Alarm-Hub 2

Benutzerhandbuch

ZHEJIANG DAHUA VISION TECHNOLOGY CO.LTD. V1.1.0

Vorwort

Allgemein

Dieses Handbuch stellt die Installation, die Funktionen und den Betrieb des Alarm-Hubs 2 (im Folgenden als "Hub" bezeichnet) vor. Lesen Sie das Handbuch vor der Verwendung des Geräts sorgfältig durch und bewahren Sie es zum späteren Nachschlagen auf.

Sicherheitshinweise

Die folgenden Signalwörter können in der Anleitung vorkommen.

Signalwörter	Bedeutung
DANGER	Weist auf eine hohe potentielle Gefahr hin, die, wenn sie nicht vermieden wird, zum Tod oder zu schweren Verletzungen führen wird.
WARNING	Weist auf ein mittleres oder geringes Gefahrenpotenzial hin, das, wenn es nicht vermieden wird, zu leichten oder mittelschweren Verletzungen führen kann.
CAUTION	Weist auf ein potenzielles Risiko hin, das, wenn es nicht vermieden wird, zu Sachschäden, Datenverlust, Leistungseinbußen oder unvorhersehbaren Ergebnissen führen kann.
TIPS	Bietet Methoden, die Ihnen helfen, ein Problem zu lösen oder Zeit zu sparen.
NOTE	Bietet zusätzliche Informationen als Ergänzung zum Text.

Geschichte der Revision

Version	Revision Inhalt	Freigabezeit
V1.1.0	Überarbeitete Nabenkonfiguration.	April 2024
V1.0.0	Erste Veröffentlichung.	Dezember 2023

Hinweis zum Schutz der Privatsphäre

Als Nutzer des Geräts oder als für die Datenverarbeitung Verantwortlicher erheben Sie möglicherweise personenbezogene Daten anderer Personen, wie z. B. deren Gesicht, Ton, Fingerabdrücke und Nummernschild. Sie müssen die örtlichen Datenschutzgesetze und -vorschriften einhalten, um die legitimen Rechte und Interessen anderer Personen zu schützen, indem Sie Maßnahmen ergreifen, die unter anderem Folgendes umfassen Bereitstellung einer eindeutigen und sichtbaren Kennzeichnung, um Personen über die Existenz des Überwachungsbereichs zu informieren und die erforderlichen Kontaktinformationen bereitzustellen.

Über das Handbuch

- Das Handbuch dient nur als Referenz. Leichte Unterschiede zwischen dem Handbuch und dem Produkt sind möglich.
- Wir haften nicht für Schäden, die durch einen von der Anleitung abweichenden Betrieb des Produkts entstehen.
- Das Handbuch wird entsprechend den neuesten Gesetzen und Vorschriften der jeweiligen Länder aktualisiert. Ausführliche Informationen finden Sie im gedruckten Benutzerhandbuch, auf unserer CD-ROM, durch Scannen des QR-Codes oder auf unserer offiziellen Website. Das Handbuch ist nur als Referenz gedacht. Leichte Unterschiede zwischen der elektronischen Version und der Papierversion sind möglich.
- Alle Designs und Software können ohne vorherige schriftliche Ankündigung geändert werden. Bei Produktaktualisierungen kann es zu Unterschieden zwischen dem tatsächlichen Produkt und dem Handbuch kommen. Bitte wenden Sie sich an den Kundendienst, um das aktuelle Programm und die ergänzende Dokumentation zu erhalten.
- Es kann zu Druckfehlern oder Abweichungen bei der Beschreibung der Funktionen, der Bedienung und der technischen Daten kommen. Im Zweifelsfall behalten wir uns das Recht auf endgültige Klärung vor.
- Aktualisieren Sie die Reader-Software oder versuchen Sie es mit einer anderen gängigen Reader-Software, wenn das Handbuch (im PDF-Format) nicht geöffnet werden kann.
- Alle Marken, eingetragenen Marken und Firmennamen in diesem Handbuch sind Eigentum ihrer jeweiligen Inhaber.
- Bitte besuchen Sie unsere Website, wenden Sie sich an den Lieferanten oder den Kundendienst, wenn bei der Verwendung des Geräts Probleme auftreten.
- Bei Unklarheiten oder Meinungsverschiedenheiten behalten wir uns das Recht auf eine endgültige Erklärung vor.

Wichtige Sicherheitsvorkehrungen und Warnhinweise

In diesem Abschnitt werden Inhalte zum richtigen Umgang mit dem Gerät, zur Vermeidung von Gefahren und zur Vermeidung von Sachschäden vorgestellt. Lesen Sie diesen Abschnitt sorgfältig durch, bevor Sie das Gerät benutzen, und halten Sie sich bei der Verwendung des Geräts an diese Richtlinien.

Anforderungen an den Betrieb

- Vergewissern Sie sich vor dem Gebrauch, dass die Stromversorgung des Geräts einwandfrei funktioniert.
- Ziehen Sie das Netzkabel des Geräts nicht heraus, während es eingeschaltet ist.
- Verwenden Sie das Gerät nur innerhalb des Nennleistungsbereichs.
- Transportieren, verwenden und lagern Sie das Gerät unter den zulässigen Feuchtigkeits- und Temperaturbedingungen.
- Verhindern Sie, dass Flüssigkeiten auf das Gerät spritzen oder tropfen. Stellen Sie sicher, dass sich keine mit Flüssigkeit gefüllten Gegenstände auf dem Gerät befinden, damit keine Flüssigkeiten in das Gerät fließen.
- Nehmen Sie das Gerät nicht auseinander.

Anforderungen an die Installation

- Schließen Sie das Gerät vor dem Einschalten an den Adapter an.
- Halten Sie sich strikt an die örtlichen elektrischen Sicherheitsnormen und vergewissern Sie sich, dass die Spannung in der Umgebung konstant ist und den Leistungsanforderungen des Geräts entspricht.
- Schließen Sie das Gerät nicht an mehr als eine Stromversorgung an. Andernfalls könnte das Gerät beschädigt werden.

- Beachten Sie alle Sicherheitsmaßnahmen und tragen Sie die erforderliche Schutzausrüstung, die Ihnen bei Arbeiten in der Höhe zur Verfügung steht.
- Setzen Sie das Gerät nicht direktem Sonnenlicht oder Wärmequellen aus.
- Installieren Sie das Gerät nicht an feuchten, staubigen oder rauchigen Orten.
- Stellen Sie das Gerät an einem gut belüfteten Ort auf, und blockieren Sie nicht die Belüftung des Geräts.

- Verwenden Sie das vom Hersteller des Geräts bereitgestellte Netzteil oder das Netzteil des Gehäuses.
- Die Stromversorgung muss den Anforderungen von ES1 in der Norm IEC 62368-1 entsprechen und darf nicht höher als PS2 sein. Beachten Sie, dass die Anforderungen an die Stromversorgung von der Gerätekennzeichnung abhängen.
- Schließen Sie elektrische Geräte der Klasse I an eine Steckdose mit Schutzerdung an.

Inhaltsübersicht

1 Einleitung

1.1 Überblick

Der Alarm-Hub ist ein zentrales Gerät im Sicherheitssystem, das den Betrieb aller angeschlossenen Peripheriegeräte steuert. Wenn das Sicherheitssystem die Anwesenheit, das Eindringen oder den Versuch des Eindringens eines Eindringlings in den bewachten Bereich feststellt, empfängt der Hub die Alarmsignale von den Meldern und alarmiert dann die Benutzer.

1.2 Technische Daten

Dieser Abschnitt enthält die technischen Daten des Geräts. Bitte beachten Sie die Angaben, die Ihrem Modell entsprechen.

Tabelle 1-1 Technische Daten

Typ	Parameter	Beschreibung
Hafen	Drahtlose Zone	150 Kanäle drahtlose Peripheriegeräte (6 Sirenen, 64 PIR-Kameras, 64 Schlüsselanhänger, 8 Tastaturen und 4 Repeater)
	Netzwerk-Modus	Europa: Unterstützt die Installation von zwei SIM-Karten. Es kann jeweils nur eine Karte aktiviert werden. Außerdem werden mehrere Frequenzbänder für die SIM-Karten unterstützt (GSM: 900/1, 800 MHz, WCDMA: B1/B5/B8, LTE-FDD: B1/B3/B5/B7/B8/B20/B28A, LTE-TDD:B38/B40/B41). USA: Unterstützt die Installation von Dual-SIM-Karten. Es kann jeweils nur eine Karte aktiviert werden. Außerdem werden mehrere Frequenzbänder für die SIM-Karten unterstützt (GSM: 850/900/1800/1900 MHz, WCDMA:B1/B2/B4/B5/B8, LTE-FDD:B1/B2/B3/B4/B5/B7/B8/B28, LTE-TDD: B40) Nur bei 4G-Modellen verfügbar.
	Netzwerkanschluss	1 RJ-45, 10 Mbps/100 Mbps Ethernet-Anschluss.
	Akku	Eine eingebaute wiederaufladbare 4.750-mah-Lithium-Batterie.

Typ	Parameter	Beschreibung
Audio und Video	Video-Eingang	8-Kanal-IPC, der nur das Hochladen von Alarmvideos unterstützt.
	Audio-Ausgang	1 Kanal
	Lautstärkeregelung	Ja
	Sprachübertragung	• 4G: Telefon und lokaler Lautsprecher • Wi-Fi: Lokaler Lautsprecher
Funktion	Anzeigelampe	Die Anzeige zeigt den Status der Alarme, der Scharf- und Unscharfschaltung, der Netzwerkverbindung und des Geräteausfalls an.
	Schaltfläche	Enthält eine Reset-Taste, eine Spannungstaste und eine AP-Schalttaste.
	SMS	Ja (bis zu 5 Rufnummern) Nur bei 4G-Modellen verfügbar.
	Telefonanruf	Ja (bis zu 5 Rufnummern) Nur bei 4G-Modellen verfügbar.
	Video-Verknüpfung	Ja
	Offline-Cache	Speichert bis zu 50 Alarmmeldungen.
	Methode zum Scharfmachen und Entschärfen	App, Tastatur, Fernbedienung, Karte, geplante Scharf- und Unscharfschaltung.
	Fernaktualisierung	Cloud-Update
	Erkennung von niedrigem Batteriestand	Ja
	Benutzerverwaltung	Die Funktionen können von den App-Benutzern gemeinsam genutzt werden. Dazu gehören 33 App-Benutzer (31 allgemeine Benutzer, 1 Admin-Benutzer und 1 Installateur) und 32 Keypad-Benutzer
	Stromausfallsicherung für konfigurierte Parameter	Ja
	Protokolle	Bis zu 5.000 Einträge

Typ	Parameter	Beschreibung	
	Übertragungsprotokoll	SIA, SoftGuard	
RF	Trägerfrequenz	DHI-ARC3800H-FW2(868)/DHI-ARC3800H-FW2: 868,0 MHz-868,6 MHz	DHI-ARC3800H-FW2/DHI-ARC3800H-W2: 433,1 MHz-434,6 MHz
	Leistung des Senders (EIRP)	DHI-ARC3800H-FW2(868)/DHI-ARC3800H-FW2: Grenzwert 25 mW	DHI-ARC3800H-FW2/DHI-ARC3800H-W2: Grenzwert 10 mW
	Mechanismus der Kommunikation	Zwei-Wege	
	Kommunikation Abstand	DHI-ARC3800H-FW2(868)/DHI-ARC3800H-FW2: Bis zu 2.000 m (6.561,68 ft) in einem offenen Raum.	DHI-ARC3800H-FW2/DHI-ARC3800H-W2: Bis zu 1.200 m (3.937,01 ft) in einem offenen Raum
	Verschlüsselungsmodus	AES128	
	Frequenzsprungverfahren	Ja	
	Wi-Fi	2.4 G	
Grundlegend	Sprache	• 4G-Modelle: Es werden bis zu 7 Sprachen für SMS unterstützt: Englisch, Spanisch (Lateinamerika), Französisch, Italienisch, Arabisch, Türkisch und Dänisch. Standardmäßig ist sie auf Englisch eingestellt. Die Alarm-Sprachnachrichtenfunktion und der lokale Lautsprecher unterstützen nur Englisch. • Wi-Fi-Modelle: Englisch	
	Stromversorgung	100-240 VAC, 50/60 Hz	
	Standby-Zeit	Der Akku hält bis zu 12 Stunden, wenn er vollständig aufgeladen ist und die folgenden Bedingungen erfüllt sind: Es ist mit dem Wi-Fi verbunden, seine ID ist mit der Alarmempfangszentrale verbunden, das Herzschlagintervall beträgt 1.800 Sekunden, und es ist mit 8 Peripheriegeräten und der Cloud verbunden.	
	Stromverbrauch	≤12 W	

Typ	Parameter	Beschreibung
	Betriebstemperatur	Wenn der Akku nicht geladen wird: -10 °C bis +55 °C (+14 °F bis +131 °F) Wenn der Akku geladen wird: 0 °C bis +45 °C (+32°F bis +113 °F)
	Luftfeuchtigkeit im Betrieb	10%-90% (RH)
	Produkt Abmessungen	174,8 mm × 174,8 mm × 38,3 mm (6,88" × 6,88" × 1,51") (L × B × H)
	Nettogewicht	510 g (1,12 lb)
	Bruttogewicht	860 g (1,90 lb)
	Einrichtung	Unterstützt die Wand- und Tischmontage.
	Material des Gehäuses	PC + ABS
	Zertifizierungen	CE
	Korrosionsschutz Level	Grundlegender Schutz
	Lagertemperatur	-10 °C bis +55 °C (+14 °F bis +131 °F)
	Luftfeuchtigkeit bei Lagerung	10%-90% (RH)
	Verpackung Abmessungen	254 mm × 211 mm × 61 mm (10.00" × 8.31" × 2.40") (L × B × H), freistehend im Innenkarton 524 mm × 508 mm × 442 mm (20,63" × 20,00" × 17,40") (L × B × H), Schutzhülle
Stromversorgung	PS-Typ	Typ A
	Hauptstrom	100-240 VAC, 0,4A
	Batteriekapazität	3,7 V/4750 mAh
	Batterie Standby	bis zu 12 Stunden Wenn die folgenden Bedingungen erfüllt sind, kann die Standby-Zeit bis zu 12 Stunden betragen: • Verbindet sich mit Wi-Fi, GPRS/3G/4G. • Stellt eine Verbindung zu ARC her und das Heartbeat-Intervall beträgt 1800 Sekunden. • Zum Anschluss von 8 Eingängen und 1 Sirene. • Verbindet sich mit der Cloud.
	Akku-Typ	Akku-Typ: Eingebauter wiederaufladbarer Lithium-Ionen-Polymer-Akku; Batteriemodell: 01DQ0023-69

Typ	Parameter	Beschreibung
	Max. verfügbarer Strom	1.3 A
	Stromverbrauch	Max. 12 W
	Stromverbrauch	Normal: 370 mA; Alarm: 440 mA
	Schwellenwert für niedrigen Batteriestand	3.675 VDC
	Schwellenwert für die Wiederherstellung der Batterie	3.675 VDC
	Spannung freigeben	< 3 V
	Akku-Ladezeit	80% ca. 11 Std.
ARC-Signalisierung	ATS-Kategorie	DP2/SP2 (LAN/Wi-Fi und GPRS/4G)
	Quittierungsvorgang	Durchgehen
	Protokolle	SIA-DC09
	Primärer Übertragungsweg	LAN /Wi-Fi (NO 50136-2)
	Sekundärer Übertragungsweg	GPRS/4G
	Ausrüstung für die Notifizierung	C/E/F

Tabelle 1-2 ATE-Kategorie

ATE-Kategorie	Meldezeit	Protokolle	Kommunikationsgeräte			Zu verwendendes Kommunikationsgerät
			PSTN	2G/3G	IP	
SP2	25 h	Standard	√			Das angekreuzte Kommunikationsgerät
SP3	30 min	Standard		√	√	Nur eines der beiden angekreuzten Kommunikationsgeräte

ATE-Kategorie	Meldezeit	Protokolle	Kommunikationsgeräte			Zu verwendendes Kommunikationsgerät
			PSTN	2G/3G	IP	
SP4	3 min	Verschlüsselt		√	√	Nur eines der beiden angekreuzten Kommunikationsgeräte
SP5	90 s	Verschlüsselt		√	√	Nur eines der beiden angekreuzten Kommunikationsgeräte
DP1	25 h	Standard	√	√	√	Nur zwei der drei angekreuzten Kommunikationsgeräte
DP2	30 min	Standard	√	√	√	Nur zwei der drei angekreuzten Kommunikationsgeräte
DP3	3 min	Verschlüsselt		√	√	Die beiden angekreuzten Kommunikationsgeräte
DP4	90 s	Verschlüsselt		√	√	Die beiden angekreuzten Kommunikationsgeräte

ATE-Kategorie	Meldezeit	Protokolle	Kommunikationsgeräte			Zu verwendendes Kommunikationsgerät
			PSTN	2G/3G	IP	

ATE: Al-Arm-Übertragungsgerät.

SPx (Single Path): Ein Wert, der den von einem einzelnen Kommunikationsgerät erreichten Leistungsgrad gemäß der Norm EN 50136-1 angibt.

DPx (Double Path): Ein Wert, der den Leistungsgrad angibt, der durch eine Kombination von zwei Kommunikationsgeräten gemäß der Norm EN 50136-1 erreicht wird.

Meldezeit: Die Meldezeit wird auf der Grundlage des Standards der jeweiligen Leistungsstufe vorgeschrieben. Die Meldezeit ist die maximal verfügbare Zeit für die Meldung, wenn eine Alarmübertragungseinrichtung ausfällt. Alarmübertragungseinrichtungen erfüllen diese Anforderung, indem sie ihren Status regelmäßig durch eine spezifische symbolische Testfunktion melden.

Protokolle: Gibt die Sicherheitsstufe der Protokolle an, die für die Meldung von Störungen verwendet werden sollen. Standardprotokolle und Sprachprotokolle sind verschlüsselt. Hochsichere Protokolle werden mit einem AES 128-Bit- oder AES 256-Bit-Schlüssel verschlüsselt.

Kommunikationsgeräte: Implementierte Kommunikationsgeräte.

Zu verwendende Kommunikationsgeräte: Gibt die Anzahl und die Art der Kommunikationsgeräte an, die je nach ATE-Kategorie verwendet werden sollen.

1.3 Checkliste

Überprüfen Sie das Paket anhand der folgenden Liste. Wenn einer der Artikel beschädigt ist oder fehlt, wenden Sie sich an den Kundendienst.

Abbildung 1-1 Checkliste

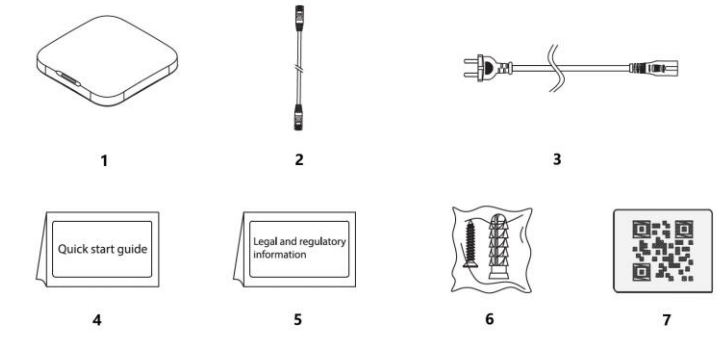


Tabelle 1-3 Checkliste

Nein.	Artikel Name	Menge	Nein.	Artikel Name	Menge
1	Alarm-Hub 2	1	5	Rechtliche und regulatorische Informationen	1
2	Kabel	1	6	Paket mit Schrauben	2
3	Adapter	1	7	QR-Code	1
4	Schnellstart-Anleitung	1	-	-	-

2 Entwurf

2.1 Erscheinungsbild

Abbildung 2-1 Erscheinungsbild

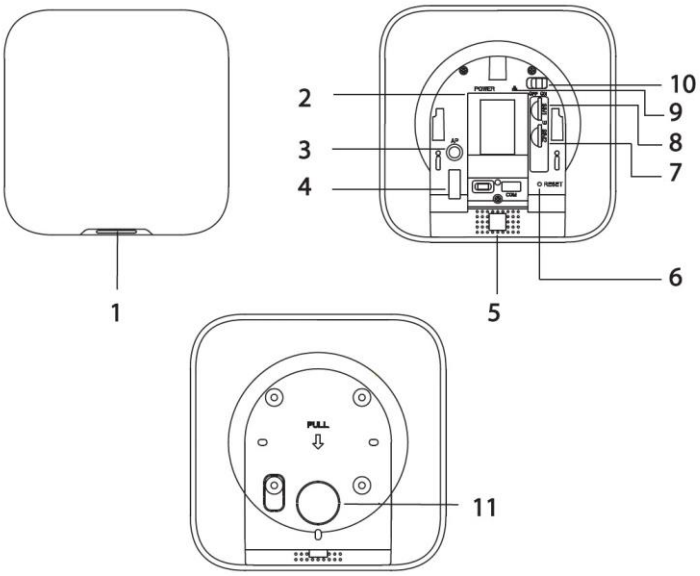


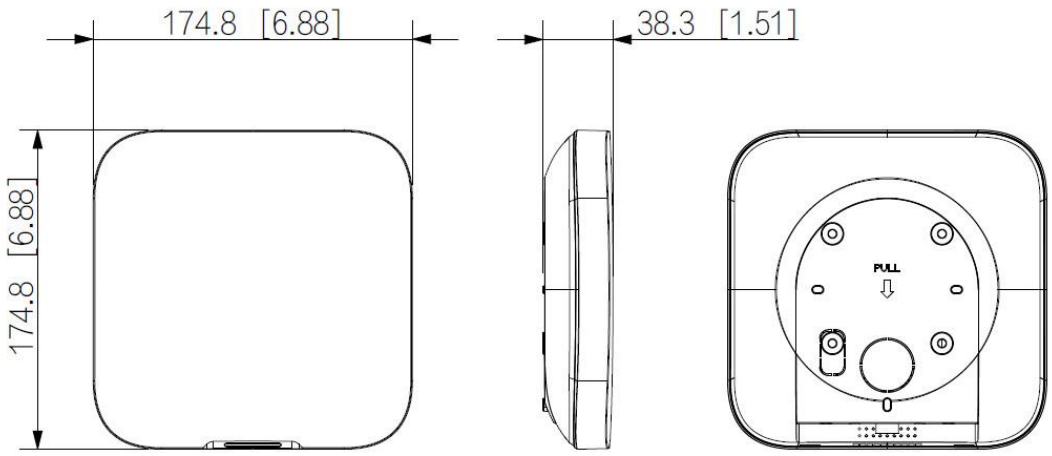
Tabelle 2-1 Aufbau

Nein.	Name	Beschreibung
1	Indikator	• Blinkt langsam grün: Modus mit reduzierter Empfindlichkeit. • Blinkt grün: Der Hub beginnt zu arbeiten. • Durchgehend gelb: Die Verbindung zur Cloud konnte nicht hergestellt werden. • Dauerhaft grün: Entschärfungsmodus. • Durchgehend blau: Aktivierungsmodus. • Blinkt rot: Alarmereignis wurde ausgelöst. • Blinkt gelb: Es wurde eine Fehlfunktion erkannt. • Blinkt blau: AP-Konfiguration läuft oder der Hub wird mit Peripheriegeräten gekoppelt. • Blinkt schnell blau: Kartenausgabemodus.
2	Stromanschluss	An das Stromnetz anschließen.

Nein.	Name	Beschreibung
3	AP-Taste	Halten Sie die Taste 2 Sekunden lang gedrückt, um die AP-Funktion einzuschalten. Das Telefon verbindet sich dann über den Hub mit dem Hotspot und synchronisiert Wi-Fi-Benutzername und Passwort mit dem Hub. Sie können den AP auch ausschalten, indem Sie die Taste 2 Sekunden lang gedrückt halten, wenn der AP aktiviert ist.
4	Sabotageschalter	Wenn der Sabotageschalter losgelassen wird, wird der Sabotagealarm ausgelöst.
5	Sprecher	Erzeugen Sie Ton.
6	Reset-Taste	Halten Sie die Taste 10 Sekunden lang gedrückt, um den Hub neu zu starten und die Werkseinstellungen wiederherzustellen.
7	Steckplatz für SIM 2	Setzen Sie die Hauptkarte in den ersten Steckplatz und die Standby-Karte in den zweiten Steckplatz ein. • Unterstützt Dual-SIM-Karten und Single-Standby. • SIM-Karten ermöglichen dem Hub die Nutzung von Mobilfunkdaten und Push-Alarmbenachrichtigungen. 📖 • Die SIM-Karten funktionieren erst, wenn die Netzkonfiguration abgeschlossen ist. • Die SIM-Funktion ist nur bei bestimmten Modellen verfügbar.
8	Steckplatz für SIM 1	
9	Buchse für Ethernet-Kabel	Verbinden Sie den Hub mit dem Ethernet.
10	Netzschalter	Schalten Sie den Hub ein oder aus.
11	Umschlagrückseite	Wenn die hintere Abdeckung geöffnet wird, wird der Manipulationsalarm ausgelöst.

2.2 Abmessungen

Abbildung 2-2 Abmessungen (Einheit: mm[Zoll])



3 Inbetriebnahme

3.1 Benutzer

Benutzer können nur in der DMSS-App angelegt werden. Ordnen Sie die Benutzer in verschiedene Rollen ein, so dass sie unterschiedliche Zugriffsebenen für die Bedienung der Geräte haben können.

Benutzer-Zugangsstufe

Tabelle 3-1 Benutzerzugriffsebene

Benutzer	Zugangsebene
DMSS-Admin-Benutzer	L2
DMSS allgemeiner Benutzer	L2
Installateur	L3

- Installateur: Installateure bieten Endbenutzern Betriebs- und Wartungsdienste an. Diese Rolle muss beim Endbenutzer (DMSS-Admin-Benutzer) die Berechtigungen für den Betrieb des Geräts beantragen. Sie können Berechtigungen wie Gerätekonfiguration und Benutzerverwaltung erhalten.
- DMSS-Administrator-Benutzer: Der Administrator-Benutzer ist ein Endbenutzer. Diese Rolle kann nicht geändert werden und verfügt über Berechtigungen, wie z. B. Gerätekonfiguration und Benutzerverwaltung. Der DMSS-Admin-Benutzer hat nicht die Berechtigung, das Gerät zu konfigurieren, wenn Installateure ihm den Hub ausleihen oder wenn sie den Hub dem Installateur anvertrauen.
- DMSS allgemeiner Benutzer: Dies sind Benutzer, für die ein DMSS-Admin-Benutzer Geräte über die DMSS-App freigibt. Diese Rolle kann geändert werden und verfügt nur über grundlegende Berechtigungen, wie das Anzeigen des Gerätestatus und das Scharf- und Unscharfschalten von Räumen.

Geschäftsablauf

Nachfolgend finden Sie den Prozess für die Freigabe und das Teilen von Geräten in der DMSS-App. Installateure und Endbenutzer können den Prozess zur Freigabe und Betrauung von Geräten befolgen.

Abbildung 3-1 Geschäftsablauf (DMSS-Benutzer)

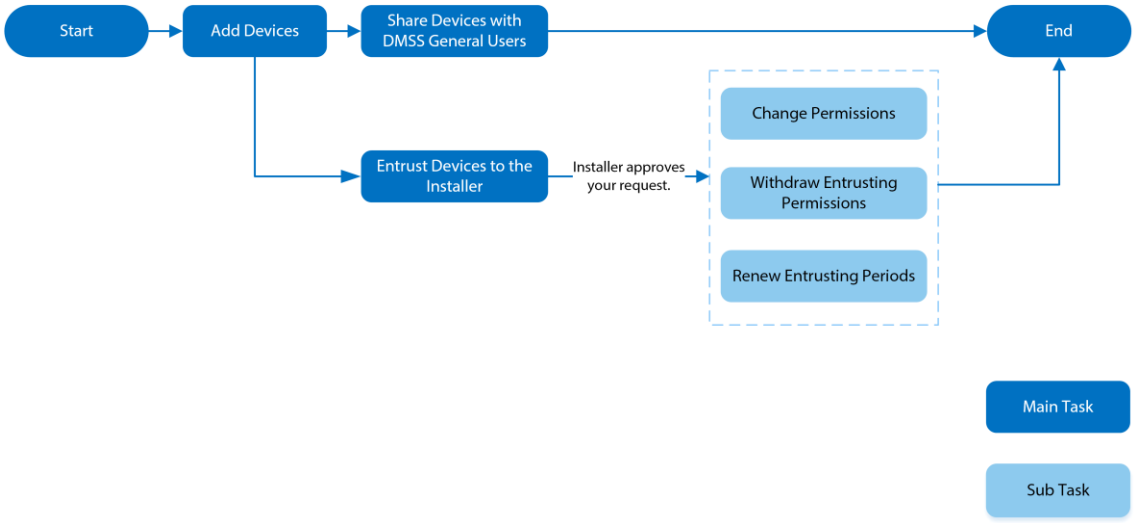
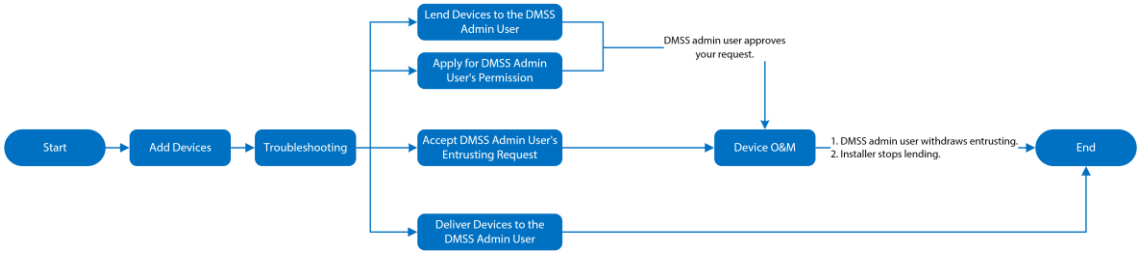


Abbildung 3-2 Geschäftsablauf (Installateur)



3.2 Betriebsablauf

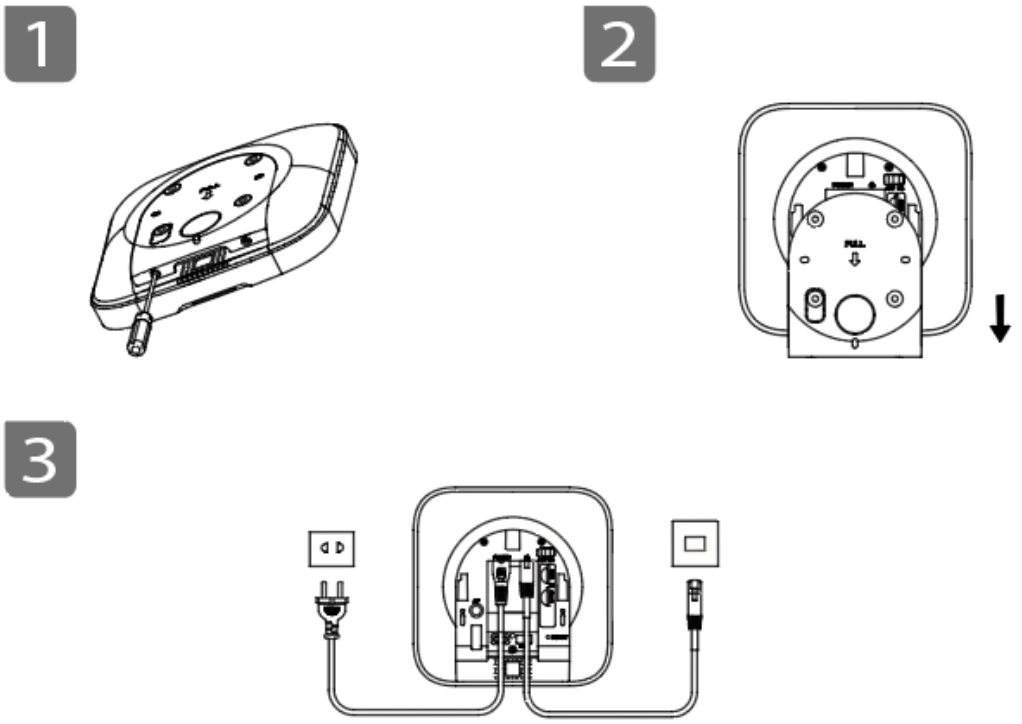
Gehen Sie wie folgt vor, um das drahtlose Alarmsystem einzuschalten.

Abbildung 3-3 Betriebsablauf

Einschalten

Schließen Sie den Hub an das Ethernet an, und schalten Sie ihn ein.

Abbildung 3-4 Einschalten



Hinzufügen von Geräten

1. Fügen Sie den Hub zur DMSS-App hinzu.
2. Fügen Sie die Peripheriegeräte zum Hub hinzu.

Installation des Hubs

Wir empfehlen die Verwendung von Dehnschrauben zur Installation der Nabe. Bringen Sie die Nabe nicht in den folgenden Bereichen an:

- Im Freien.
- Orte in der Nähe von Metallobjekten, die eine Dämpfung und Abschirmung des Funksignals verursachen.
- Orte mit schwachem GSM-Signal.
- Orte in der Nähe von Funkstörquellen, die weniger als 1 Meter vom Router und den Stromkabeln entfernt sind.
- Orte, an denen die Temperatur und die Luftfeuchtigkeit die zulässigen Grenzen überschreiten.

Abbildung 3-5 Installation

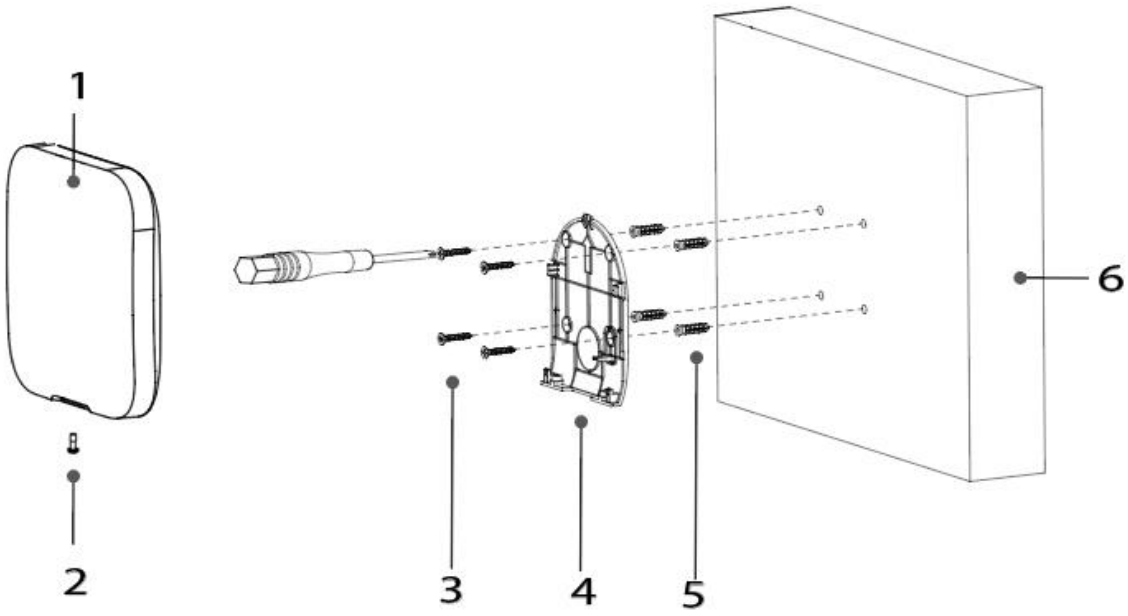


Tabelle 3-2 Einbauelemente

Nein.	Artikel Name	Nein.	Artikel Name
1	Nabe	4	Montageplatte
2	M3 × 8 mm Senkkopfschraube	5	Dehnschraube
3	Selbstschneidende Schraube ST4 × 25 mm	6	Wand

1. Bestätigen Sie die Position der Schraubenlöcher und bohren Sie sie dann in die Montageplatte.
2. Setzen Sie die Spreizbolzen in die Löcher ein.
3. Befestigen Sie die Montageplatte an der Wand und richten Sie die Schraubenlöcher an der Platte mit den Dehnungsbolzen aus.
4. Befestigen Sie die Montageplatte mit selbstschneidenden Schrauben ST4 × 25 mm.
5. Setzen Sie die Alarmnabe von oben nach unten in die Montageplatte ein.
6. Befestigen Sie die Alarmnabe und die Montageplatte mit M3 × 8 mm Senkkopfschrauben.

Konfigurieren des Hubs

Konfigurieren Sie den Hub in der DMSS-App.

Scharfschalten der Alarmanlage

Sie können die Tastatur, den Schlüsselanhänger und die App verwenden, um Ihr System zu aktivieren. Nachdem ein Scharfschaltbefehl an die DMSS-App gesendet wurde, prüft das System den Status des Systems. Wenn das System einen Fehler aufweist, müssen Sie entscheiden, ob Sie es zwangsscharfschalten möchten. Einzelheiten zu den Peripheriegeräten

finden Sie im Benutzerhandbuch des entsprechenden Geräts.

4 DMSS-Betrieb für Endbenutzer

Die DMSS-App bietet professionelle Sicherheitsüberwachungsdienste für Endbenutzer. DMSS-Admin-Benutzer können den Hub mit allgemeinen DMSS-Benutzern gemeinsam nutzen und ihn einem Unternehmen anvertrauen. Peripheriegeräte, die mit dem Hub geliefert werden, können gleichzeitig freigegeben und anvertraut werden. Um den Hub selbst freizugeben und anzuvertrauen, müssen Sie die neueste Version der DMSS-App installieren.

Die Abbildungen dienen nur als Referenz und können von der tatsächlichen Schnittstelle abweichen.

4.1 Anmeldung bei DMSS

Das Sicherheitssystem wird über die DMSS-App konfiguriert und gesteuert. Sie können auf die DMSS-App unter iOS und Android zugreifen. In diesem Abschnitt werden die Vorgänge auf iOS als Beispiel verwendet.

Stellen Sie sicher, dass Sie die neueste Version der App installiert haben.

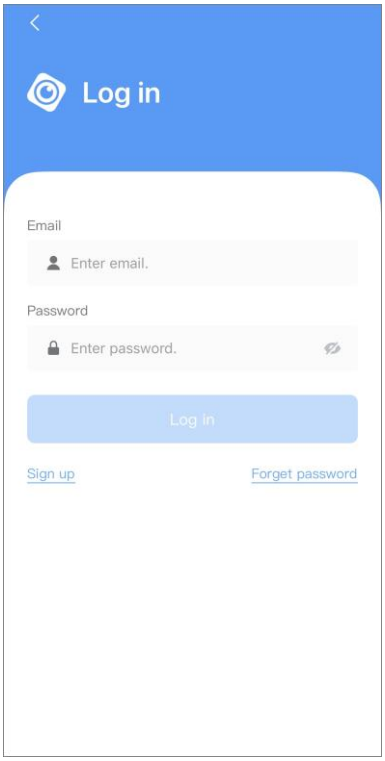
Verfahren

Schritt 1Suchen Sie im App-Store nach DMSS, und laden Sie die App dann herunter.

Android-Nutzer können DMSS bei Google Play herunterladen.

Schritt 2 Tippen Sie auf Ihrem Handy auf , um die App zu starten.

Abbildung 4-1 Anmeldung



Schritt 3Erstellen Sie ein Konto.

1) Tippen Sie auf dem Anmeldebildschirm auf **Anmelden**.
2) Geben Sie Ihre E-Mail Adresse und Ihr Passwort ein.

Tippen Sie auf , um das Passwort anzuzeigen, und das Symbol wird zu .

3) Lesen Sie die **Nutzungsvereinbarung** und die **Datenschutzrichtlinie** und aktivieren Sie dann das Kontrollkästchen **Ich habe sie gelesen und stimme zu**.
4) Tippen Sie auf **Verifizierungscode abrufen**, suchen Sie in Ihrem E-Mail-Postfach nach dem Verifizierungscode und geben Sie den Code ein.

Verwenden Sie den Verifizierungscode innerhalb von 60 Sekunden nach Erhalt. Andernfalls wird der Verifizierungscode ungültig.

5) Tippen Sie auf **OK**.

Schritt 4 Geben Sie auf dem Anmeldebildschirm Ihre E-Mail-Adresse und Ihr Passwort ein und tippen Sie dann auf **Anmelden**.

Sie können das Passwort auf der Seite **Ich** > **Kontoverwaltung** > **Passwort ändern** ändern.

4.2 Hinzufügen von Geräten

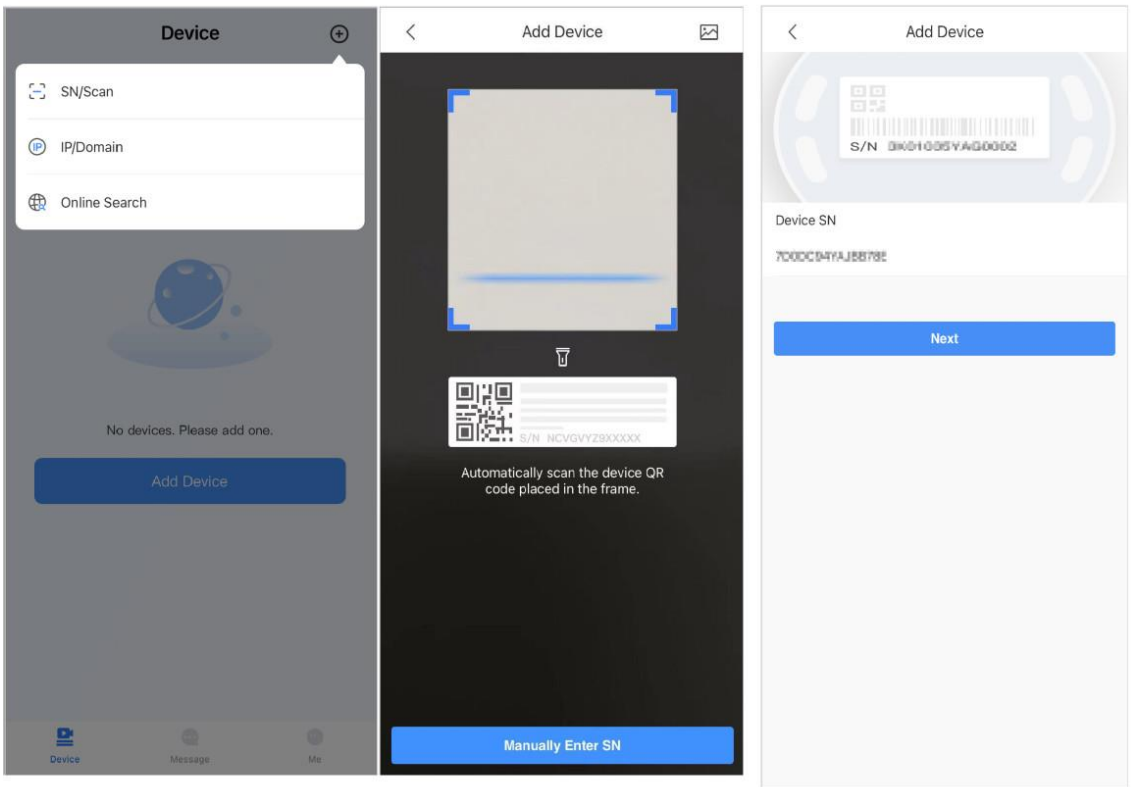
Für Endbenutzer können Sie Alarmgeräte zur DMSS-App hinzufügen.

4.2.1 Hinzufügen des Hubs

Verfahren

Schritt 1 Tippen Sie auf dem Bildschirm **Gerät** auf⊕ und wählen Sie dann **SN/Scan**.

Abbildung 4-2 Hinzufügen nach SN/QR-Code



Schritt 2Fügen Sie ein Gerät hinzu.

- Scannen Sie den QR-Code des Geräts direkt, oder tippen Sie auf und importieren Sie das QR-Code-Bild, um ein Gerät hinzuzufügen.
- Tippen Sie auf **SN manuell eingeben** und geben Sie dann die SN des Geräts ein, um ein Gerät manuell hinzuzufügen.

Schritt 3Wählen Sie den Gerätetyp und tippen Sie dann auf **Weiter**.

Tippen Sie auf **Weiter**, wenn das System den Gerätetyp automatisch identifiziert.

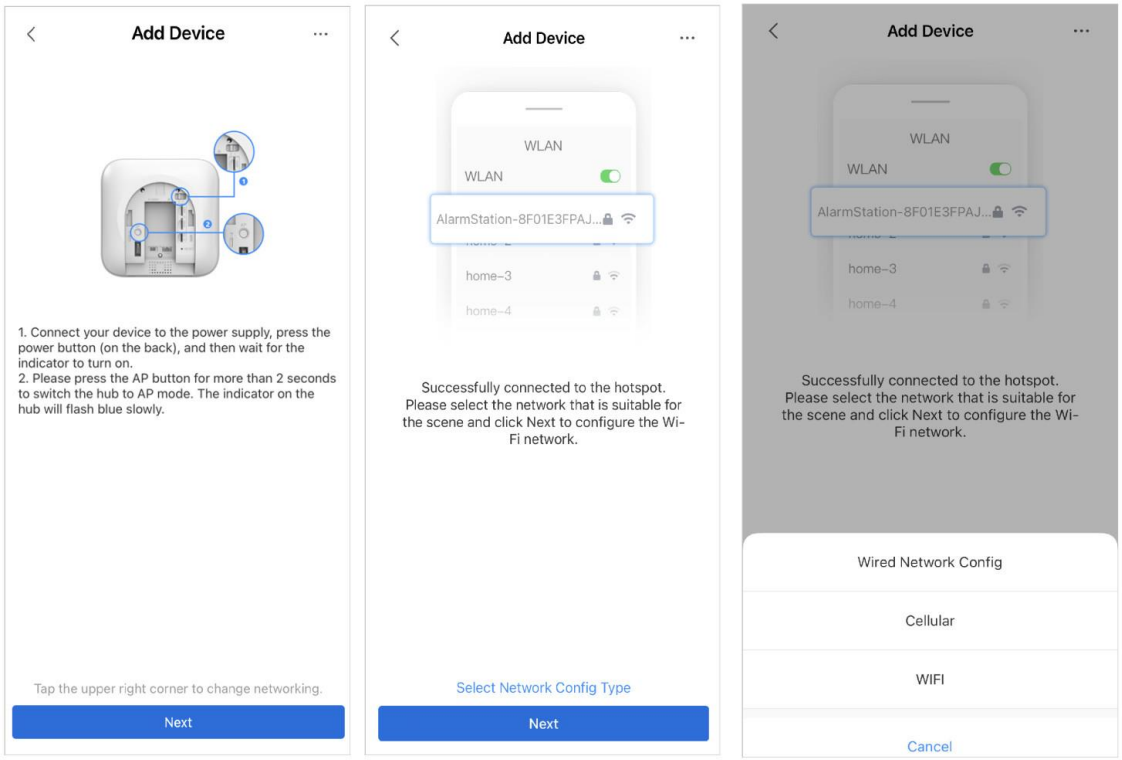
Schritt 4 Passen Sie auf dem Bildschirm **Gerät hinzufügen** den Gerätenamen an, geben Sie den Benutzernamen und das Gerätepasswort ein und tippen Sie dann auf **Speichern**.

Schritt 5Konfigurieren Sie die Netzwerkeinstellungen.

1) Tippen Sie im Fenster **Gerät hinzufügen** auf **Weiter**, um dem Hotspot des Hubs beizutreten.
2) Wenn die Verbindung erfolgreich hergestellt wurde, tippen Sie auf **Netzwerkkonfigurationstyp auswählen**.
3) Wählen Sie die Netzwerktypen aus, die Sie konfigurieren möchten.

- Verkabeltes Netzwerk: Aktivieren Sie die DHCP-Funktion, oder geben Sie IP-Adresse, Subnetzmaske, Gateway, DNS und MAC-Adresse manuell ein.
- Zellular: Konfigurieren Sie den APN, den Autho-Modus, den Benutzernamen, das Passwort, die Wählnummer und die Roaming-Daten für die SIM-Karte.
- Wi-Fi: Wählen Sie ein Wi-Fi-Netzwerk aus und geben Sie das Kennwort ein, um eine Verbindung damit herzustellen.

Abbildung 4-3 Netzwerktypen konfigurieren



4.2.2 Hinzufügen von Peripheriegeräten

Sie können dem Hub mehrere Peripheriegeräte hinzufügen. Einzelheiten zum Hinzufügen von

Peripheriegeräten finden Sie in den Benutzerhandbüchern der jeweiligen Peripheriegeräte.

Verfahren

Schritt 1Gehen Sie zum Hub-Bildschirm und tippen Sie dann auf **Peripheriegerät**, um das Peripheriegerät hinzuzufügen

Schritt 2Tippen Sie auf **+**, um den QR-Code auf der Unterseite des Geräts zu scannen, und tippen Sie dann auf **Weiter**.

Schritt 3Tippen Sie auf **Weiter**, nachdem das Gerät gefunden wurde.

Schritt 4Befolgen Sie die Anweisungen auf dem Bildschirm, schalten Sie das Gerät ein und tippen Sie dann auf **Weiter**.

Schritt 5Warten Sie die Kopplung ab.

Schritt 6Passen Sie den Namen des Geräts an , wählen Sie den Bereich aus und tippen Sie anschließend auf **Fertig stellen**.

4.2.3 Hinzufügen von IPC

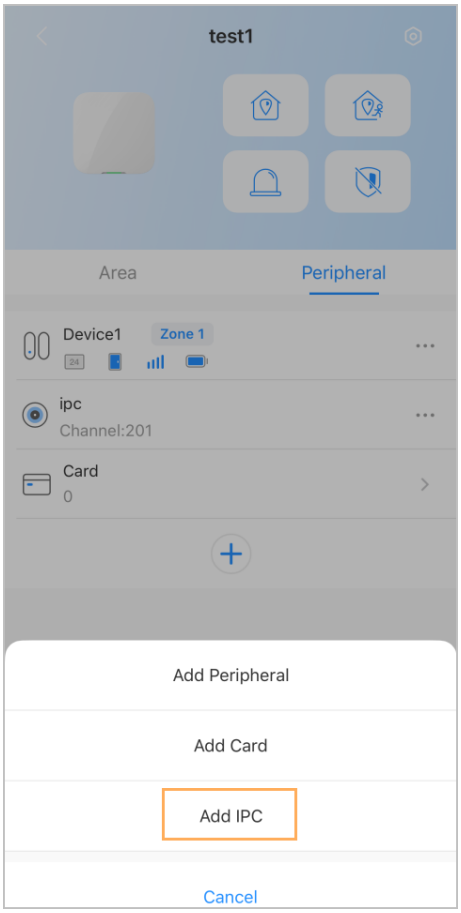
Fügen Sie IPCs zum Hub hinzu.

Verfahren

Schritt 1 Tippen Sie auf dem Nabenbildschirm auf **Peripheriegerät** und dann auf **+**.

Schritt 2Wählen Sie **IPC hinzufügen**.

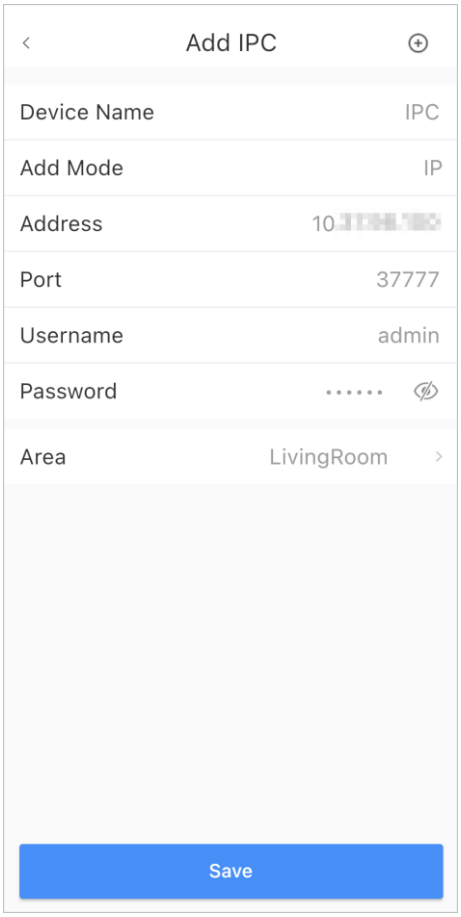
Abbildung 4-4 IPC hinzufügen



Schritt 3 Fügen Sie dem Hub einen IPC hinzu.

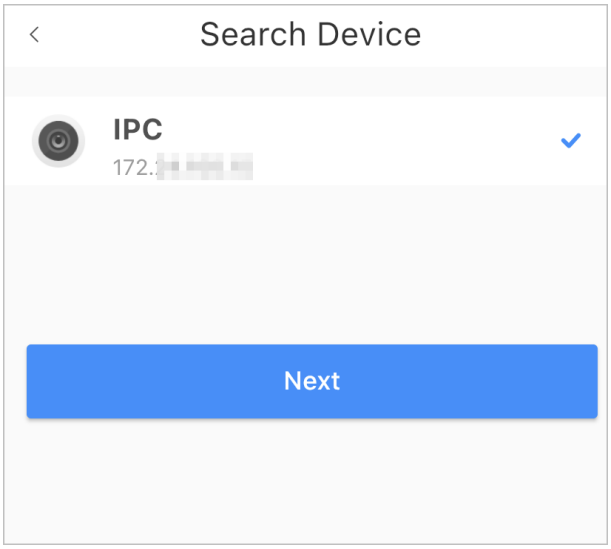
- Manuell hinzufügen:
  1. Konfigurieren Sie den Gerätenamen, die IP-Adresse des IPCs, die Portnummer, den Benutzernamen und das Passwort des IPCs und wählen Sie den Bereich aus, dem der IPC zugewiesen ist.
  2. Tippen Sie auf **Speichern**.

Abbildung 4-5 Manuelles Hinzufügen



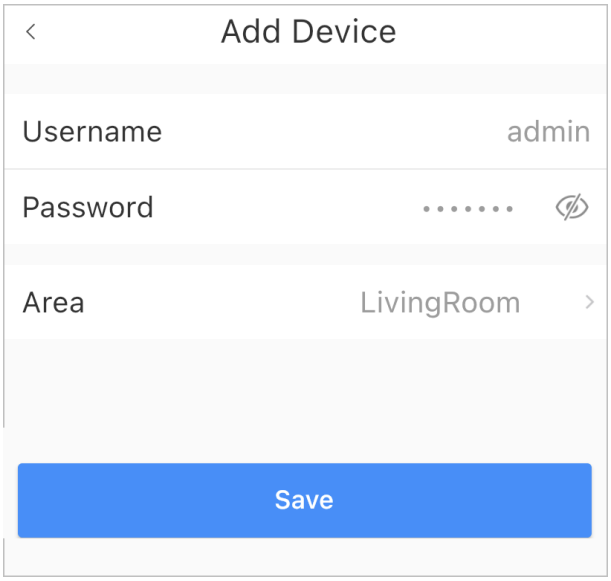
- Online-Suche:
  1. Tippen Sie auf ⊕ , um nach dem IPC im selben Netzwerksegment zu suchen.

Abbildung 4-6 Online-Suche



  2. Tippen Sie auf **Weiter**.
  3. Geben Sie das Passwort des IPC ein und wählen Sie den Bereich aus, dem der IPC zugewiesen ist, und tippen Sie dann auf **Speichern**.

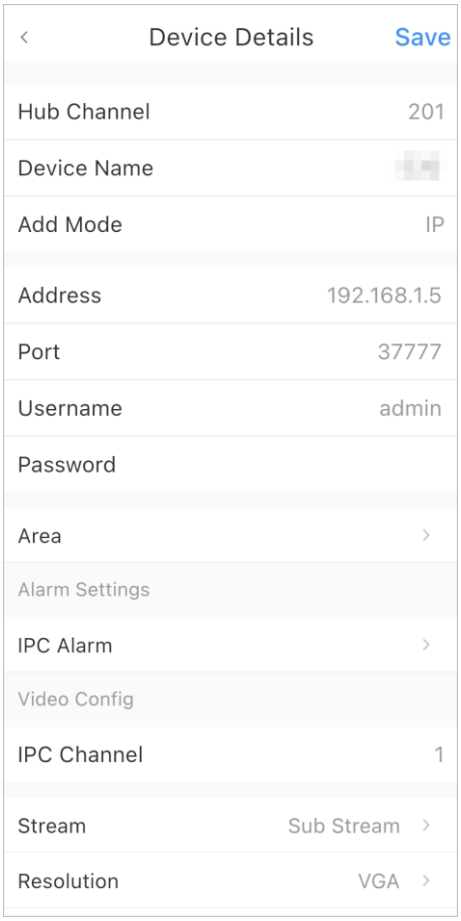
Abbildung 4-7 Passwort eingeben



Verwandte Operationen

Konfigurieren Sie auf dem Bildschirm **Gerätedetails** die Parameter des IPCs.

Abbildung 4-8 IPC konfigurieren



4.3 Konfigurieren der Alarmverknüpfung Video

Konfigurieren Sie die Alarmverknüpfung für Peripheriegeräte so, dass Sie Videoclips anzeigen können, wenn der Alarm ausgelöst wird.

Voraussetzungen

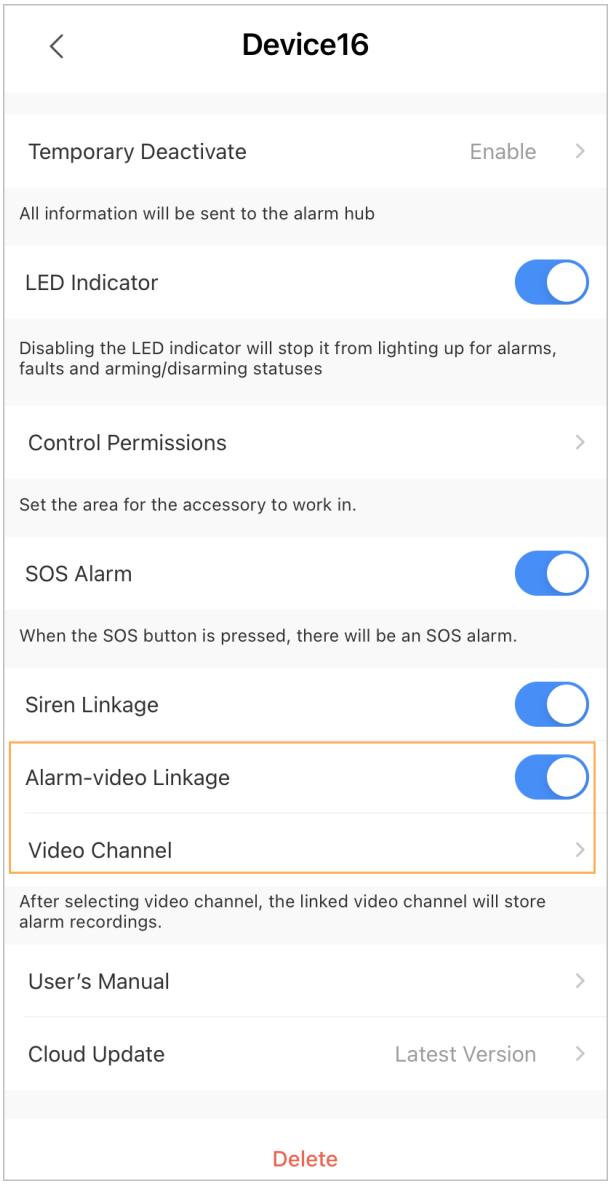
- Vergewissern Sie sich, dass der Hub scharf geschaltet ist, bevor Sie die Alarm-Video-Kopplung konfigurieren.
- Vergewissern Sie sich, dass Sie dem Hub Peripheriegeräte hinzugefügt haben.

Verfahren

Schritt 1 Wählen Sie auf dem Hub-Bildschirm ein Peripheriegerät in der Liste **Peripheriegerät** aus und tippen Sie dann auf auf dem Bildschirm **Gerätedetails**, um die Parameter zu konfigurieren.

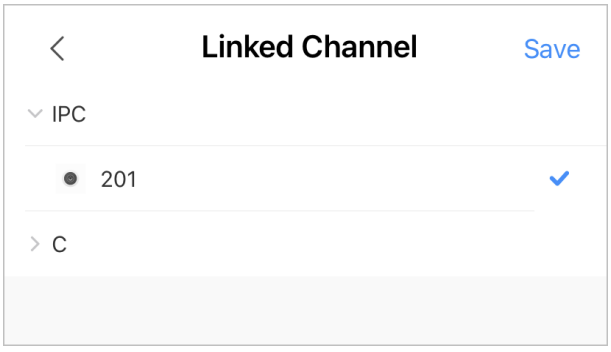
Schritt 2 Aktivieren Sie die **Alarm-Video-Verknüpfung**, und wählen Sie dann **Videokanal**.

Abbildung 4-9 Konfigurationsbildschirm



Schritt 3Wählen Sie einen Videokanal aus der Liste der **verknüpften Kanäle aus,** und tippen Sie auf **Speichern**.

Abbildung 4-10 Verknüpfter Kanal



4.4 Allgemeine Hub-Einstellungen

Sie können grundlegende Geräteinformationen anzeigen und bearbeiten.

Verfahren

Schritt 1 Tippen Sie im Hub-Bildschirm auf , um zum Bildschirm **Gerätedetails zu** gelangen.

Tabelle 4-1 Parameterbeschreibung

Parameter	Beschreibung
Hub-Status	Status des Hubs anzeigen.
Nabeneinstellung	Konfigurieren Sie die Parameter des Hubs.
Hauptstromausfallverzögerung	Konfigurieren Sie die Verzögerungszeit für alle Geräte im System, um Funktionen zu aktivieren, wenn die Hauptstromversorgung unterbrochen wird. Tippen Sie auf **Aktivieren** und legen Sie dann die Verzögerungszeit fest.
Netzwerk-Konfiguration	Tippen Sie auf **Netzwerkkonfiguration**, um Ihre aktuellen Netzwerkinformationen anzuzeigen.
Zeitzone	Tippen Sie auf **Zeitzone**, um Ihre Zeitzone auszuwählen, und aktivieren Sie ggf. die Sommerzeit. • **Zeitzone**: Wählen Sie die Zeitzone, in der der Hub arbeitet. • **Sommerzeit**: Wählen Sie das Datum oder die Woche und dann die Start- und Endzeit.
Gemeinsame Nutzung von Geräten	Tippen Sie auf **Gerätefreigabe**, um den Status des Hubs mit anderen Benutzern zu teilen.
Geräte-Sprachen	Wählen Sie die Sprache, die mit der SMS-Sprachausgabe verknüpft werden soll. Sie können zwischen Englisch, Arabisch, Dänisch, Französisch, Italienisch, Spanisch und Türkisch wählen.
Gerät entrusting	Überlassen Sie Ihre Geräte Dienstleistern, damit diese für Sie Alarmdienste durchführen.
Benutzerhandbuch	Tippen Sie auf **Benutzerhandbuch**, um das Benutzerhandbuch des Alarm-Hubs aufzurufen.
Cloud-Update	Online aktualisieren. Eine Aktualisierung ist nicht möglich, wenn sich der Hub im scharfgeschalteten Zustand befindet oder der Batteriestand niedrig ist.

Parameter	Beschreibung
Protokolle	Geräte- und Anwendungsprotokolle. • Geräteprotokoll: Wählen Sie **Protokoll** > **Geräteprotokoll**, um die Alarmprotokolle des Geräts anzuzeigen. Sie können auch auf auf dem Bildschirm **Geräteprotokoll** tippen, um Alarmprotokolle an die verknüpfte E-Mail zu senden. • App-Protokoll: Wählen Sie **Protokoll** > **App-Protokoll**, um Alarmprotokolle anzuzeigen. Sie können auch auf auf dem Bildschirm "**App-Protokoll**" tippen, um Alarmprotokolle an die verknüpfte E-Mail zu senden.

4.4.1 Anzeigen des Hub-Status

Wählen Sie auf dem Hub-Bildschirm > **Hub-Status**, um den Status des Hubs anzuzeigen.

Tabelle 4-2 Status

Parameter	Beschreibung
LTE-Signalstärke	Die Signalstärke des Mobilfunknetzes für die aktive SIM-Karte. • : Sehr niedrig. • : Niedrig. • : Mäßig. • : Hoch. • : Nein.
Wi-Fi-Signalstärke	Status der Internetverbindung des Hubs über Wi-Fi. Für eine höhere Zuverlässigkeit empfehlen wir, den Hub an Orten mit einer Signalstärke von mindestens 2 Balken zu installieren. • : Sehr niedrig. • : Niedrig. • : Mäßig. • : Hoch. • : Nein.
Batteriestand	Zeigt den verbleibenden Strom der Batterie an. • : Vollständig geladen. • : Ausreichend. • : Mäßig. • : Unzureichend.
Anti-Manipulation	Dies ist die Antimanipulationsfunktion für das Peripheriegerät. Der Hub reagiert, wenn ein Peripheriegerät demontiert wird.

Parameter	Beschreibung
Status der Hauptstromversorgung	Zeigt den Status der Hauptstromversorgung an.
LTE-Verbindungsstatus	Status der Internetverbindung des Hubs über SIM-Karte, Wi-Fi und Ethernet. • : Verbunden. • : Getrennt.
Status der Wi-Fi-Verbindung	
Status der Netzwerkkabelverbindung	
SIM-Karte	Verbindungsstatus der SIM-Karte. • : SIM-Karte 1 ist aktiv. • : SIM-Karte 2 ist aktiv. • : Keine SIM-Karte.
SIM-Karten-Status	Diese Statusleiste wird nur unterstützt, wenn eine SIM-Karte in den Hub eingelegt ist. • : Die SIM-Karte ist freigeschaltet. • : Die SIM-Karte ist gesperrt.
Programm-Version	Die Programmversion des Hubs.

4.4.2 Konfigurieren des Hubs

Verfahren

Schritt 1Tippen Sie auf dem Bildschirm **Hub** auf

Schritt 2 Betrachten und bearbeiten Sie die allgemeinen Informationen des Hubs.

Tabelle 4-3 Beschreibung der Hub-Parameter

Parameter	Beschreibung

Benutzer-Manager	Sie können Benutzer hinzufügen, ändern oder löschen, wenn das Keypad unscharf geschaltet ist. • **Hinzufügen von Benutzern**: Tippen Sie auf ⊕ , um einen Benutzer hinzuzufügen. Geben Sie Ihren Benutzernamen, den Tastaturcode (4- bis 6-stellig) und den Sicherheitscode (optional) ein und wählen Sie dann die Scharf- und Unscharfschaltberechtigung für den Raum aus. ◇ Es sind bis zu 64 Keypad-Benutzer zulässig (32 manuell hinzugefügte Benutzer und 32 automatisch erstellte Benutzer). Der erste manuell erstellte Benutzer ist standardmäßig der Admin-Benutzer. Alle Berechtigungen sind für den Benutzer admin verfügbar. ◇ DMSS erstellt jedes Mal automatisch einen Keypad-Benutzer, wenn ein Gerät zum ersten Mal hinzugefügt wird. Die laufende Nummer der vom System erstellten Keypad-Benutzer beginnt automatisch bei 33 und hat ein Symbol neben ihrem Konto. ◇ Für gemeinsam genutzte Benutzer wird automatisch ein Keypad-Benutzer erstellt. Abbildung 4-11 Keypad-Benutzer hinzufügen  • **Benutzer löschen**: Wählen Sie den Benutzer aus und streichen Sie dann nach links, um den Benutzer zu löschen. Der Admin-Benutzer muss der letzte sein, der gelöscht wird. • **Ändern von Benutzerinformationen**: Tippen Sie auf den Benutzer, den Sie bearbeiten möchten, und ändern Sie dann die Benutzerinformationen, einschließlich Benutzername, Tastaturcode, Nötigungscode, Scharf- und Unscharfschaltungsberechtigung auf der Seite mit den Benutzerinformationen. • **Karte hinzufügen**: Tippen Sie auf . ⊕ in der oberen rechten Ecke der Benutzerinformationsseite, um eine Karte für den Benutzer hinzuzufügen. Drücken Sie eine beliebige Taste, um das Tastenfeld aufzuwecken, und halten Sie dann die Karte

Parameter	Beschreibung
	in die Nähe des Kartenlesebereichs des Tastenfelds, um innerhalb von 30 Sekunden den Verknüpfungsvorgang zu starten. Wenn die Karteninformationen erfolgreich erkannt wurden, wird die Karten-ID auf der Seite mit den Benutzerinformationen angezeigt, und das Keypad gibt einen Signalton aus. Nachdem Sie die Konfigurationen gespeichert haben, verfügt die Karte über die Berechtigungen des Benutzers. Es können bis zu 8 Karten mit einem Benutzer verknüpft werden. • **Karte löschen**: Wählen Sie die Karte aus und wischen Sie dann nach links, um die Karte zu löschen.
App SOS-Alarm Typ	Konfigurieren Sie die App SOS-Alarmtypen, einschließlich Notfallalarm, Panikalarm und Verbindung zur Sirene, medizinischer Alarm, medizinischer Alarm und Verbindung zur Sirene, Feueralarm, Feueralarm und Verbindung zur Sirene. Drücken Sie nach der Konfiguration auf dem Hub-Bildschirm , um den Alarm auszulösen. Wenn mehrere Alarmtypen ausgewählt sind, werden Sie in einem Pop-up-Fenster daran erinnert, einen Alarm auszuwählen, der dieses Mal ausgelöst werden soll.
Globale Scharfschaltung/Entschärfung	Schalten Sie alle Melder in allen Bereichen mit einem Tastendruck scharf oder unscharf.
Zeitplan Scharf-/Unscharfschalten	Aktivieren oder deaktivieren Sie die Bereiche nach Zeitplan. • **Gebiet**: Wählen Sie das Gebiet, in dem der Hub arbeitet. • **Befehlseinstellung**: Wählen Sie je nach Bedarf einen Scharfschaltmodus aus, indem Sie auf **Home**, **Away** oder **Disarm** tippen. • **Zeit**: Wählen Sie die Zeitspanne aus, in der der Hub arbeitet. • **Wiederholen**: Kopieren Sie den Scharf- oder Unscharfschaltplan. • **Scharfschalten erzwingen**: Sie können das System aktivieren, wenn in den Zonen Fehler auftreten.
Einstellung des Klingeltons	• Lautstärke: Wählen Sie die Lautstärke für den Alarm. • Alarm/Sabotage-Ton: Aktivieren Sie die Funktion, damit beim Auftreten eines Alarms oder eines Manipulationsereignisses ein Ton ertönt. • Dauer des Alarmtons: Legen Sie die Dauer für den Ton fest. • Verzögerungszeit beim Betreten und Verlassen und Klingelton beim Scharf-/Unscharfschalten: Aktivieren Sie die Funktion, damit der Klingelton in diesen Szenarien verwendet wird.

Parameter	Beschreibung
LED-Anzeige	**Die LED-Anzeige** ist standardmäßig aktiviert. Wenn die **LED-Anzeige** deaktiviert ist, bleibt die LED-Anzeige aus, unabhängig davon, ob der Hub normal funktioniert oder nicht.
Gegensprechanlagen-Dienst	Aktivieren Sie den **Intercom-Service**, um die Funktion zu erreichen. • Intercom-Zeitlimit: Wenn ein Alarm ausgelöst wird, können Intercom-Dienste innerhalb des konfigurierten Zeitintervalls gestartet werden. Wenn die Zeit abgelaufen ist, kann keine neue Interkom-Sitzung mehr gestartet werden. Die Dauer jeder Interkom-Sitzung darf 20 Minuten nicht überschreiten. • Gegensprechanlage: ◇ App Gegensprechanlage: Gegensprechanlage zwischen der Sirene und der DMSS-App. Wählen Sie die Sirene aus, die verschiedenen Bereichen zugewiesen ist, oder wählen Sie **Nicht verbinden**. ◇ SIP-Sprechanlage: Gegensprechanlage zwischen der Sirene und der Plattform eines Drittanbieters. ○ Wählen Sie die Sirene für die Gegensprechanlage. Die Auswahl gefiltert nach Sirene und Bereich wird unterstützt. ○ SIP-Server-Konfiguration： Benutzername/Passwort: Vorbehaltlich der Konfiguration in der Drittanbieterplattform. SIP-Server-Adresse: Geben Sie die IP-Adresse der Plattform des Drittanbieters ein. SIP-Server-Port/lokaler Port: Muss mit der Portnummer der Plattform des Drittanbieters übereinstimmen. Registrierungsstatus: Zeigt den Status an, ob das SIP konfiguriert ist oder nicht.

Parameter	Beschreibung
Rufnummernverwaltung	Tippen Sie oben rechts auf der Seite auf "**Hinzufügen**", um eine Telefonnummer hinzuzufügen, die das Ereignis empfangen soll, und wählen Sie dann den Ereignistyp aus, für den eine SMS gesendet werden soll. Zu den Ereignistypen gehören Alarm, Störung, Betrieb und ob der Alarm mit dem Telefon verknüpft ist. Nach dem Hinzufügen können Sie nach links wischen, um Anrufe und SMS-Nachrichten zu testen, um zu überprüfen, ob die aktuelle Telefonnummer gültig ist. Sie können auch nach links wischen, um die Mobiltelefonnummer zu löschen. Tippen Sie auf die Telefonnummer, um die Seite zur Bearbeitung der Telefonnummer aufzurufen. Sie können dann die Nummer bearbeiten und den Ereignistyp auswählen, der eine SMS senden soll. Nur 2G/4G-Geräte unterstützen diese Funktion.
Test-Modus	Tippen Sie auf **Start**, um den Status der Peripheriegeräte zu testen, die in verschiedenen Bereichen mit dem Hub verbunden sind, und tippen Sie dann auf **Stopp**, um die Erkennung abzuschließen.
Modus mit reduzierter Empfindlichkeit	Aktivieren Sie den **Modus "Reduzierte Empfindlichkeit"**, dann wird die Sendeleistung des Hubs reduziert.
Cloud-Service-Verbindung	Legen Sie das Ping-Intervall zwischen Server und Hub im Bereich von 150 bis 900 Sekunden fest (Standard: 150 Sekunden). Wenn die D-Cloud feststellt, dass der Hub länger als 150 Sekunden offline ist, meldet sie den Hub-Status über die App an den Benutzer.

Parameter	Beschreibung
Herzschlag	Konfigurieren Sie das Ping-Intervall für den Hub-Detektor. Die Einstellungen legen fest, wie häufig der Hub mit den Peripheriegeräten kommuniziert und wie schnell ein Verbindungsverlust erkannt wird. • **Detektor-Ping-Intervall**: Die Häufigkeit der angeschlossenen Peripheriegeräte, die vom Hub bedient werden, wird im Bereich von 12 Sekunden bis 300 Sekunden konfiguriert (standardmäßig 60 Sekunden). Je kürzer das Ping-Intervall des Detektors ist, desto kürzer ist die Lebensdauer der Batterie. • **Anzahl der nicht zugestellten Pakete zur Bestimmung des Verbindungsfehlers**: Es wird ein Zähler für nicht zugestellte Pakete im Bereich von 3 bis 60 konfiguriert (standardmäßig 15 Pakete). ◇ Je kleiner die Zahl, desto häufiger wird der Offline-Status von Peripheriegeräten erkannt und gemeldet. ◇ Wenn der Hub ständig die Verbindung zu den Peripheriegeräten verliert und deren definierte Heartbeats nicht erkennen kann, meldet er deren Offline-Status an das System.
Link Sirene für Manipulation	• **Sirene für Manipulation verknüpfen**: Wenn die **Sirenenverknüpfung für Sabotage** aktiviert ist, verknüpft die Zentrale den Alarmton im Scharfschaltzustand. Die Sirene schlägt Alarm, wenn die Klappen der Nabe und der Peripheriegeräte geöffnet sind. • **Immer aktiv**: Legen Sie fest, ob der Alarmton im unscharfen Zustand verknüpft werden soll. Sie ist standardmäßig deaktiviert. Nach der Aktivierung von **Immer aktiv**, wenn die **Sirene für Manipulationen verknüpfen** aktiviert ist, verknüpft der Hub den Alarmton sowohl im Aktivierungs- als auch im Deaktivierungszustand. Dies entspricht nicht der EN50131-1-Zertifizierung.

Parameter	Beschreibung
Prüfung der Systemintegrität	Wenn diese Funktion aktiviert ist, prüft der Hub vor dem Scharfschalten den Status aller Melder, z. B. den Ladezustand der Batterie, Sabotagevorfälle und die Konnektivität. Wenn Fehler erkannt werden, werden Warnungen angezeigt. • Für den Schlüsselanhänger blinkt die Anzeige grün und wird dann rot. • Bei der App wird eine Alarmmeldung angezeigt. • Bei der Tastatur piept es 1 Sekunde lang, die Scharf- und Unscharfschaltanzeige blinkt 2 Sekunden lang grün und schaltet dann in den normalen Status.
CMS	Geben Sie IP/Domain, Port und Geräte-ID ein, und dann können Sie den Hub beim DSS Pro oder Konverter registrieren.

Alarmempfangszentrale	Wählen Sie Alarmempfangszentrale 1 oder 2 und gehen Sie zum entsprechenden Konfigurationsbildschirm. Aktivieren Sie die Funktion, und konfigurieren Sie dann die Parameter. • **Protokoll**: Wählen Sie zwischen **SIA-DC09**, **Softguard** und **Privat**. • **Bevorzugter IP/Domänenname**: Geben Sie die IP-/Domänenadresse und die Portnummer der ARC ein. • **Alternativer IP-/Domänenname**: Geben Sie die alternative IP-/Domain-Adresse und die Portnummer der ARC ein. ◇ Nachrichten werden nur dann an die alternative IP/Domain-Adresse gesendet, wenn die bevorzugte IP-Adresse die Nachricht nicht empfangen kann. ◇ Wenn das **Heartbeat-Intervall** aktiviert ist, entscheidet das System, ob die Nachricht an die bevorzugte oder an die alternative IP-Adresse gesendet werden soll. • **IP-Protokoll**: Wählen Sie standardmäßig **TCP**. • **Heartbeat-Intervall**: Legen Sie das Heartbeat-Intervall im Bereich von 0 Sekunden bis 24 Stunden fest (Standard: 60 Sekunden). 0 Sekunden bedeutet, dass das **Heartbeat-Intervall** deaktiviert ist. • **Zentrales Konto**: Geben Sie die vom ARC erstellte Kontonummer ein, die zur Identifizierung des Hubs verwendet werden soll, wenn der Hub Informationen an das ARC sendet. • **Zeitraum für erneutes Hochladen**: Wählen Sie den Zeitraum für das erneute Hochladen aus der Liste aus. • **Verschlüsselung**: Der Hub verwendet ein Verschlüsselungsformat für die Informationssicherheit, wenn Sie die ARC konfigurieren. Standardmäßig ist **AES128** eingestellt. • **Ereignisse hochladen**: Tippen Sie auf neben einem Ereignis, um es hochzuladen. ◇ **Alarm**: Alarmmeldung. ◇ **Störungen**: Stromausfall, Unterspannung der Batterie, Manipulation und Offline. ◇ **Ereignisse**: Verbieten Sie die Verwendung von Peripheriegeräten, fügen Sie Peripheriegeräte hinzu oder löschen Sie sie, und fügen Sie Benutzer hinzu oder löschen Sie sie. ◇ **Scharf-/Unscharfschalten**: Benachrichtigung über die Scharfschaltung und Entschärfung des Systems.

Parameter	Beschreibung
	• **Kommunikationstest**: Unterstützt **manuellen Test** und **geplanten Test**. ◇ **Manueller Test**: Testen Sie manuell, ob die Parameter der bevorzugten und alternativen Alarmzentralen normal sind. Wenn der Test erfolgreich ist, kann die Zentrale das Testereignis empfangen. ◇ **Geplanter Test**: Der planmäßige Test wird durch einen Fehler deaktiviert. Nach der Aktivierung meldet der Hub regelmäßig periodische Testereignisse.
Störungsprüfung	• **Ausfall der Hauptstromversorgung**: Diese Option ist standardmäßig aktiviert. Nach der Deaktivierung wird ein Ausfall der Hauptstromversorgung des Hubs nicht mehr angezeigt und gemeldet. • **Alarm Hub Manipulation**: Diese Funktion ist standardmäßig aktiviert. Nach der Deaktivierung, wenn der Deckel der Nabe geöffnet ist, wird die Nabe nicht anzeigen und benachrichtigen. • **Verbindungen zur Cloud-Plattform**: Sie ist standardmäßig aktiviert. Nach der Deaktivierung wird die Verbindung zwischen dem Hub und der Cloud-Plattform nicht mehr angezeigt und benachrichtigt, wenn die Verbindung gestört ist. • **Kabelgebundenes Netzwerk und Wi-Fi-Fehler**: Diese Funktion ist standardmäßig aktiviert. Nach der Deaktivierung wird der Hub bei einem Ausfall des kabelgebundenen Netzwerks und des WLANs nicht mehr angezeigt und benachrichtigt. • **Zellulare Netzwerk-Fehler**: Diese Option ist standardmäßig aktiviert. Nach der Deaktivierung wird der Hub bei einem Ausfall des Mobilfunknetzes des Hubs nicht mehr angezeigt und benachrichtigt. • **RF-Störungen**: Sie ist standardmäßig aktiviert. Nach der Deaktivierung wird der Hub, wenn er HF-Störungen erkennt, nicht mehr anzeigen und benachrichtigen, aber das Ereignis kann im Protokoll angezeigt werden. Die Deaktivierung einer dieser Funktionen führt dazu, dass das System nicht der EN50131-1 entspricht und die Fehlermeldungen, die sich auf die deaktivierte Funktion beziehen, nicht gesendet werden.

4.5 Netzwerkkonfiguration

Tippen Sie in der **allgemeinen Konfiguration** des Bildschirms **Gerätedetails** auf **Netzwerkkonfiguration** und wählen Sie dann das Netzwerk für den Hub aus:

kabelgebundenes Netzwerk, drahtloses Netzwerk oder Mobilfunknetz.

4.5.1 Konfiguration des kabelgebundenen Netzwerks

Verfahren

Schritt 1Wählen Sie **Netzwerkeinstellungen** > **Kabelgebundene Netzwerkkonfiguration**.

Schritt 2Konfigurieren Sie die Verbindungsparameter für das kabelgebundene Netzwerk.

Tabelle 4-4 Beschreibung der drahtgebundenen Netzwerkparameter

Parameter	Beschreibung
DHCP	Wenn ein DHCP-Server im Netzwerk vorhanden ist, können Sie **DHCP** aktivieren, und der Hub erhält dann automatisch eine dynamische IP-Adresse.
IP-Adresse	Stellen Sie die IP-Adresse manuell ein: Stellen Sie IP-Adresse, Subnetzmaske, Standard-Gateway, DNS und MAC-Adresse manuell für den Hub ein.
Subnetz-Maske	
Gateway	
DNS	
DNS 2	
MAC-Adresse	

4.5.2 Konfiguration des Wi-Fi-Netzwerks

Verfahren

Schritt 1Wählen Sie **Netzwerkeinstellungen** > **Wi-Fi-Netzwerkkonfiguration**.

Schritt 2Wählen Sie ein verfügbares Wi-Fi-Netzwerk in der Umgebung aus und geben Sie dann das Netzwerkpasswort ein, um eine Verbindung mit dem Netzwerk herzustellen.

4.5.3 Zelluläre Konfiguration

Verfahren

Schritt 1Wählen Sie **Netzeinstellungen** > **Mobilfunknetz**.

Schritt 2Konfigurieren Sie die zellularen Parameter.

Tabelle 4-5 Beschreibung der zellularen Parameter

Parameter	Beschreibung
Zellulär	Tippen Sie auf neben dem Feld **Mobilfunk**, um das Mobilfunknetz zu aktivieren.

Parameter	Beschreibung
Priorität	Tippen Sie auf neben **Priorität**, um bei der Auswahl des Netzes dem Mobilfunknetz den Vorrang zu geben.
SIM 1	• Unterstützt Dual-SIM-Karten und Single-Standby. • SIM-Karten ermöglichen dem Hub die Nutzung von Mobilfunkdaten und Push-Alarmbenachrichtigungen.
SIM 2	
APN	Der Zugangspunktname (APN) ist der Name der Einstellungen, die Ihr Gerät liest, um eine Verbindung für das Gateway zwischen dem Mobilfunknetz Ihres Anbieters und dem öffentlichen Internet herzustellen.
Autorisierungsmodus	Authentifizierungsmodus des zellularen Netzwerks.
Benutzername	Den Benutzernamen und das Passwort des Mobilfunknetzes.
Passwort	
Nummer wählen	Die Nummer, die der Hub anrufen soll.
Roaming-Daten	Aktivieren Sie die Funktion, wenn Sie außerhalb des Empfangsgebiets reisen, um eine Internetverbindung herzustellen.
Mobile Datennutzung	Anzeige der Nutzung der mobilen Daten.
Statistik zurücksetzen	Setzen Sie die mobile Datennutzung zurück, um die Zählung neu zu starten.
PIN	Unterstützt die Eingabe der PIN von SIM 1 bzw. SIM 2 zum Schutz der Privatsphäre, falls erforderlich. Es ist verboten, den PIN-Code einzugeben, wenn der Status der SIM-Karte nicht gesperrt ist. Sperren Sie die Karte, wenn Sie den PIN-Code eingeben möchten.

4.6 Benutzer verwalten

4.6.1 Benutzer hinzufügen

Für DMSS-Admin-Benutzer können Sie sowohl Installateure als auch allgemeine DMSS-Benutzer hinzufügen.

4.6.1.1 Hinzufügen eines allgemeinen DMSS-Benutzers

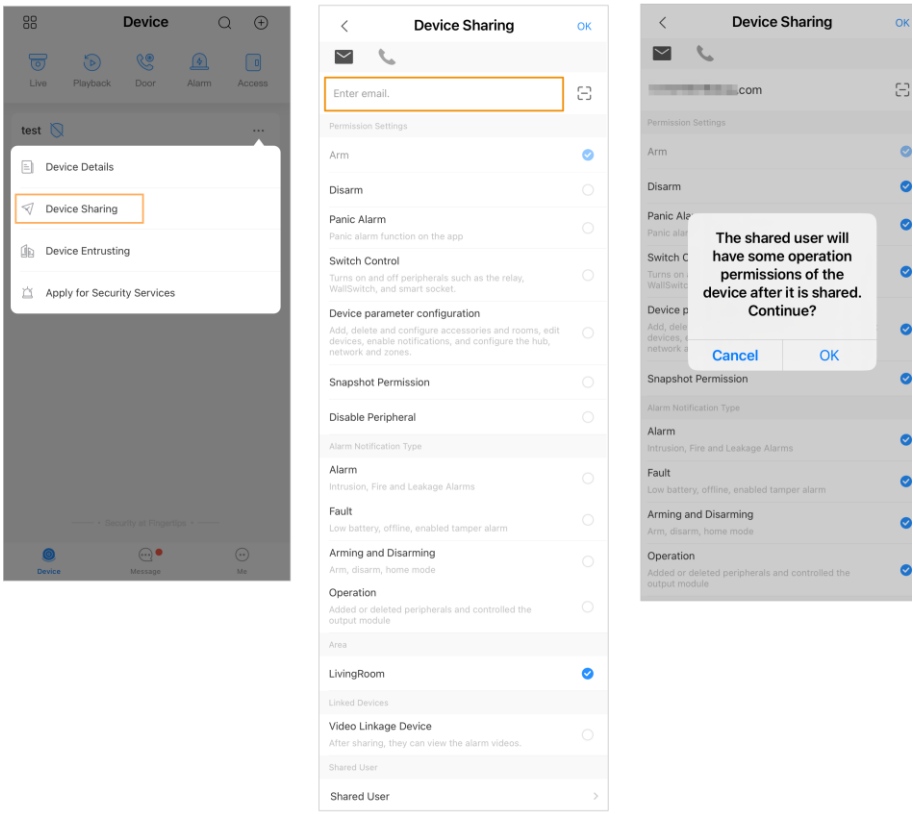
Sie können zu > **Gerätedetails** > oder > **Gerätedetails** > **Gerätefreigabe** gehen, um das Gerät freizugeben. Diese Methoden sind ähnlich. In diesem Abschnitt wird die

Freigabe von Geräten unter ••• > **Gerätefreigabe** als Beispiel verwendet.

Verfahren

Schritt 1 Tippen Sie auf dem Bildschirm **Gerät** auf ••• neben einem Gerät und dann auf **Gerätefreigabe**.

Abbildung 4-12 Gerät freigeben



Schritt 2 Geben Sie auf dem Bildschirm **Gerätefreigabe** das Gerät für den Benutzer frei, indem Sie sein DMSS-Konto eingeben oder seinen QR-Code scannen.

Schritt 3Wählen Sie die Geräteberechtigungen für Benutzer entsprechend Ihrem tatsächlichen Bedarf aus .

Schritt 4Tippen Sie auf **OK**.

Das Konto, für das Sie das Gerät freigegeben haben, wird im Abschnitt **Freigegebener Benutzer** des Bildschirms **Gerätefreigabe** angezeigt.

4.6.1.2 Installateur hinzufügen

Für DMSS-Administratoren können Sie Installateure hinzufügen, indem Sie ihnen Geräte anvertrauen. Sie können dem Installateur Geräte einzeln oder in Stapeln anvertrauen.

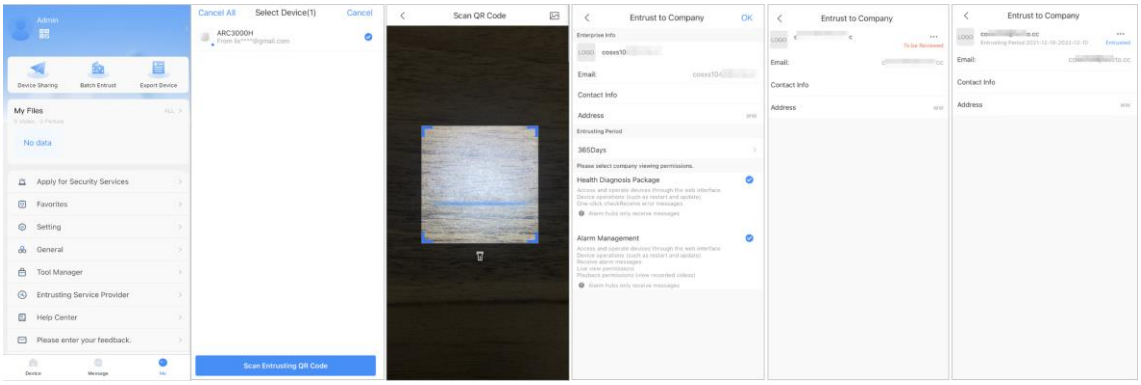
4.6.1.2.1 Betrauung von Geräten in Chargen

Sie können einem Unternehmen Geräte in Stapeln anvertrauen.

Verfahren

Schritt 1Wählen Sie **Ich** > **Batch Entrust**.

Abbildung 4-13 Entrust-Geräte in Stapeln



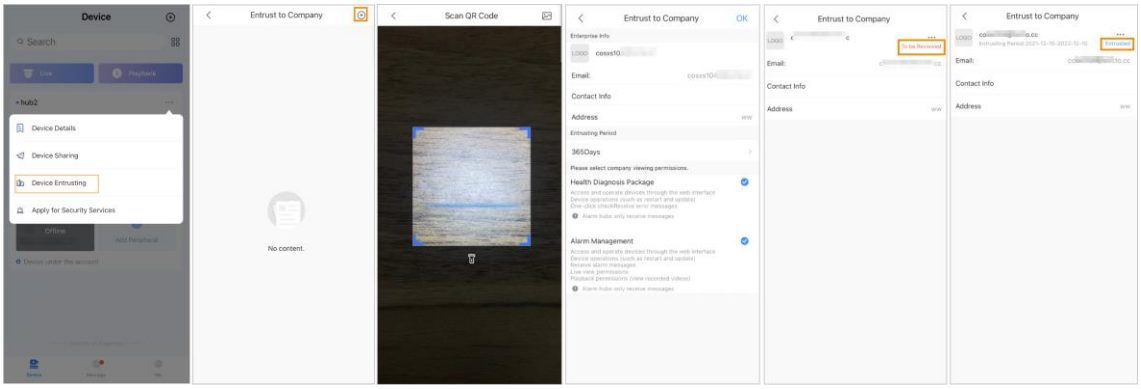
Schritt 2 Wählen Sie auf dem Bildschirm "**Gerät auswählen**" die Geräte aus, die Sie dem Unternehmen anvertrauen möchten, und vertrauen Sie diese dann dem Unternehmen an. Das Verfahren für die Beauftragung mehrerer Geräte ist dasselbe wie für die Beauftragung eines einzelnen Geräts.

4.6.1.2.2 Gerät einzeln anvertrauen

Verfahren

Schritt 1 Tippen Sie auf dem Bildschirm **Gerät** auf ••• neben einem Gerät und dann auf **Geräteentrusting**.

Abbildung 4-14 Entrust a device



Schritt 2 Tippen Sie auf dem Bildschirm **Unternehmen beauftragen** auf ⊕ und scannen Sie den entsprechenden QR-Code des Installateurs oder tippen Sie auf und importieren Sie das QR-Code-Bild, um das Gerät dem Installateur zu beauftragen.

Sie können die Installateure nach ihren QR-Codes fragen.

Schritt 3 Wählen Sie auf dem Bildschirm **Unternehmen anvertrauen** den Zeitraum der Anvertrauung und die Anzeigeberechtigung für das Unternehmen aus und tippen Sie auf **OK**.

- Sie müssen das **Paket Gesundheitsdiagnose** oder **Alarmverwaltung** auswählen, um die Berechtigungen anzuzeigen.
- Die Unternehmensinformationen werden automatisch erkannt, nachdem Sie den QR-Code des Installationsprogramms gescannt haben.

Schritt 4 Betrachten Sie die Betrauungsdetails auf dem Bildschirm **Unternehmen betrauen**. Nach erfolgreicher Beauftragung ändert sich "**Zu überprüfen**" in "**Zugestellt**".

Nachdem eine Betrauungsanfrage erfolgreich gesendet wurde, erscheint eine Meldung auf dem Startbildschirm. Sie müssen auf eine Antwort des Installateurs warten, die auf dem Bildschirm **Persönlich** angezeigt wird. Gehen Sie dazu auf **Ich** > **Mailbox** > **Persönlich**.

Verwandte Operationen

- Um die Berechtigungen zu ändern, gehen Sie zum Bildschirm **Unternehmen anvertrauen** und tippen Sie dann auf **Berechtigungen ändern**.
- Um die Betrauung zurückzuziehen, gehen Sie zum Bildschirm **Unternehmen betrauen** und tippen Sie dann auf **Zurückziehen**.
- Um die Betrauungszeiträume zu verlängern, gehen Sie zum Bildschirm **Unternehmen betrauen** und tippen Sie dann auf **Verlängern**.

4.6.2 Benutzer löschen

Bei DMSS-Admin-Benutzern können Sie sowohl Installateure als auch allgemeine DMSS-Benutzer löschen.

4.6.2.1 Aufhebung der Gerätefreigabe

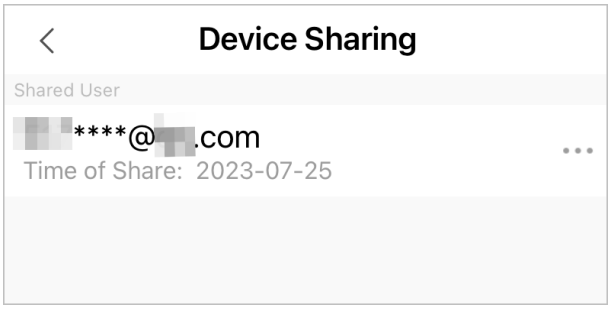
DMSS-Admin-Benutzer können DMSS-Benutzer löschen, wenn sie die gemeinsame Nutzung von Geräten mit ihnen auf dem Bildschirm "**Gerätefreigabe**" beenden. Dieser Vorgang wird in diesem Abschnitt anhand des Pfades > **Gerätefreigabe** erläutert.

Verfahren

Schritt 1 Tippen Sie auf dem Bildschirm **Gerät** auf neben einem Gerät und dann auf **Gerätefreigabe**.

Schritt 2 Wählen Sie in der Kontoliste des Bildschirms **Gerätefreigabe** ein Konto aus und tippen Sie auf ••• .

Abbildung 4-15 Gemeinsamer Benutzer



Schritt 3 Wählen Sie **Freigabe aufheben** und tippen Sie anschließend auf **OK**, um die Freigabe aufzuheben.

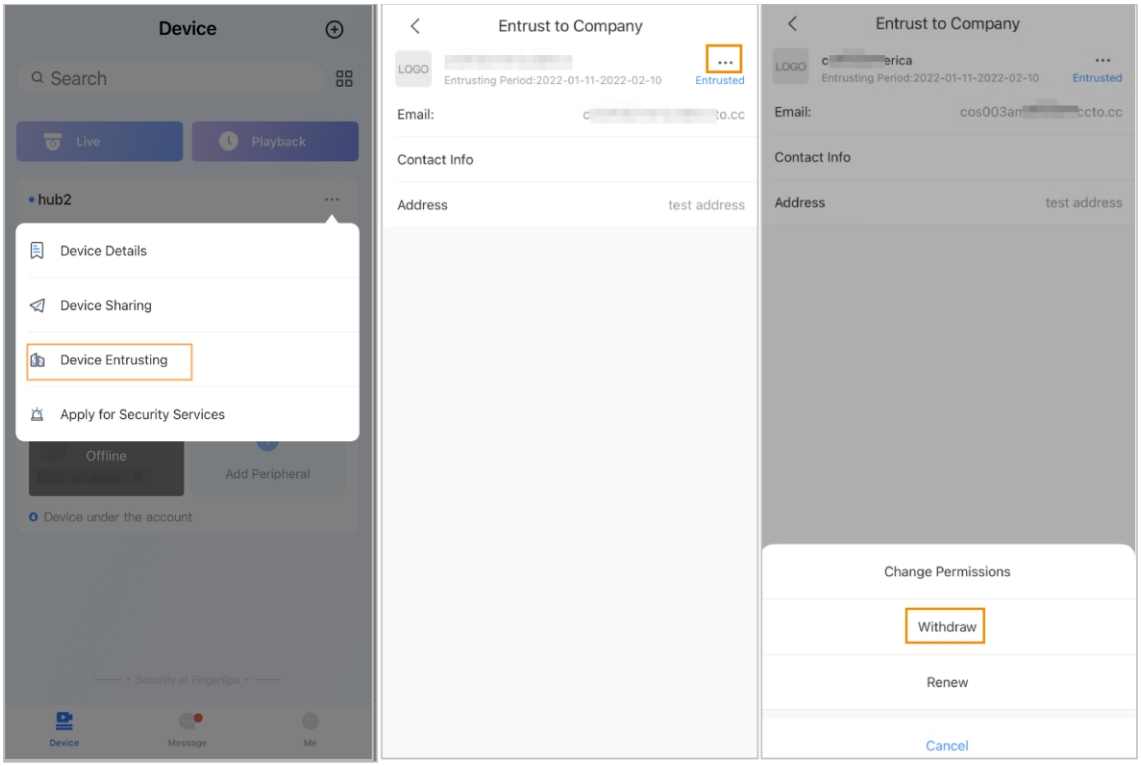
4.6.2.2 Aufhebung der Beauftragung der Anwendung

DMSS-Admin-Benutzer können ein Installationsprogramm löschen, indem sie die beauftragte Anwendung abbrechen.

Verfahren

Schritt 1 Tippen Sie auf dem Bildschirm **Gerät** auf ••• neben einem Gerät und dann auf **Geräteentrusting**.

Abbildung 4-16 Betrauungsantrag zurückziehen



Schritt 2 Wählen Sie auf dem Bildschirm **Device Entrusting** die Option ••• > **Entziehen** und tippen Sie anschließend auf **OK**.

Es wird eine Nachricht an das Konto des Installateurs gesendet. Nachdem der Installateur die Nachricht gelesen und Ihren Antrag auf Beendigung der Betrauung mit DoLynk Care genehmigt hat, wird Ihre Anwendung beendet.

4.6.2.3 Gerät löschen

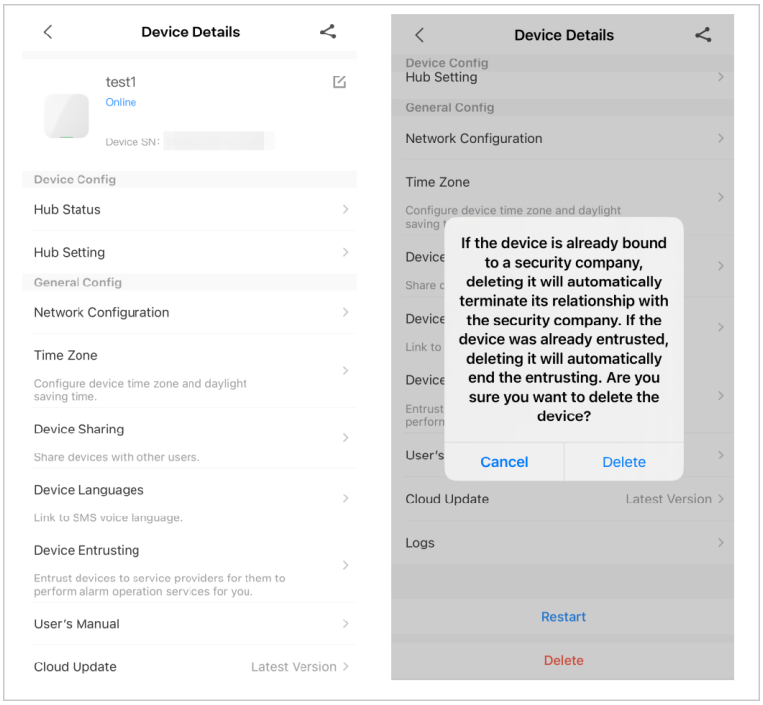
Für DMSS-Administrator-Benutzer können Sie sowohl Installateure als auch DMSS-Benutzer durch Löschen von Geräten löschen.

Der DMSS-Admin-Benutzer kann einen Installateur nicht löschen, wenn die Geräte vom Installateur freigegeben sind.

Verfahren

Schritt 1 Wählen Sie auf dem Bildschirm **Gerät** > **Gerätedetails**.

Abbildung 4-17 Löschen Sie das Gerät



Schritt 2Tippen Sie auf dem Bildschirm **Gerätedetails** auf **Löschen**.

Schritt 3Tippen Sie auf **Löschen**, um die Geräte zu löschen.

5 Allgemeiner Betrieb

Der Benutzer der Stufe 2 oder 3 hat die Berechtigung, das System scharf und unscharf zu schalten. In diesem Abschnitt wird die Bedienung des DMSS durch den Endbenutzer als Beispiel verwendet.

Voraussetzungen

- Vergewissern Sie sich, dass Sie einen Hub hinzugefügt haben, bevor Sie Konfigurationen vornehmen.
- Stellen Sie sicher, dass der Hub über eine stabile Internetverbindung verfügt.
- Stellen Sie sicher, dass die Nabe entschärft ist.

Hintergrundinformationen

Sie können Alarmzentralen und Peripheriegeräte verwalten und Vorgänge wie das Scharf- und Unscharfschalten sowie die Konfiguration von Alarmgeräten durchführen.

Verfahren

Schritt 1 Tippen Sie auf dem Hub-Bildschirm auf **Peripheriegerät**, um die Peripheriegeräte hinzuzufügen. Einzelheiten zum Hinzufügen von Peripheriegeräten finden Sie im Benutzerhandbuch des entsprechenden Geräts.

Schritt 2Schalten Sie die Melder in einem einzelnen Bereich oder in allen Bereichen durch manuelle oder geplante Vorgänge ein und aus.

- Einzelne Scharf- und Unscharfschaltung: Scharf- und Unscharfschalten der Melder in einem einzigen Bereich.
- Globale Scharf- und Unscharfschaltung: Scharf- und Unscharfschalten der Melder in allen Bereichen.
- Manuelles Scharfstellen und Entschärfen: Schalten Sie das Sicherheitssystem über die DMSS-App, das Tastenfeld oder den Schlüsselanhänger scharf.
- Scharf- und Unscharfschalten nach Zeitplan: Scharf- und Unscharfschalten der Melder nach Zeitplan.

5.1 Einzelne Scharf- und Unscharfschaltung

Sie können die Melder in einem einzigen Bereich scharf- und unscharfschalten.

Verfahren

Schritt 1 Tippen Sie auf dem Hub-Bildschirm auf **Bereich**.

Schritt 2 Tippen Sie auf einen Bereich und wählen Sie dann im Pop-up-Fenster zwischen **Zuhause**, **Abwesend**, **Entschärfen** und **Deaktivieren**.

- **Zuhause**: Schaltet das System scharf, wenn Sie sich im Bereich der Alarmanlage

befinden.

- **Abwesend**: Schaltet das System scharf, wenn Sie den Bereich der Alarmanlage verlassen.
- **Entschärfen**: Schaltet das Sicherheitssystem aus. Das Gegenteil von Scharfschalten.
- **Deaktivieren**: Schließen Sie den aktuellen Bildschirm.

5.2 Globale Scharf- und Unscharfschaltung

Voraussetzungen

Vergewissern Sie sich, dass Sie die Funktion "Globales **Scharfstellen/Entschärfen"** aktiviert haben. Wählen Sie auf dem Hub-Bildschirm > **Hub-Einstellung** und aktivieren Sie dann **Globale Scharf-/Entschärfung**.

Hintergrundinformationen

Sie können die Melder in allen Bereichen scharf- und unscharfschalten.

Verfahren

Schritt 1Gehen Sie zum Hub-Bildschirm.

Schritt 2Wählen Sie auf dem oberen Bildschirm zwischen **Zuhause**, **Abwesend** und **Entschärfen**.

5.3 Manuelles Scharf- und Unscharfschalten

Sie können das Sicherheitssystem über die DMSS-App oder den Schlüsselanhänger aktivieren.

- Zum Scharf- und Unscharfschalten der Melder in einem einzelnen Bereich oder in allen Bereichen, siehe " Einzelne Scharf- und Unscharfschaltung" und " Globale Scharf- und Unscharfschaltung" .
- Für die Bedienung über den Keyfob und das Keypad müssen Sie dem Keyfob und dem Keypad zunächst die Steuerberechtigungen der Bereiche zuweisen. Einzelheiten dazu finden Sie in der Bedienungsanleitung des entsprechenden Keys und Keypads.

5.4 Zeitgesteuerte Scharf- und Unscharfschaltung

Sie können einen Zeitplan für das Scharf- und Unscharfschalten von Meldern festlegen. Sie können Scharfschaltpläne konfigurieren, einschließlich Scharfschaltbereich, Modi und

Zeiträume.

Verfahren

Schritt 1 Wählen Sie auf dem Hub-Bildschirm > **Hub-Einstellung** > **Zeitgesteuertes Scharf-/Unscharfschalten**.

Schritt 2 Tippen Sie auf dem Bildschirm **Geplante Scharf-/Unscharfschaltung** auf **Hinzufügen** und konfigurieren Sie dann die Scharfschaltpläne.

- **Name**: Legen Sie einen Namen für die Scharfschaltpläne fest.
- **Bereich**: Wählen Sie einen oder mehrere Bereiche aus, die Sie scharfschalten möchten.
- **Befehlseinstellung**: Wählen Sie zwischen **Zuhause**, **Auswärts** und **Entschärfen**.
- **Zeit**: Stellen Sie eine Scharfschaltzeit ein.

  Um die Aktivierungszeit auf andere Tage zu übertragen, tippen Sie auf **Wiederholen** und wählen Sie die gewünschten Tage aus.
- **Erzwungene Scharfschaltung**: Nach Bedarf auswählen.

Anhang 1 Scharfschaltfehler-Ereignisse und Beschreibung

Anhang Tabelle 1-1 Scharfschaltfehler und Beschreibung (Peripheriegeräte)

Nein.	Grund	Beschreibung
1	ModulVerlust	Das Peripheriegerät war offline.
2	HeartError	Es wurden seit mehr als 18 Minuten keine Heartbeat-Pakete mehr gesendet.
3	Alarm	Alarm (24 Stunden).
4	Öffnen Sie	Die hintere Abdeckung des Geräts war geöffnet.
5	exOpen	Die hintere Abdeckung des externen Geräts war geöffnet.
6	Manipulation	Peripheriealarm für Manipulationen wurde ausgelöst.
7	LowBattery	Es wurde eine schwache Batterie des Geräts festgestellt.
8	PriPowerLoss	Es wurde ein Ausfall der peripheren Hauptstromversorgung festgestellt.
9	BatterieVerlust	Ein Batterieausfall wurde festgestellt.
10	ÜberSpannung	Es wurde eine Überspannung festgestellt.
11	Überstrom	Es wurde ein Überstrom festgestellt.
12	Überhitzung	Es wurde eine Überhitzung festgestellt.
13	Feueralarm	Der Feueralarm wurde ausgelöst.
14	MedicalAlarm	Medizinischer Alarm wurde ausgelöst.
15	SOS-Alarm	SOS-Alarm wurde ausgelöst.
16	PanicAlarm	Panikalarm wurde ausgelöst.
17	Gasalarm	Ein Gasleckalarm wurde ausgelöst.
18	IntrusionAlarm	Einbruchsalarm wurde ausgelöst.
19	HoldUpAlarm	Panikalarm wurde ausgelöst.

Anhang Tabelle 1-2 Scharfschalt-Fehlerereignisse und Beschreibung (Nabe)

Nein.	Grund	Beschreibung
1	SOSAlert	Der Panikalarm kann über die DMSS-App ausgelöst werden.

Nein.	Grund	Beschreibung
2	Manipulation	Der Manipulationsalarm der Alarmzentrale wurde ausgelöst.
3	Server-Verbindungsfehler	Der Hub war offline.
4	SIAServer Connect Fehler	Es liegt ein Fehler in der Verbindung zwischen dem Hub und der SIA-Alarmempfangszentrale vor.
5	LowBattery	Es wurde eine schwache Batterie festgestellt.
6	HauptVerlust	Es wurde ein Ausfall der Hauptstromversorgung festgestellt.
7	BatterieVerlust	Ein Batterieausfall wurde festgestellt.
8	NoGSM	Es wurden 2G/4G-Modulfehler festgestellt.
9	ATS-Störung	Es wurde ein Fehler im Alarmübertragungssystem festgestellt.
10	ATP-Fehler im Mobilfunknetz	Es wurde ein Fehler in der Alarmübertragungsstrecke (Ausfall des Mobilfunknetzes) festgestellt.
11	ATP-Fehler im kabelgebundenen Netzwerk/Wi-Fi	Es wurde ein Fehler in der Alarmübertragungsstrecke (Ausfall des Drahtlos- oder Wi-Fi-Netzwerks) festgestellt.
12	AP-Modus	Es wurde ein Fehler im AP-Modus festgestellt.

Anhang 2 SIA Event Codes und Beschreibung

Anhang Tabelle 2-1 SIA-Ereigniscodes und Beschreibung

Nein.	Veranstaltung	CID-Code	Beschreibung
1	Erkannte Bewegung	130	Einbruchsalarm.
		133	24-Stunden-Alarm (Safe).
		134	Alarm beim Betreten und Verlassen.
2	Öffnungsvorgang erkannt/Schließvorgang erkannt	130	Einbruchsalarm.
		133	24-Stunden-Alarm (Safe).
		134	Alarm beim Betreten und Verlassen.
3	Externer Kontakt wurde geöffnet/externer Kontakt wurde geschlossen	130	Einbruchsalarm.
		133	24-Stunden-Alarm (Safe).
		134	Alarm beim Betreten und Verlassen.
4	Bedrohungsalarm	121	Bedrohungsalarm.
5	Der Panikknopf wurde gedrückt	122	Panikalarm (stumm).
		123	Panik-Alarm (Unhaltbar).
6	Einbruchsalarm	130	Einbruchsalarm.
		133	24-Stunden-Alarm (Safe).
		134	Eingangs-/Ausgangsalarm.
7	Feueralarm	110	Feueralarm.
8	Gasleck entdeckt	151	Alarm bei Gaserkennung.
9	Taste für medizinischen Alarm wurde gedrückt	100	Medizinischer Alarm.
10	Überbrückungstaste wurde betätigt	122	Panikalarm (stumm).
		123	Panik-Alarm (Unhaltbar).
11	Glasbruch erkannt	130	Einbruchsalarm.
		133	24-Stunden-Alarm (Safe).
		134	Eingangs-/Ausgangsalarm.
12	Neigung erkannt	130	Einbruchsalarm.
		133	24-Stunden-Alarm (Safe).
		134	Eingangs-/Ausgangsalarm.

Nein.	Veranstaltung	CID-Code	Beschreibung
13	Schock erkannt	130	Einbruchsalarm.
		133	24-Stunden-Alarm (Safe).
		134	Alarm beim Betreten und Verlassen.
14	Tripwire-Alarm/ Tripwire-Alarm gestoppt	131	Perimeter-Alarm
15	Der Deckel des Bedienfelds wurde geöffnet/der Deckel des Bedienfelds wurde geschlossen	137	Manipulation.
16	Peripherer Deckel wurde geöffnet/peripherer Deckel wurde geschlossen	137	Sensormanipulation.
17	Externer Deckel wurde geöffnet/externer Deckel wurde geschlossen	137	Sensormanipulation.
18	Wasserleck entdeckt /Wasserleck gestoppt	154	Wasseraustritt.
19	Niedriger Batteriestand/Batteriestand wiederhergestellt	302	Schwache Systembatterie.
20	Batteriefehler/Batterie wiederhergestellt	311	Batterie fehlt/ist tot.
21	Ausfall der Hauptstromversorgung/ Wiederherstellung der Hauptstromversorgung	301	AC-Verlust.
22	RF-Störungen	344	RF-Empfänger Stauerkennung.
23	Alarmübertragungssystem defekt/repariert	350	Kommunikationsprobleme.

Nein.	Veranstaltung	CID-Code	Beschreibung
24	Alarmübertragungsweg:Drahtnetzwerk/Wi-Fi Fehler/Wiederhergestellt	350	Kommunikationsprobleme.
25	Alarmübertragungsweg: Zelluläres Netzwerk gestört/wiederhergestellt	350	Kommunikationsprobleme.
26	Peripherieverbindung verloren/Peripherieverbindung wiederhergestellt	355	Verlust der Aufsicht - RF.
27	Hub ist Offline/ Hub ist Online	356	Verlust der zentralen Abfrage
28	Peripheriegerät mit niedrigem Batteriestand/Peripheriegerät mit wiederhergestelltem Batteriestand	302	Schwache Systembatterie.
29	Peripherie-Batterie defekt/Peripherie-Batterie wiederhergestellt	311	Batterie fehlt/ist tot.
30	Peripherie-Hauptstromausfall/Peripherie-Hauptstrom wiederhergestellt	301	AC-Verlust.
31	RF-HD-Verbindung fehlgeschlagen/RF-HD-Verbindung wiederhergestellt	354	Versäumnis, das Ereignis mitzuteilen.
32	Gerät gesperrt und entriegelt	501	Zutrittsleser deaktivieren.
33	Überspannungsschutz ausgelöst/Überspannungsschutz wiederhergestellt	319	Überspannung der Stromversorgung.

Nein.	Veranstaltung	CID-Code	Beschreibung
34	Überstromschutz ausgelöst Überstromschutz wiederhergestellt	312	Überstrom in der Stromversorgung.
35	Überhitzungsschutz ausgelöst/Überhitzungsschutz wiederhergestellt	318	Überhitzung des Netzteils.
36	Hohe Temperatur/ Normale Temperatur	158	Hohe Temp.
37	Niedrige Temperatur/ Normale Temperatur	159	Niedrige Temperatur.
38	Bewaffnet	400 (App)	Öffnen/Schließen.
		401 (Tastenfeld)	O/C durch Benutzer.
		403 (Planmäßige Scharfschaltung)	Automatik O/C.
		407 (Schlüsselanhänger)	Ferngesteuertes Scharf-/Unscharfschalten.
		408	Schneller Arm.
		409	Schlüsselschalter O/C
39	Entschärft	400 (App)	Öffnen/Schließen.
		401 (Tastenfeld)	O/C durch Benutzer.
		403 (Planmäßige Scharfschaltung)	Automatik O/C.
		407 (Schlüsselanhänger)	Ferngesteuertes Scharf-/Unscharfschalten.
		409	Schlüsselschalter O/C
40	Home-Modus aktiviert	441	Bewaffneter STAY.
		442	Schlüsseltaster Armed STAY
41	Fehlgeschlagene Scharfschaltung	454 (Scharfschaltung fehlgeschlagen)	Schließen fehlgeschlagen.
		455 (Geplante Scharfschaltung fehlgeschlagen)	Automatische Scharfschaltung fehlgeschlagen.
		457 (Ausfall der Scharfschaltung der Ausstiegsverzögerung)	Fehler beim Beenden (Benutzer).

Nein.	Veranstaltung	CID-Code	Beschreibung
42	Mit Fehlern bewaffnet	450	Ausnahme O/C.
43	Vorübergehend deaktiviert/reaktivier t	502	Vorübergehend deaktiviert.
44	Vorübergehend deaktivierte Benachrichtigungen für den Deckel / Aktivierte Benachrichtigungen für den Deckel	503	Vorübergehend deaktiviert.
45	Testbericht wurde manuell ausgelöst	601	Manueller Auslösetestbericht.
46	Regelmäßiger Testbericht	602	Regelmäßiger Prüfbericht.

Anhang 3 Sicherheitsverpflichtung und Empfehlung

Dahua Vision Technology Co., Ltd. (im Folgenden als "Dahua" bezeichnet) misst der Cybersicherheit und dem Schutz der Privatsphäre große Bedeutung bei und investiert weiterhin spezielle Mittel, um das Sicherheitsbewusstsein und die Fähigkeiten der Dahua-Mitarbeiter umfassend zu verbessern und angemessene Sicherheit für Produkte zu gewährleisten. Dahua hat ein professionelles Sicherheitsteam eingerichtet, das den gesamten Lebenszyklus von Produktdesign, Entwicklung, Tests, Produktion, Lieferung und Wartung überwacht. Unter Einhaltung des Prinzips der Minimierung der Datenerfassung, der Minimierung von Diensten, des Verbots der Implantierung von Hintertüren und der Entfernung unnötiger und unsicherer Dienste (wie z. B. Telnet) führen Dahua-Produkte weiterhin innovative Sicherheitstechnologien ein und bemühen sich, die Fähigkeiten zur Gewährleistung der Produktsicherheit zu verbessern, indem sie den Benutzern weltweit Sicherheitsalarm- und 24/7-Reaktionsdienste für Sicherheitsvorfälle bieten, um die Sicherheitsrechte und -interessen der Benutzer besser zu schützen. Gleichzeitig ermutigt Dahua Benutzer, Partner, Lieferanten, Regierungsbehörden, Industrieorganisationen und unabhängige Forscher, potenzielle Risiken oder Schwachstellen, die auf Dahua-Geräten entdeckt wurden, an Dahua PSIRT zu melden. Die spezifischen Meldeverfahren finden Sie im Bereich Cybersicherheit auf der offiziellen Dahua-Website.

Die Produktsicherheit erfordert nicht nur die ständige Aufmerksamkeit und die Bemühungen der Hersteller in den Bereichen Forschung und Entwicklung, Produktion und Auslieferung, sondern auch die aktive Beteiligung der Benutzer, die dazu beitragen können, das Umfeld und die Methoden der Produktnutzung zu verbessern, um die Sicherheit der Produkte nach ihrer Verwendung besser zu gewährleisten. Aus diesem Grund empfehlen wir, dass die Benutzer das Gerät sicher verwenden, einschließlich, aber nicht beschränkt auf:

Kontoführung

1. **Verwenden Sie komplexe Passwörter**

   Bitte beachten Sie die folgenden Vorschläge zum Festlegen von Passwörtern:

   - Die Länge sollte nicht weniger als 8 Zeichen betragen;
   - Enthalten Sie mindestens zwei Arten von Zeichen: Groß- und Kleinbuchstaben, Zahlen und Symbole;
   - Enthalten Sie nicht den Kontonamen oder den Kontonamen in umgekehrter Reihenfolge;
   - Verwenden Sie keine fortlaufenden Zeichen, wie z. B. 123, abc usw.;
   - Verwenden Sie keine sich wiederholenden Zeichen, wie z. B. 111, aaa usw.

2. **Ändern Sie Passwörter regelmäßig**

Es wird empfohlen, das Gerätepasswort regelmäßig zu ändern, um das Risiko zu verringern, dass es erraten oder geknackt wird.

3. **Angemessene Zuweisung von Konten und Berechtigungen**
   Fügen Sie je nach Dienst- und Verwaltungsanforderungen Benutzer hinzu und weisen Sie den Benutzern Mindestberechtigungen zu.
4. **Aktivieren Sie die Kontosperrfunktion**
   Die Funktion zur Kontosperrung ist standardmäßig aktiviert. Es wird empfohlen, sie zum Schutz der Kontosicherheit aktiviert zu lassen. Nach mehreren fehlgeschlagenen Passwortversuchen werden das entsprechende Konto und die Quell-IP-Adresse gesperrt.
5. **Rechtzeitige Festlegung und Aktualisierung der Informationen zum Zurücksetzen des Passworts**
   Das Dahua-Gerät unterstützt die Funktion zum Zurücksetzen des Passworts. Um das Risiko zu verringern, dass diese Funktion von Bedrohungsakteuren genutzt wird, ändern Sie die Informationen bitte rechtzeitig, wenn sie sich ändern. Es wird empfohlen, beim Festlegen von Sicherheitsfragen keine leicht zu erratenden Antworten zu verwenden.

Dienst-Konfiguration

1. **Aktivieren Sie HTTPS**
   Es wird empfohlen, HTTPS zu aktivieren, um über sichere Kanäle auf Webdienste zuzugreifen.
2. **Verschlüsselte Übertragung von Audio und Video**
   Wenn Ihre Audio- und Videodaten sehr wichtig oder sensibel sind, empfehlen wir Ihnen, die verschlüsselte Übertragungsfunktion zu verwenden, um das Risiko zu verringern, dass Ihre Audio- und Videodaten während der Übertragung abgehört werden.
3. **Schalten Sie nicht benötigte Dienste aus und verwenden Sie den abgesicherten Modus**
   Falls nicht erforderlich, empfiehlt es sich, einige Dienste wie SSH, SNMP, SMTP, UPnP, AP-Hotspot usw. zu deaktivieren, um die Angriffsfläche zu verringern.
   Falls erforderlich, wird dringend empfohlen, sichere Modi zu wählen, einschließlich, aber nicht beschränkt auf die folgenden Dienste:
   - SNMP: Wählen Sie SNMP v3, und richten Sie starke Verschlüsselungs- und Authentifizierungskennwörter ein.
   - SMTP: Wählen Sie TLS für den Zugriff auf den Mailbox-Server.
   - FTP: Wählen Sie SFTP, und richten Sie komplexe Kennwörter ein.
   - AP-Hotspot: Wählen Sie den Verschlüsselungsmodus WPA2-PSK, und richten Sie komplexe Passwörter ein.
4. **Ändern Sie HTTP- und andere Standarddienstports**
   Es wird empfohlen, den Standard-Port von HTTP und anderen Diensten auf einen beliebigen Port zwischen 1024 und 65535 zu ändern, um das Risiko zu verringern, von Bedrohungsakteuren erraten zu werden.

Netzwerk-Konfiguration

1. **Aktivieren Sie Liste zulassen**
   Es wird empfohlen, die Funktion "Liste zulassen" zu aktivieren und nur den IP-Adressen in der Liste den Zugriff auf das Gerät zu erlauben. Stellen Sie daher sicher, dass Sie die IP-Adresse Ihres Computers und die IP-Adresse des unterstützenden Geräts in die Erlaubnisliste aufnehmen.
2. **MAC-Adressbindung**
   Es wird empfohlen, die IP-Adresse des Gateways an die MAC-Adresse des Geräts zu binden, um das Risiko von ARP-Spoofing zu verringern.
3. **Aufbau einer sicheren Netzwerkumgebung**
   Um die Sicherheit der Geräte besser zu gewährleisten und potenzielle Cyber-Risiken zu verringern, werden folgende Maßnahmen empfohlen:
   - Deaktivieren Sie die Port-Mapping-Funktion des Routers, um einen direkten Zugriff auf die Intranet-Geräte aus dem externen Netz zu vermeiden;
   - Partitionieren Sie das Netzwerk entsprechend den tatsächlichen Netzwerkanforderungen: Wenn kein Kommunikationsbedarf zwischen den beiden Teilnetzen besteht, empfiehlt es sich, das Netzwerk mithilfe von VLAN, Gateway und anderen Methoden zu partitionieren, um eine Netzwerkisolierung zu erreichen;
   - Einrichtung eines 802.1x-Zugangsauthentifizierungssystems, um das Risiko des illegalen Zugangs von Endgeräten zum privaten Netz zu verringern.

Sicherheitsprüfung

1. **Online-Nutzer überprüfen**
   Es wird empfohlen, Online-Nutzer regelmäßig zu überprüfen, um illegale Nutzer zu identifizieren.
2. **Geräteprotokoll prüfen**
   Anhand der Protokolle können Sie sich über die IP-Adressen informieren, die versuchen, sich beim Gerät anzumelden, sowie über die wichtigsten Vorgänge der angemeldeten Benutzer.
3. **Netzwerkprotokoll konfigurieren**
   Aufgrund der begrenzten Speicherkapazität der Geräte ist das gespeicherte Protokoll begrenzt. Wenn Sie das Protokoll über einen längeren Zeitraum speichern müssen, empfiehlt es sich, die Netzwerkprotokollfunktion zu aktivieren, um sicherzustellen, dass die kritischen Protokolle zur Nachverfolgung mit dem Netzwerkprotokollserver synchronisiert werden.

Software-Sicherheit

1. **Rechtzeitige Aktualisierung der Firmware**
   Gemäß den Industriestandard-Betriebsspezifikationen muss die Firmware von Geräten rechtzeitig auf die neueste Version aktualisiert werden, um sicherzustellen, dass das Gerät

über die neuesten Funktionen und die neueste Sicherheit verfügt. Wenn das Gerät mit dem öffentlichen Netz verbunden ist, wird empfohlen, die Funktion zur automatischen Erkennung von Online-Upgrades zu aktivieren, um die vom Hersteller freigegebenen Informationen zur Aktualisierung der Firmware rechtzeitig zu erhalten.

2. **Rechtzeitige Aktualisierung der Client-Software**
   Wir empfehlen Ihnen, die neueste Client-Software herunterzuladen und zu verwenden.

Physischer Schutz

Es wird empfohlen, Geräte (insbesondere Speichergeräte) physisch zu schützen, z. B. durch Unterbringung des Geräts in einem speziellen Maschinenraum und Schrank sowie durch Zugangskontrolle und Schlüsselverwaltung, um zu verhindern, dass unbefugtes Personal die Hardware und andere Peripheriegeräte (z. B. USB-Flash-Disk, serieller Anschluss) beschädigt.

ENABLING A SMARTER SOCIETY AND BETTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188