gilt die Person als verspätet.

Hinweis

Sie sollten die Benachrichtigungs-Funktion der Zentrale in **Kommunikationsparameter** → **Ereigniskommunikation** bevor Sie die Funktion „Deadline Unscharfschalten“ aktivieren.

Wochenendausnahme

Aktivieren Sie die Funktion und die Zone wird am Wochenende nicht scharfgeschalten.

Feiertagsausnahme

Aktivieren Sie die Funktion und die Zone wird am Feiertag nicht scharf-/unscharfgeschalten. Sie sollten den Feiertagsplan nach der Aktivierung festlegen.

Hinweis

Es können bis zu 6 Feiertagsgruppen festgelegt werden.

Alarmdauer der Zentrale

Wenn Sie die Perimeter Zone eingestellt haben, können Sie die Zeitdauer des Alarms einstellen.

Hinweis

Die verfügbare Dauer liegt zwischen 1 und 900 Sekunden.

5. Klicken Sie auf **Speichern**.

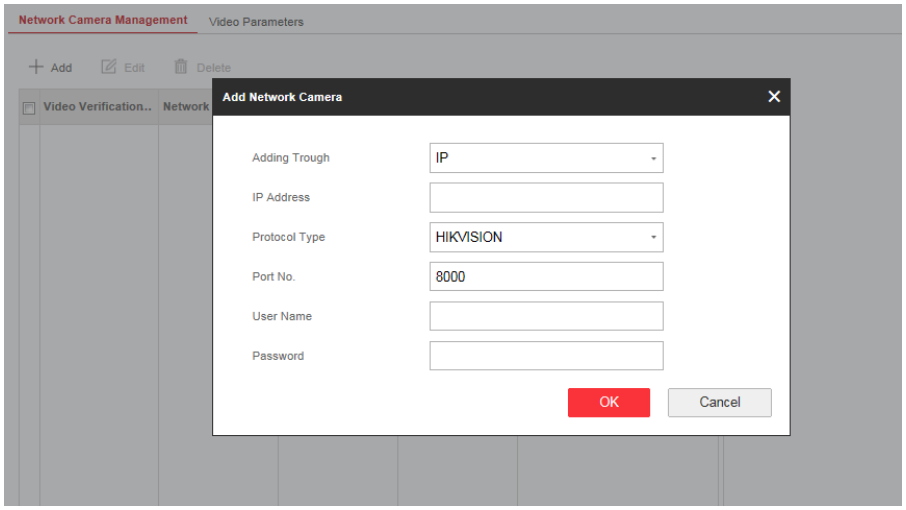
4.3.4 Videoverwaltung

Sie können der AX PRO Zentrale zwei Netzwerkkameras hinzufügen und die Kamera mit einer Zone für die Videoüberwachung verknüpfen. Sie können das Ereignisvideo auch über die App und E-Mail empfangen und anzeigen.

Kameras zu AX PRO hinzufügen

Vorgehensweise

1. Klicken Sie auf **Gerät →Netzwerkkamera**, um die Netzwerkkamera-Verwaltungsseite aufzurufen.



2. Klicken Sie auf **Hinzufügen** und geben Sie die grundlegenden Informationen der Kamera ein, wie z.B. IP-Adresse und Port-Nr., und wählen Sie den Protokolltyp aus.
3. Geben Sie den Benutzernamen und das Passwort der Kamera ein.
4. Klicken Sie auf **Bestätigen**.
5. Optional: Klicken Sie auf **Bearbeiten** oder **Löschen**, um die ausgewählte Kamera zu bearbeiten oder zu löschen.

Verknüpfen einer Kamera mit der Zone

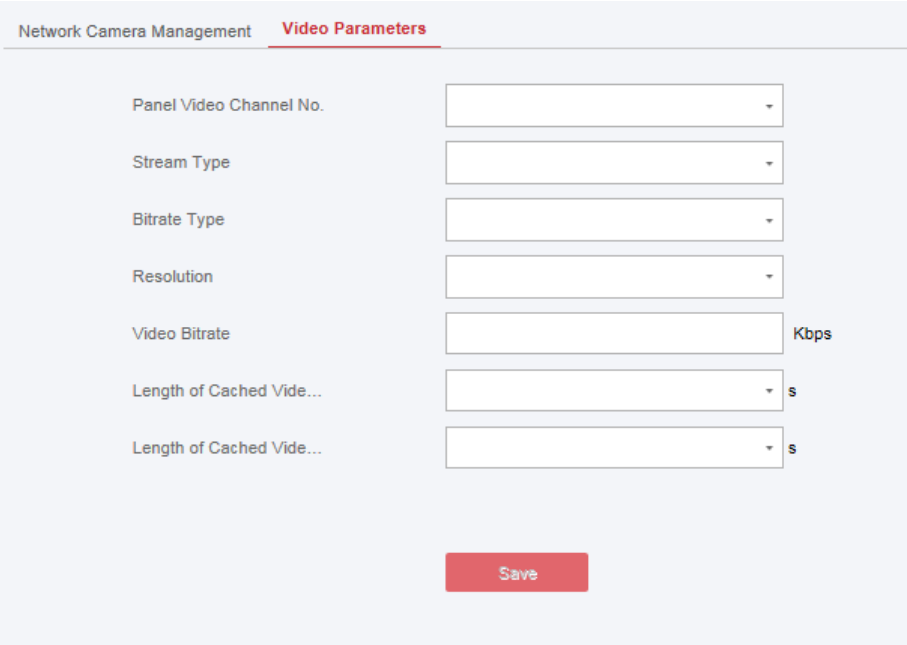
Vorgehensweise

1. Klicken Sie auf **Gerät → Zone**, um die Konfigurationsseite aufzurufen.
2. Wählen Sie eine Zone aus, die Sie für die Videoüberwachung einschließen möchten, und klicken Sie auf die Schaltfläche ⚙.
3. Wählen Sie die **Videokanal-Nr. der Zentrale**.
4. Klicken Sie auf **Bestätigen**.

Videoparameter einstellen

Vorgehensweise

1. Klicken Sie auf **Gerät →Netzwerkkamera** → Video zum Aufrufen der Seite.



2. Wählen Sie eine Kamera aus und stellen Sie die Videoparameter ein.

Stream Typ

Main Stream: Wird für die Aufnahme- und HD-Vorschau verwendet und verfügt über eine hohe Auflösung, Bitrate und Bildqualität.
Sub Stream: Wird für das Videostreaming und Vorschaubilder verwendet, mit niedrigerer Auflösung, Bitrate und Bildqualität.

Bitratentyp

Wählen Sie den Bitratentyp als Konstant oder Variable aus.

Auflösung

Wählen Sie die Auflösung des Videoausgangs aus.

Video Bitrate

Der höhere Wert entspricht der höheren Videoqualität, aber eine höhere Bandbreite ist erforderlich.

4.3.5 Berechtigungsverwaltung

Fernbedienung hinzufügen/bearbeiten/löschen

Sie können eine Fernbedienung der AX PRO Zentrale hinzufügen und Zentrale damit steuern. Sie

können die Informationen der Fernbedienung bearbeiten oder aus der AX PRO Zentrale löschen.

Vorgehensweise

1. Klicken Sie auf **Gerät** → **Fernbedienung**, um die Seite „Verwaltung Fernbedienungen“ aufzurufen.
2. Klicken Sie auf **Hinzufügen** und drücken Sie eine beliebige Taste auf der Fernbedienung.
3. Stellen Sie die Parameter der Fernbedienung ein.

   Name

   Passen Sie einen Namen für die Fernbedienung an.

   Berechtigungseinstellungen

   Überprüfen Sie verschiedene Elemente, um Berechtigungen zuzuweisen.

   Einzeltasten-Einstellungen

   Wählen Sie aus der Dropdown-Liste, um die Funktionen der Tasten I und II einzustellen

   Einstellungen für Kombinationstasten

   Wählen Sie aus der Dropdown-Liste aus, um die Funktionen der Kombinationstasten einzustellen.
4. Klicken Sie auf **Bestätigen**.
5. Optional: Klicken Sie auf , um die Informationen der Fernbedienung zu bearbeiten.
6. Optional: Löschen Sie eine Fernbedienung oder wählen Sie mehrere Fernbedienungen aus und wählen Sie **Löschen**, um mehrere gleichzeitig zu löschen.

Hinweis

Die Kommunikation von Funkkomponenten, wie die Funkfernbedienung, wird durch die SN-Nummer identifiziert, die während der Übertragung verschlüsselt wird. Die Seriennummer fängt mit dem Buchstaben Q bis Z an und es folgen 8 Ziffern, z.B. Q02235774. Daraus ergeben sich maximal 100.000.000 Kombinationen.

Transponder hinzufügen/bearbeiten/löschen

Sie können dem AX PRO System einen Transponder hinzufügen und diesen dazu verwenden, um eine Zone zu scharf/unscharf zu schalten. Sie können die Transponder-Informationen bearbeiten oder aus dem AX PRO System löschen.

Hinweis

Die Kommunikation des Transponders wird durch die SN-Nummer identifiziert, die während der Übertragung verschlüsselt wird. Die Seriennummer umfasst 32 Ziffern, daraus ergeben sich maximal 4.294.967.296 Kombinationen.

Vorgehensweise

1. Klicken Sie auf **Gerät** → **Transponder**, um die Verwaltungsseite aufzurufen.
2. Klicken Sie auf **Hinzufügen** und halten Sie den Transponder an den Transponder-Lesebereich der AX PRO Zentrale.
3. Ändern Sie den Namen für den Transponder.
4. Wählen Sie den Transponder-Typ und den verknüpften Tag-Bereich aus.
5. Wählen Sie die Berechtigung für den Transponder aus.

Hinweis

Sie sollten mindestens eine Berechtigung für den Transponder zuweisen.

6. Klicken Sie auf **Bestätigen** und die Transponder-Informationen werden in der Liste angezeigt.

Hinweis

Der Transponder unterstützt mindestens 20.000 Seriennummern.

7. Optional: Klicken Sie auf ✎ und Sie können den Namen vom Transponder ändern.
8. Optional: Löschen Sie einen einzelnen Transponder oder markieren Sie mehrere Transponder und klicken Sie auf **Löschen**, um mehrere gleichzeitig zu löschen.

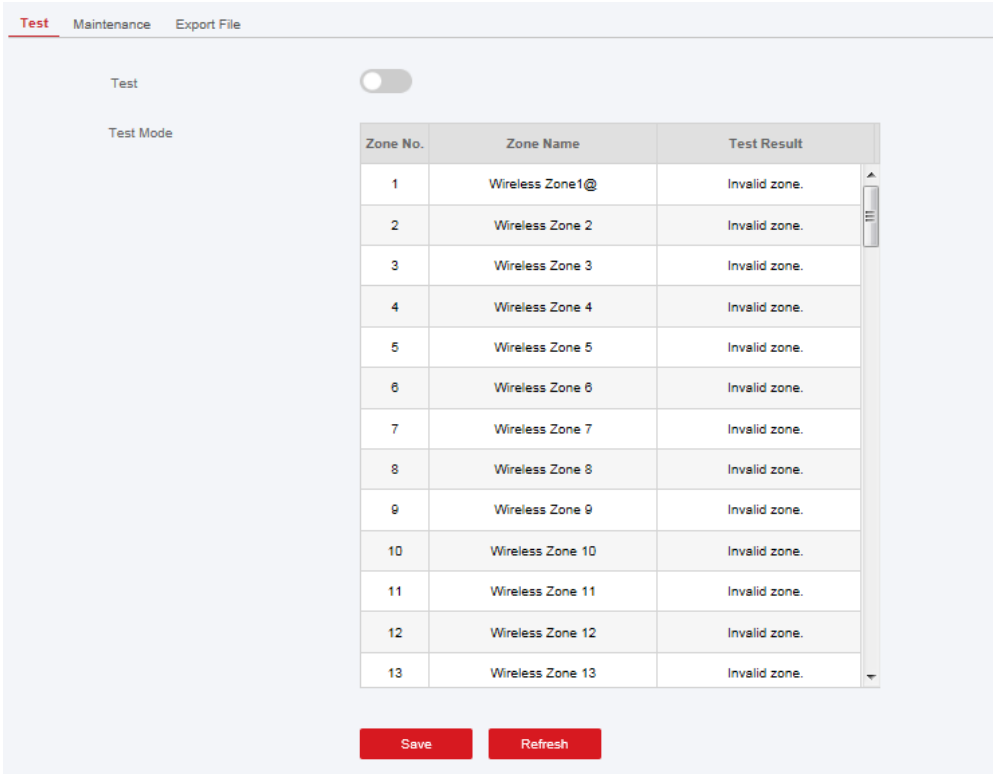
4.3.6 Wartung

Test

Die AX PRO Zentrale unterstützt die Gehtestfunktion.

Vorgehensweise

1. Wählen Sie **Projektverwaltung** →**Wartung** → **Test** → um die Funktion zu aktivieren.



Hinweis

Nur wenn alle Melder fehlerfrei sind, können Sie in den TEST-Modus wechseln.

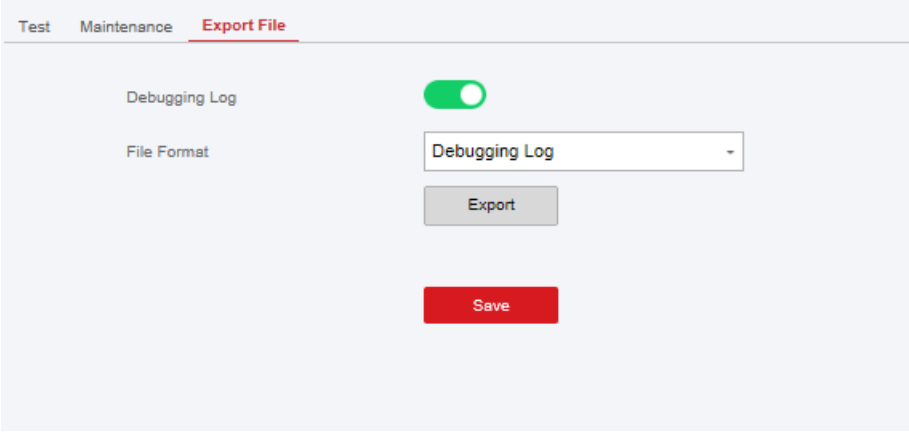
2. Klicken Sie das Kontrollkästchen **Test**, um den Gehtest zu starten.
3. Klicken Sie auf **Speichern** um die Einstellungen abzuschließen.
4. Lösen Sie jeden Melder in jeder Zone aus.
5. Prüfen Sie das Testergebnis.

Datei exportieren

Sie können die Debugging-Datei auf den PC exportieren.

Vorgehensweise

1. Klicken Sie auf **Wartung** → **Datei exportieren**, um die Seite aufzurufen.

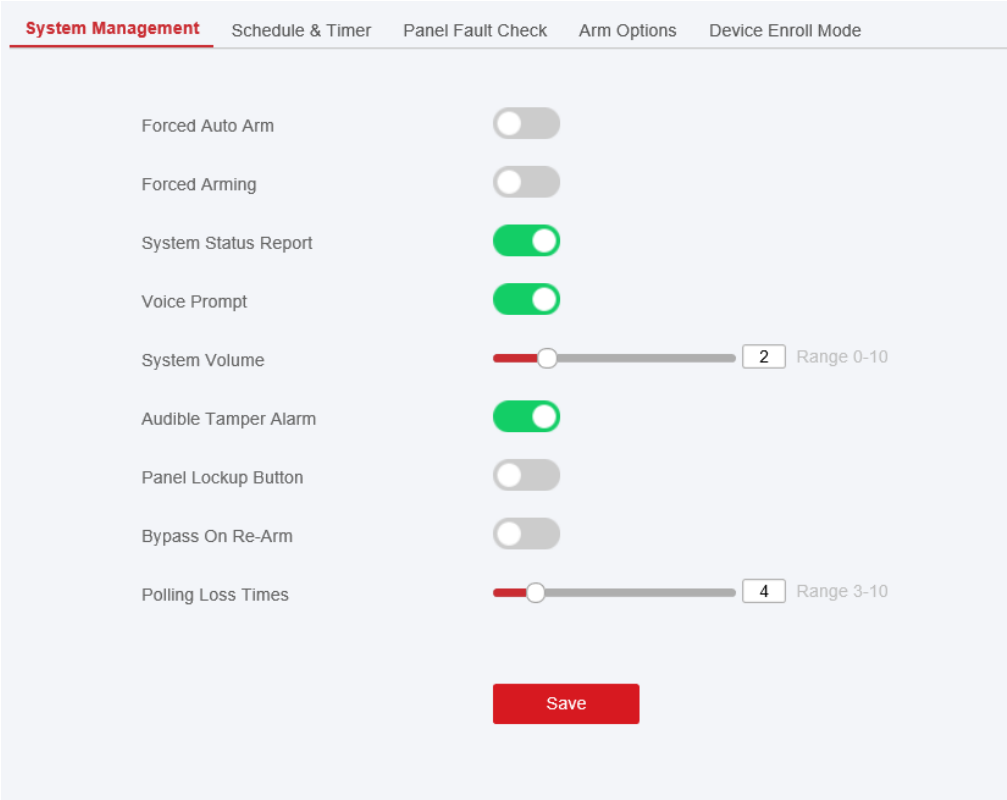


2. Aktivieren Sie das Kontrollkästchen, um die Funktion zu aktivieren.
3. Klicken Sie auf **Exportieren**, um die Debugging-Datei im PC zu speichern.

4.3.7 Systemeinstellungen

Verwaltung von Berechtigungen

Stellen Sie die Berechtigungsoptionen ein.
Klicken Sie auf **System** → **Systemoptionen** → Systemverwaltung, um die Seite Systemoptions Verwaltung aufzurufen.



Überprüfung der Funkkomponenten

Wenn die Option aktiviert ist, erkennt das System den Heartbeat aller Funkkomponenten. Wenn kein Heartbeat der Peripherie erkannt wird, lädt das System ein Ereignis hoch.

Hinweis

Für EN Konformität nicht auf AUS schalten.

Scharfschalten mit Fehler

Wenn die Option aktiviert ist und aktive Fehler in einer Zone vorliegen, wird die Zone beim Scharfschalten automatisch Bypassed (umgangen).

Hinweis

Sie sollten die Scharfschaltfunktion auf der Seite Erweiterte Einstellungen deaktivieren. Ansonsten ist das Scharfschalten der AX PRO Zentrale mit Fehler nicht möglich.

AX PRO-Statusbenachrichtigung

Wenn die Option aktiviert ist, lädt das Gerät den Bericht automatisch hoch, wenn der AX PRO-Status geändert wird.

Funktionstaste deaktivieren

Wenn die Option aktiviert ist, werden alle Funktionstasten deaktiviert.

Sprachausgabe

Wenn die Option aktiviert ist, ist die Sprachausgabe für die AX PRO Zentrale aktiviert.

Sprachaufforderung zum Unscharfschalten und Löschen des Alarms

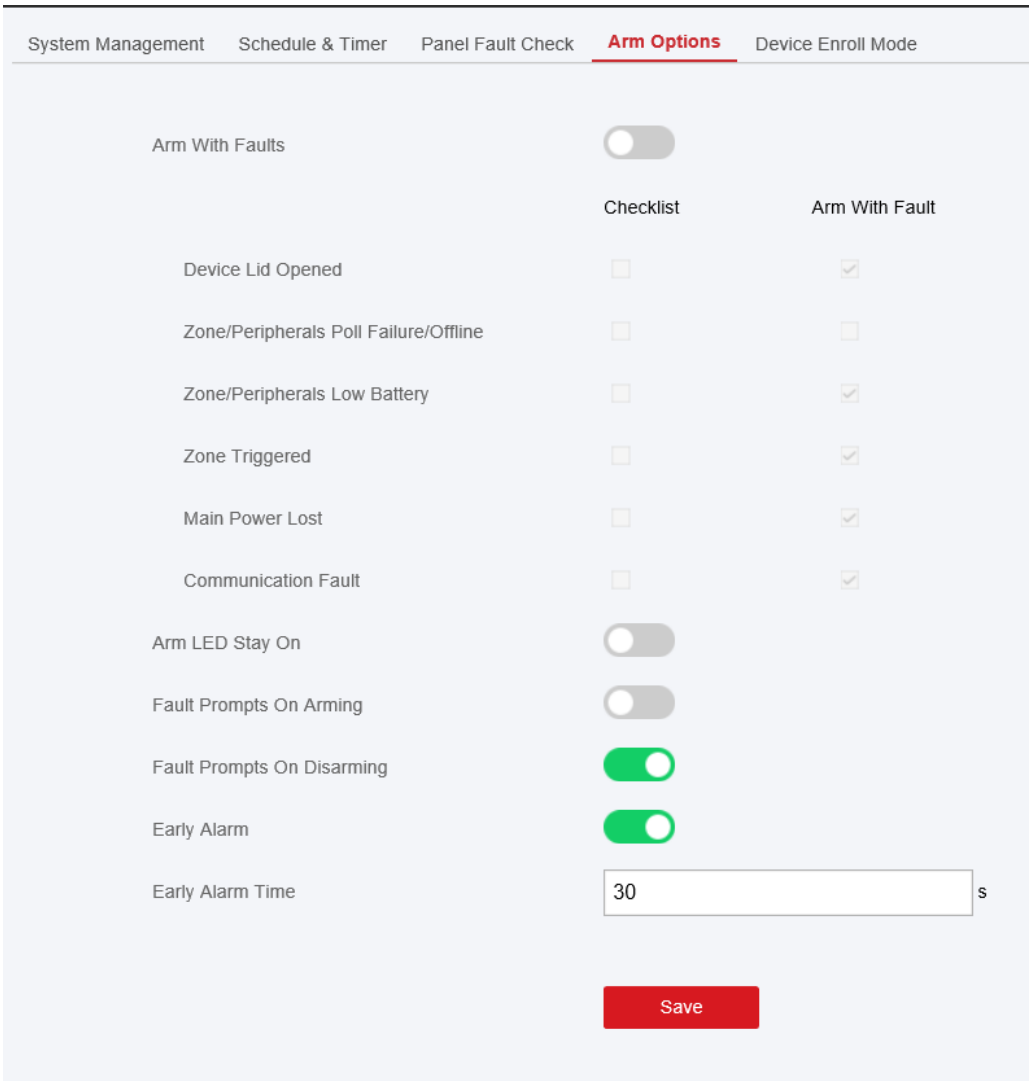
Wenn die Option aktiviert ist, sendet die AX PRO Zentrale alle Systemfehler vor der Unscharfschaltung und Löschen der Alarme. Bevor Sie diese Funktion aktivieren, müssen Sie **Sprachausgabe** aktivieren.

Systemlautstärke

Der Lautstärke liegt zwischen 0 und 10.

Scharfschalte-Optionen

Legen Sie erweiterte Berechtigungsparameter fest.
Klicken Sie auf **System** → **Systemoptionen** → **Scharfschalte-Optionen**, um die Seite „Erweiterte Einstellungen“ aufzurufen.



Sie können die folgenden Parameter einstellen:

Scharfschalten mit Fehler aktivieren

Überprüfen Sie die Fehler in der Liste. Die Zentrale unterbricht die Scharfschaltung nicht, auch wenn Fehler aufgetreten sind.

Fehler-Checkliste

Das System prüft ob der Scharfschaltung Fehler vorliegen.

Scharfschalten LED bleibt eingeschaltet

Wenn das Gerät den EN-Standard anwendet, ist die Funktion standardmäßig deaktiviert. Wenn das Gerät aktiviert ist, leuchtet die Anzeige 5 Sekunden lang durchgehend blau. Wenn die Zentrale unscharfgeschalten ist, blinkt die Anzeige 5 Mal.
Wenn die Funktion aktiviert ist, und das Gerät scharfgeschalten ist, leuchtet die Anzeige dauerhaft. Und wenn die Zentrale unscharfgeschalten ist, ist die Anzeige aus.

Fehler Eingabeaufforderung beim scharf-/unscharfschalten

Wenn das Gerät den EN-Standard anwendet, ist die Funktion standardmäßig deaktiviert. In

diesem Fall gibt das Gerät während des scharf-/unscharfschalten keine Fehler aus.

Frühalarm aktivieren

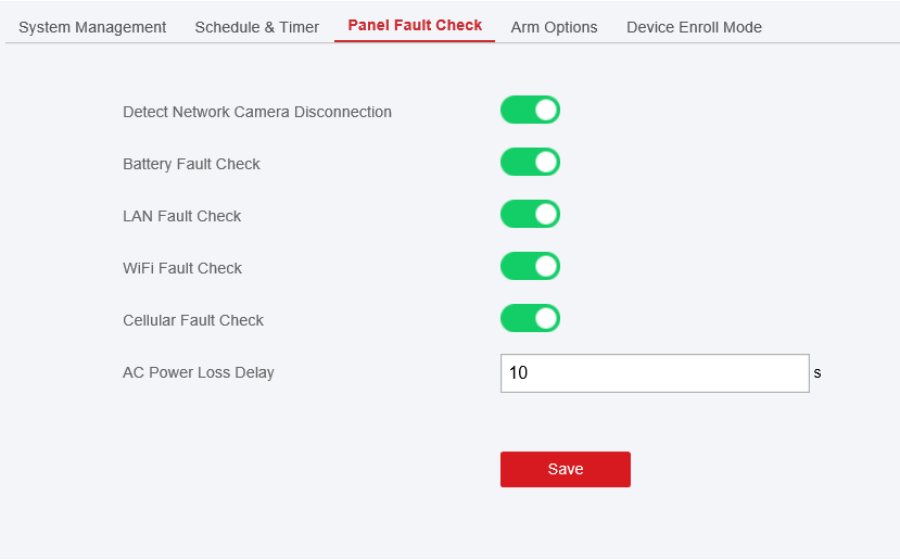
Wenn Sie die Funktion aktivieren und die Zone scharfgeschalten und ausgelöst wird, wird der Alarm nach der eingestellten Verzögerungszeit ausgelöst.

Hinweis

Der Frühalarm wird erst nach Auslösung der verzögerten Zone wirksam.

Fehlerprüfung

Das System bestimmt, ob die auf Seite aufgeführten Fehler überprüft werden sollen. Das System prüft nur den ausgewählten Fehler.
Klicken Sie auf **System** → **Systemoptionen** →**Fehlerprüfung**, um die Seite aufzurufen.



Netzwerkkamera- Getrennte Verbindung erkennen

Wenn die Option aktiviert ist und die verknüpfte Netzwerkkamera getrennt wird, wird ein Alarm ausgelöst.

Batteriefehlerprüfung

Wenn die Option aktiviert ist, lädt das Gerät Ereignisse hoch, wenn die Batterie getrennt oder nicht geladen ist.

LAN-Fehlerprüfung

Wenn die Option aktiviert ist, wenn das drahtgebundene Netzwerk getrennt ist oder andere Fehler vorliegen, wird der Alarm ausgelöst.

WLAN-Fehlerprüfung

Wenn die Option aktiviert ist, wenn die WLAN-Verbindung getrennt wird oder andere Fehler vorliegen, wird der Alarm ausgelöst.

Überprüfung des Mobilfunknetzfehlers

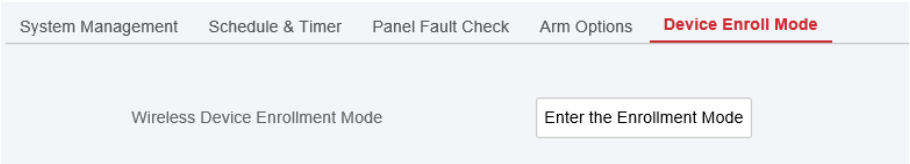
Wenn die Option aktiviert ist, wenn das Mobilfunk-Datennetzwerk getrennt ist oder andere Fehler vorliegen, wird der Alarm ausgelöst.

Strom AC-Stromausfall Verzögerungszeit

Das System prüft den Fehler nach der konfigurierten Zeitdauer nach dem Stromausfall. Um die EN 50131 3 zu erfüllen, sollte die Prüfzeitdauer 10 Sekunden betragen.

Geräte Einlernmodus

Klicken Sie auf Einlernmodus, um den Einlernmodus zu starten.

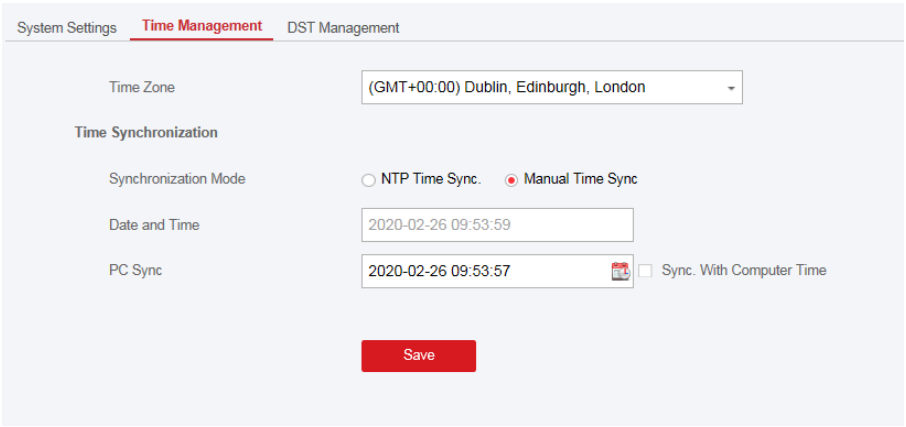


Zeiteinstellungen

Sie können die Zeitzone des Geräts einstellen, die Gerätezeit synchronisieren und die Sommerzeit einstellen. Das Gerät unterstützt die Zeitsynchronisierung über **Hik-Connect Guarding Vision** Server.

Zeitverwaltung

Klicken Sie auf **System** → **Systemeinstellungen** → **Uhrzeit**, um die Seite Zeitmanagement aufzurufen.



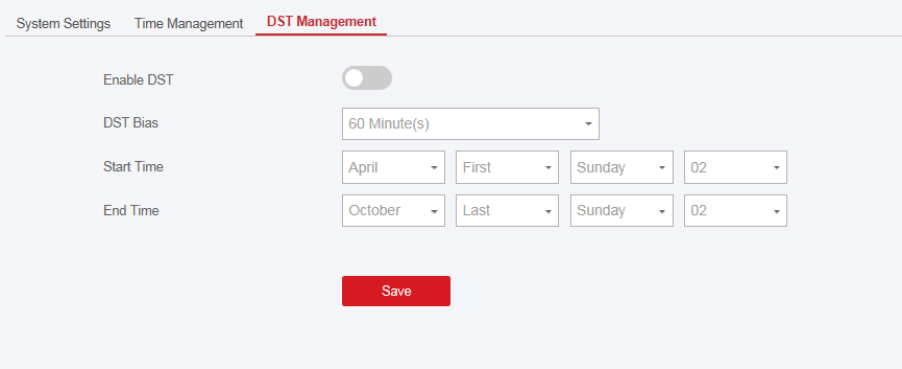
Sie können eine Zeitzone aus der Dropdown-Liste auswählen.
Sie können die Gerätezeit manuell mit NTP synchronisieren. Aktivieren Sie das Kontrollkästchen von **NTP-Zeitsynchronisierung.**, geben Sie die Serveradresse und Port-Nr. ein und legen Sie das Synchronisierungsintervall fest.
Sie können die Gerätezeit manuell synchronisieren. Oder überprüfen Sie **Synchronisierung mit Computerzeit**, um die Gerätezeit mit der Computerzeit zu synchronisieren.

Hinweis

Während Sie die Zeit manuell oder mit der Computerzeit synchronisieren, wird in dem Protokoll „SDK Synchronisation“ eingetragen.

DST Verwaltung

Klicken Sie auf **System** → **Systemeinstellungen** → **DST Verwaltung**, um die Seite Zeitmanagement aufzurufen.



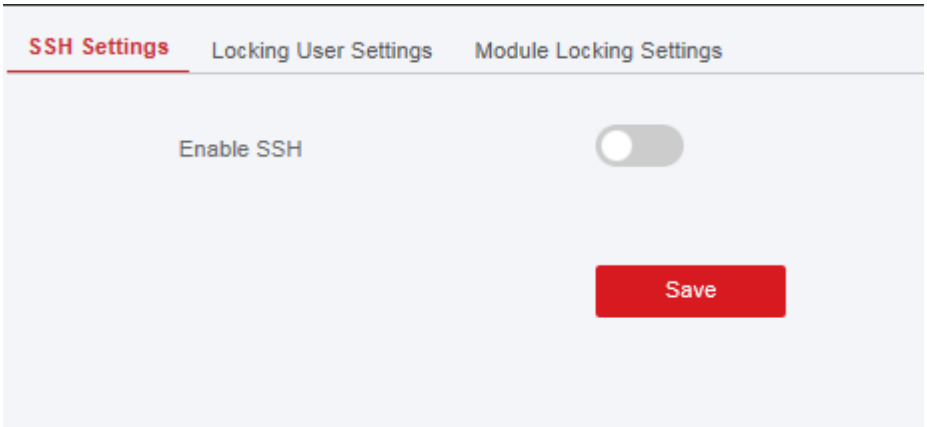
Sie können die Sommerzeit aktivieren und die Sommerzeit-Bias, die Sommerzeit-Startzeit und die Sommerzeit-Endzeit einstellen.

Sicherheitseinstellungen

SSH-Einstellungen

Aktivieren oder deaktivieren Sie SSH (Secure Shell) entsprechend Ihren tatsächlichen Anforderungen.

Klicken Sie auf **System** → **Systemsicherheit** → **SSH-Einstellungen**, um die Seite SSH-Einstellungen aufzurufen. Sie können die SSH-Funktion aktivieren oder deaktivieren.



Sperren von Benutzereinstellungen

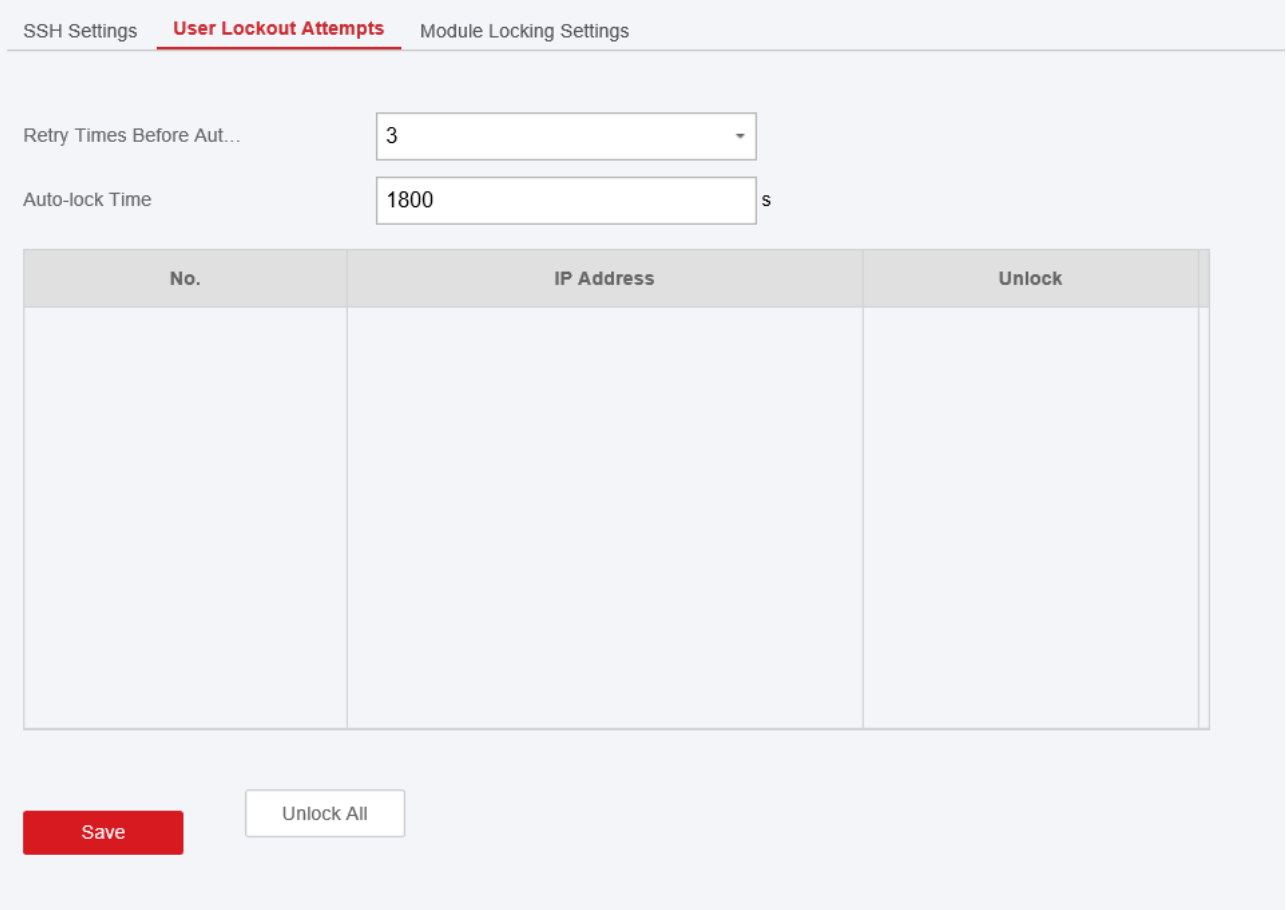
Das Gerät nach 3 fehlgeschlagenen Anmeldeversuchen innerhalb 1 Minute für 90 Sekunden gesperrt in einer Minute.
Sie können den gesperrten Benutzer anzeigen oder einen Benutzer entsperren und die Benutzersperrdauer festlegen.

Hinweis

Um die EN-Anforderungen zu erfüllen, zeichnet das System das gleiche Protokoll nur dreimal kontinuierlich auf.

Vorgehensweise

1. Klicken Sie auf **System** → **System Sicherheit** → **Benutzersperrversuche**, um die Seite aufzurufen.



2. Legen Sie die folgenden Parameter fest:

Anzahl Versuche vor automatischer Sperrung

Wenn der Benutzer mehrfach das falsche Passwort eingibt, wird das Konto gesperrt.

Hinweis

Der Administrator hat zwei weitere Versuche als der konfigurierte Wert.

Gesperrte Dauer

Legen Sie die Dauer für die Kontosperrung fest.

Hinweis

Die Dauer der Kontosperrung beträgt zwischen 5 bis 1.800 Sekunden.

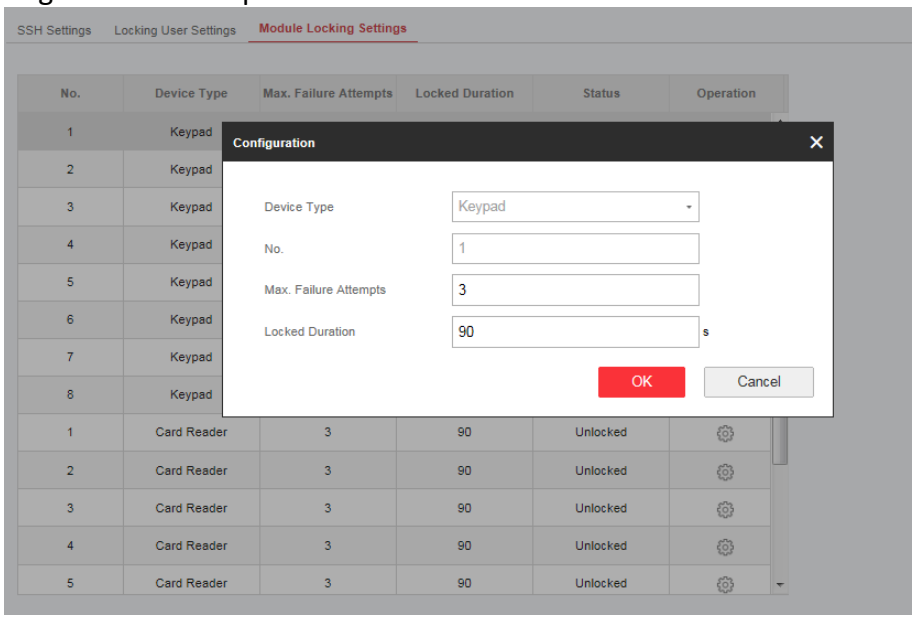
3. Klicken Sie auf um das Konto zu entsperren oder klicken Sie auf **Alle entsperren** um alle gesperrten Benutzer in der Liste zu entsperren.
4. Klicken Sie auf **Speichern**.

Einstellungen der Modulsperre

Legen Sie die Modulsperrparameter fest, einschließlich der maximalen Fehlerversuche und der Dauer der Sperre. Das Modul wird für die programmierte Zeitdauer gesperrt, sobald die Modulauthentifizierung für die Anzahl der Fehlversuche erreicht ist.

Vorgehensweise

1. Klicken Sie auf **System** → **System Sicherheit** → **Einstellungen für die Modulsperre**, um die Seite Einstellungen der Modulsperre aufzurufen.



2. Wählen Sie ein Modul aus der Liste aus und klicken Sie auf Symbol.
3. Stellen Sie die folgenden Parameter des ausgewählten Moduls ein.

Max. Anzahl Fehlerversuch

Wenn ein Benutzer kontinuierlich versucht, ein Passwort für mehr als die konfigurierten zulässigen Versuche zu authentifizieren, wird die Tastatur für die programmierte Dauer gesperrt.

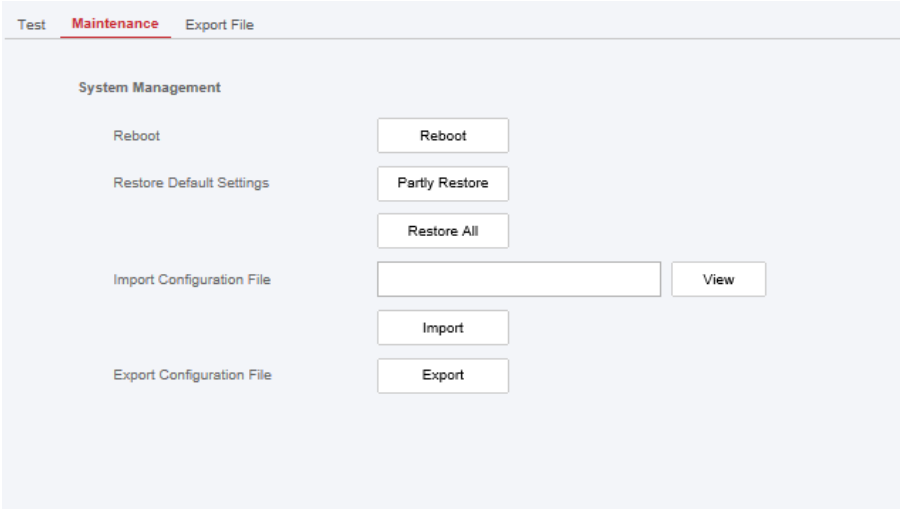
Sperrdauer

Stellen Sie die Sperrdauer der Bedienteile ein. Nach der konfigurierten Dauer werden die Bedienteile entsperrt.

4. Klicken Sie auf **Bestätigen**.
5. Optional: Klicken Sie auf die Schaltfläche **Sperren**, um das gesperrte Modul zu entsperren.

Systemwartung

Sie können das Gerät neu starten, die Standardeinstellungen wiederherstellen, die Konfigurationsdatei importieren/exportieren oder das Gerät remote aktualisieren.
Wählen Sie das Gerät aus und klicken Sie auf in der Client-Software oder geben Sie die IP-Adresse des Geräts in die Adressleiste des Webbrowsers ein. Klicken Sie auf **Projektverwaltung** →**Wartung**.



Neustarten

Klicken Sie auf **Neustarten**, um das Gerät neu zu starten.

Standardeinstellungen wiederherstellen

Klicken Sie auf **Teilweise Wiederherstellung**, um alle Parameter mit Ausnahme von Admin-Benutzerinformationen, drahtgebundenem Netzwerk, WLAN, Melderinformationen und Peripherieinformationen zurückzusetzen.
Klicken Sie auf **Alle wiederherstellen**, um alle Parameter auf die Werkseinstellungen zurückzusetzen.

Konfigurationsdatei importieren

Klicken Sie auf **Ansehen**, um die Konfigurationsdatei vom PC auszuwählen und klicken Sie auf **Konfigurationsdatei importieren**, um die Konfiguration in das Gerät zu importieren. Zum Importieren der Konfigurationsdatei muss das zum Zeitpunkt des Exports festgelegte Passwort eingegeben werden.

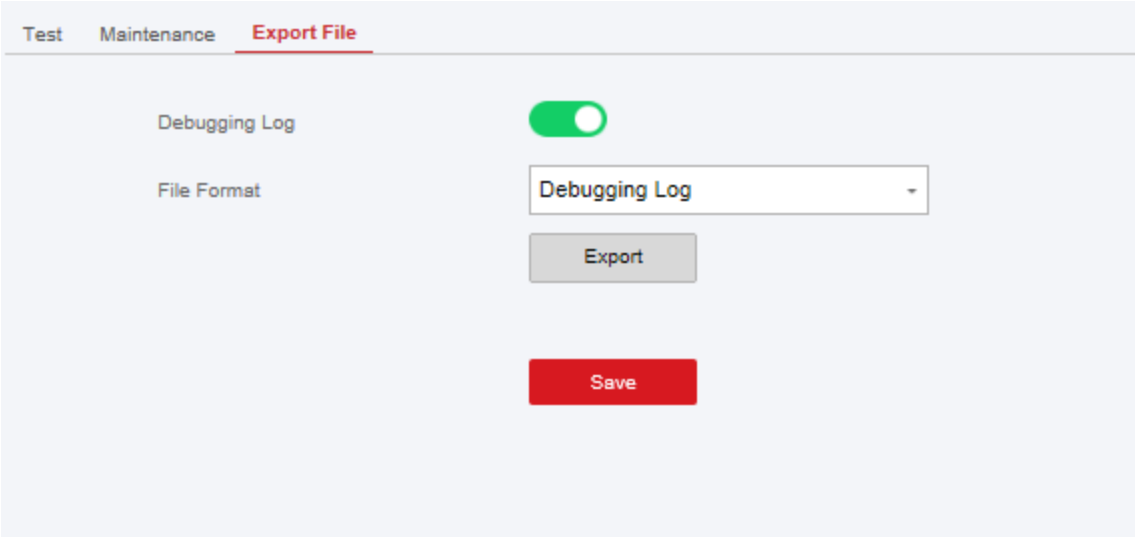
Konfigurationsdatei exportieren

Klicken Sie auf **Konfigurationsdatei exportieren**, um die Gerätekonfiguration auf den PC zu

exportieren. Für das Exportieren der Konfigurationsdatei muss ein Passwort für die Dateiverschlüsselung verwendet werden.

Datei exportieren

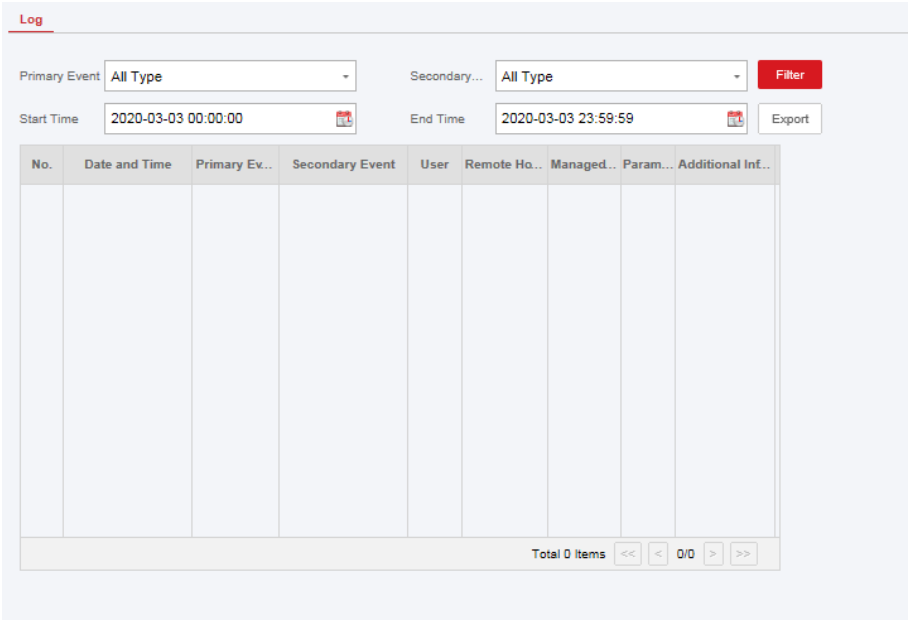
Klicken Sie auf **Projektverwaltung** → **Wartung** → **Datei exportieren**
Aktivieren Sie **Debug Protokoll**.



Der ausgewählte Dateityp muss exportiert werden.
Klicken Sie auf Exportieren, um die Datei zu exportieren.

Lokale Protokollsuche

Sie können das Protokoll auf dem Gerät durchsuchen.
Klicken Sie auf **Projektverwaltung** → **Protokoll**.



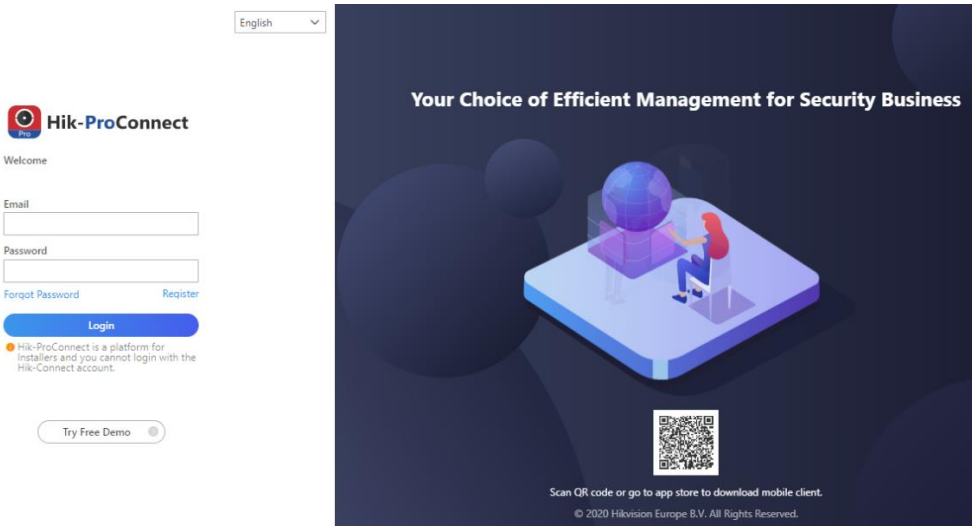
Wählen Sie einen Filter aus der Dropdown-Liste aus, legen Sie die Start- und Endzeit fest und klicken Sie auf **Filtern**. Alle gefilterten Protokollinformationen werden in der Liste angezeigt. Sie können auch auf **Zurücksetzen** klicken, um alle Suchbedingungen zurückzusetzen.

Geräte-Upgrade

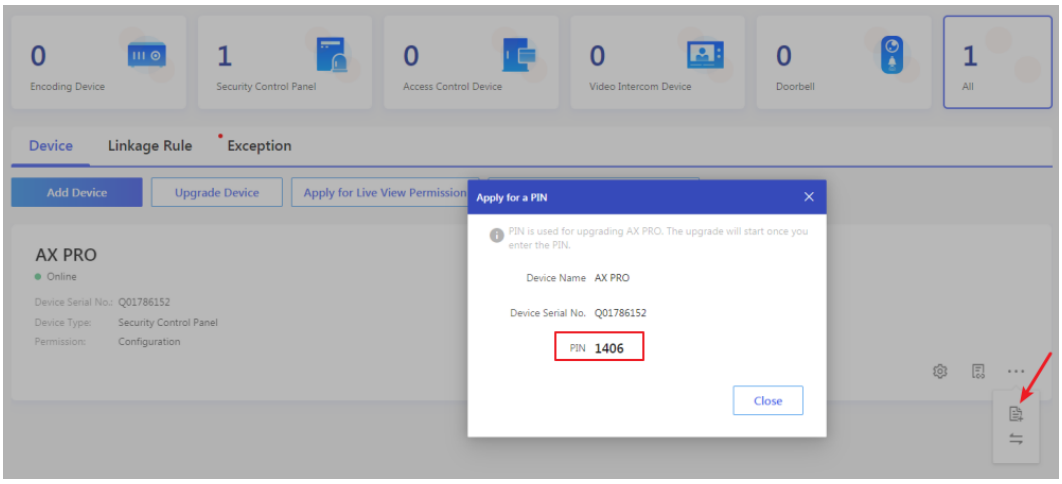
Hersteller-PIN abrufen

Zum Aktualisieren des Geräts wird eine Hersteller-PIN für die Authentifizierung benötigt. Die Hersteller-PIN kann nur vom Hik-ProConnect-Dienst abgerufen werden, was bedeutet, dass der Errichter, der vom Administrator auf Zugriffsebene 2 autorisiert wurde, den Zugriff auf Ebene 4 autorisiert hat. Die Hersteller-PIN kann ist nur einmal gültig.

- **PIN von Hik-ProConnect-Dienst abrufen**



Melden Sie sich mit dem Errichter-Konto an und rufen Sie die Seite des Geräts auf, das aktualisiert werden soll. Klicken Sie auf **Weiteres Menü** unten rechts auf der Seite und wenden Sie den PIN an.

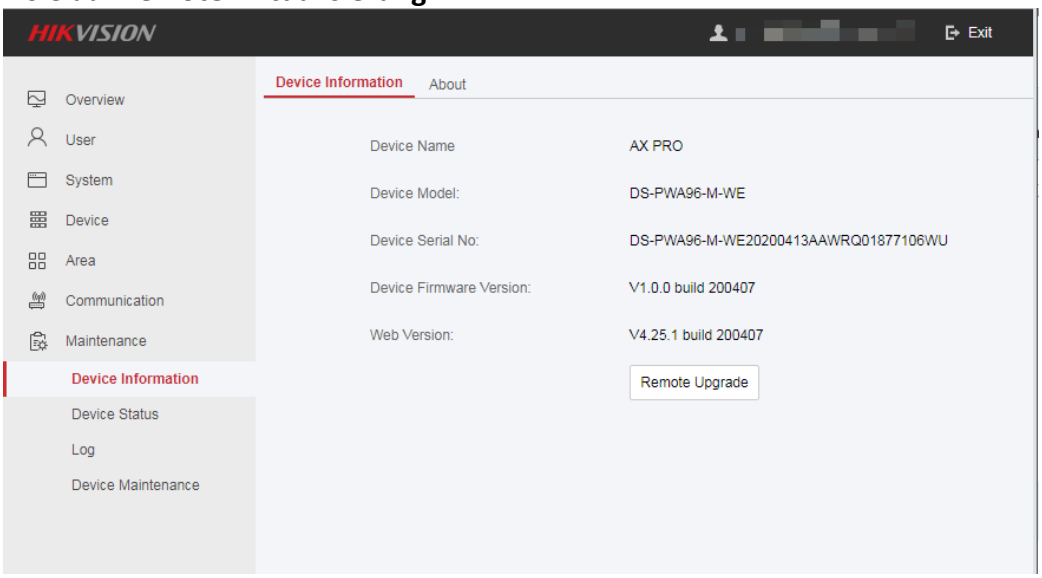


- **PIN vom technischen Support von HIKVISION erhalten**
  Es ist besser, den Remote-Desktop für den Zugriff auf den lokalen Web-Client der Systemsteuerung zu verwenden. Die PIN wird gemäß dem Standardverfahren des Technischen Support autorisiert.

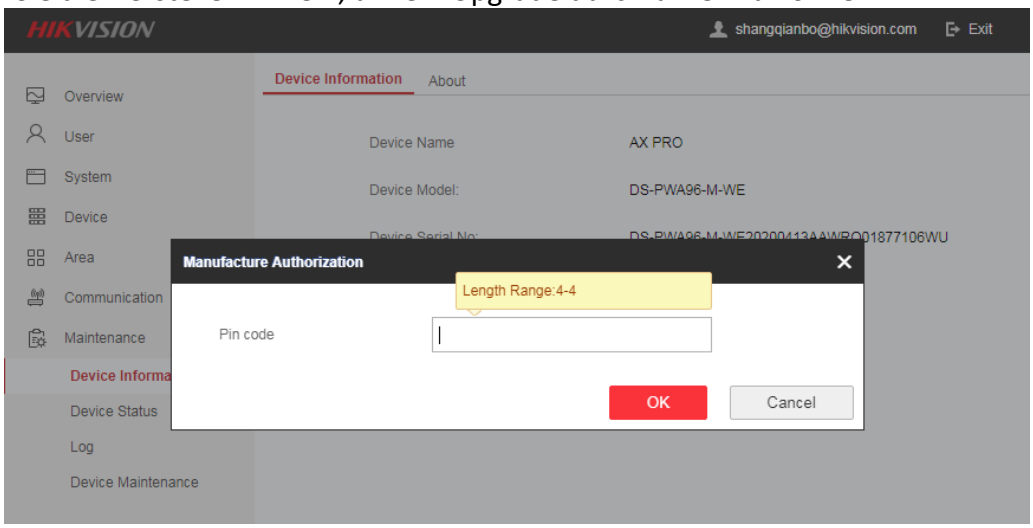
Firmware-Upgrade

Vorgehensweise:

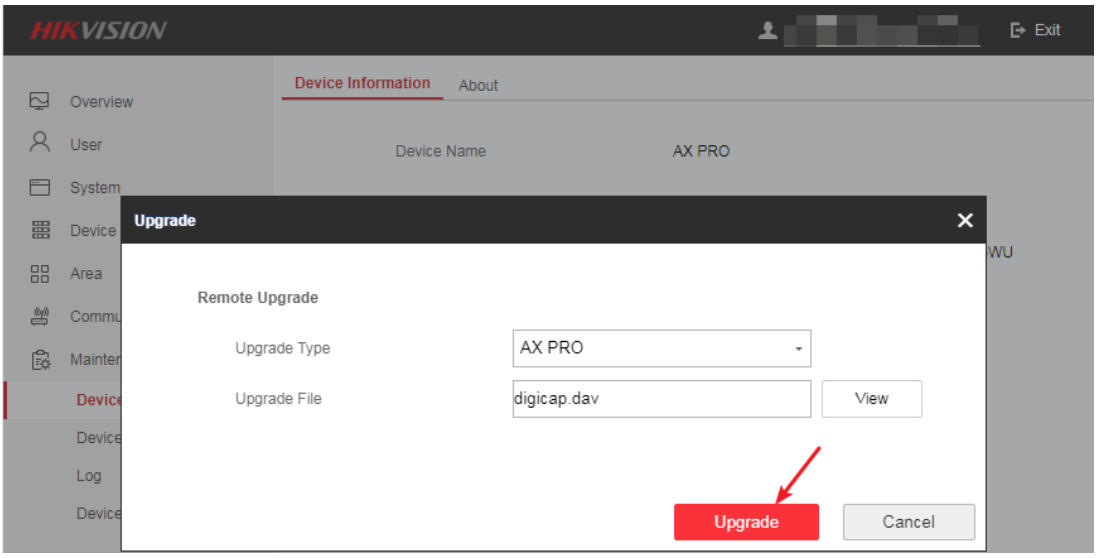
1. Klicken Sie auf **Wartung** → **Geräteinformationen**.
2. Klicken Sie auf **Remote-Aktualisierung**.



3. Geben Sie die Hersteller-PIN ein, um ein Upgrade durchführen zu können.



4. Klicken Sie auf **Ansehen**, um die Firmware-Datei mit dem Namen digicap.dav zu finden.
5. Klicken Sie auf **Upgrade**, um das Upgrade zu starten.



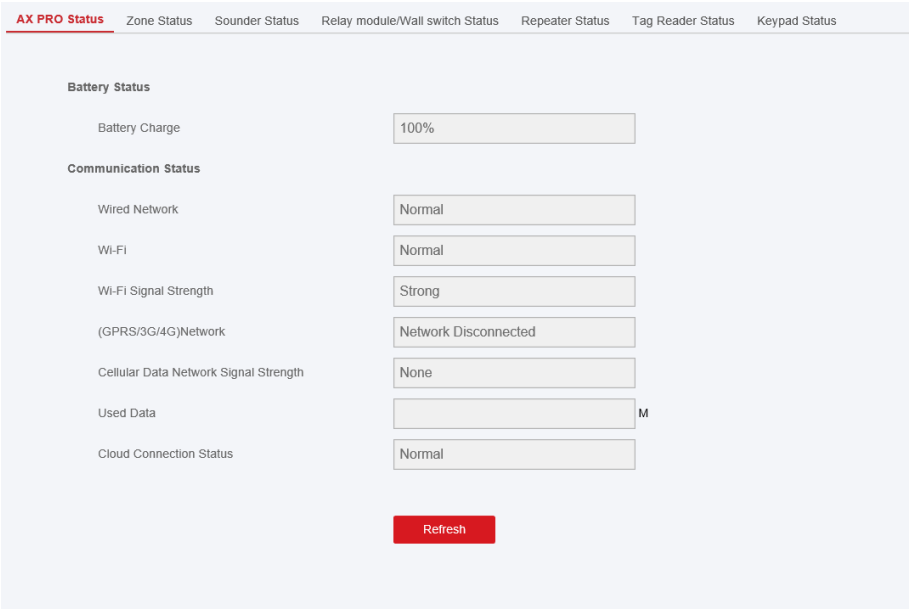
Hinweis

Sowohl die Benutzer- als auch die Konfigurationsinformationen werden nach Abschluss des Upgrades beibehalten.

4.3.8 Status Überprüfung

Nachdem Sie die Zone, den Repeater und andere Parameter eingestellt haben, können Sie deren Status einsehen.

Klicken Sie auf **Status**. Sie können den Status von Zone, Relais, Signalgeber, Tastatur, Lesegerät, Batterie und Kommunikation einsehen.



- Zone: Sie können den Zonenstatus, den Alarmstatus, die Melder-Batteriekapazität und die Signalstärke einsehen.
- Signalgeber: Sie können den Status des Signalgebers, den Batteriestatus und die Signalstärke

einsehen.

- Ausgang: Sie können Relaisstatus, Batteriestatus und Signalstärke einsehen.
- Bedienteil: Sie können den Bedienteilstatus, den Batteriestatus und die Signalstärke einsehen.
- Repeater: Sie können den Arbeitsstatus des Repeaters einsehen.
- Lesegerät: Sie können den Status des Lesegeräts, den Batteriestatus und die Signalstärke einsehen.

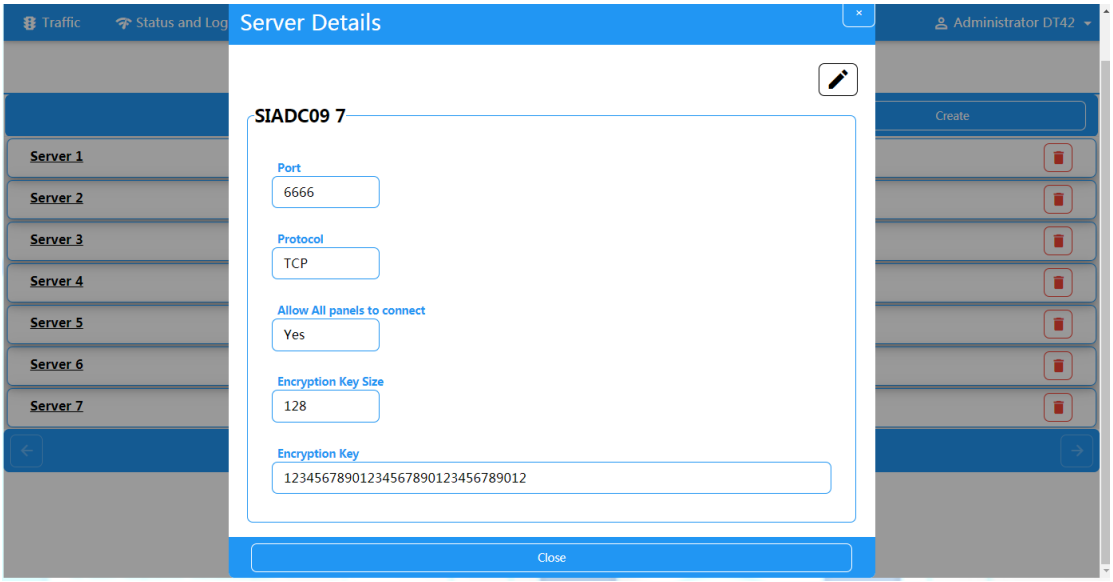
4.4 Meldung an Leitstelle

Das AX PRO Bedienteil ist mit einem eingebauten Sender-Empfänger, gemäß den Richtlinien EN 50131-10 und EN 50136-2, ausgestattet. Kategorie DP2 wird mit primärer Netzwerkschnittstelle von LAN/WLAN und sekundärer Netzwerkschnittstelle von GPRS oder 3G/4G LTE bereitgestellt. Das ATS (Alarmübertragungssystem) ist so konzipiert, dass es immer wenn verfügbar LAN/WLAN verwendet, um die mobile Datennutzung zu reduzieren. Die sekundäre Netzwerkschnittstelle bietet Stabilität und Zuverlässigkeit während eines Netzausfalls.

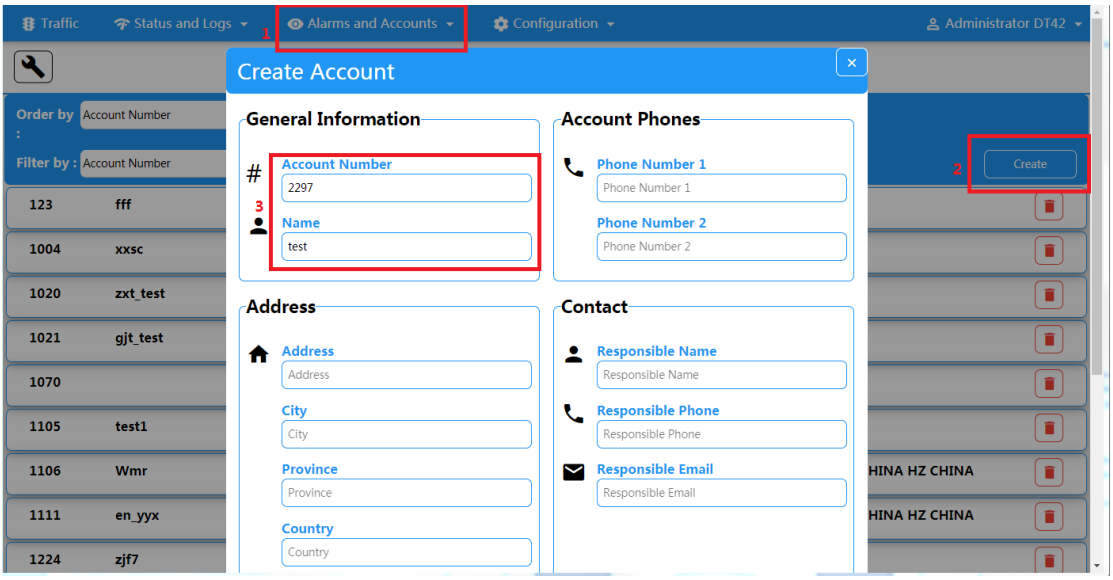
ATS in Empfänger-Leitstelle einrichten

Vorgehensweise:

1. Melden Sie sich beim WebClient der Leitstelle an.
2. Klicken Sie auf **Konfiguration** → **IP-Empfang** und erstellen Sie einen empfangenden Server, wie unten gezeigt.

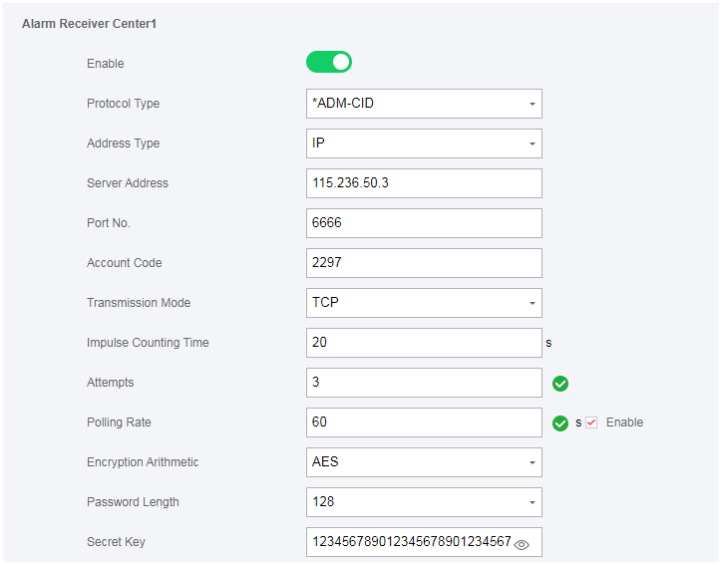


3. Klicken Sie auf **Alarme und Konten** → **Kontenverwaltung** und weisen ein Konto der Zentrale zu, wie unten gezeigt.



Einrichten von ATS im Transceiver der Zentrale
Vorgehensweise:

1. Melden Sie sich mit dem Errichter-Konto vom lokalen WebClient an.
2. Klicken Sie auf **Kommunikation** → **Leitstelle** und aktivieren **Leitstelle 1**.



- = Protokolleinstellung =

Protokolltyp

— ADM-CID
— SIA-DCS
— *ADM-CID
— *SIA-DCS

Wählen Sie das vom Empfänger in der Leitstelle unterstützte Token aus. Wählen Sie das Token mit der Markierung „* “, um die Kommunikationssicherheit zu verbessern.

- = Servereinstellung =

■ *Addresstyp* — IP-Adresse — Domänenname
■ *Serveradresse/Domänenname*
■ *Port* Geben Sie die IP-Adresse oder den Domänennamen der Leitstelle ein. Eingangs-Port des von der Leitstelle bereitgestellten Servers

- = Kontoeinstellung =

■ *Kontocode* Geben Sie das zugewiesene Konto ein, das von der Leitstelle bereitgestellt wurde.

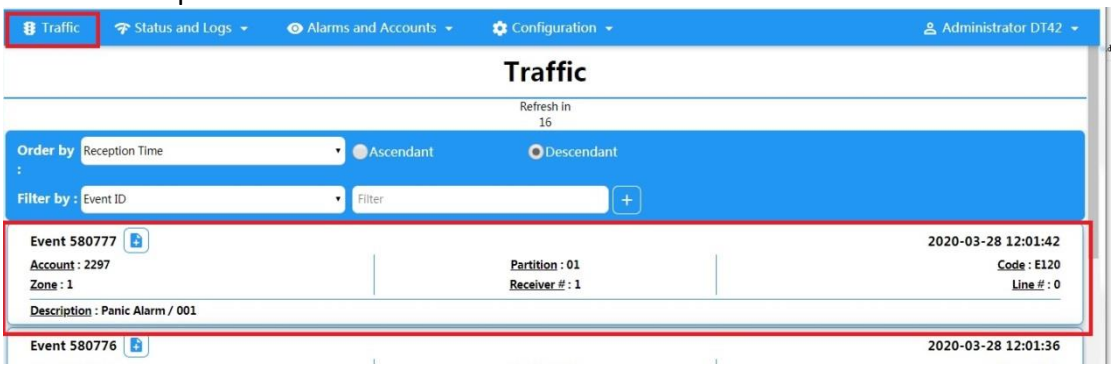
- = SIA DC-09 Protokolleinstellung =

■ Übertragungsmethode — TCP — UDP Für die Übertragung werden sowohl TCP als auch UDP unterstützt. UDP wird vom SIA DC-09 Standard empfohlen.
■ *Verbindungseinstellung* ○ *Impulszählzeit/Wiederholungs-Timeout-Zeit* Stellen Sie die Timeout-Periode ein, die auf die Antwort des Empfängers wartet. Eine erneute Übertragung wird veranlasst, wenn der Empfänger des empfangenden Zentrums eine Zeitüberschreitung hat. ○ *Versuche* Richten Sie die maximale Anzahl von Versuchen für die erneute Übertragung ein. ○ *Abfrage-Intervall* Legen Sie das Abfrage-Intervall zwischen 2 Live-Abfragen fest.
■ *Verschlüsselungseinstellung* ○ *Verschlüsselung arithmetisch* — AES ○ *Passwortlänge* — 128 — 192 — 256 ○ *Geheimer Schlüssel* Legen Sie die Länge des Verschlüsselungsschlüssels fest und geben Sie den von der Leitstelle bereitgestellten Schlüssel ein.

Alarmierungstest

Aktivieren Sie einen Überfallalarm am Bedienteil.

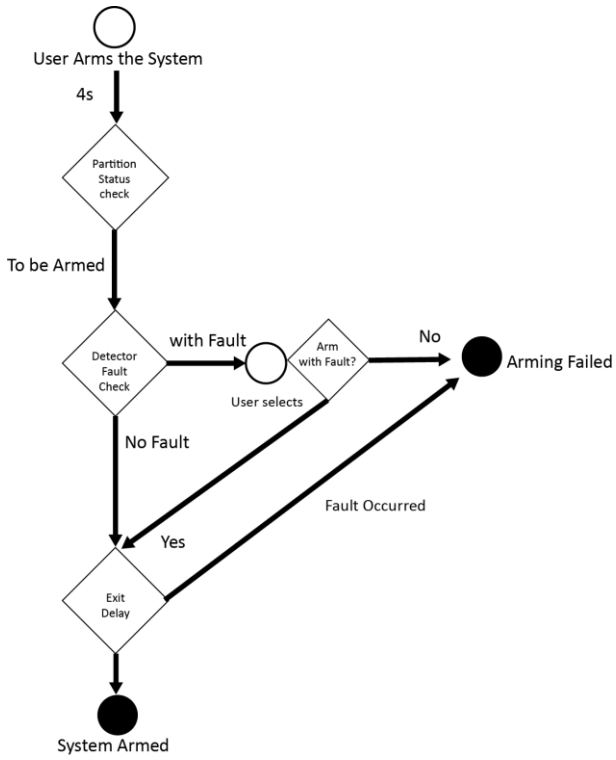
Melden Sie sich beim Empfänger an. Klicken Sie auf **Datenverkehr**, um alle empfangenen Nachrichten zu überprüfen.



Kapitel 5 Allgemeine Vorgänge

5.1 Scharfschalten

Sie können das Bedienteil, die Fernbedienung, den Transponder, die Client-Software und die App verwenden, um Ihr System scharf zu schalten.
Nachdem der Scharfschaltbefehl an AX PRO Zentrale gesendet wurde, prüft das System den Status der Melder. Wenn ein Melder fehlerhaft ist, müssen Sie wählen, ob das System mit Fehler scharfgeschalten werden soll.
Während das System scharfgeschalten wird, gibt die AX PRO Zentrale das Ergebnis innerhalb 5 Sekunden aus und speichert den Scharfschaltbericht.



Zugriffsebene der Scharfschaltung

Der Benutzer in Stufe 2 oder 3 hat die Berechtigung, das System scharf zu schalten oder teilweise scharf zu schalten.

Scharfschaltungsanzeige

Die Anzeige für das Scharf/Unscharfschalten wird 5 Sekunden lang durchgehend blau leuchten.

Grund für den Scharfschaltungsfehler

- Melder hat ausgelöst (außer Melder auf der Ausgangsroute).

- Überfallalarmgerät ausgelöst.
- Es ist ein Sabotagealarm aufgetreten.
- Kommunikationsfehler
- Fehler bei der Hauptstromversorgung
- Fehler Notstrombatterie
- Alarmempfangsfehler
- Fehler Signalgeber
- Niedriger Batteriestand Fernbedienung
- Sonstiges

Scharfschalten mit Fehler

Während die Scharfschaltung mit Fehler gestoppt wird, hat der Benutzer in Ebene 2 die Berechtigung, das System mit Fehler zu scharf zu schalten (Zwangs-Scharfschaltung).
Die Zwangs-Scharfschaltung wirkt sich nur auf den aktuellen Scharfschaltungsvorgang aus.
Die Zwangs-Scharfschaltung wird im Ereignisprotokoll aufgezeichnet.

5.2 Unscharfschalten

Sie können das System mit dem Bedienteil, Fernbedienung, Transponder, Client-Software oder App unscharfschalten.

Unscharfschalten Anzeige

Die Anzeige für das Scharf/Unscharfschalten blinkt 30 Sekunden, während der Benutzer das System über die Ein-/Ausgangsroute erfolgreich unscharf schaltet.
Das System meldet das Ergebnis der Unscharfschaltung nach Abschluss des Vorgangs.

Dauer Eingangsverzögerung

Stellen Sie sicher, dass der Timer nicht länger als 45 Sekunden eingestellt ist, um die Norm EN50131-1 zu erfüllen.

Frühalarm

Wenn entweder der Einbruchs- oder Sabotagealarm in einer Ein-/Ausgangsroute auftritt, während sich die AX PRO Zentrale im Status der Eingangsverzögerung befindet, wechselt die AX PRO Zentrale in den Frühalarmmodus.
Die Frühalarmdauer kann eingestellt werden (> 30 s).
Die AX PRO Zentrale meldet den Alarm nur dann, wenn das Alarmereignis über die Dauer des Frühalarms andauert, mit der zusätzlichen Eingangsverzögerung.

5.3 SMS

Sie können das Sicherheitssystem per SMS steuern, und der Befehl wird unten angezeigt.
SMS-Format für Scharfschaltung/Unscharfschaltung/Stummschalten des Alarms:

{Befehl} + {Bedientyp} + {Ziel}

Befehl: 2 Stellen, 00- Unscharfschalten, 01- Extern Scharfschalten, 02- Intern Scharfschalten, 03- Stummer Alarm
Bedientyp: 1- Bereich
Ziel: Nicht mehr als 3 Stellen, 0-Alle Bereiche, 1-Bereich 1(Zone1) - alle weiteren Bereiche und Zonen werden hochgezählt.

A. Fehlerbehebung

A.1 Kommunikationsfehler

A.1.1 IP-Konflikt

Fehlerbeschreibung:
Die IP-Adresse, die die Zentrale automatisch oder manuell eingestellt hat, ist die gleiche wie andere Geräte, was zu IP-Konflikten führt.
Lösung:
Suche nach IP-Adressen via Ping. Ändern Sie die IP-Adresse und melden Sie sich erneut an.

A.1.2 Webseite ist nicht zugänglich

Fehlerbeschreibung:
Verwenden Sie den Browser, um verfügbare und zugängliche Webseiten anzuzeigen.
Lösungen:
1. Prüfen Sie, ob das Netzwerkkabel lose ist und die Zentrale das einen Netzwerkfehler anzeigt.
2. Der Port der Zentrale wurde geändert. Bitte fügen Sie einen Port zur Webadresse hinzu, um weiter darauf zuzugreifen.

A.1.3 Hik-Connect ist offline

Fehlerbeschreibung:
Die Webseite zeigt, dass Hik-Connect offline ist.
Lösung:
Die Netzwerkkonfiguration der Zentrale ist fehlerhaft, es kann nicht von extern auf das Gerät zugegriffen werden.

A.1.4 Netzwerkkamera verliert Verbindung

Fehlerbeschreibung:
Das System meldet mehrere Ereignisprotokolle der IPC-Trennung und Verbindung.
Lösung:
Prüfen Sie, ob die Netzwerkkommunikation oder die Live-Ansicht der Kamera korrekt ist.

A.1.5 Fehler beim Hinzufügen des Geräts zur App

Fehlerbeschreibung:

Wenn Sie die App zum Hinzufügen von Geräten verwenden, wird die Meldung angezeigt, dass das Gerät nicht hinzugefügt werden konnte, das Gerät nicht gefunden wurde usw.
Lösung:
Überprüfen Sie die Webseite, ob Hik-Connect offline ist.

A.1.6 Alarminformationen werden nicht an die App/iVMS4200/Alarmzentrale gemeldet

Fehlerbeschreibung:
Nach Auslösung des Alarms erhält die Alarmzentrale der App/iVMS4200/ nicht die Alarmmeldung.
Lösung:
"Push-Benachrichtigung" - "Alarm und Sabotage Benachrichtigung" ist nicht aktiviert. Sie sollten „Alarm und Sabotage Benachrichtigung“ aktivieren.

A.2 Gemeinsamer Ausschluss von Funktionen

A.2.1 Einlernmodus kann nicht aufgerufen werden

Fehlerbeschreibung:
Klicken Sie auf die Funktionstaste der Zentrale und die Eingabeaufforderungstaste ist ungültig.
Lösung:
Die Zentrale befindet sich im "Hotspot"-Modus. Schalten Sie die Zentrale in den Stationsmodus und versuchen Sie dann erneut, in den Einlernmodus zu wechseln.

A.3 Zonen Fehler

A.3.1 Zone ist offline

Fehlerbeschreibung:
Status der Zonen anzeigen, die offline angezeigt werden.
Lösung:
Prüfen Sie, ob der Melder Unterspannung meldet. Ersetzen Sie die Batterie des Melders

A.3.2 Zonen Sabotagegesichert

Fehlerbeschreibung:
Status der Zonen anzeigen, die Sabotagegesichert sind.
Lösung:
Den Sabotagekontakt des Melders drücken.

A.3.3 Zone ausgelöst/Fehler

Fehlerbeschreibung:
Status der Zonen anzeigen, die ausgelöst/Fehler anzeigen.
Lösung:
Melder auf Werkseinstellungen setzen.

A.4 Probleme beim Scharfschalten

A.4.1 Fehler beim Scharfschalten (wenn die Scharfschaltung noch nicht gestartet wurde)

Fehlerbeschreibung:
Wenn die Zentrale scharfgeschalten wird, wird ein Fehler ausgegeben.
Lösung:
Das Zentrale aktiviert nicht die Zwangs-Scharfschaltung, und wenn ein Fehler in der Zone vorliegt, schlägt die Scharfschaltung fehl. Bitte schalten Sie die Aktivierung "Zwangs-Scharfschaltung" ein oder setzen Sie die Zone auf den normalen Status zurück.

A.5 Betriebsfehler

A.5.1 Fehler beim Aufrufen des Test-Modus

Fehlerbeschreibung:
Der Test-Modus konnte nicht aktiviert werden und es wird die Meldung „Ein Fehler in der Zone“ angezeigt.
Lösung:
Fehler in Zonenstatus, Alarmstatus oder Zonenleistung.

A.5.2 Der Vorgang Alarm löschen an der Zentrale erzeugt keinen Alarmlöschbericht

Fehlerbeschreibung:
Der Vorgang Alarm löschen an der Zentrale erzeugt keinen Alarmlöschbericht.
Lösung:
Wenn kein Alarm vorliegt, wird kein Bericht für Scharfschalten hochgeladen.

A.6 Fehler bei E-Mail-Zustellung

A.6.1 Fehler beim Senden der Test-E-Mail

Fehlerbeschreibung:
Wenn Sie die E-Mail-Parameter konfigurieren, klicken Sie auf „Inbox testen“ und der Aufforderungstest schlägt fehl.
Lösung:
Falsche Konfiguration der E-Mail-Parameter. Bearbeiten Sie die E-Mail-Parameter, wie in Tabelle 1/1 dargestellt.

A.6.2 Fehler beim Senden von E-Mails während der Verwendung

Fehlerbeschreibung:
Überprüfen Sie das Fehlerprotokoll der Zentrale. Es liegt ein „Fehler beim Senden der E-Mail“ vor.
Lösung:
Der Mailbox-Server hat eingeschränkten Zugriff. Melden Sie sich bei der Mailbox an, um zu sehen, ob die Mailbox gesperrt ist.

A.6.3 Fehler beim Senden von E-Mails an Gmail

Fehlerbeschreibung:
Die Mailbox des Empfängers ist Gmail. Klicken Sie auf „Test Inbox“ und Sie erhalten eine Fehlermeldung.
1. Google verhindert, dass Benutzer mit Apps/Geräten, die nicht ihren Sicherheitsstandards entsprechen, auf Gmail zugreifen.
Lösung:
Melden Sie sich auf folgende Website an (https://www.google.com/settings/security/lesssecureapps) und aktivieren Sie „Weniger sichere Apps zulassen. Das Gerät kann E-Mails ohne Fehler senden.
2. Gmail entfernt die CAPTCHA-Authentifizierung nicht.
Lösung: Klicken Sie auf den untenstehenden Link und dann auf „Weiter“ (https://accounts.google.com/b/0/displayunlockcaptcha).

A.6.4 Fehler beim Senden von E-Mails an QQ oder Fox Mail

Fehlerbeschreibung:
Die Mailbox des Empfängers ist QQ oder Fox Mail. Klicken Sie auf „Test Inbox“ und Sie erhalten eine Fehlermeldung.
1. Falsches QQ-Konto oder Passwort.
Lösung:
Das für die QQ-Kontoanmeldung erforderliche Passwort ist nicht das Passwort, das für die normale

Anmeldung verwendet wird. Der spezifische Pfad ist: E-Mail-Konto aufrufen → Gerät → Konto → ein Autorisierungscode generieren, und verwenden Sie den Autorisierungscode als Anmeldepasswort.
2. SMTP-Anmeldeberechtigung ist zum Öffnen erforderlich.

A.6.5 Fehler beim Senden von E-Mails an Yahoo

Fehlerbeschreibung:
Die Mailbox des Empfängers ist Yahoo. Klicken Sie auf „Test Inbox“ und Sie erhalten eine Fehlermeldung.
1. Die Sicherheitsstufe der Mailbox ist zu hoch.
Lösung:
Gehen Sie zu Ihrem E-Mail-Konto und aktivieren Sie „weniger sichere Anmeldung“.

A.6.6 E-Mail-Konfiguration

Tabelle A-1 E-Mail-Konfiguration

E-Mail-Typ	E-Mail Server	SMTP-Anschluss	Unterstützte Protokolle
Gmail	smtp.gmail.com	587	TLS/STARTTLS (TLS)
Outlook	smtp.office365.com	587	STARTTLS (TLS)
Hotmail	smtp.office365.com	587	STARTTLS (TLS)
QQ	smtp.qq.com	587	STARTTLS (TLSv1.2)
Yahoo	smtp.mail.yahoo.com	587	STARTTLS (TLSv1.2)
126	smtp.126.com	465	SSL/TLS
Sina	smtp.sina.com	25/465/587	SSL/TLS/STARTTLS (SSL/TLS)

Hinweis

Über E-Mail-Konfiguration:

- SMTP-Port Standardmäßig wird Port 25 ohne Verschlüsselung verwendet oder Port 465 verwendet, wenn SSL/TLS verwendet wird. Port 587 wird hauptsächlich für den STARTTLS-Protokollmodus verwendet.
  Der STARTTLS-Protokollmodus, der normalerweise bei der Auswahl von TLS verwendet wird.
- Benutzername von Outlook und Hotmail erfordern vollständige Namen und andere E-Mails erfordern ein Präfix vor @.

B. Eingabetypen

Tabelle B-1 Eingangstypen

Eingabetypen	Bedienung
Normal Alarm Zone	Das System gibt sofort einen Alarm aus, wenn es ein auslösendes Ereignis erkennt, nachdem das System Scharfgeschalten wurde. Akustisches Signal Auslösen des Systemtons und des Signaltons. Sprachausgabe: Alarm in Zone X.
Perimeter Zone	Das System gibt sofort einen Alarm aus, wenn es ein auslösendes Ereignis erkennt, nachdem das System Scharfgeschalten wurde. Akustische Rückmeldung: Systemton und -sirene auslösen. Es gibt ein konfigurierbares Intervall zwischen Alarm- und Signalgeberalarmierung, dass es Ihnen ermöglicht, den Alarm zu überprüfen und den Signalgeberalarmierung während des Intervalls abzubrechen. Sprachausgabe: Perimeteralarm in Zone X.
Verzögerte Zone	Das System gibt Ihnen Zeit, den Bereich ohne Alarm zu verlassen oder zu betreten. Akustische Rückmeldung: Systemton und -sirene auslösen. Sprachausgabe: Alarm in Zone X.
Folge Zone	Die Zone agiert als verzögerte Zone während der Eingangsverzögerung, ansonsten agiert diese als Normal Alarm Zone. Akustische Rückmeldung: Systemton und -sirene auslösen. Sprachausgabe: Folgealarm in Zone X.
24-Stunden-Stummschaltzone	Bei dieser Zone wird ein Alarm auftritt keine Sirene angesteuert. Akustische Rückmeldung: Kein Systemton (Sprachansage oder Tongeber).
Überfall Zone	Die Zone ist ständig aktiviert. Akustische Rückmeldung: Systemton und -sirene auslösen.

Eingabetypen	Bedienung
	Sprachausgabe: Überfallalarm in Zone X.
Feuer Zone	Diese Zone wird immer Sirenen aktivieren, wenn ein Alarm auftritt. Akustische Rückmeldung: Systemton und -sirene auslösen. Sprachausgabe: Feueralarm in Zone X.
Gas Zone	Diese Zone wird immer Sirenen aktivieren, wenn ein Alarm auftritt. Akustische Rückmeldung: Systemton und -sirene auslösen. Sprachausgabe: Gasalarm in Zone X.
Medizinische Zone	Die Zone wird immer mit einem Signalton aktiviert, wenn ein Alarm auftritt. Akustische Rückmeldung: Systemton und -sirene auslösen. Sprachausgabe: Medizinischer Alarm in Zone X.
Timeout Zone	Die Zone ist ständig aktiviert. Der Zonen Typ wird verwendet, um den Status „AKTIV“ einer Zone zu überwachen und zu melden, aber er meldet und alarmiert diesen Status nur, nachdem die programmierte Zeit abgelaufen ist (1 bis 599) Sekunden.
Deaktivierte Zone	Alarme werden nicht aktiviert, wenn die Zone ausgelöst oder sabotiert wurde. Akustische Rückmeldung: Kein Systemton (Sprachansage oder Tongeber).
Virtuelle Zone (Bedienteil/Fernbedienung)	Das System gibt sofort einen Alarm aus, wenn es ein auslösendes Ereignis erkennt, nachdem das System Scharfgeschalten wurde. Akustische Rückmeldung: Systemton und -sirene auslösen. Sprachausgabe: Signalton ertönt.
Sabotagealarm	Das System gibt sofort einen Alarm aus, wenn es ein auslösendes Ereignis erkennt, nachdem das System Scharfgeschalten wurde. Akustische Rückmeldung: Systemton und -sirene auslösen. Sprachausgabe: Sabotagealarm in Zone X.
Verknüpfung	Das verknüpfte Gerät auslösen, wenn ein Ereignis eintritt. z.B. Die Relais der Erweiterung werden aktiviert, wenn die AX

Eingabetypen	Bedienung
	PRO Zentrale scharfgeschalten wird.
Scharfschalten	Bei Scharfschaltung: Sprachausgabe bei Fehler. Sie können den Fehler entsprechend der Sprachausgabe behandeln. ● Systemton beim Scharfschalten mit Transponder oder Fernbedienung. ● Sprachausgabe bei Fehler. Sie können den Fehler entsprechend der Sprachausgabe behandeln.

Das Fehlerereignis wird auf dem Client angezeigt. Sie können den Fehler über die Client-Software oder der App beheben.

Sprachausgabe: Scharfschaltung fehlgeschlagen.

C. Ausgangstypen

Tabelle C-1 Ausgangstypen

Ausgangstypen	Aktiv	Wiederherstellen
Scharfschalten	AX PRO Zentrale Scharfschalten	Nach der konfigurierten Ausgangsverzögerung
Unscharfschalten	AX PRO Zentrale Unscharfschalten	Nach der konfigurierten Ausgangsverzögerung
Alarm	Wenn ein Alarmereignis auftritt. Der Alarmausgang wird nach der konfigurierten Ausgangs-/Eingangsverzögerung aktiviert.	Nach der konfigurierten Ausgangsverzögerung schalten Sie die Zentral unscharf oder löschen Sie den Alarm
Zonenverknüpfung	Wenn ein Alarmereignis auftritt, wird das verknüpfte Relais geschalten.	Nach der konfigurierten Ausgangsdauer
Manueller Betrieb	Relais manuell aktivieren	Auslösezeit überschritten oder Relais manuell deaktivieren

D. Ereignistypen

Tabelle D-1 Ereignistypen

Ereignistypen	Benutzerdefiniert	Standard 1 (Client-Software-Benachrichtigung)	Standard 2 (Alarm Leistelle 1/2)	Standard 3 (App)	Standard 4 (Telefon)
Alarm und Sabotage	×/√	√	√	√	√
Life Safety Ereignis	×/√	√	√	√	√
Systemstatus	×/√	√	×	×	×
Zentralen Verwaltung	×/√	√	×	×	×

E. Zugriffsebenen

Stufe	Beschreibung
1	Zugriff durch eine beliebige Person.
2	Benutzerzugriff durch einen Benutzer und Administrator.
3	Benutzerzugriff durch einen Errichter, z.B. ein Alarmunternehmensexperte.

Tabelle E-1 Berechtigung der Zugriffsebene

Funktion	Berechtigung		
	1	2	3
Scharfschalten	Nein	Ja	Ja
Unscharfschalten	Nein	Ja	Ja
Wiederherstellen/Löschen des Alarms	Nein	Ja	Ja
Gehtestmodus wird gestartet	Nein	Ja	Ja
Bypass(Zone)/Deaktivierung/Scharfschalten erzwungen	Nein	Ja	Ja
Hinzufügen/Ändern des Verifizierungscodes	Nein	Ja[d]	Ja[d]
Hinzufügen/Bearbeiten von Level-2 Benutzer- und Verifizierungscode	Nein	Ja	Ja
Hinzufügen/Bearbeiten von Konfigurationsdaten	Nein	Nein	Ja
Ersetzen von Software und Firmware	Nein	Nein	Nein

Hinweis

[a] Durch die Bedingung, vom Benutzer in Stufe 2 akkreditiert zu sein.

[b] Durch die Bedingung, vom Benutzer in Stufe 2 und 3 akkreditiert zu sein

[d] Benutzer können nur ihren eigenen Benutzercode bearbeiten.

- Benutzer der Stufe 2 können Anmeldeberechtigung für die Zentrale für Benutzerebene 3 auf der Einstellungsseite zuweisen.
- Die Benutzerebene 2 sollte dem Benutzerebene 3 Berechtigungen zuweisen, wenn der

Benutzerebene 3 sich anmelden möchte.

- Wenn die Zentrale Bypassed (umgangen) wird, kann die Benutzerebene 3 die Zentrale ohne die Berechtigungszuweisung der Benutzerebene 2 anmelden.
- Wenn die Zentrale Bypassed (umgangen) wird, kann die Benutzerebene 3 die Zentrale ohne die Berechtigungszuweisung der Benutzerebene 2 anmelden.
- Die Benutzerebene 4 kann sich nur in der Zentrale anmelden, wenn die Benutzerebene 2 oder 3 dem Benutzerebene 4 Berechtigungen zugewiesen hat.

F. Signalisierung

Erkennung von ATP/ATS-Fehlern

ATP (Alarmübertragungspfad) Fehler werden erkannt, wenn die Netzwerkschnittstelle der Zentrale getrennt wird oder der Übertragungspfad zum Sender-Empfänger des Empfangszentrums in der Leistelle irgendwo zwischen blockiert wird. Eine ATS (Alarmübertragungssystem) Fehler wird gemeldet, wenn ATP-Fehler auf beiden Übertragungspfaden erkannt werden.
Die ATP-Wiederherstellung wird erkannt, sobald die Netzwerkschnittstelle verbunden ist und der Übertragungspfad zum Transceiver des Empfangszentrums wiederhergestellt wurde. Die ATS-Wiederherstellung wird gemeldet, wenn die ATP-Wiederherstellung eines Übertragungspfads erkannt wird.

Die Detektionszeit von ATP-Fehlern und Wiederherstellungen wird in der folgenden Tabelle angezeigt.

	TN	Maximale Zeit der Detektion
Primärer ATP-Fehler/Wiederherstellung	LAN/WLAN	10 Minuten
Sekundärer ATP-Fehler/Wiederherstellung	GPRS	60 Minuten
	3G/4G LTE	20 Minuten (wenn primäres ATP fehlgeschlagen ist)

Die Signalisierung wird immer vom primären ATP übertragen, wenn er betriebsbereit ist. Andernfalls wird er automatisch auf den sekundären Übertragungspfad umgeschaltet, der momentan betriebsbereit ist. Sowohl primäre als auch sekundäre ATP-Fehler- und Wiederherstellungsereignisse werden an die Leitstelle gesendet, wenn ein ATP in Betrieb ist. Sie werden auch im obligatorischen Protokollspeicher mit einer Kapazität von 1.000 Datensätzen, die im nichtflüchtigen Flashspeicher zugeordnet sind, sowie im ATS-Fehlerprotokoll aufgezeichnet. Die Details der Berichte und Protokolldatensätze sind in der folgenden Tabelle aufgeführt.

	Ereigniscode bei Signalisierung	Beschreibung des Ereignisprotokolls
Primärer ATP-Fehler/Wiederherstellung	E351/R351	LAN-Pfad fehlgeschlagen/LAN-Pfad Wiederherstellung
Sekundärer ATP-Fehler/Wiederherstellung	E352/R352	Mobile Net Path fehlgeschlagen/Mobile Net Path Wiederherstellung
ATS Fehler/Wiederherstellung	-	ATS fehlgeschlagen
Fehler/Wiederherstellung der primären Netzwerkschnittstelle	E351/R351	LAN-Pfad fehlgeschlagen/LAN-Pfad Wiederherstellung
Fehler/Wiederherstellung der sekundären Netzwerkschnittstelle	E352/R352	Mobile Net Path fehlgeschlagen/Mobile Net Path Wiederherstellung

ATS-Kategorie

Die ATS-Kategorie von AXPRO ist DP2. Während die Alarmzentrale scharfgeschalten ist. Die Zentrale lädt den Alarmbericht über den Hauptpfad (LAN oder WLAN) oder den Backup-Pfad (3G/4G) in das Empfängerzentrum hoch. Wenn die Zentrale ordnungsgemäß mit dem LAN oder WLAN verbunden ist, wird der Hauptpfad als Übertragungspfad ausgewählt. Ist die Hauptpfadverbindung ausgefallen, wird der Pfad auf 3G/4G umgestellt. Und wenn die Verbindung

zum Hauptpfad wiederhergestellt wird, wird der Pfad wieder auf LAN/WLAN umgestellt. Die Zentrale prüft kontinuierlich den Verbindungsstatus und erzeugt Übertragungsfehler Protokolle für jeden der Pfade. Während beide Pfade ungültig sind, bestimmt die Zentrale den ATS-Fehler.

G. SIA- und CID-Code

Tabelle F-1 SIA und CID-Code

SIA Code	CID Code	Beschreibung
BA	E130	Einbruchalarm
BH	R130	Einbruchalarm wiederhergestellt
HA	E122	Stummer Überfallalarm
HH	R122	Stiller Notruf-Alarm wiederhergestellt
NA	E780	Timeout Alarm
BH	R780	Timeout Alarm wiederhergestellt
PA	E120	Überfallalarm
PH	R120	Überfallalarm wiederhergestellt
BA	E131	Perimeteralarm
BH	R131	Perimeteralarm wiederhergestellt
BA	E134	Eingang/Ausgang Alarm
BH	R134	Eingang/Ausgang Alarm wiederhergestellt
TA	E137	Sabotagealarm Gerät
TR	R137	Sabotagealarm Gerät wiederhergestellt
TA	E383	Sabotagealarm Melder
TR	R383	Sabotagealarm Melder wiederhergestellt
TA	E321	Sabotagealarm Funk Sirene
TR	R321	Sabotagealarm Funk Sirene wiederhergestellt
TA	E334	Sabotagealarm Funk Repeater

SIA Code	CID Code	Beschreibung
TR	R334	Sabotagealarm Funk Repeater wiederhergestellt
ES	E341	Sabotagealarm Erweiterung oder Funkkomponente
EJ	R341	Sabotagealarm Erweiterung oder Funkkomponente wiederhergestellt
PA	E120	Überfallalarm Fernbedienung
MA	E100	Medical Alarm
MH	R100	Medizinischer Alarm wiederhergestellt
GA	E151	Gasleckage Alarm
GH	R151	Gasleckage Alarm wiederhergestellt
FA	E110	Feueralarm
FH	R110	Feueralarm wiederhergestellt
OP	E401	Unscharfschalten
CL	R401	Extern Scharfschalten
OA	E403	Automatisches Unscharfschalten
CA	R403	Automatisches Scharfschalten
BC	E406	Alarm löschen
CL	R441	Intern Scharfschaltung
CD	E455	Automatisches Scharfschalten fehlgeschlagen
BB	E570	Zone Bypassed (umgangen)
BU	R570	Zonen Bypassed (umgangen) wiederhergestellt
CT	E452	Deadline Unscharfschalten
AT	E301	Stromausfall
AR	R301	Stromausfall wiederhergestellt

SIA Code	CID Code	Beschreibung
YT	E302	Niedriger Batteriestand Systembatterie
YR	R302	Niedrige Systembatterie wiederhergestellt
XT	E384	Niedriger Batteriestand Fernbedienung
XR	R384	Niedriger Batteriestand der Fernbedienung wiederhergestellt
YM	E311	Batteriefehler
YR	R311	Batteriefehler wiederhergestellt
DK	E501	Tastatur gesperrt
DO	R501	Tastatur entsperrt
TS	E607	Testmodus gestartet
TE	R607	Test Modus beendet
RN	E305	AX PRO zurücksetzen
UY	E321	Funk Sirene getrennt
UJ	R321	Funk Sirene verbunden
UY	E381	Funk Melder getrennt
UJ	R381	Funk Melder verbunden
XT	E384	Funkmelder niedrige Spannung
XR	R384	Funkmelder normale Spannung
ET	E333	Erweiterung oder Funkkomponente getrennt
ER	R333	Erweiterung oder Funkkomponente verbunden
UY	E334	Funk Repeater getrennt
UJ	R334	Funk Repeater verbunden
NT	E352	Mobilfunknetz getrennt

SIA Code	CID Code	Beschreibung
NR	R352	Mobilfunknetz verbunden
NT	E352	SIM-Karten Fehler
NR	R352	SIM-Karte wiederhergestellt
NT	E352	Netzwerkfluss überschritten
NT	E351	IP-Adressen Konflikt
NR	R351	IP-Adresse normal
NT	E351	Fehler drahtgebundenes Netzwerk
NR	R351	Drahtgebundenes Netzwerk normal
NT	E351	WLAN-Kommunikationsfehler
NR	R351	WLAN verbunden
XQ	E344	Fehler Funksignal
XH	R344	Funksignal normal
/	E306	Erweiterung gelöscht
/	R306	Erweiterung hinzugefügt
/	E306	Melder gelöscht
/	R306	Melder hinzugefügt
/	E306	Funk Repeater gelöscht
/	R306	Funk Repeater hinzugefügt
/	E306	Funk Signalgeber gelöscht
/	R306	Funk Signalgeber hinzugefügt
BA	E130	Einbruchalarm
BH	R130	Einbruchalarm wiederhergestellt
XT	E338	Niedriger Batteriestand Funkkomponente
XR	R338	Niedriger Batteriestand Funkkomponente wiederhergestellt
LB	E627	Programmiermodus gestartet

SIA Code	CID Code	Beschreibung
LX	E628	Programmiermodus beendet
CI	E454	Scharfschalten fehlgeschlagen
/	R250	Patrouille
/	E306	Funkkomponente gelöscht
/	R306	Funkkomponente hinzugefügt
XT	E384	Niedriger Batteriestand der Funk Sirene
XR	R384	Niedriger Batteriestand Funk Sirene wiederhergestellt
NT	E351	Kabelgebundenes Netzwerk/WLAN-ATP fehlgeschlagen
NR	R351	Drahtgebundenes Netzwerk/WLAN ATP wiederhergestellt
NT	E352	ATP des Mobilfunknetzes fehlgeschlagen
NR	R352	ATP des Mobilfunknetzes wiederhergestellt
CS	1409	Schlüsselzone unscharfgeschalten
OS	3409	Schlüsselzone scharfgeschalten