Zugangs-Controller mit Gesichtserkennung

Benutzerhandbuch

V1.0.0

Vorwort

Allgemein

Dieses Handbuch erläutert die Installation und die wesentlichen Funktionen des Zugangs-Controllers mit Gesichtserkennung (im Folgenden als „Zugangs-Controller“ bezeichnet).

Sicherheitshinweise

Die folgenden kategorisierten Signalwörter mit definierter Bedeutung können im Handbuch auftauchen.

Signalwörter	Bedeutung
HINWEIS	Bietet zusätzliche Informationen als Hervorhebung oder Ergänzung zum Text.

Änderungsverlauf

Version	Inhaltliche Überarbeitung	Veröffentlichungsdatum
V1.0.0	Erste Veröffentlichung.	Mai 2020

Über das Handbuch

- Das Handbuch dient nur der Veranschaulichung. Bei Unstimmigkeiten zwischen Handbuch und dem jeweiligen Produkt hat das jeweilige Produkt Vorrang.
- Wir haften nicht für Verluste durch den Betrieb verursacht werden, der nicht den Anweisungen im Handbuch entspricht.
- Das Handbuch wird gemäß den neuesten Gesetzen und Vorschriften des jeweiligen Lands aktualisiert. Weitere Informationen finden Sie in der gedruckten Anleitung, auf der beiliegenden CD-ROM, über den QR-Code oder auf unserer offiziellen Website. Bei Widersprüchen zwischen dem gedruckten Handbuch und der elektronischen Version hat die elektronische Version Vorrang.
- Änderungen des Designs und der Software vorbehalten. Produktaktualisierungen können zu Abweichungen zwischen dem jeweiligen Produkt selbst und dem Handbuch führen. Wenden Sie sich für neueste Programm und zusätzliche Unterlagen und den Kundendienst.
- Es können immer noch Abweichungen in den technischen Daten, Funktionen und der Beschreibung der Inbetriebnahme oder Druckfehler vorhanden sein. Bei Unklarheiten oder Streitigkeiten nehmen Sie Bezug auf unsere endgültige Erläuterung.
- Aktualisieren Sie die Reader-Software oder probieren Sie eine andere Mainstream-Readersoftware aus, wenn das Handbuch (im PDF-Format) nicht geöffnet werden kann.

- Alle eingetragenen Warenzeichen und Firmennamen im Handbuch sind Eigentum ihrer jeweiligen Besitzer.
- Wenn beim Einsatz des Geräts Probleme aufgetreten, besuchen Sie unsere Website oder wenden Sie sich und den Lieferanten bzw. Kundendienst.
- Bei Unklarheiten oder Widersprüchen konsultieren Sie unsere endgültige Erläuterung.

Wichtige Sicherheits- und Warnhinweise

In diesem Kapitel werden der korrekte Umgang mit dem Zugangs-Controller zur Gefahrenabwehr und Vermeidung von Sachschäden beschrieben. Lesen Sie diese Aneitungen vor der Inbetriebnahme des Zugangs-Controllers aufmerksam durch, halten Sie sie beim Gebrauch ein und bewahren Sie das Handbuch zum späteren Nachschlagen auf.

Betriebsanforderungen

- Installieren Sie den Zugangs-Controller nicht an einem Ort, an dem er direkter Sonneneinstrahlung ausgesetzt ist oder in unmittelbarer Nähe einer Wärmequelle.
- Schützen Sie den Zugangs-Controller vor Feuchtigkeit, Staub und Ruß.
- Halten Sie den Zugangs-Controller waagerecht an einem stabilen Ort installiert, um ein Herunterfallen zu verhindern.
- Lassen Sie keine Flüssigkeiten auf den Zugangs-Controller tropfen oder spritzen und stellen Sie keine mit Flüssigkeit gefüllten Gegenstände auf den Zugangs-Controller, damit keine Flüssigkeiten in ihn eindringen.
- Installieren Sie den Zugangs-Controller an einem gut belüfteten Ort und blockieren Sie nicht seine Lüftungsöffnungen.
- Betreiben Sie den Zugangs-Controller innerhalb des Nennbereichs der Leistungsaufnahme und -abgabe.
- Demontieren Sie den Zugangs-Controller nicht.
- Transportieren, verwenden und lagern Sie den Zugangs-Controller unter den zulässigen Luftfeuchtigkeits- und Temperaturbedingungen.
- Für Zugangs-Controller mit Temperaturüberwachung:
  - ◇ Installieren Sie die Temperaturüberwachungseinheit in einer windstillen Innenumgebung und halten Sie die Raumtemperatur auf 15 °C bis 32 °C.
  - ◇ Wärmen Sie die Temperaturüberwachungseinheit nach dem Einschalten für mehr als 20 Minuten auf, damit sie das thermische Gleichgewicht erreichen kann.

Elektrische Sicherheit

- Unsachgemäße Verwendung von Batterien kann zu Feuer, Explosion oder Entzündung führen.
- Achten Sie beim Austausch von Batterien stets darauf, das gleiche Modell zu verwenden.
- Verwenden Sie die empfohlenen Netzkabel und entsprechend der Nennleistung in Ihrem Land.
- Verwenden Sie das mit dem Zugangs-Controller mitgelieferte Netzteil, anderenfalls sind Verletzungen und Geräteschäden nicht auszuschließen.

- Die Spannungsversorgung muss den Anforderungen von SELV (Safety Extra Low Voltage) und der Nennspannungsversorgung der Stromquelle mit begrenzter Leistung gemäß IEC60950-1 entsprechen. Die genaue Spannungsversorgung entnehmen Sie dem Typenschild des Geräts.
- Schließen Sie das Gerät (I-Struktur) an einer Steckdose mit Schutzerdung an.
- Der Gerätestecker ist die Trennvorrichtung. Der Netzstecker muss für einfache Bedienung leicht zugänglich sein.

Inhaltsverzeichnis

1 Überblick

1.1 Beschreibung

Der Zugangs-Controller ist eine Zugangskontrollzentrale, die das Entriegeln durch Gesichter, Passwörter und Karten sowie Kombinationen davon unterstützt.

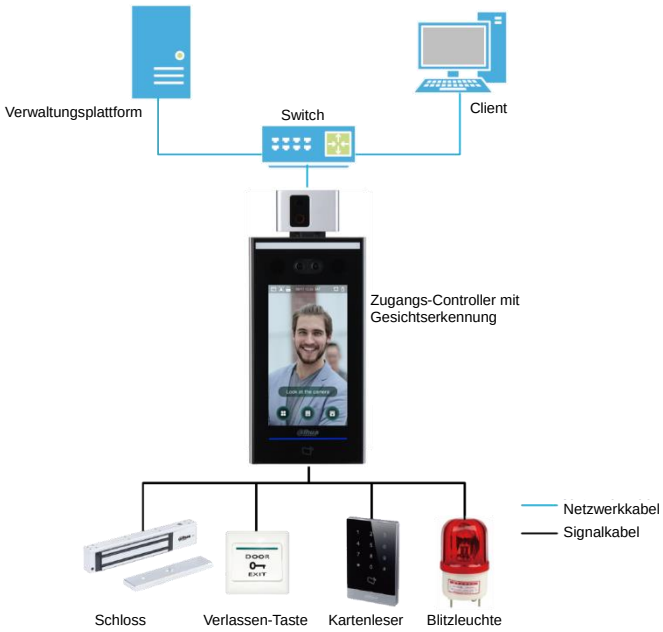
1.2 Schlüsselmerkmale

- LCD-Display, die Auflösung des 7-Zoll-Zugangs-Controllers beträgt 1024 × 600.
- Unterstützt Entriegelung durch Gesicht, IC-Karte und Passwort sowie nach Zeitraum
- Mit Gesichtserfassungsrahmen; das größte Gesicht unter den gleichzeitig erscheinenden Gesichtern wird zuerst erkannt; die maximale Gesichtsgröße kann im Internet konfiguriert werden
- 2-MP-Weitwinkel-WDR-Objektiv mit automatischer/manueller Ausleuchtung
- Mit dem Gesichtserkennungsalgorithmus kann der Zugangs-Controller mehr als 360 Positionen auf dem menschlichen Gesicht erkennen
- Genauigkeit der Gesichtsverifizierung >99,5 %; niedrige Falscherkennungsrate
- Profilerkennung unterstützt; der Profilwinkel beträgt 0° - 90°
- Unterstützt Lebenderkennung
- Unterstützt Nötigungsalarm, Sabotagealarm, Einbruchalarm, Zeitüberschreitungsalarm für Türkontakte und Alarm bei Überschreitung des Schwellenwerts für ungültige Karten
- Unterstützt allgemeine Benutzer, Patrouillen-Benutzer, Benutzer auf der Schwarzen Liste, VIP-Benutzer, Gast-Benutzer und spezielle Benutzer
- Verschiedene Anzeigemodi des Entriegelungsstatus schützen die Privatsphäre der Benutzer
- Unterstützt die Überwachung der Körpertemperatur durch eine periphere Temperaturüberwachungseinheit

1.3 Anwendung

Der Zugangs-Controller ist für Parks, Bürogebäude, Schulen, Fabriken, Wohngebiete und andere Orte geeignet. Die Identität wird durch Gesichtserkennung verifiziert, um einen Durchgang ohne Wahrnehmung zu erreichen.

Abbildung 1–1 Vernetzung



1.4 Abmessungen und Komponenten

Abbildung 1–2 Abmessungen und Komponenten des Modell X mit einer Temperaturüberwachungseinheit (mm [Zoll])

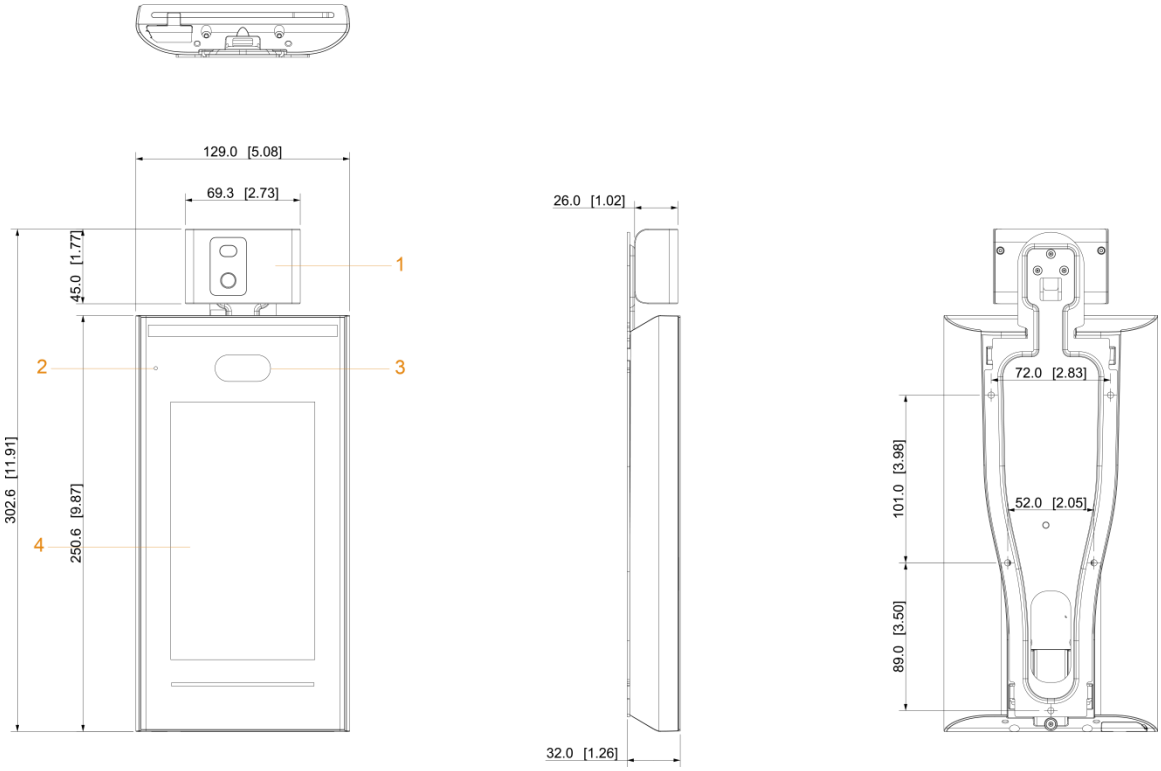


Tabelle 1–1 Beschreibung der Komponenten (3)

Nr.	Name	Nr.	Name
1	Temperaturüberwachungseinheit	3	Doppelkamera
2	Mikrofon	4	Anzeige

2 Anschluss und Installation

2.1 Kabelanschlüsse

Der Zugangs-Controller muss an Geräte wie Sirene, Lesegerät und Türkontakte angeschlossen werden. Zum Kabelanschluss siehe Tabelle 2–1.

Tabelle 2–1 Beschreibung der Ports

Port	Kabelfarbe	Name des Kabels	Beschreibung
CON1	Schwarz	RD-	Minus externer Kartenleser.
	Rot	RD+	Plus externer Kartenleser.
	Blau	GEHÄUSE	Sabotagealarmeingang externer Kartenleser.
	Weiß	D1	Wiegand D1-Eingang (angeschlossen an externem Kartenleser)/Ausgang (angeschlossen an Controller).
	Grün	D0	Wiegand D0-Eingang (angeschlossen an externem Kartenleser)/Ausgang (angeschlossen an Controller).
	Braun	LED	Angeschlossen an externer Eingangsanzeige des Lesegeräts
	Gelb	B	RS-485-Eingang Minus (angeschlossen an externem Kartenleser)/Ausgang (angeschlossen an Controller oder an Türsteuerungs-Sicherheitsmodul). Wenn das Sicherheitsmodul aktiviert ist, müssen Sie das Zugangskontroll-Sicherheitsmodul separat erwerben. Das Sicherheitsmodul benötigt eine separate Stromversorgung. Sobald das Sicherheitsmodul aktiviert ist, sind die Ausgangstaste, die Schlosssteuerung und die Feuerlöschverbindung ungültig.
	Violett	A	RS-485-Eingang Plus (angeschlossen an externem Kartenleser)/Ausgang (angeschlossen an Controller oder Türsteuerungs-Sicherheitsmodul). Wenn das Sicherheitsmodul aktiviert ist, müssen Sie das Zugangskontroll-Sicherheitsmodul separat erwerben. Das Sicherheitsmodul benötigt eine separate Stromversorgung. Sobald das Sicherheitsmodul aktiviert ist, sind die Ausgangstaste, die Schlosssteuerung und die Feuerlöschverbindung ungültig.

Port	Kabelfarbe	Name des Kabels	Beschreibung
CON2	Weiß und Rot	ALARM1_NO	Alarm 1 Arbeitskontakt-Ausgang.
	Weiß und Orange	ALARM1_COM	Alarm 1 gemeinsamer Ausgang.
	Weiß und Blau	ALARM2_NO	Alarm 2 Arbeitskontakt-Ausgang.
	Weiß und Grau	ALARM2_COM	Alarm 2 gemeinsamer Ausgang.
	Weiß und Grün	Masse	Angeschlossen an gemeinsamem Masseanschluss.
	Weiß und Braun	ALARM1	Alarm 1 Eingang.
	Weiß und Gelb	Masse	Angeschlossen an gemeinsamem Masseanschluss.
	Weiß und Violett	ALARM2	Alarm 2 Eingang.
CON3	Schwarz und Rot	RX	RS-232-Empfangs-Port.
	Schwarz und Orange	TX	RS-232-Sende-Port.
	Schwarz und Blau	Masse	Angeschlossen an gemeinsamem Masseanschluss.
	Schwarz und Grau	SR1	Zur Türkontakterkennung.
	Schwarz und Grün	PUSH1	Türöffner-Taste Tür 1
	Schwarz und Braun	DOOR1_COM	Gemeinsamer Anschluss Verriegelungssteuerung.
	Schwarz und Gelb	DOOR1_NO	Verriegelungssteuerung Arbeitskontakt-Anschluss.
	Schwarz und Violett	DOOR1_NC	Verriegelungssteuerung Ruhekontakt-Anschluss.

2.2 Hinweise zur Installation

- Wenn die Lichtquelle 0,5 Meter vom Zugangs-Controller entfernt ist, darf die Mindestbeleuchtung nicht weniger als 100 Lux betragen.
- Wir empfehlen, den Zugangs-Controller in Innenräumen zu installieren, mindestens 3 Meter von Fenstern und Türen und 2 Meter von Lichtquellen entfernt.
- Vermeiden Sie Gegenlicht und direkte Sonneneinstrahlung.

Anforderungen an die Umgebungsbeleuchtung

Abbildung 2–1 Anforderungen an die Umgebungsbeleuchtung

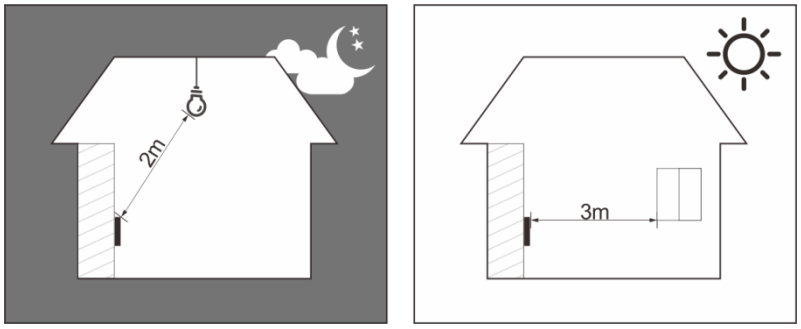
Kerze: 10 Lux Glühbirne: 100 Lux - 850 Lux Sonnenlicht: ≥1200 Lux

Anforderungen an die Temperaturüberwachung

- Wir empfehlen, die Temperaturüberwachungseinheit in einer windstillen Innenumgebung (ein relativ isolierter Bereich vom Außenbereich) zu installieren und die Umgebungstemperatur auf 15 °C bis 32 °C zu halten.
- Wärmen Sie die Temperaturüberwachungseinheit nach dem Einschalten für mehr als 20 Minuten auf, damit sie das thermische Gleichgewicht erreichen kann.
- Wenn es keine geeignete Innenumgebung gibt (einschließlich Bereiche, die direkt zu Innen- und Außenbereichen und Außentüren führen), richten Sie einen vorübergehenden Durchgang mit stabiler Umgebungstemperatur zur Temperaturüberwachung ein.
- Faktoren wie Sonnenlicht, Wind, Kaltluft sowie kalte und warme Luft aus Klimaanlagen können leicht die Hauttemperatur des menschlichen Körpers und den Betriebszustand des Zugangs-Controllers beeinflussen, wodurch eine Temperaturabweichung zwischen der überwachten Temperatur und der tatsächlichen Temperatur verursacht wird.
- Einflussfaktoren der Temperaturüberwachung
  - ◇ Wind: Der Wind führt die Wärme von der Stirn ab, wodurch die Genauigkeit der Temperaturüberwachung beeinträchtigt wird.
  - ◇ Schwitzen: Schwitzen ist eine Möglichkeit für den Körper, sich automatisch abzukühlen und Wärme abzuleiten. Wenn der Körper schwitzt, sinkt auch die Temperatur.
  - ◇ Raumtemperatur: Wenn die Raumtemperatur niedrig ist, sinkt die Oberflächentemperatur des menschlichen Körpers. Ist die Raumtemperatur zu hoch, beginnt der menschliche Körper zu schwitzen, was die Genauigkeit der Temperaturüberwachung beeinträchtigt.
  - ◇ Die Temperaturüberwachungseinheit ist empfindlich für Lichtwellen mit einer Wellenlänge von 10 µm bis 15 µm. Vermeiden Sie die Verwendung in der Sonne, fluoreszierende Lichtquellen, Auslässe von Klimaanlagen, Heizungen, Kaltluftauslässe und Glasflächen.

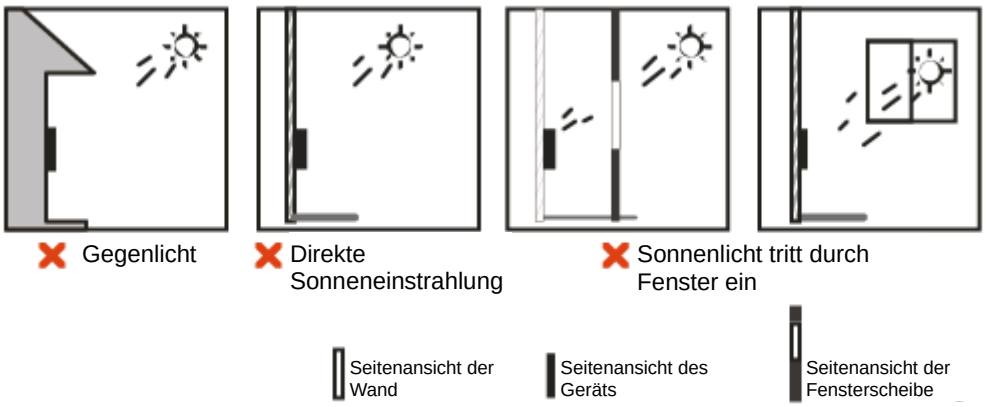
Empfohlene Orte

Abbildung 2–2 Empfohlene Orte



Nicht empfohlene Orte

Abbildung 2–3 Nicht empfohlene Orte



2.3 Installation

Achten Sie darauf, dass der Abstand zwischen der Kamera und dem Boden 1,4 m beträgt.

Abbildung 2–4 Installationshöhe

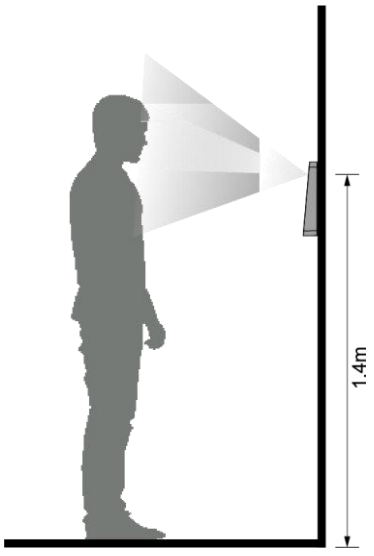
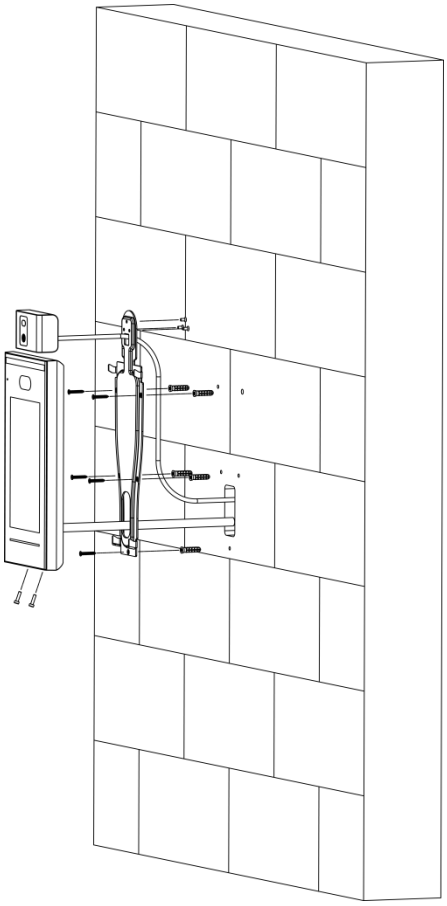


Abbildung 2–5 Montageschema



Installationsmethode

Schritt 1: Befestigen Sie die Temperaturüberwachungseinheit mit 3 Schrauben an der Halterung.

Schritt 2: Bohren Sie sechs Löcher (fünf Montagelöcher für die Halterung und eine Kabeldurchführung) in die Wand entsprechend den Löchern in der Halterung.

Schritt 3: Befestigen Sie die Halterung an der Wand, indem Sie die Dübel in den sechs Montagelöchern der Halterung anbringen.

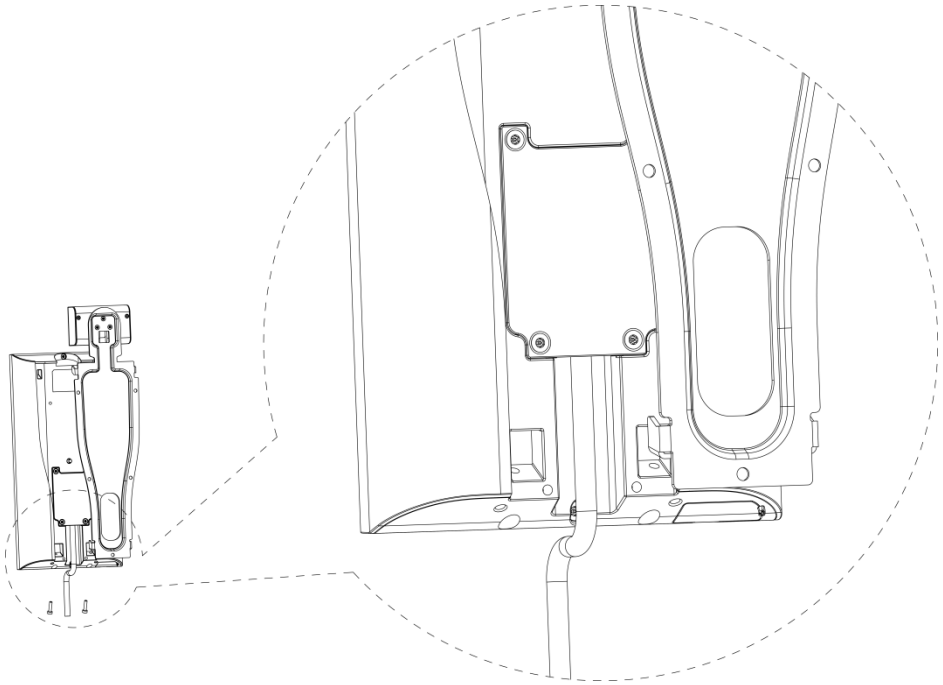
Schritt 4: Schließen Sie die Kabel für den Zugangs-Controller an. Siehe „2.1 Kabelanschlüsse“.

Schritt 5: Hängen Sie den Zugangs-Controller an den Haken der Halterung.

Schritt 6: Ziehen Sie die Schrauben an der Unterseite des Zugangs-Controllers fest.

Schritt 7: Bringen Sie am Kabelausgang des Zugangs-Controllers Silikondichtmittel auf.

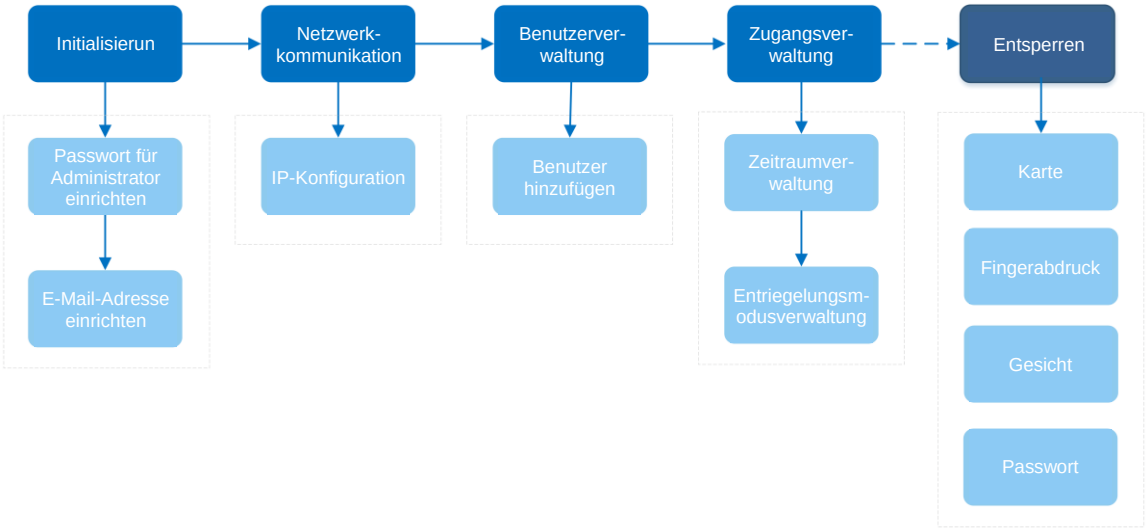
Abbildung 2–6 Silikondichtmittel aufbringen



3 Systembetrieb

3.1 Allgemeine Konfigurationsmethode

Abbildung 3–1 Allgemeine Konfigurationsmethode



3.2 Verwendete Symbole

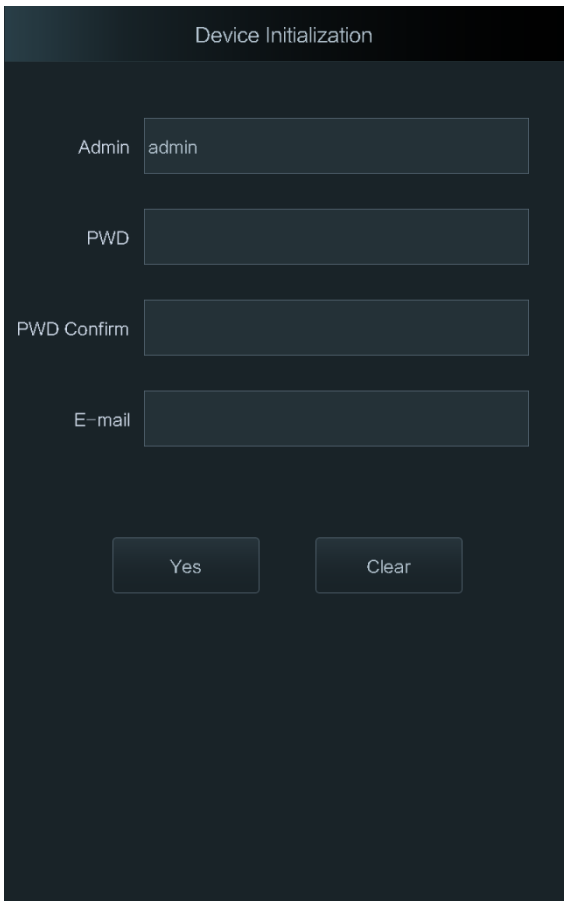
Tabelle 3–1 Beschreibung der Symbole

Symbol	Beschreibung
	Hauptmenü-Symbol.
	Bestätigungs-Symbol.
	Zur ersten Seite der Liste wechseln.
	Zur letzten Seite der Liste wechseln.
	Zur vorherigen Seite der Liste wechseln.
	Zur nächsten Seite der Liste wechseln.
	Zum vorherigen Menü zurückkehren.
	Aktivieren.
	Deaktiv.

3.3 Initialisierung

Beim ersten Einschalten des Zugangs-Controllers oder nach einer Rücksetzung muss ein Administrator-Passwort und eine E-Mail-Adresse eingerichtet werden, sonst kann der Zugangs-Controller nicht verwendet werden.

Abbildung 3–2 Initialisierung



- Administrator und Passwort, die auf diesem Menü eingerichtet werden, dienen zum Anmelden bei der Web-Management-Plattform.
- Das Administrator-Passwort kann über die eingegebene E-Mail-Adresse zurückgesetzt werden, falls der Administrator das Passwort vergisst.
- Das Passwort muss aus 8 bis 32 nicht leeren Zeichen bestehen und mindestens zwei Arten von Zeichen von Groß- und Kleinschreibung, Ziffer und Sonderzeichen enthalten (außer ' " ; : &).

3.4 Standby-Menü

Sie können die Tür durch Gesichter, Passwörter und Karten entriegeln. Siehe Abbildung 3–3.

- Wenn es innerhalb von 30 Sekunden keinen Betriebsvorgang gibt, wechselt der Zugangs-Controller in den Standby-Modus.
- Das Standby-Menü kann je nach Version variieren und das tatsächliche Menü ist maßgebend.

Abbildung 3–3 Startseite

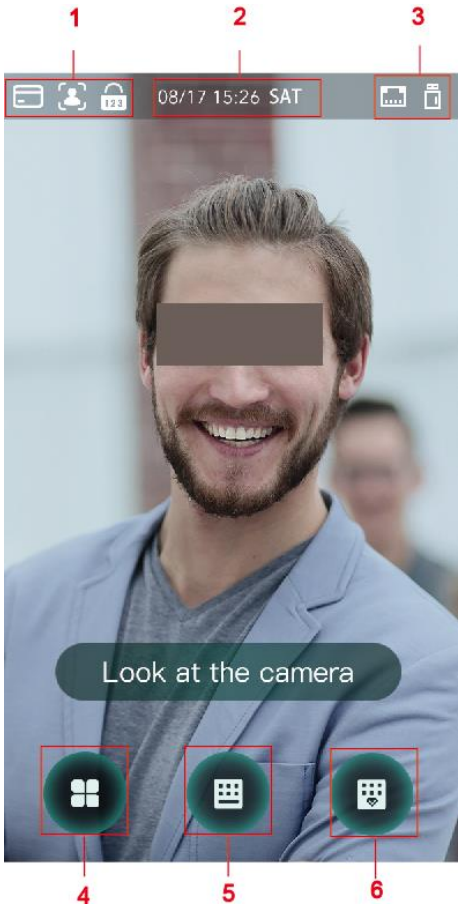


Tabelle 3–2 Beschreibung der Startseite

Nr.	Beschreibung
1	Entriegelungsmethoden: Karte, Gesicht und Passwort. Wenn Karte, Gesicht und Passwort als Entriegelungsmodus eingestellt sind, wird das Passwortsymbol in der linken oberen Ecke des Zugangs-Controllers nicht angezeigt.
2	Datum und Zeit. Zeigt das aktuelle Datum und die Uhrzeit an.
3	Zeigt den Netzwerkstatus und den USB-Status an.
4	Hauptmenü-Symbol. Nur Benutzer mit Administrator-Berechtigung können das Hauptmenü aufrufen.
5	Symbol zum Entsperren des Passworts.
6	Symbol zum Entsperren des Administrator-Passworts.

3.5 Hauptmenü

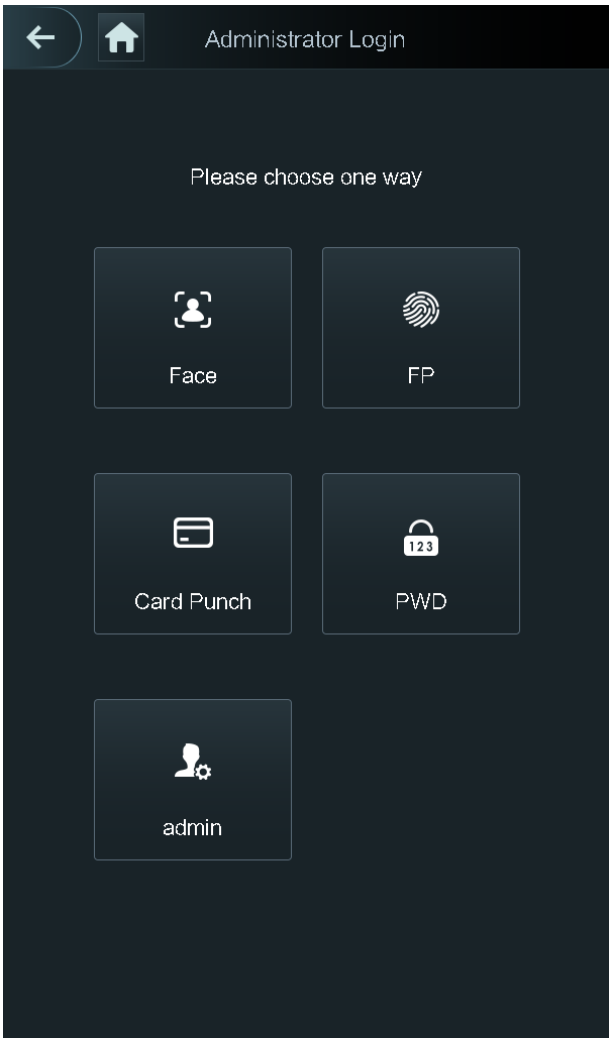
Administratoren können im Hauptmenü Benutzer verschiedener Ebenen hinzufügen, Zugangsparameter einstellen, Netzwerkkonfigurationen vornehmen, Zugangsdaten und Systemdaten anzeigen und vieles mehr.

Schritt 1: Tippen Sie im Standby-Menü auf  .

Schritt 2: Wählen Sie eine Eingabemethode für das Hauptmenü.

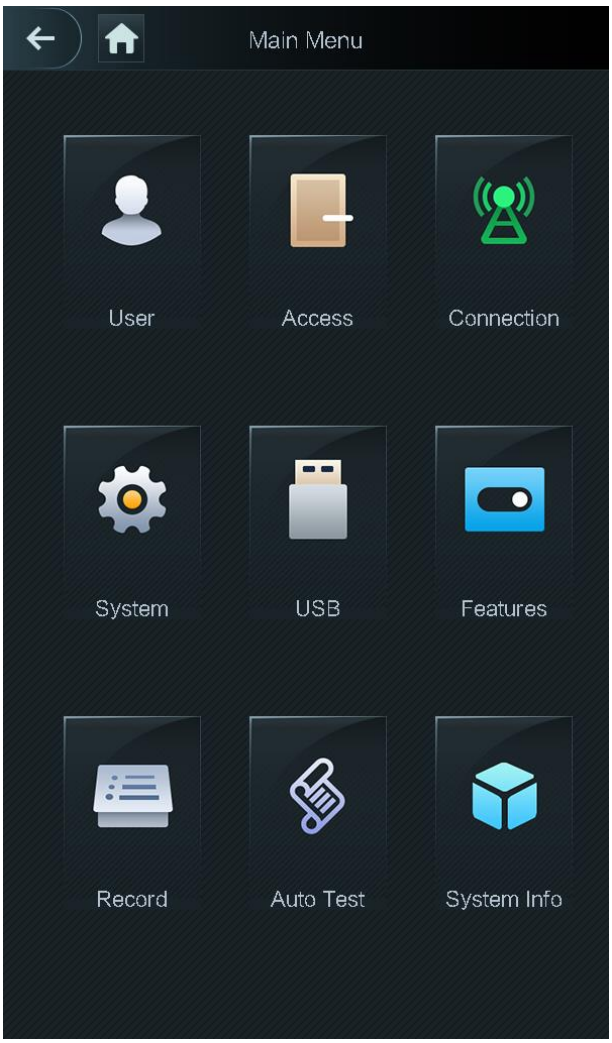
Verschiedene Modi unterstützen unterschiedliche Entriegelungsmethoden und das jeweilige Menü ist maßgebend.

Abbildung 3–4 Administrator-Anmeldung



Das Hauptmenü wird angezeigt.

Abbildung 3–5 Hauptmenü



3.6 Entriegelungsmethoden

Sie können die Tür durch Gesichter, Passwörter und Karten entriegeln.

3.6.1 Karten

Halten Sie die Karte an den Durchziehbereich, um die Tür zu entriegeln.

3.6.2 Gesicht

Achten Sie darauf, dass Ihr Gesicht mittig im Rahmen der Gesichtserkennung liegt, um die Tür zu entriegeln.

3.6.3 Benutzerpasswort

Geben Sie das Benutzerpasswort ein, um die Tür zu entriegeln.

Schritt 1: Tippen Sie auf der Startseite auf  .

Schritt 2: Geben Sie die Benutzer-ID ein und tippen Sie auf ☑.

Schritt 3: Geben Sie das Benutzerpasswort ein und tippen Sie auf ☑.

Die Tür wird entriegelt.

3.6.4 Administrator-Passwort

Geben Sie das Administrator-Passwort ein, um die Tür zu entriegeln. Es gibt nur ein Administrator-Passwort für einen Zugangs-Controller. Das Administrator-Passwort kann die Tür entriegeln, ohne dass es von Benutzerebenen, Entsperrmodi, Zeiträumen, Urlaubsplänen und Anti-Durchschlüpfen abhängig ist.

Das Administrator-Passwort kann nicht verwendet werden, wenn NC als „3.8.1.5 NC-Zeitraum“ gewählt ist.

Schritt 1: Tippen Sie auf der Startseite auf  .

Schritt 2: Tippen Sie auf **Bitte Administrator-Passwort eingeben** (Please Enter Administrator PWD).

Schritt 3: Geben Sie das Administrator-Passwort ein und tippen Sie auf ☑.

Die Tür wird entriegelt.

3.7 Benutzerverwaltung

Sie können neue Benutzer hinzufügen, Benutzerlisten und Administrator-Listen anzeigen und das Administrator-Passwort im Menü **Benutzer** (User) ändern.

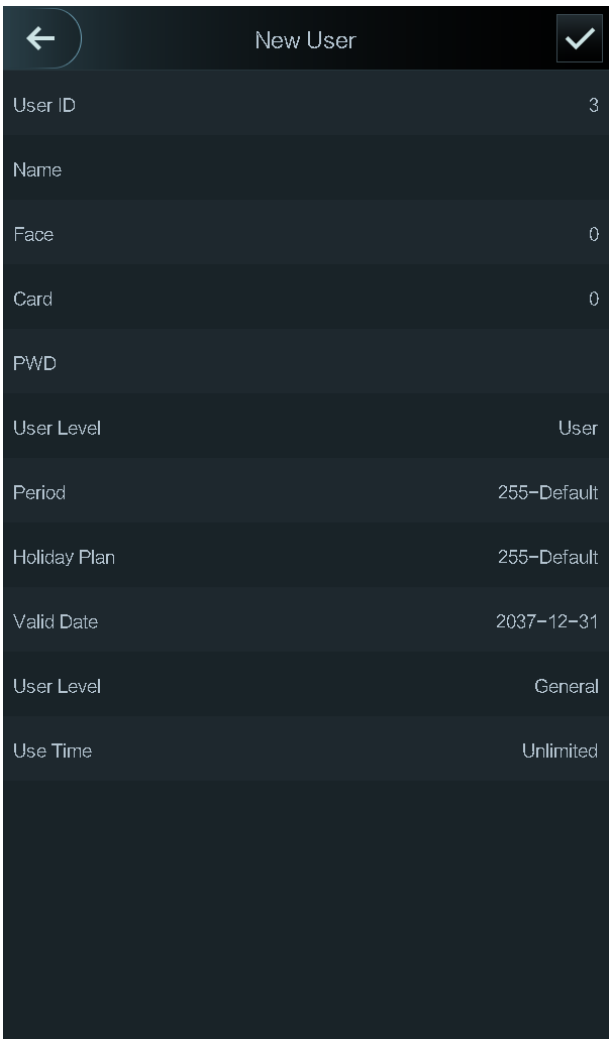
3.7.1 Neue Benutzer hinzufügen

Sie können neue Benutzer hinzufügen, indem Sie Benutzer-IDs, Namen, Gesichtsbilder, Karten oder Passwörter eingeben, Benutzerebenen wählen und vieles mehr.

Die folgenden Abbildungen dienen nur als Referenz und das tatsächliche Menü ist maßgebend.

Schritt 1: Wählen Sie **Benutzer > Neuer Benutzer** (User > New User).

Abbildung 3–6 Neue Benutzerdaten



Schritt 2: Konfigurieren Sie die Parameter im Menü.

Tabelle 3–3 Beschreibung neue Benutzerparameter

Parameter	Beschreibung
Benutzer-ID	Geben Sie Benutzer-IDs ein. Die IDs können Zahlen, Buchstaben und deren Kombinationen sein, und die maximale Länge der ID beträgt 32 Zeichen. Jede ID ist eindeutig.
Name	Geben Sie Namen mit maximal 32 Zeichen ein (einschließlich Zahlen, Symbolen und Buchstaben).
Gesicht	Achten Sie darauf, dass Ihr Gesicht in der Mitte des Bildaufnahmerahmens liegt, damit fotografiert der Zugangs-Controller das Gesicht des neuen Benutzers automatisch.
Karte	Sie können maximal fünf Karten je Benutzer registrieren. Geben Sie im Kartenregistrierungsmenü Ihre Kartennummer ein oder ziehen Sie Ihre Karte durch, dann werden die Kartendaten vom Zugangs-Controller gelesen. Sie können die Funktion **Nötigungskarte** (Duress Card) im Kartenregistrierungsmenü aktivieren. Wenn eine Nötigungskarte zum Entriegeln der Tür verwendet wird, werden Alarme ausgelöst. Nur bestimmte Modelle unterstützen die Entriegelung durch Karte.

Parameter	Beschreibung
PWD	Das Passwort zur Türentriegelung. Die maximale Länge des Passworts ist 8-stellig. Wenn der Zugangs-Controller keinen Touchscreen hat, müssen Sie ihn an einem peripheren Kartenleser anschließen. Auf dem Kartenleser befinden sich Tasten.
Benutzerebene	Sie können eine Benutzerebene für neue Benutzer wählen. Es gibt zwei Optionen: ● Benutzer: Benutzer haben nur die Berechtigung zum Entriegeln von Türen. ● Admin: Administratoren können die Tür entriegeln und haben außerdem die Berechtigung zur Konfiguration von Parametern. Unabhängig davon, ob es im Zugangs-Controller einen Administrator gibt, ist eine Authentifizierung der Administratoridentität erforderlich.
Zeitraum	Sie können einen Zeitraum festlegen, in dem der Benutzer die Tür entriegeln kann.
Urlaubsplan	Sie können einen Urlaubsplan festlegen, in dem der Benutzer die Tür entriegeln kann.
Gültiges Datum	Sie können einen Zeitraum festlegen, in dem die Daten des Benutzers zur Entriegelung gültig sind.
Benutzerebene	Es gibt sechs Ebenen: ● Allgemein: Allgemeine Benutzer können die Tür normal entriegeln. ● Blacklist: Wenn Benutzer auf der schwarzen Liste die Tür entriegeln, erhält das Dienstpersonal eine Meldung. ● Gast: Gäste dürfen die Tür zu bestimmten Zeiten entriegeln. Sobald sie die maximale Anzahl überschritten haben, können sie die Tür nicht mehr entriegeln. ● Streife: Patrouillierende Benutzer können ihre Anwesenheit verfolgen lassen, haben aber keine Berechtigung zum Entriegeln. ● VIP: Wenn ein VIP die Tür entriegelt, erhält das Dienstpersonal eine Meldung. ● Spezial: Wenn spezielle Personen die Tür entriegeln, gibt es eine Verzögerung von 5 Sekunden, bevor sich die Tür schließt.
Anwendungszeit	Wenn die Benutzerebene Gast ist, können Sie die maximale Anzahl der Entriegelungen festlegen, die der Benutzer vornehmen darf.

Schritt 3: Tippen Sie auf , um die Konfiguration zu speichern.

3.7.2 Benutzerdaten anzeigen

Sie können die Benutzerliste, die Administrator-Liste und das Administrator-Passwort über das Benutzermenü anzeigen.

3.8 Zugangsverwaltung

Sie können die Zugangsverwaltung nach Zeitraum, Entsperrmodus, Alarm, Türstatus und Schlosshaltezeit durchführen.

Tippen Sie auf **Zugang** (Access) um das Zugangsverwaltungsmenü aufzurufen.

3.8.1 Zeitraumverwaltung

Sie können Zeiträume, Urlaubszeiträume, Urlaubsplanzeiträume, Zeiträume, in denen die Tür normalerweise entriegelbar ist, Zeiträume, in denen die Tür normalerweise verriegelt ist und Fernüberprüfungszeiträume festlegen.

3.8.1.1 Zeitraumkonfiguration

Sie können 128 Zeiträume (Wochen) konfigurieren, deren Nummernbereich 0 - 127 ist. Sie können vier Zeiträume für jeden Tag eines Zeitraums (einer Woche) einrichten. Die Benutzer können die Tür nur in den von Ihnen eingerichteten Zeiträumen entriegeln.

3.8.1.2 Urlaubsgruppe

Sie können Gruppenurlaub einstellen und dann Pläne für Urlaubsgruppen festlegen. Sie können 128 Gruppen konfigurieren, deren Nummernbereich 0 - 127 ist. Sie können 16 Feiertage zu einer Gruppe hinzufügen. Konfigurieren Sie die Startzeit und die Endzeit einer Urlaubsgruppe, dann können Benutzer die Tür nur in den von Ihnen festgelegten Zeiträumen entriegeln.

Sie können Namen mit 32 Zeichen eingeben (Zahlen, Symbole und Buchstaben). Tippen Sie auf  , um den Urlaubsgruppennamen zu speichern.

3.8.1.3 Urlaubsplan

Sie können Urlaubsgruppen zu Urlaubsplänen hinzufügen. Sie können Urlaubspläne verwenden, um die Zugangsberechtigung der Benutzer in verschiedenen Urlaubsgruppen zu verwalten. Benutzer können die Tür nur in dem von Ihnen festgelegten Zeitraum entriegeln.

3.8.1.4 NO-Zeitraum

Wenn ein Zeitraum zum NO-Zeitraum hinzugefügt wird, ist die Tür in diesem Zeitraum normalerweise offen.

Die Berechtigungen für den NO/NC-Zeitraum sind höher als Berechtigungen in anderen Zeiträumen.

3.8.1.5 NC-Zeitraum

Wenn dem NC-Zeitraum ein Zeitraum hinzugefügt wird, dann ist die Tür normalerweise in diesem Zeitraum geschlossen. Der Benutzer kann die Tür in diesem Zeitraum nicht entriegeln.

3.8.1.6 Zeitraum der Fernverifizierung

Wenn Sie den Zeitraum für die Fernverifizierung konfiguriert haben, ist eine Fernverifizierung erforderlich, wenn die Türen während des von Ihnen konfigurierten Zeitraums entriegelt werden. Um die Tür in diesem Zeitraum zu entriegeln, ist eine von der Verwaltungsplattform gesendete Türentriegelungsanweisung erforderlich.

Sie müssen den Zeitraum für die Fernverifizierung aktivieren.

- 

bedeutet aktiviert.
- 

bedeutet nicht aktiviert.

3.8.2 Entsperren

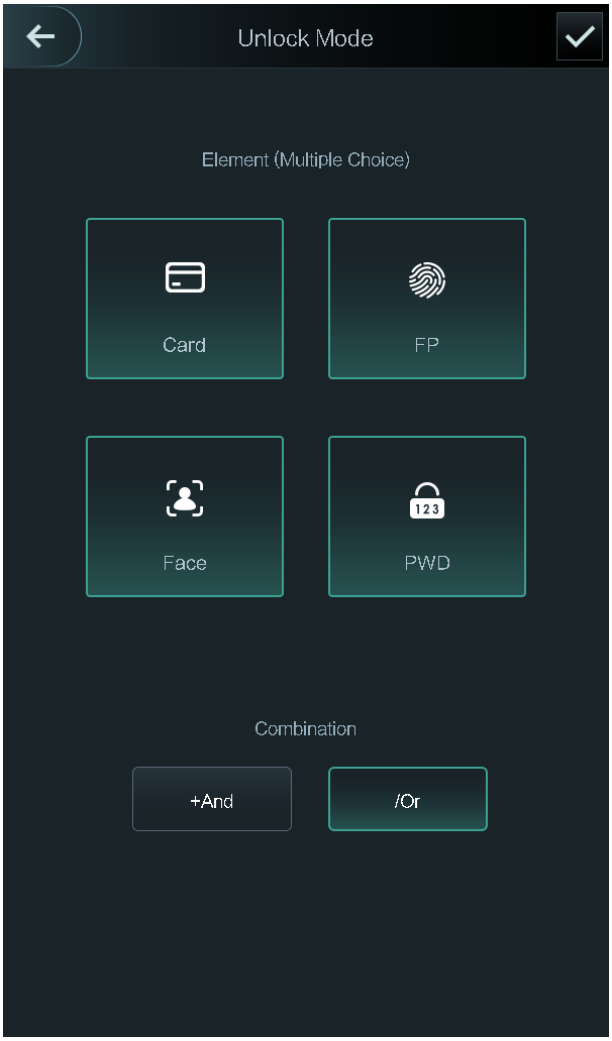
Es gibt drei Entriegelungsmodi: Entriegelungsmodus, Entriegelung nach Zeitraum und Gruppenkombination. Die Entriegelungsmodi variieren je nach Controller-Zugangsmodell und der tatsächliche Controller-Zugang ist maßgebend.

3.8.2.1 Entriegelungsmodus

Wenn der **Entriegelungsmodus** (Unlock Mode) aktiviert ist, können Benutzer mit Karten, Gesichtern, Passwörtern oder einer beliebigen anderen Methode entriegeln.

Schritt 1: Wählen Sie **Zugang > Entriegelungsmodus > Entriegelungsmodus** (Access > Unlock Mode > Unlock Mode).

Abbildung 3–7 Element (Mehrfachauswahl)



Schritt 2: Wählen Sie den Entriegelungsmodus.

Tippen Sie erneut auf einen gewählten Entriegelungsmodus, damit wird der Entriegelungsmodus gelöscht.

Schritt 3: Wählen Sie einen Kombinationsmodus.

- **+ Und** (+ And) bedeutet „und“. Wenn Sie beispielsweise Karte + PWD wählen, bedeutet dies, dass Sie zum Entriegeln der Tür zuerst Ihre Karte durchziehen und dann das Passwort eingeben müssen.
- ***/* Oder** (/ Or) bedeutet „oder“. Wenn Sie beispielsweise Karte/PWD wählen, bedeutet dies, dass Sie, um die Tür zu entriegeln, entweder Ihre Karte durchziehen oder das Passwort eingeben müssen.

Schritt 4: Tippen Sie auf , um die Einstellungen zu speichern.

Dann wird das Menü **Entriegelungsmodus** (Unlock Mode) angezeigt.

Schritt 5: Aktivieren Sie den Entriegelungsmodus.

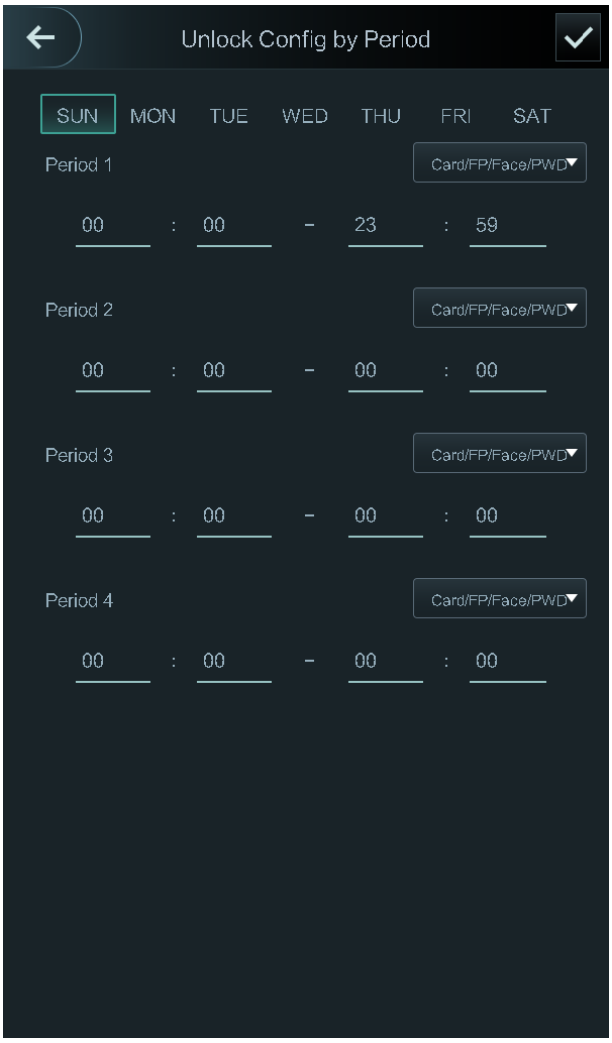
- ON bedeutet aktiviert.
- OFF bedeutet nicht aktiviert.

3.8.2.2 Nach Zeitraum entriegeln

Die Türen können in verschiedenen Zeiträumen durch verschiedene Modi entriegelt werden. Zum Beispiel kann in Zeitraum 1 die Tür nur durch Karten entriegelt werden und in Zeitraum 2 können Türen nur durch Gesichter verriegelt werden.

Schritt 1: Wählen Sie **Zugang > Entriegelungsmodus > Nach Zeitraum entriegeln** (Access > Unlock Mode > Unlock by Period).

Abbildung 3–8 Nach Zeitraum entriegeln



Schritt 2: Stellen Sie Startzeit und Endzeit für einen Zeitraum ein und wählen Sie einen Entriegelungsmodus.

Schritt 3: Tippen Sie auf  , um die Einstellungen zu speichern.

Das Menü **Entriegelungsmodus** (Unlock Mode) wird angezeigt.

Schritt 4: Aktivieren Sie die Entriegelungsfunktion nach Zeitraum.

- 

bedeutet aktiviert.
- 

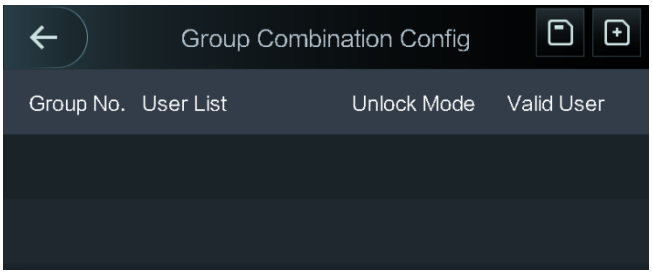
bedeutet nicht aktiviert.

3.8.2.3 Gruppenkombination

Türen können nur dann von einer Gruppe oder Gruppen, die aus mehr als zwei Benutzern bestehen, entriegelt werden, wenn die Gruppenkombination aktiviert ist.

Schritt 1: Wählen Sie **Zugang > Entriegelungsmodus > Gruppenkombination** (Access > Unlock Mode > Group Combination).

Abbildung 3–9 Gruppenkombination



Schritt 2: Tippen Sie zum Erstellen einer Gruppe auf .

Abbildung 3–10 Gruppe hinzufügen

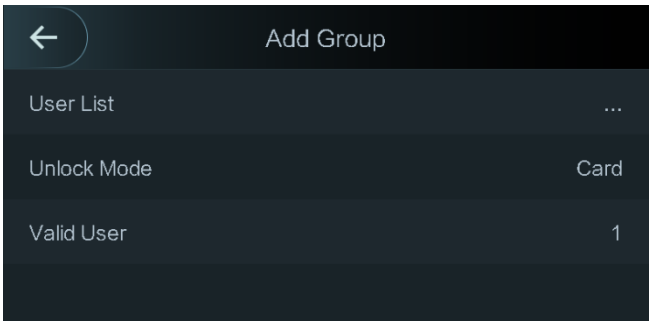


Tabelle 3–4 Gruppenparameter

Parameter	Beschreibung
Benutzerliste	Fügen Sie der neu erstellten Gruppe Benutzer hinzu. 1. Tippen Sie auf **Benutzerliste** (User List). Das Menü **Benutzerliste** (User List) wird angezeigt. 2. Tippen Sie auf und geben Sie eine Benutzer-ID ein. 3. Tippen Sie auf , um die Einstellungen zu speichern.
Entriegelungsmodus	Hier haben Sie drei Optionen: **Karte** (Card), **Passwort** (PWD) und **Gesicht** (Face).

Parameter	Beschreibung
Gültiger Benutzer	Gültige Benutzer sind diejenigen, die die Berechtigung zum Entriegeln haben. Türen können nur dann entriegelt werden, wenn die Anzahl der Benutzer, die die Türen entriegeln können, mit der gültigen Anzahl der Benutzer übereinstimmt. ● Gültige Benutzer können die Gesamtzahl der Benutzer in einer Gruppe nicht überschreiten. ● Wenn die Anzahl der gültigen Benutzer der Gesamtzahl der Benutzer in einer Gruppe entspricht, können Türen nur von allen Benutzern in der Gruppe entriegelt werden. ● Wenn die Anzahl der gültigen Benutzer kleiner als die Gesamtzahl der Benutzer in einer Gruppe ist, können Türen von allen Benutzern entriegelt werden, deren Anzahl gleich der Anzahl der gültigen Benutzer ist.

Schritt 3: Tippen Sie auf , um in das vorherige Menü zurückzukehren.

Schritt 4: Tippen Sie auf , um die Einstellungen zu speichern.

Schritt 5: Aktivieren Sie die **Gruppenkombination** (Group Combination).

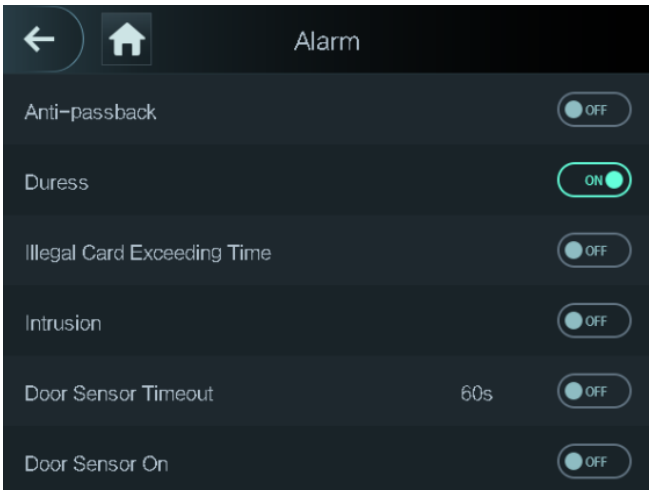
- bedeutet aktiviert.
- bedeutet nicht aktiviert.

3.8.3 Alarmkonfiguration

Administratoren können die Entriegelungsberechtigung von Besuchern über die Alarmkonfiguration verwalten.

Wählen Sie **Zugang > Alarm** (Access > Alarm). Das Fenster Alarm wird angezeigt.

Abbildung 3–11 Alarm



- bedeutet aktiviert.
- bedeutet nicht aktiviert.

Tabelle 3–5 Parameter im Alarmmenü

Parameter	Beschreibung
Anti-Durchschlüpfen	Nachdem die Funktion Anti-Durchschlüpfen aktiviert wurde, müssen Benutzer die Identität sowohl für den Ein- als auch für den Ausgang verifizieren, anderenfalls wird ein Alarm ausgelöst. ● Wenn eine Person mit verifizierter Identität eintritt und ohne verifizierte Identität austritt, wird ein Alarm ausgelöst, wenn die Person erneut versucht, einzutreten und die Person hat keine Berechtigung mehr, die Tür zu entriegeln. ● Wenn eine Person ohne Identitätsprüfung eintritt, wird ein Alarm ausgelöst, wenn die Person versucht, die Tür mit der geprüften Identität wieder zu verlassen und die Person hat keine Berechtigung mehr, die Tür zu entriegeln.
Nötigung	Ein Alarm wird ausgelöst, wenn eine Nötigungskarte oder ein Nötigungspasswort verwendet wird, um die Tür zu entriegeln.
Unzulässige Zeitüberschreitung der Karte	Nachdem die Tür mit einer unberechtigten Karte mehr als 5 Mal innerhalb von 50 Sekunden versucht wurde zu entriegeln, wird ein Alarm ausgelöst.
Einbruch	Ein Einbruchalarm wird ausgelöst, wenn eine Tür entriegelt wird, ohne dass der Türkontakt freigegeben wird.
Zeitüberschreitung des Türsensors	Ein Zeitüberschreitungsalarm wird ausgelöst, wenn die Zeit, die ein Benutzer benötigt, um die Tür zu entriegeln, die Überschreitungszeit des Türsensors überschreitet. Der Zeitbereich für die Zeitüberschreitung beträgt 1 - 9999 Sekunden.
Türsensor ein	Nur wenn **Türsensor ein** (Door Sensor On) aktiviert ist, kann der Einbruchalarm und Türsensor-Zeitüberschreitungsalarm ausgelöst werden.

3.8.4 Türstatus

Hier haben Sie drei Optionen: **NO**, **NC** und **Normal**.

- NO: Wenn **NO** gewählt wird, ist der Türstatus normalerweise offen, was bedeutet, dass die Tür nie geschlossen wird.
- NC: Wenn**NC** gewählt wird, ist der Türstatus normalerweise geschlossen, was bedeutet, dass die Tür nicht entriegelt wird.
- Normal: Wenn **Normal** gewählt wird, wird die Tür je nach Ihren Einstellungen entriegelt und verriegelt.

3.8.5 Schlosshaltezeit

Schlosshaltezeit (Lock Holding Time) ist die Dauer, in der das Schloss entriegelt ist. Wenn das Schloss für einen Zeitraum entriegelt wurde, der die Dauer überschreitet, wird das Schloss automatisch verriegelt.

3.9 Netzwerkkommunikation

Damit der Zugangs-Controller normal funktioniert, müssen Sie die Parameter für Netzwerk, serielle Ports und Wiegand-Ports konfigurieren.

3.9.1 IP-Adresse

3.9.1.1 IP-Konfiguration

Konfigurieren Sie eine IP-Adresse für den Zugangs-Controller, damit dieser mit dem Netzwerk verbunden wird. Siehe Abbildung 3–12 und Tabelle 3–6.

Abbildung 3–12 IP-Adressenkonfiguration

Tabelle 3–6 IP-Konfigurationsparameter

Parameter	Beschreibung
IP-Adresse/Subnetzmaske/Gateway-IP-Adresse	IP-Adresse, Subnetzmaske und Gateway-IP-Adresse müssen sich im gleichen Netzwerksegment befinden. Nach der Konfiguration tippen Sie auf ✓, um die Konfigurationen zu speichern.
DHCP	DHCP (Dynamic Host Configuration Protocol). Wenn DHCP aktiviert ist, kann die IP-Adresse automatisch bezogen werden und IP-Adresse, Subnetzmaske und Gateway-IP-Adresse können nicht manuell konfiguriert werden.
P2P	P2P ist eine Traversaltechnologie für private Netzwerke, die es dem Benutzer ermöglicht, Geräte zu verwalten, ohne DDNS, Port-Mapping oder Transit-Server zu benötigen.

- Vergewissern Sie sich, dass sich der Computer, mit dem Sie sich im Internet anmelden, im gleichen LAN wie das Gerät befindet.
- 7-Zoll-Modell X Zugangs-Controller haben zwei NICs. Die Standard-Verwaltungsadresse für den 1000M-Netzwerk-Port lautet 192.168.1.108 und für den 100M-Netzwerk-Port 192.168.2.108.

3.9.1.2 Aktiv registrieren

Durch die aktive Registrierung können Sie den Zugangs-Controller mit der Verwaltungsplattform verbinden, um dann den Zugangs-Controller über die Verwaltungsplattform verwalten zu können.

Konfigurationen, die Sie vorgenommen haben, können auf der Verwaltungsplattform gelöscht werden und der Zugangs-Controller kann initialisiert werden. Sie müssen die Verwaltungsberechtigung der Plattform für den Fall eines Datenverlusts durch unsachgemäßen Betrieb schützen.

Aktive Registrierungsparameter siehe Tabelle 3–7.

Tabelle 3–7 Aktiv registrieren

Name	Parameter
Server IP-Adresse	IP-Adresse der Verwaltungsplattform.
Port	Port-Nummer der Verwaltungsplattform.
Geräte-ID	Untergeordnete Gerätenummer auf der Verwaltungsplattform.

3.9.1.3 WLAN

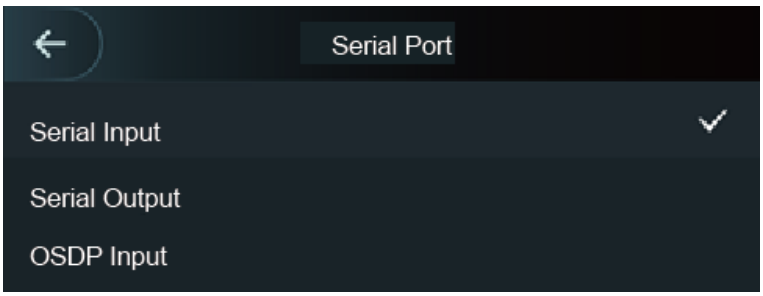
Sie können den Zugangs-Controller über WLAN mit dem Netzwerk verbinden, wenn der Zugangs-Controller über eine WLAN-Funktion verfügt.

3.9.2 Serielle Schnittstellen einstellen

Wählen Sie je nach Verwendung der externen Geräte seriellen Eingang oder seriellen Ausgang.

Wählen Sie **Anschluss > Serielle Schnittstelle** (Connection > Serial Port), damit wird das Menü **Serielle Schnittstelle** (Serial Port) angezeigt.

Abbildung 3–13 Serielle Schnittstelle



- Wählen Sie **Serieller Eingang** (Serial Input), wenn externe Geräte mit Kartenlese- und -schreibfunktionen an den Zugangs-Controller angeschlossen sind. **Serieller Eingang** (Serial Input) wird gewählt, wenn Zugangskartendaten an den Zugangs-Controller und die Management-Plattform gesendet werden sollen.
- Bei Zugangs-Controllern mit Gesichtserkennung, Kartenlese- und -schreibfunktionen, wenn Sie **Serieller Ausgang** (Serial Output) wählen, sendet der Zugangs-Controller Verriegelungs-/Entriegelungsdaten an den Zugangs-Controller. Es gibt zwei Arten von Verriegelungs-/Entriegelungsdaten:
  - ◇ Benutzer-ID
  - ◇ Kartennr.
- Wählen Sie OSDP-Eingang, wenn ein Kartenleser mit OSDP-Protokoll am Zugangs-Controller angeschlossen ist. Der Zugangs-Controller kann Kartendaten an die Verwaltungs-Plattform senden.

3.9.3 Wiegand-Konfiguration

Wählen Sie **Wiegand-Eingang** (Wiegand Input) oder **Wiegand-Ausgang** (Wiegand Output).

Wählen Sie **Anschluss > Wiegand** (Connection > Wiegand), damit wird das Wiegand-Menü angezeigt.

Abbildung 3–14 Wiegand

- Wählen Sie **Wiegand-Eingang** (Wiegand Input), wenn ein externer Karten-Durchzugsmechanismus am Zugangs-Controller angeschlossen ist.
- Wählen Sie **Wiegand-Ausgang** (Wiegand Output), wenn der Zugangs-Controller als Lesegerät arbeitet, das am Controller angeschlossen werden kann. Siehe Tabelle 3–8.

Tabelle 3–8 Wiegand-Ausgang

Parameter	Beschreibung
Wiegand-Ausgangstyp	Der **Wiegand-Ausgangstyp** (Wiegand Output Type) bestimmt die Kartennummer oder die Ziffer der Nummer, die vom Zugangs-Controller erkannt werden kann. ● Wiegand26, drei Bytes, sechs Ziffern. ● Wiegand34, vier Bytes, acht Ziffern. ● Wiegand66, acht Bytes, sechzehn Ziffern.
Impulsbreite	Sie können Impulsbreite und Impulsabstand einstellen.
Impuls Intervall	

Parameter	Beschreibung
Ausgabedatentyp	Sie können die Arten der Ausgabedaten wählen. ● Benutzer-ID: Wenn Benutzer-ID gewählt ist, wird die Benutzer-ID ausgegeben. ● Kartennr.: Wenn Kartennr. gewählt ist, wird die Kartennummer ausgegeben.

3.10 System

3.10.1 Zeit

Sie können Einstellungen für Datumformat, Datum, Zeit, Sommerzeit, NTP-Prüfung und Zeitzone vornehmen.

- Wenn Sie **Netzwerkzeitprotokoll** (Network Time Protocol) (NTP) wählen, müssen Sie zuerst die NTP-Prüffunktion aktivieren. Server IP-Adresse: Geben Sie die IP-Adresse des Zeitservers ein, damit wird die Zeit des Zugangs-Controllers mit dem Zeitserver synchronisiert.
- Port: Geben Sie die Portnummer des Zeitservers ein.
- Intervall (min): NPT-Prüfintervall. Tippen Sie auf das Speichern-Symbol, um zu speichern.

3.10.2 Gesichtsparameter

Abbildung 3–15 Gesichtsparameter

Tippen Sie auf einen Parameter und führen Sie die Konfiguration durch, dann tippen Sie auf ☑.

Tabelle 3–9 Gesichtsparameter

Name	Beschreibung
Schwelle der Gesichtserkennung	Die Genauigkeit der Gesichtserkennung kann eingestellt werden. Je größer der Wert ist, desto höher ist die Genauigkeit.
Max. Winkel der Gesichtserkennung	Stellen Sie den Aufnahmewinkel der Profile im Bedienfeld ein. Je größer der Wert ist, desto größer ist der Umfang der Profile, die erkannt werden.
Pupillenabstand	Der Pupillenabstand ist der Pixelwert des Bildes zwischen den Mittelpunkten der Pupillen in beiden Augen. Sie müssen einen geeigneten Wert einstellen, damit der Zugangs-Controller bei Bedarf Gesichter erkennen kann. Der Wert ändert sich in Abhängigkeit von den Gesichtsgrößen und dem Abstand zwischen den Gesichtern und dem Objektiv. Je näher das Gesicht am Objektiv ist, desto größer sollte der Wert sein. Wenn sich ein Erwachsener 1,5 m vom Objektiv entfernt befindet, kann der Wert für den Pupillenabstand zwischen 50 und 70 liegen.
Zeitüberschreitung bei Erkennung	Wenn eine Person, die nicht über eine Zugangsberechtigung verfügt, vor dem Zugangs-Controller steht und das Gesicht erkannt wird, meldet der Controller, dass die Gesichtserkennung fehlgeschlagen ist. Das Meldeintervall wird als Zeitüberschreitung bei Erkennung bezeichnet.
Erkennungsintervall	Wenn eine Person, die eine Zugangsberechtigung hat, vor dem Zugangs-Controller steht und das Gesicht erkannt wird, meldet der Controller, dass die Gesichtserkennung erfolgreich war. Das Meldetintervall ist das Erkennungsintervall.
Ungültiges Gesichtsmeldeintervall	Wenn ein Gesicht ohne Zugangsberechtigung vor dem Zugangs-Controller steht, meldet der Controller, dass das Gesicht ungültig ist. Das Meldeintervall ist ein ungültiges Gesichtsmeldeintervall.
Fälschungs-Schwellenwert	Diese Funktion verhindert, dass Personen durch menschliche Gesichtsbilder oder Gesichtsmodelle entriegeln können. Je größer der Wert ist, desto schwieriger können Gesichtsbilder die Tür entriegeln. Der empfohlene Wertebereich liegt über 80.

Name	Beschreibung
Temperaturüberwachung	Stellen Sie ein, ob die Überwachung der Körpertemperatur aktiviert werden soll. ● Temperatureinheit: Wählen Sie eine Temperatureinheit. ● Temperaturrechteck: Stellen Sie ein, ob die Temperaturüberwachung aktiviert werden soll oder nicht. ● Abstand der Temperaturüberwachung (cm): Der Wert ist standardmäßig 0. Stellen Sie andere Werte ein, um die Temperaturüberwachung innerhalb eines definierten Abstands zu ermöglichen. 80 cm wird empfohlen. ● Temperatur-Schwellenwert (°C): Stellen Sie die Temperaturschwelle ein. Die überwachte Körpertemperatur wird als hohe Temperatur gewertet, wenn sie größer oder gleich dem eingestellten Wert ist. ● Temperatur-Korrekturwert: Dieser Parameter dient Testzwecken. Die Differenz der Temperaturüberwachungsumgebung kann zu einer Temperaturabweichung zwischen der überwachten Temperatur und der Ist-Temperatur führen. Sie können mehrere überwachte Proben für den Test auswählen und dann die Temperaturabweichung um diesen Parameter entsprechend dem Vergleich zwischen der überwachten Temperatur und der Ist-Temperatur korrigieren. Wenn beispielsweise die überwachte Temperatur um 0,5 °C niedriger als die Ist-Temperatur ist, wird der Korrekturwert auf 0,5 °C eingestellt; wenn die überwachte Temperatur um 0,5 °C höher als die Ist-Temperatur ist, wird der Korrekturwert auf -0,5 °C eingestellt. Nur der Zugangs-Controller mit einer Temperaturüberwachungseinheit unterstützt diesen Parameter.
Masken-Modus	● Nicht erkannt: Maske wird bei der Gesichtserkennung nicht erkannt. ● Maske Erinnerung: Maske wird bei der Gesichtserkennung erkannt. Wenn die Person erkannt wird, ohne eine Maske zu tragen, erinnert das System an die Maske, und der Durchgang wird erlaubt. ● Maske abfangen: Maske wird bei der Gesichtserkennung erkannt. Wenn die Person erkannt wird, ohne eine Maske zu tragen, erinnert das System an die Maske, und der Durchgang wird nicht erlaubt.

3.10.3 Bildmodus

Hier haben Sie drei Optionen:

- Innen: Wählen Sie **Innen** (Indoor), wenn der Zugangs-Controller in Innenräumen installiert ist;
- Außenbereich: Wählen Sie **Außenbereich** (Outdoor), wenn der Zugangs-Controller im Freien installiert ist;
- Sonstige: Wählen Sie **Sonstige** (Other), wenn der Zugangs-Controller an Orten mit Gegenlicht wie Korridoren und Fluren installiert ist.

3.10.4 Aufhelllichtmodus einstellen

Sie können Aufhelllichtmodi nach Bedarf wählen. Es gibt drei Modi:

- Auto: Wenn der Fotosensor erkennt, dass die Umgebung nicht dunkel ist, ist das Aufhelllicht normalerweise ausgeschaltet, anderenfalls ist das Aufhelllicht eingeschaltet.
- NO: Das Aufhelllicht ist normalerweise eingeschaltet.
- NC: Das Aufhelllicht ist normalerweise ausgeschaltet.

3.10.5 Einstellung der Helligkeit des Aufhelllichts

Sie können die Helligkeit des Aufhelllichts nach Bedarf wählen.

3.10.6 Lautstärke einstellen

Tippen Sie auf  oder  , um die Lautstärke einzustellen.

3.10.7 IR-Lichthelligkeit einstellen

Je größer der Wert ist, desto klarer sind die Bilder, anderenfalls sind die Bilder undeutlicher.

3.10.8 Zu den Werkseinstellungen zurücksetzen

- Wenn Sie den Zugangs-Controller auf die Werkseinstellungen zurücksetzen, gehen Daten verloren.
- Nachdem der Zugangs-Controller auf die Werkseinstellungen zurückgesetzt wurde, wird die IP-Adresse nicht geändert.

Sie können wählen, ob Benutzerdaten und Protokolle erhalten bleiben sollen.

- Sie können wählen, ob der Zugangs-Controller auf die Werkseinstellungen zurückgesetzt werden soll, wobei alle Benutzer- und Gerätedaten gelöscht werden.
- Sie können wählen, ob der Zugangs-Controller auf die Werkseinstellungen zurückgesetzt werden soll, wobei die Benutzer- und Gerätedaten erhalten bleiben.

3.10.9 Neustart

Wählen Sie **Einstellung > Neustart** (Setting > Reboot) und tippen Sie auf **Neustart** (Reboot), damit wird der Zugangs-Controller neu gestartet.

3.11 USB

- Vergewissern Sie sich, dass das USB-Speichermedium angeschlossen ist, bevor Sie Benutzerdaten exportieren und aktualisieren. Ziehen Sie während des Exports oder der Aktualisierung das USB-Speichermedium nicht ab und führen Sie keine anderen Operationen durch, anderenfalls schlägt der Export bzw. die Aktualisierung fehl.
- Sie müssen Daten von einem Zugangs-Controller auf das USB-Speichermedium importieren, bevor Sie das USB-Speichermedium verwenden können, um Daten in einen anderen Zugangs-Controller zu importieren.
- Ein USB-Speichermedium kann ebenfalls verwendet werden, um das Programm zu aktualisieren.

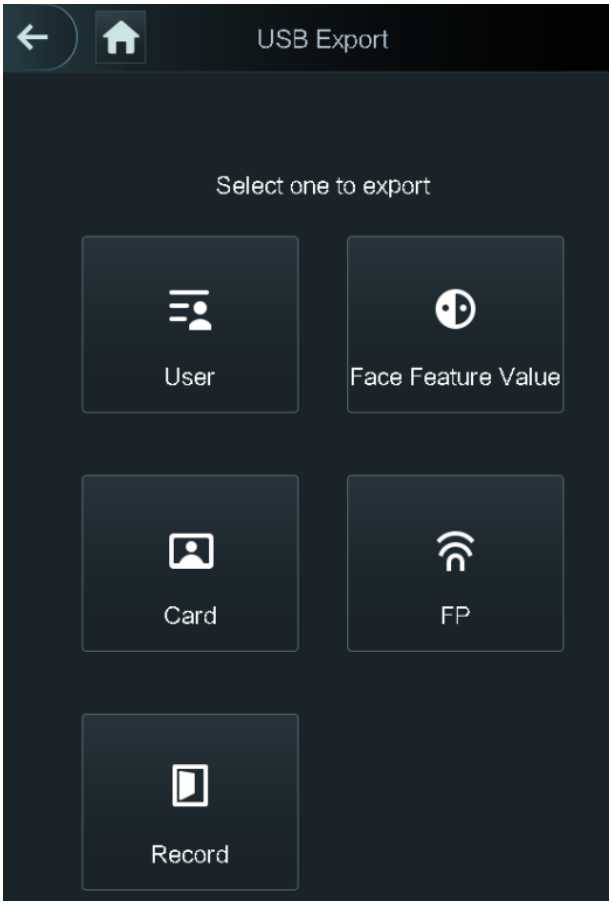
3.11.1 USB-Export

Sie können Daten vom Zugangs-Controller auf das USB-Speichermedium exportieren, nachdem Sie das USB-Gerät angeschlossen haben. Die exportierten Daten sind verschlüsselt und können nicht bearbeitet werden.

Schritt 1: Wählen Sie **USB > USB-Export** (USB > USB Export).

Das Menü **USB-Export** (USB Export) wird angezeigt. Siehe Abbildung 3–16.

Abbildung 3–16 USB-Export

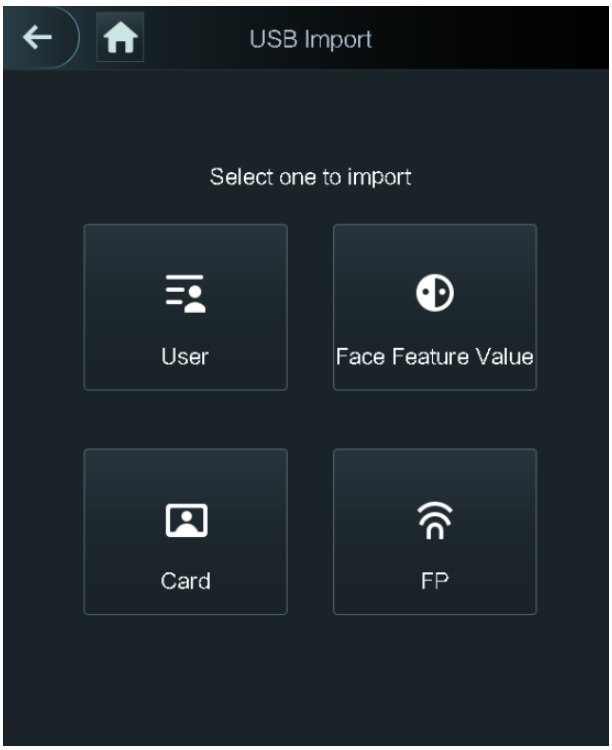


Schritt 2: Wählen Sie den Datentyp, den Sie exportieren möchten.
Sie werden aufgefordert, den Export zu bestätigen.
Schritt 3: Tippen Sie auf **OK**.
Die exportierten Daten werden auf dem USB-Speichermedium gespeichert.

3.11.2 USB-Import

Nur Daten auf dem USB-Speichermedium, die von einem Zugangs-Controller exportiert wurden, können in einen anderen Zugangs-Controller importiert werden.
Schritt 1: Wählen Sie **USB > USB-Import** (USB > USB Import).
Das Menü **USB-Import** (USB Import) wird angezeigt. Siehe Abbildung 3–17.

Abbildung 3–17 USB-Import



Schritt 2: Wählen Sie den Datentyp, den Sie importieren möchten.
Die Meldung **Import bestätigen** (Confirm to import) wird angezeigt.
Schritt 3: Tippen Sie auf **OK**.
Die Daten auf dem USB-Speichermedium werden in den Zugangs-Controller importiert.

3.11.3 USB-Aktualisierung

Ein USB-Flash-Laufwerk kann zur Aktualisierung des Systems verwendet werden.
Schritt 1: Benennen Sie die Aktualisierungsdatei in „update.bin“ um und speichern Sie die Datei „update.bin“ im Stammverzeichnis des USB-Flash-Laufwerks.

- Vergewissern Sie sich, dass sich der Computer, mit dem Sie sich im Internet anmelden, im gleichen LAN wie das Gerät befindet.
- 7-Zoll-Modell X Zugangs-Controller haben zwei NICs. Die Standard-Verwaltungsadresse für den 1000M-Netzwerk-Port lautet 192.168.1.108 und für den 100M-Netzwerk-Port 192.168.2.108.

Schritt 2: Wählen Sie **USB > USB-Aktualisierung** (USB > USB Update).
Die Meldung **Aktualisierung bestätigen** (Confirm to Update) wird angezeigt.
Schritt 3: Tippen Sie auf **OK**.
Die Aktualisierung startet und der Zugangs-Controller startet neu, nachdem die Aktualisierung abgeschlossen ist.

3.12 Funktionen

Sie können Einstellungen zur Privatsphäre, Kartennummernumkehr, zum Sicherheitsmodul, Türsensortyp und zur Ergebnisrückmeldung vornehmen. Für Details zu den genannten Funktionen siehe Abbildung 3–18 und Tabelle 3–10.

Abbildung 3–18 Funktionen

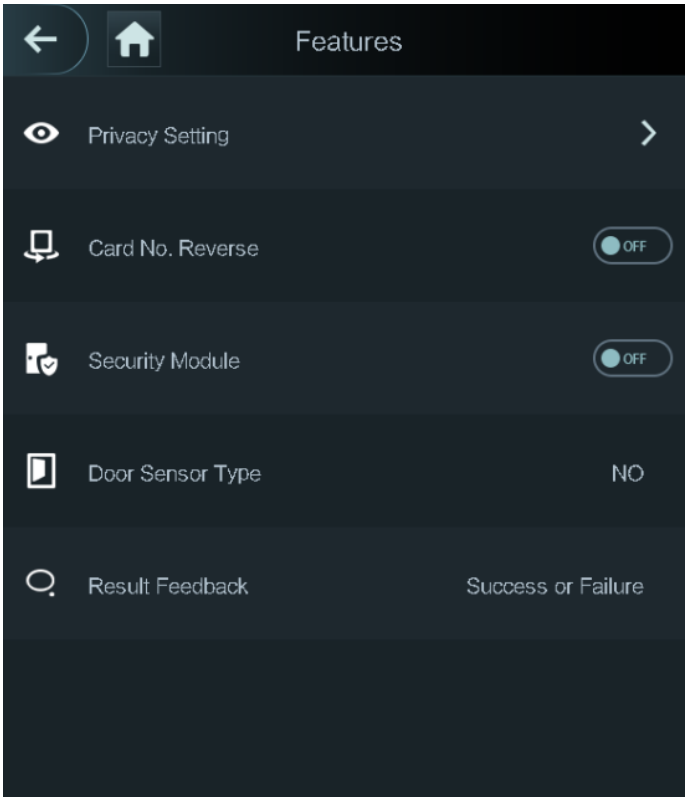


Tabelle 3–10 Beschreibung der Funktionen

Parameter	Beschreibung
Privatsphären-Einstellung	Siehe „3.12.1 Privatsphären-Einstellung“ für Details.
Kartennummernumkehr	Wenn der Kartenleser eines Drittanbieters über den Wiegand-Ausgang an den Zugangs-Controller angeschlossen werden muss, müssen Sie die Funktion Kartennummernumkehr aktivieren, anderenfalls kann die Kommunikation zwischen dem Zugangs-Controller und dem Kartenleser des Drittanbieters aufgrund von Protokollunterschieden fehlschlagen.
Sicherheitsmodul	● Wenn das Sicherheitsmodul aktiviert ist, müssen Sie das Zugangskontroll-Sicherheitsmodul separat erwerben. Das Sicherheitsmodul benötigt eine separate Stromversorgung. ● Sobald das Sicherheitsmodul aktiviert ist, sind die Ausgangstaste, die Schlosssteuerung und die Feuerlöschverbindung ungültig.
Türsensortyp	Es gibt zwei Optionen: **NO** und **NC**.
Ergebnisrückmeldung	Zeigt an, ob die Entriegelung erfolgreich war oder fehlgeschlagen ist.

3.12.1 Privatsphären-Einstellung

Abbildung 3–19 Privatsphären-Einstellung

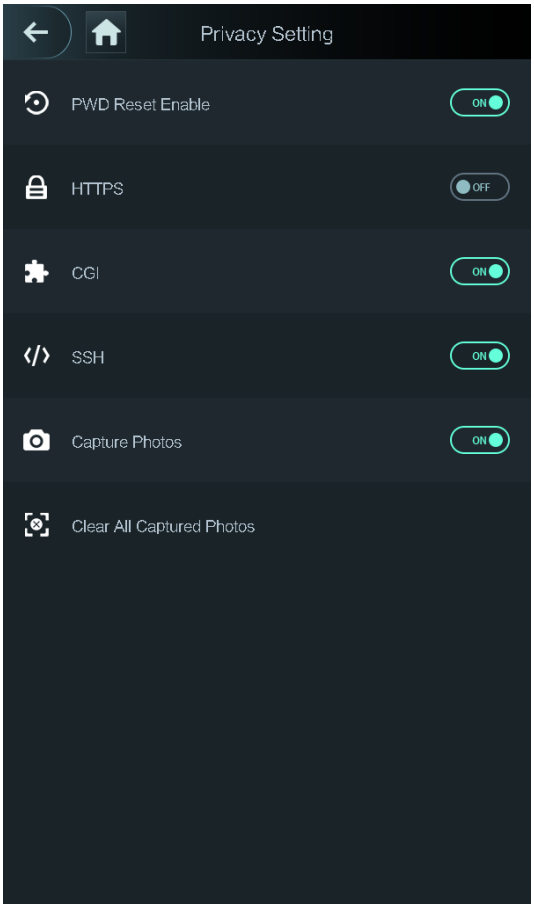


Tabelle 3–11 Funktionen

Parameter	Beschreibung
Passwort-Rücksetzung aktivieren	Wenn die Funktion **Passwort-Rücksetzung aktivieren** (PWD Reset Enable) aktiviert ist, können Sie das Passwort zurücksetzen. Die Passwort-Rücksetzfunktion ist standardmäßig aktiviert.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) ist ein Protokoll für die sichere Kommunikation über ein Computernetzwerk. Wenn HTTPS aktiviert ist, wird HTTPS für den Zugriff auf CGI-Befehle verwendet, anderenfalls wird HTTP verwendet. Wenn HTTPS aktiviert ist, wird der Zugangs-Controller automatisch neu gestartet.
CGI	Common Gateway Interface (CGI) bietet ein Standardprotokoll für Web-Server zur Ausführung von Programmen, die wie Konsolenanwendungen auf einem Server laufen, der Webseiten dynamisch generiert. Wenn CGI aktiviert ist, können CGI-Befehle verwendet werden. CGI ist standardmäßig aktiviert.

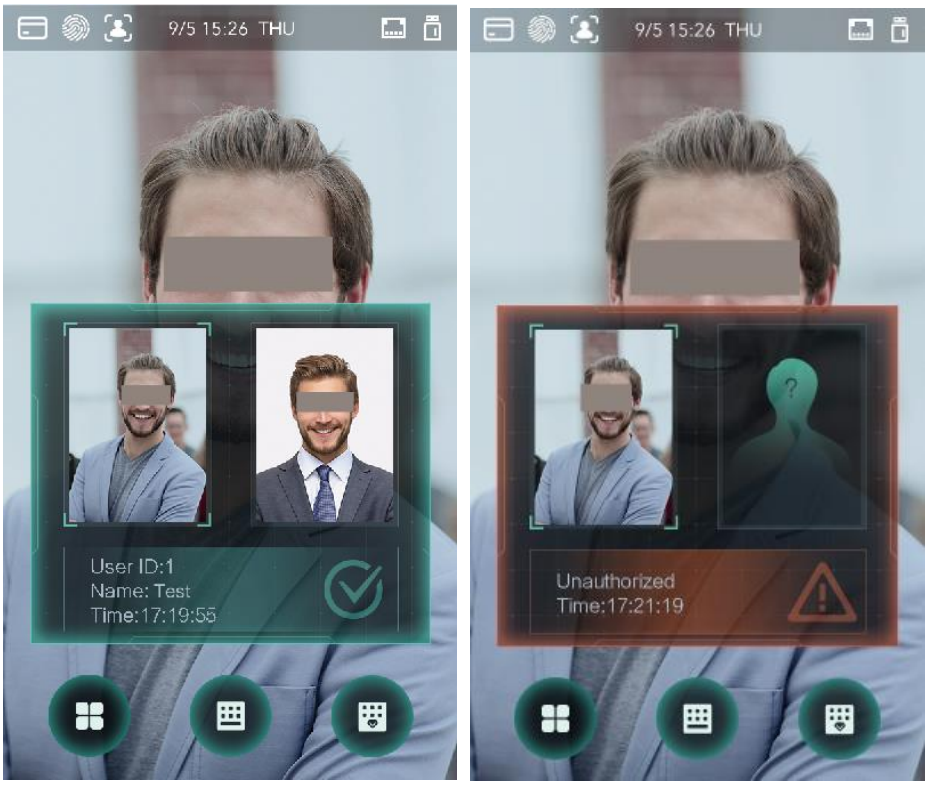
Parameter	Beschreibung
SSH	Secure Shell (SSH) ist ein kryptographisches Netzwerkprotokoll für den sicheren Betrieb von Netzwerkdiensten über ein ungesichertes Netzwerk. Wenn SSH aktiviert ist, bietet SSH einen kryptographischen Dienst für die Datenübertragung.
Foto aufnehmen	Wenn Sie EIN wählen, wird das Foto des Benutzers automatisch aufgenommen, wenn er die Tür entriegelt. Diese Funktion ist standardmäßig auf EIN eingestellt.
Alle aufgenommenen Fotos löschen	Tippen Sie auf das Symbol, um alle aufgenommenen Fotos löschen.

3.12.2 Ergebnisrückmeldung

Bei Bedarf können Sie einen Ergebnisrückmeldemodus wählen.

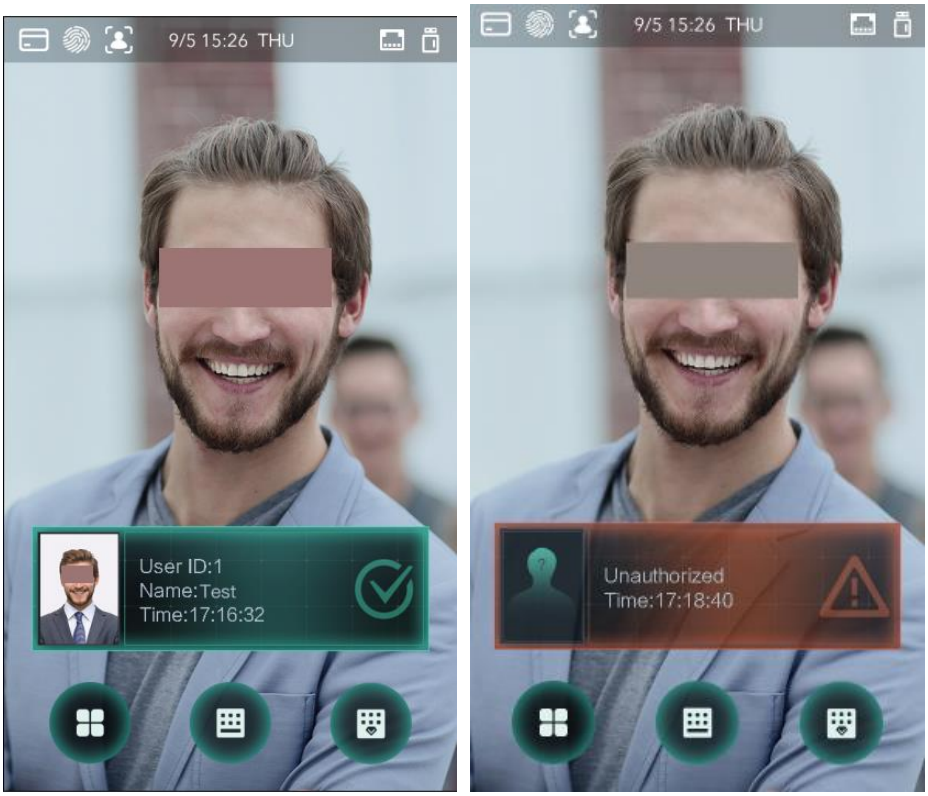
Modus 1

Abbildung 3–20 Modus 1



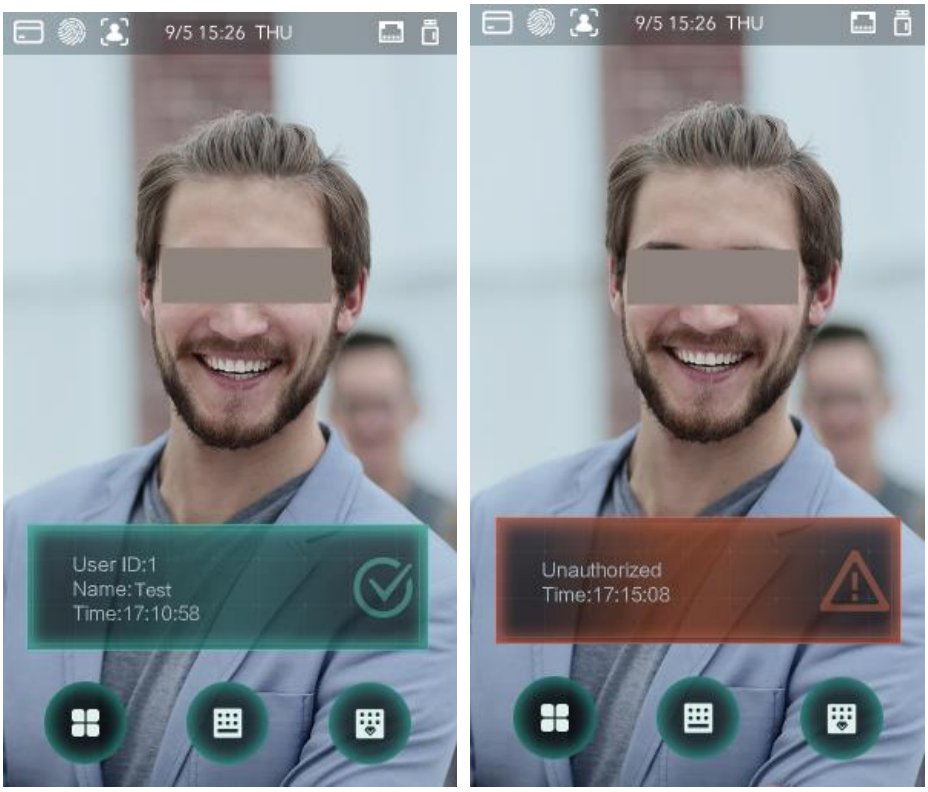
Modus 2

Abbildung 3–21 Modus 2



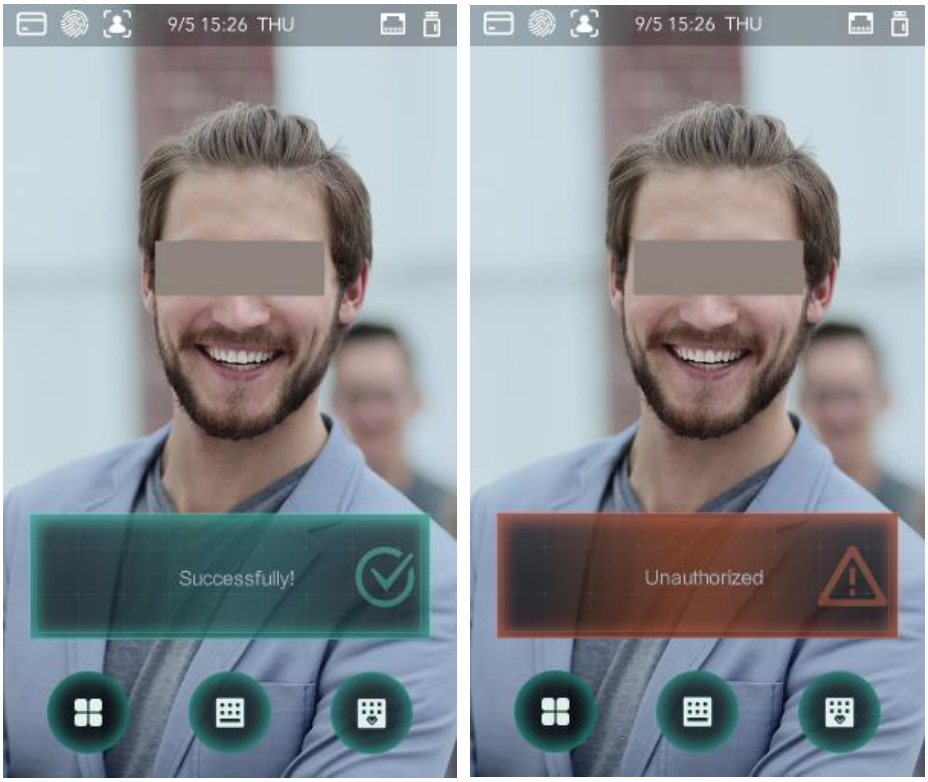
Modus 3

Abbildung 3–22 Modus 3



Modus 4

Abbildung 3–23 Modus 4



3.13 Aufnahme

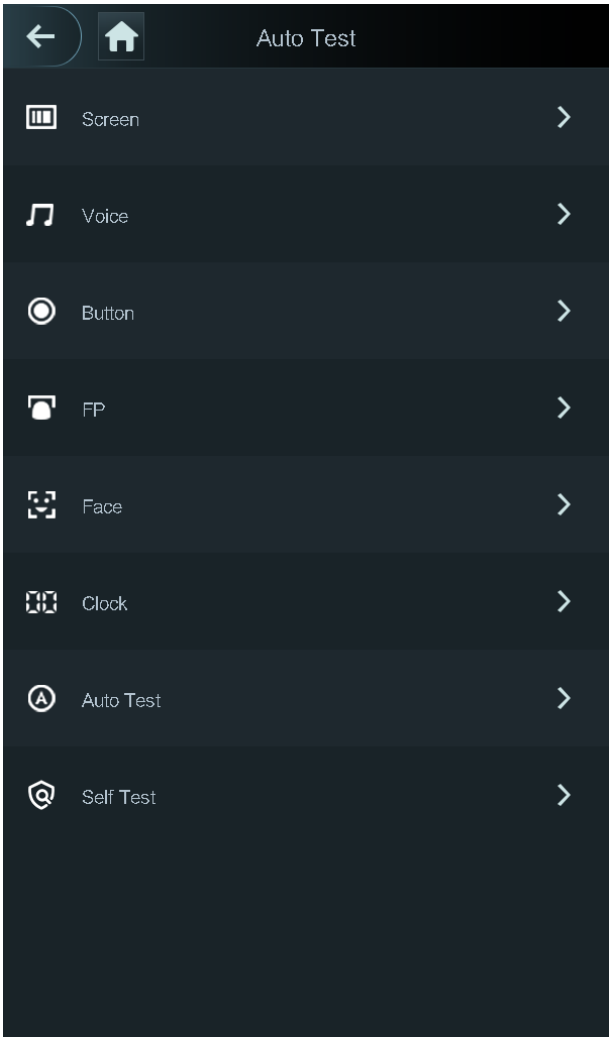
Sie können alle Entriegelungsaufnahmen abfragen.

Abbildung 3–24 Suche nach Stempelaufzeichnungen

3.14 Automatischer Test

Wenn Sie den Zugangs-Controller zum ersten Mal verwenden oder wenn der Zugangs-Controller gestört ist, können Sie mit der Automatischen Testfunktion prüfen, ob der Zugangs-Controller normal arbeiten kann. Folgen Sie den Aufforderungen.

Abbildung 3–25 Automatischer Test



Wenn Sie **Automatischer Test** (Auto Test) wählen, führt Sie der Zugangs-Controller zur Durchführung aller automatischen Tests.

3.15 Systeminformationen

Datenkapazität, Geräteversion und Firmwareinformationen des Zugangs-Controllers können Sie über das Menü **Systeminformationen** (System Info) einsehen.

4 Web-Bedienung

Der Zugangs-Controller kann über das Internet konfiguriert und bedient werden. Über das Internet können Sie Netzwerkparameter, Videoparameter und Zugangs-Controller-Parameter einstellen und Sie können das System ebenfalls warten und aktualisieren.

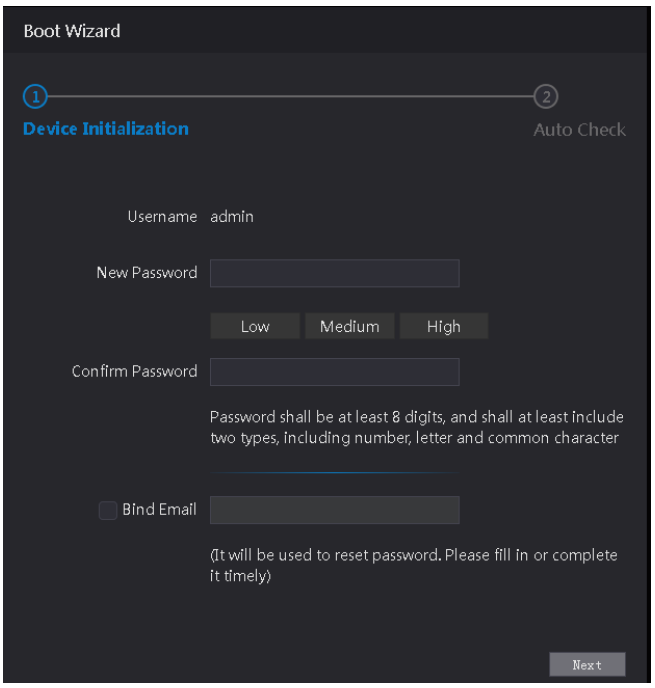
4.1 Initialisierung

Sie müssen ein Passwort und eine E-Mail-Adresse einrichten, bevor Sie sich zum ersten Mal im Internet anmelden können.

Schritt 1: Öffnen Sie den IE-Webbrowser, geben Sie die IP-Adresse (die Standardadresse ist 192.168.1.108) des Zugangs-Controllers in die Adressleiste ein und drücken Sie die Eingabetaste.

- Verwenden Sie einen neueren Browser als IE 8, sonst können Sie sich möglicherweise nicht im Internet anmelden.
- Vergewissern Sie sich, dass sich der Computer, mit dem Sie sich im Internet anmelden, im gleichen LAN wie das Gerät befindet.
- 7-Zoll-Modell X Zugangs-Controller haben zwei NICs. Die Standard-IP-Adresse für den 1000M-Netzwerk-Port lautet 192.168.1.108 und für den 100M-Netzwerk-Port 192.168.2.108.

Abbildung 4–1 Initialisierung



Schritt 2: Geben Sie das neue Passwort ein, bestätigen Sie es, geben Sie eine E-Mail-Adresse ein und klicken Sie dann auf **Weiter** (Next).

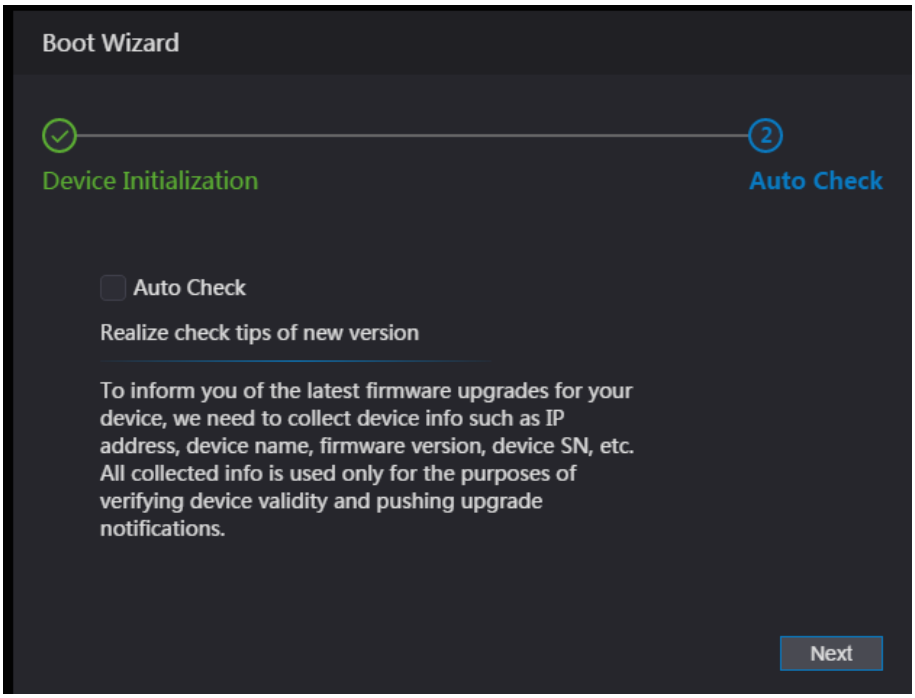
- Das Passwort muss aus 8 bis 32 nicht leeren Zeichen bestehen und mindestens zwei Arten von Zeichen von Groß- und Kleinschreibung, Ziffer und Sonderzeichen enthalten

(außer ' " ; : &). Richten Sie ein Passwort mit hoher Sicherheitsstufe entsprechend der Eingabeaufforderung für die Passwortstärke ein.

- Bewahren Sie aus Sicherheitsgründen das Passwort nach der Initialisierung korrekt auf und ändern Sie es regelmäßig.
- Wenn Sie das Administrator-Passwort durch Scannen des QR-Codes zurücksetzen müssen, benötigen Sie eine E-Mail-Adresse, um den Sicherheitscode zu erhalten.

Schritt 3: Klicken Sie auf **Weiter** (Next).

Abbildung 4–2 Automatische Überprüfung

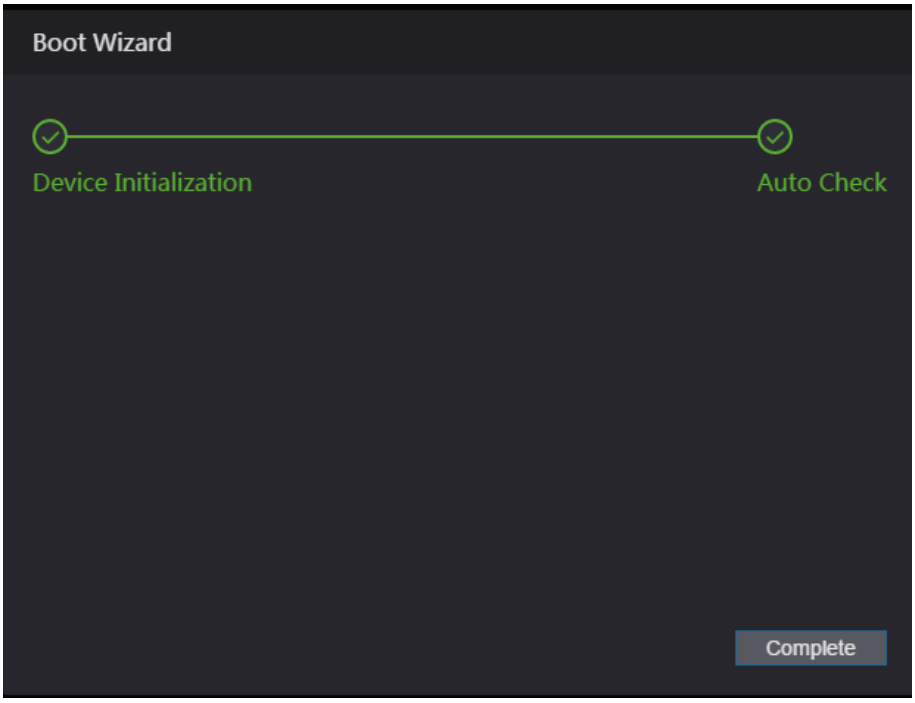


Schritt 4: Sie können entscheiden, ob Sie **Automatische Überprüfung** (Auto Check) wählen oder nicht.

Wir empfehlen, **Automatische Überprüfung** (Auto Check) zu wählen, um rechtzeitig das neueste Programm zu erhalten.

Schritt 5: Klicken Sie auf **Weiter** (Next).

Abbildung 4–3 Konfiguration beendet



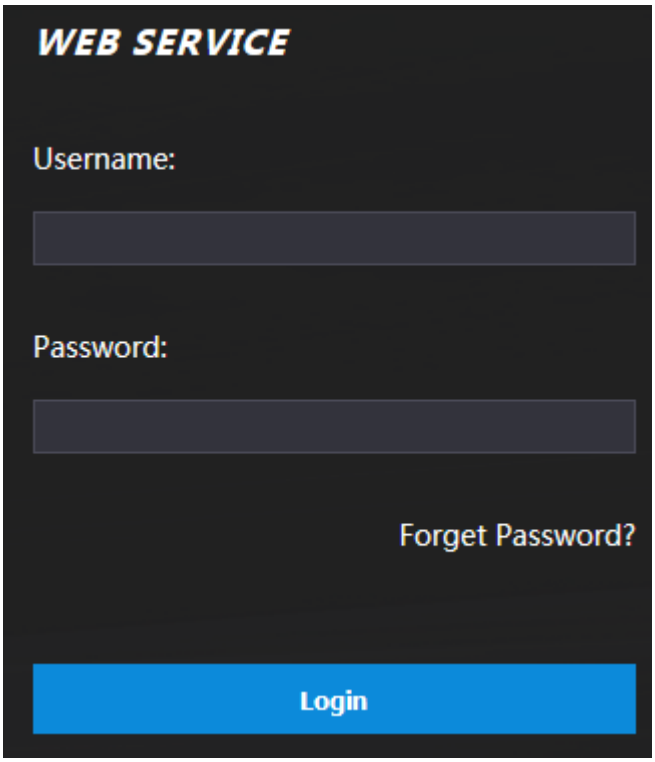
Schritt 6: Klicken Sie auf **Beenden** (Complete), damit ist die Initialisierung abgeschlossen. Das Fenster zur Internet-Anmeldung wird angezeigt.

4.2 Anmelden

Schritt 1: Öffnen Sie den IE-Webbrowser, geben Sie die IP-Adresse des Zugangs-Controllers in die Adressleiste ein und drücken Sie die **Eingabetaste** (Enter).

- Verwenden Sie einen neueren Browser als IE 8, sonst können Sie sich möglicherweise nicht im Internet anmelden.
- Vergewissern Sie sich, dass sich der Computer, mit dem Sie sich im Internet anmelden, im gleichen LAN wie das Gerät befindet.
- 7-Zoll-Modell X Zugangs-Controller haben zwei NICs. Die Standard-Verwaltungsadresse für den 1000M-Netzwerk-Port lautet 192.168.1.108 und für den 100M-Netzwerk-Port 192.168.2.108.

Abbildung 4–4 Anmeldung



Schritt 2: Geben Sie den Benutzernamen und das Passwort ein.

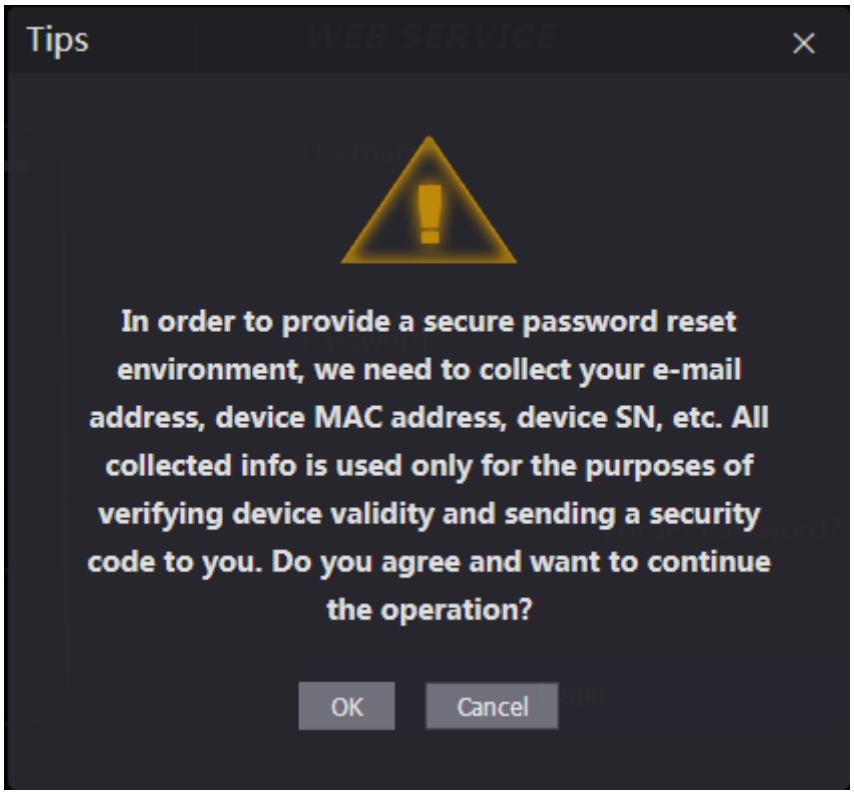
- Der standardmäßige Administratorname ist admin, und das Passwort ist das Anmeldepasswort nach der Initialisierung des Zugangs-Controllers. Ändern Sie das Administrator-Passwort regelmäßig und bewahren Sie es aus Sicherheitsgründen ordnungsgemäß auf.
- Wenn Sie das Administrator-Anmelde-Passwort vergessen haben, klicken Sie auf **Passwort vergessen?** (Forgot password?), um es zurückzusetzen. Siehe „4.3 Passwort zurücksetzen“.

Schritt 3: Klicken Sie auf **Anmelden** (Login).
Die Web-Oberfläche ist angemeldet.

4.3 Passwort zurücksetzen

Wenn Sie das Passwort des Administrator-Kontos zurücksetzen, wird Ihre E-Mail-Adresse benötigt.
Schritt 1: Klicken Sie im Anmeldefenster auf **Passwort vergessen?** (Forgot password?).
Das Menü **Tipps** (Tips) wird angezeigt.

Abbildung 4–5 Tipps

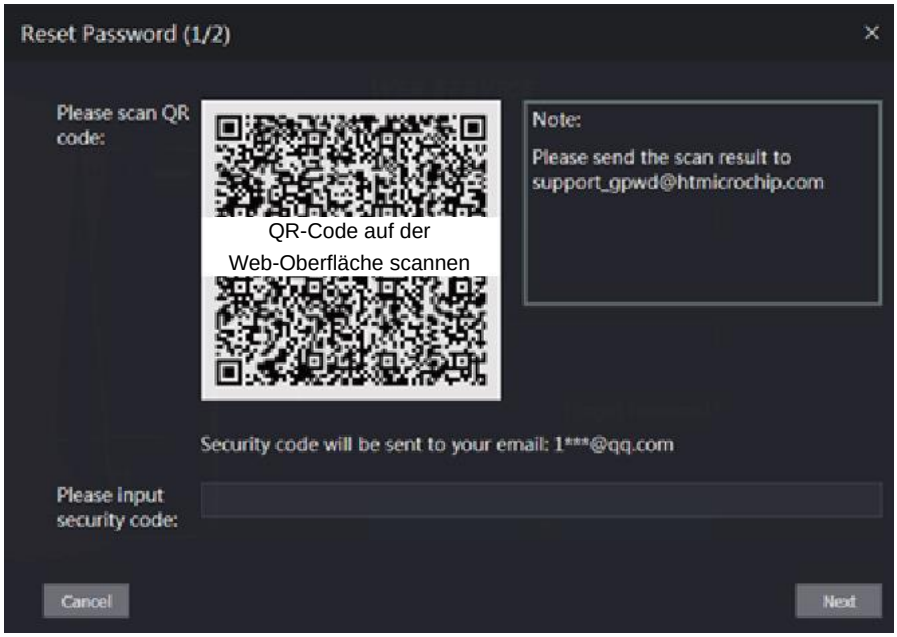


Schritt 2: Lesen Sie die Tipps.

Schritt 3: Klicken Sie auf **OK**.

Das Menü **Passwort zurücksetzen** (Reset Password) wird angezeigt.

Abbildung 4–6 Passwort zurücksetzen



Schritt 4: Scannen Sie den QR-Code, um den Sicherheitscode zu erhalten.

- Durch Scannen desselben QR-Codes werden höchstens zwei Sicherheitscodes generiert. Wenn Sicherheitscodes ungültig werden, aktualisieren Sie den QR-Code, um weitere Sicherheitscodes zu erhalten.

- Sie müssen den Inhalt, den Sie nach dem Scannen des QR-Codes erhalten, an die angegebene E-Mail-Adresse senden, danach erhalten Sie den Sicherheitscode.
- Verwenden Sie den Sicherheitscode innerhalb von 24 Stunden nach Erhalt. Andernfalls wird er ungültig.
- Wenn fünfmal hintereinander ein falscher Sicherheitscode eingegeben wird, wird der Administrator für fünf Minuten gesperrt.

Schritt 5: Geben Sie den Sicherheitscode ein, den Sie erhalten haben.
Schritt 6: Klicken Sie auf **Weiter** (Next).
Das Menü **Passwort zurücksetzen** (Reset Password) wird angezeigt.
Schritt 7: Setzen Sie das neue Passwort zurück

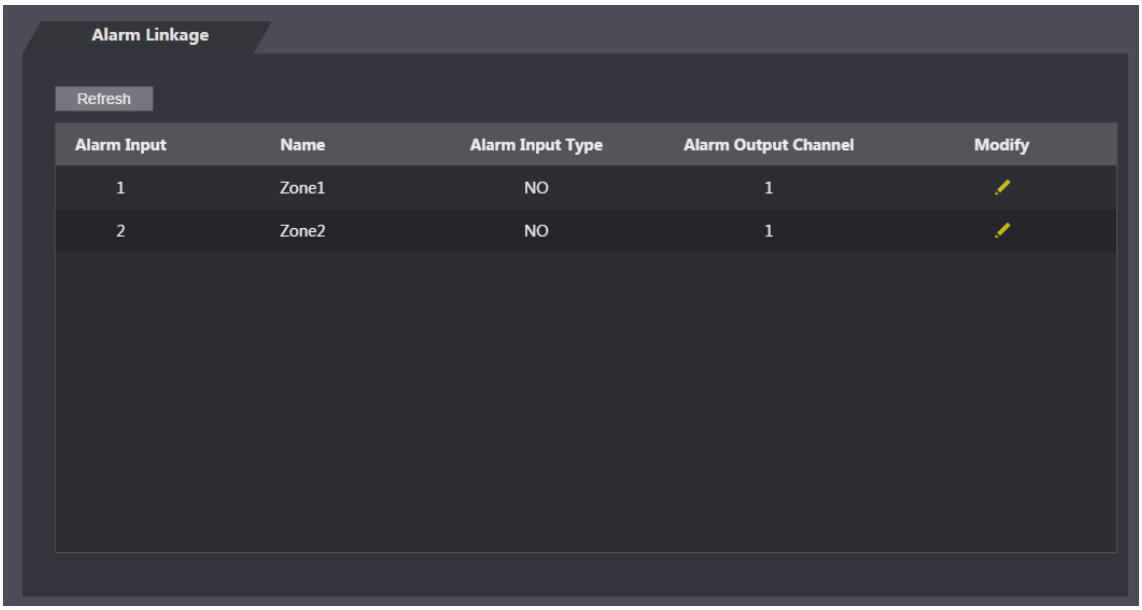
Das Passwort muss aus 8 bis 32 nicht leeren Zeichen bestehen und mindestens zwei Arten von Zeichen von Groß- und Kleinschreibung, Ziffer und Sonderzeichen enthalten (außer ' " ; : &).
Schritt 8: Klicken Sie auf **OK**, damit ist die Rücksetzung beendet.

4.4 Alarmverknüpfung

4.4.1 Alarmverknüpfung einstellen

Alarmeingangsgeräte können an den Zugangs-Controller angeschlossen werden und Sie können die Parameter für die Alarmverknüpfung nach Bedarf ändern.
Schritt 1: Wählen Sie in der Navigationsleiste **Alarmverknüpfung** (Alarm Linkage).
Das Menü **Alarmverknüpfung** (Alarm Linkage) wird angezeigt. Siehe Abbildung 4–7.

Abbildung 4–7 Alarmverknüpfung



Schritt 2: Klicken Sie auf , um die Alarmverknüpfungsparameter zu modifizieren. Siehe Abbildung 4–8

Abbildung 4–8 Alarmverknüpfungsparameter modifizieren

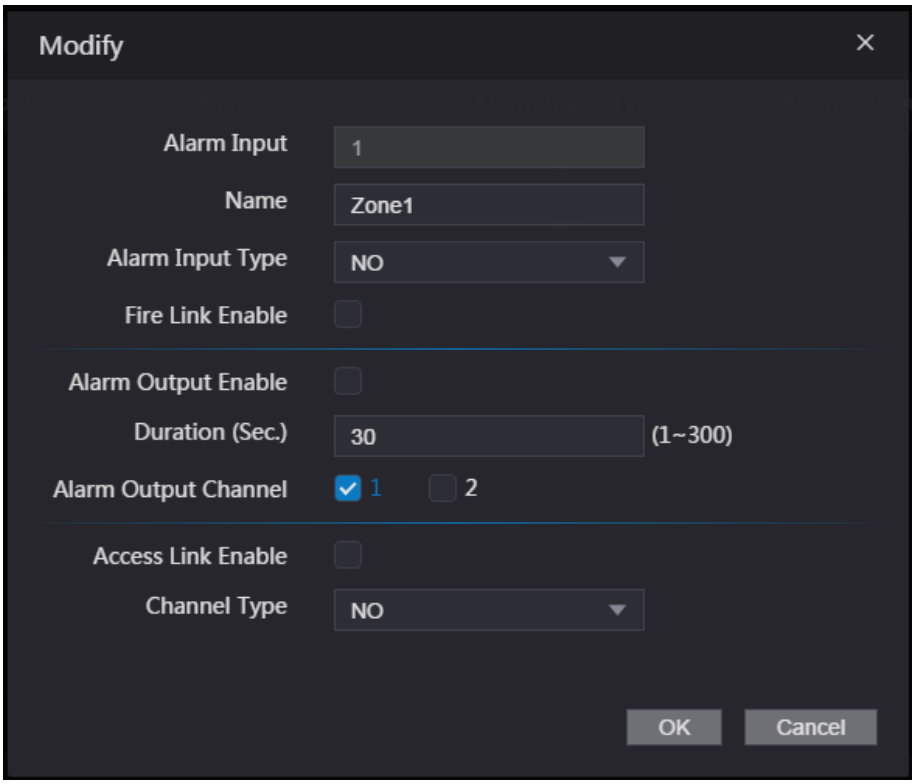


Tabelle 4–1 Beschreibung der Alarmverknüpfungsparameter

Parameter	Beschreibung
Alarmeingang	Sie können den Wert nicht ändern. Behalten Sie den Standardwert bei.
Name	Geben Sie einen Zonennamen ein.
Alarmeingangstyp	Es gibt zwei Optionen: NO und NC. Wenn der Alarmeingangstyp des von Ihnen erworbenen Alarmgeräts NO ist, müssen Sie NO wählen, anderenfalls müssen Sie NC wählen.
Brandverknüpfung aktivieren	Wenn Brandverknüpfung aktiviert ist, gibt der Zugangs-Controller Alarme aus, wenn Feueralarme ausgelöst werden. Die Alarmdetails werden im Alarmprotokoll angezeigt. Alarmausgabe und Zugangs-Verknüpfung sind standardmäßig NO, wenn Brandverknüpfung aktiviert ist.
Alarmausgabe aktivieren	Das Relais kann Alarmdaten ausgeben (wird an die Verwaltungsplattform gesendet), wenn **Alarmausgabe** (Alarm Output) aktiviert ist.
Dauer (Sekunden)	Die Alarmdauer beträgt 1 - 300 Sekunden.
Alarm-Ausgabekanal	Sie können einen Alarmausgabekanal entsprechend dem von Ihnen installierten Alarmgerät wählen. Jedes Alarmgerät kann als ein Kanal betrachtet werden.
Zugangs-Verknüpfung aktivieren	Nachdem die Zugangs-Verknüpfung aktiviert wurde, ist der Zugangs-Controller Öffner oder Schließer, wenn Eingangsalarmsignale auftreten.
Kanaltyp	Es gibt zwei Optionen: NO und NC.

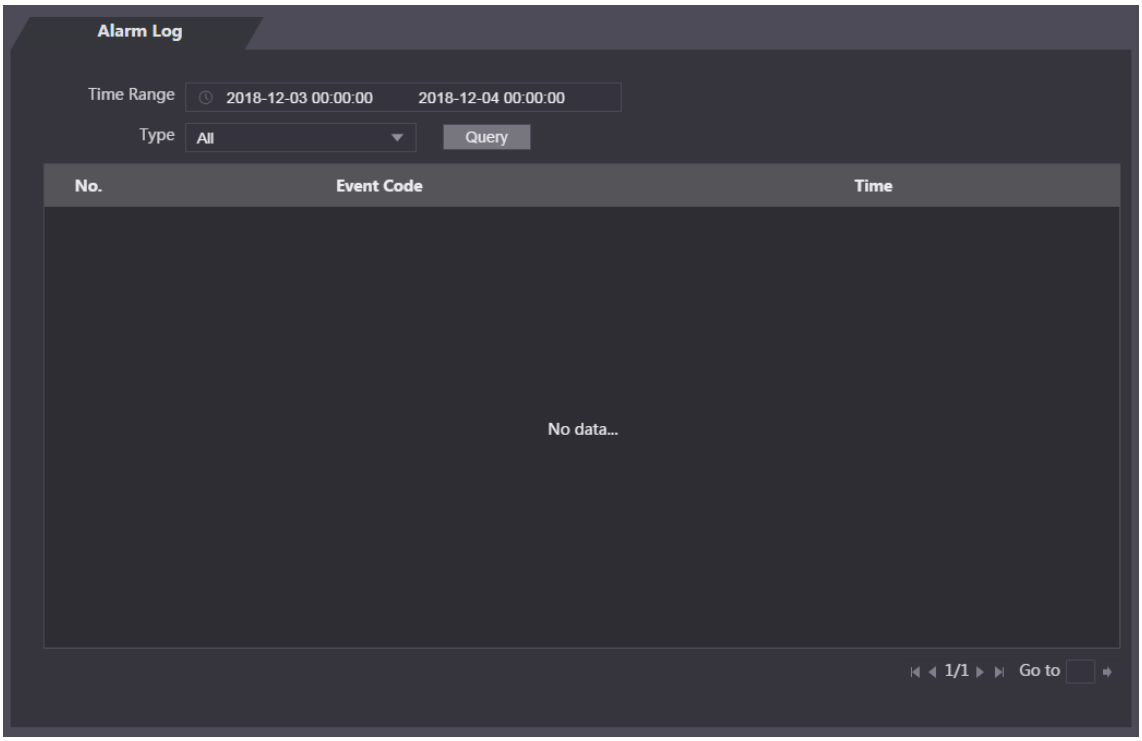
Schritt 3: Klicken Sie auf **OK**, um die Konfiguration zu beenden.

Die Konfiguration im Internet wird mit der Konfiguration im Client synchronisiert, wenn der Zugangs-Controller zu einem Client hinzugefügt wird.

4.4.2 Alarmprotokoll

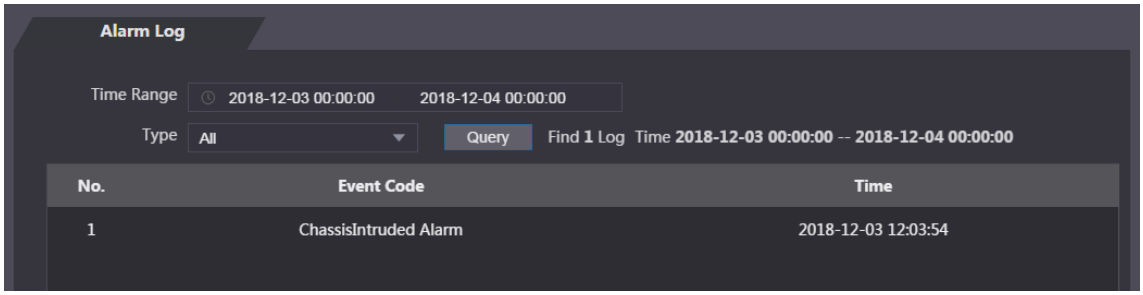
Sie können Alarmtyp und Zeitbereich im Menü **Alarmprotokoll** (Alarm Log) anzeigen.
Schritt 1: Wählen Sie **Alarmverknüpfung > Alarmprotokoll** (Alarm Linkage > Alarm Log).
Das Menü **Alarmprotokoll** (Alarm Log) wird angezeigt. Siehe Abbildung 4–9.

Abbildung 4–9 Alarmprotokoll



Schritt 2: Wählen Sie Zeitbereich und Alarmtyp und klicken Sie dann auf **Abfrage** (Query).
Die Abfrageergebnisse werden angezeigt. Siehe Abbildung 4–10.

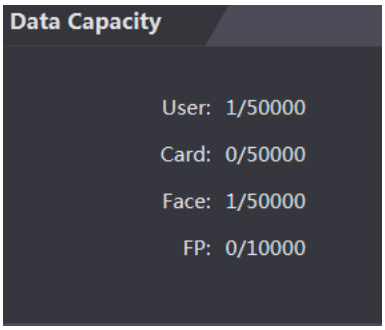
Abbildung 4–10 Abfrageergebnisse



4.5 Datenkapazität

Sie können sehen, wie viele Benutzer, Karten und Gesichtsbilder der Zugangs-Controller im Menü **Datenkapazität** (Data Capacity) halten kann.

Abbildung 4–11 Datenkapazität



4.6 Videoeinstellungen

Sie können Parameter wie Datenrate, Bildparameter (Helligkeit, Kontrast, Farbton, Sättigung und mehr) und Belichtung im Menü **Videoeinstellungen** (Video Setting) einstellen.

4.6.1 Datenrate

Abbildung 4–12 Datenrate

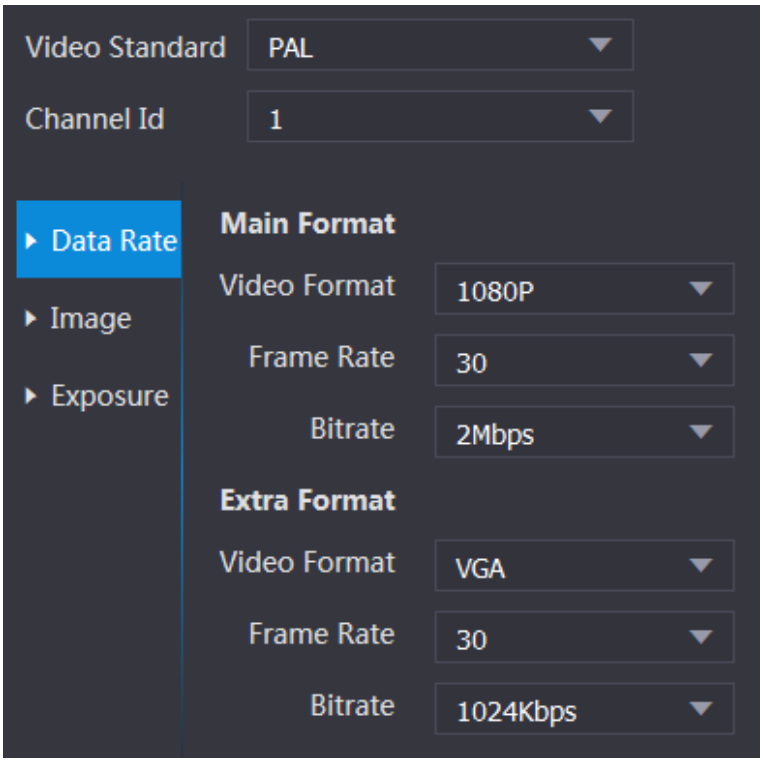


Tabelle 4–2 Beschreibung der Datenrateparameter

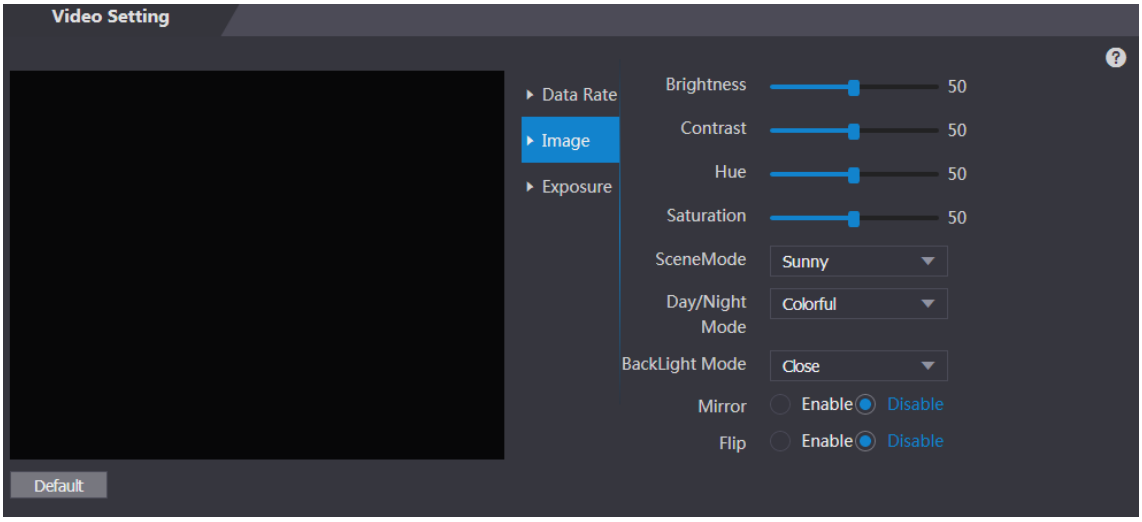
Parameter		Beschreibung
Videostandard		Es gibt zwei Optionen: NTSC und PAL. Wählen Sie einen Standard entsprechend dem Videostandard Ihrer Region.
Kanal		Es gibt zwei Optionen: 1 und 2. 1 ist Weißlichtkamera und 2 ist IR-Licht-Kamera.
Hauptformat	Videoformat	Es gibt vier Optionen: D1, VGA, 720p und 1080p. Wählen Sie eine Option entsprechend der von Ihnen gewünschten Videoqualität.
	Bildfrequenz	Die Frequenz, mit der aufeinanderfolgende Bilder auf dem Bildschirm angezeigt werden. Der Bildfrequenzbereich beträgt 1 - 30 BpS.
	Bitrate	Die Anzahl der Bits, die pro Zeiteinheit befördert oder verarbeitet werden. Es gibt fünf Optionen: 2 Mbps, 4 Mbps, 6 Mbps, 8 Mbps und 10 Mbps.
Extra-Format	Videoformat	Hier haben Sie drei Optionen: D1, VGA und QVGA.
	Bildfrequenz	Die Frequenz, mit der aufeinanderfolgende Bilder auf dem Bildschirm angezeigt werden. Der Bildfrequenzbereich beträgt 1 - 30 BpS.
	Bitrate	Die Anzahl der Bits, die pro Zeiteinheit befördert oder verarbeitet werden. Es gibt die folgenden Optionen: 512 Kbps, 640 Kbps, 768 Kbps, 896 Kbps, 1024 Kbps, 1,25 Mbps, 1,5 Mbps, 1,75 Mbps und 2 Mbps.

4.6.2 Bild

Es gibt zwei Kanäle und Sie müssen für jeden Kanal die Parameter konfigurieren.

Schritt 1: Wählen Sie **Videoeinstellungen > Videoeinstellungen > Bild** (Video Setting > Video Setting > Image).

Abbildung 4–13 BIld



Schritt 2: Wählen Sie im Gegenlichtmodus **Große Dynamik** (Wide Dynamic).

Tabelle 4–3 Beschreibung der Bildparameter

Parameter	Beschreibung
Helligkeit	Je größer der Wert ist, desto heller wird das Bild.
Kontrast	Kontrast ist der Unterschied in der Leuchtdichte oder Farbe, der ein Objekt unterscheidbar macht. Je größer der Kontrastwert ist, desto größer ist die Helligkeit und der Farbkontrast.
Farbton	Je größer der Wert ist, desto tiefer ist die Farbe.
Sättigung	Je größer der Wert ist, desto kräftiger sind die Farben.  Der Wert ändert die Bildhelligkeit nicht.
Szenenmodus	● Deaktivieren: Ohne Modi. ● Auto: Das System passt die Szenenmodi automatisch an. ● Sonnig: In diesem Modus wird der Farbton des Bildes reduziert. ● Nacht: In diesem Modus wird der Farbton des Bildes verstärkt.  **Sonnig** (Sunny) ist standardmäßig ausgewählt.
Tag/Nacht-Modus	Der Tag/Nachtmodus entscheidet über den Arbeitsstatus der Aufhellung. ● Auto: Das System passt den Tag/Nachtmodus automatisch an. ● Farbig: In diesem Modus sind die Bilder farbig. ● Schwarzweiß: In diesem Modus sind die Bilder Schwarz-Weiß.
Gegenlichtmodus	● Deaktivieren: Ohne Gegenlichtkompensation. ● BLC: Die Gegenlichtkompensation korrigiert Regionen mit extrem hohen oder niedrigen Lichtstärken, um ein normales und für das fokussierte Objekt nutzbares Lichtniveau beizubehalten. ● WDR: Im Modus mit großem Dynamikbereich dimmt das System helle Bereiche und kompensiert dunkle Bereiche, um die Definition von Objekten in den hellen und dunklen Bereichen zu gewährleisten.  Wenn menschliche Gesichter im Gegenlicht zu sehen sind, müssen Sie WDR aktivieren. ● HLC: Die Spitzlichtkompensation wird benötigt, um die Überbelichtung von Spitzlichtern oder starken Lichtquellen wie Scheinwerfern, Stirnlampen, Taschenlampen usw. auszugleichen, um ein Bild zu erzeugen, das brauchbar ist und nicht von einem hellen Licht überstrahlt wird.
Spiegeln	Wenn die Funktion aktiviert ist, werden Bilder mit umgekehrter linker und rechter Seite angezeigt.
Drehen	Wenn diese Funktion aktiviert ist, werden Bilder auf den Kopf gestellt angezeigt.

4.6.3 Belichtung

Tabelle 4–4 Beschreibung der Belichtungsparameter

Parameter	Beschreibung
Anti-Flimmern	● 50 Hz: Wenn die Netzfrequenz von Wechselstrom 50 Hz beträgt, wird die Belichtung automatisch angepasst, um zu gewährleisten, dass sich keine Streifen auf den Bildern befinden. ● 60 Hz: Wenn die Netzfrequenz von Wechselstrom 60 Hz beträgt, wird die Belichtung automatisch angepasst, um zu gewährleisten, dass keine Streifen auf den Bildern zu sehen sind. ● Außenbereich: Wenn **Außenbereich** (Outdoor) gewählt wird, kann der Belichtungsmodus umgeschaltet werden.
Belichtungsmodus	 Wenn Sie im Aufklappmenü Anti-Flimmern **Außenbereich** (Outdoor) wählen, können Sie **Verschluss Priorität** (Shutter Priority) als Belichtungsmodus wählen. Die Belichtungsmodi der verschiedenen Geräte können variieren, und das tatsächliche Produkt ist maßgebend. Sie können wählen: ● Auto: Der Zugangs-Controller passt die Helligkeit der Bilder automatisch an. ● Verschluss Priorität: Der Zugangs-Controller passt die Bildhelligkeit entsprechend dem Belichtungswertebereich des Verschlusses an. Wenn die Helligkeit des Bildes nicht ausreicht und der Verschlusswert die obere oder untere Grenze erreicht hat, passt der Zugangs-Controllerden Verstärkungswert automatisch an, um die ideale Helligkeit zu erreichen. ● Manuell: Sie können Verstärkungs- und Verschlusswert manuell konfigurieren, um die Bildhelligkeit einzustellen.
Verschluss	Je größer der Verschlusswert und je kürzer die Belichtungszeit ist, desto dunkler werden die Bilder.
Verschlusswertbereich	Wenn Sie **Benutzerdefinierter Bereich** (Customized Range) wählen, können Sie den Verschlusswertbereich anpassen.
Verstärkungswertbereich	Wenn der Verstärkungswertbereich eingestellt ist, wird die Videoqualität verbessert.
Belichtungskorrektur	Sie können die Videohelligkeit erhöhen, indem Sie den Belichtungskorrekturwert anpassen.
3D NR	Wenn die 3D-Rauschunterdrückung (RD) aktiviert ist, kann das Videorauschen reduziert werden, und es werden hochauflösende Videos produziert.
Qualität	Sie können den Wert von 3D NR einstellen, wenn 3D NR aktiviert ist. Je größer der Wert ist, desto geringer ist das Rauschen.

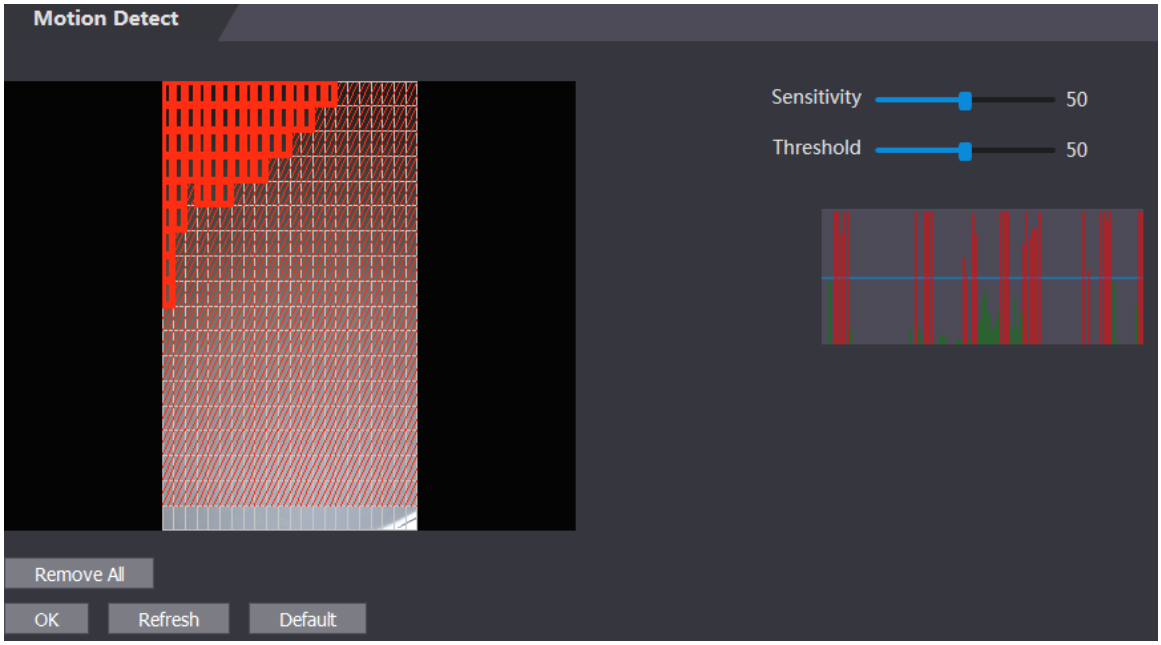
4.6.4 Bewegungserkennung

Legen Sie einen Bereich fest, in dem sich bewegende Objekte erkannt werden können.

Schritt 1: Wählen Sie **Videoeinstellungen > Videoeinstellungen > Bewegungserkennung** (Video Setting > Video Setting > Motion Detection).

Das Menü **Bewegungserkennung** (Motion Detection) wird angezeigt. Siehe Abbildung 4–14.

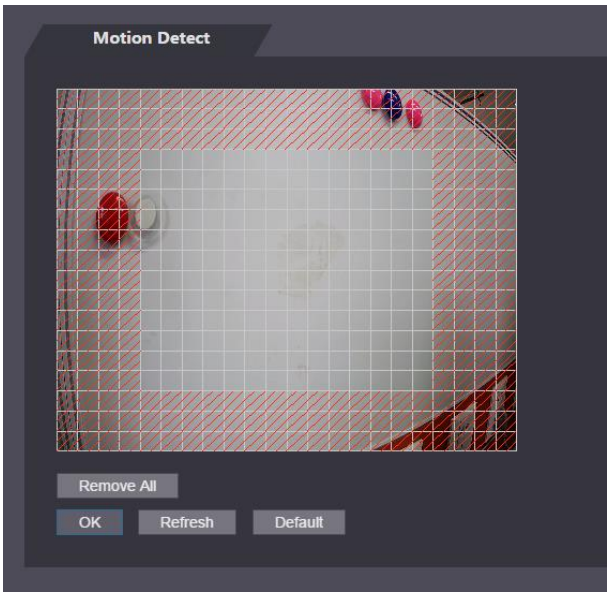
Abbildung 4–14 Bewegungserkennung



Schritt 2: Halten Sie die linke Maustaste gedrückt und ziehen Sie dann die Maus in den roten Bereich. Der **Bewegungserkennungsbereich** (Motion Detection) wird angezeigt. Siehe Abbildung 4–15.

- Die roten Rechtecke sind der Bewegungserkennungsbereich. Der standardmäßige Bewegungserkennungsbereich sind alle Rechtecke.
- Um einen Bewegungserkennungsbereich zu zeichnen, klicken Sie zunächst auf **Alle entfernen** (Remove All).
- Der von Ihnen gezeichnete Bewegungserkennungsbereich ist ein Nicht-Bewegungserkennungsbereich, wenn Sie den standardmäßigen Bewegungserkennungsbereich einzeichnen.

Abbildung 4–15 Bewegungserkennungsbereich



Schritt 3: Stellen Sie Empfindlichkeit und Schwellenwert ein.

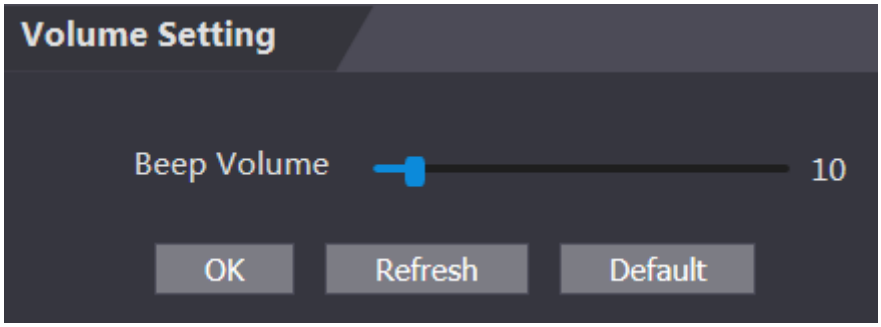
- Die Empfindlichkeit stellt die Fähigkeit jedes Rasters dar, Bewegungen zu erfassen. Je größer der Wert ist, desto höher ist die Empfindlichkeit.
- Der Schwellenwert ist die Bedingung der Bewegungserkennung. Wenn die Rasterzahl den Schwellenwert erreicht, wird die Bewegungserkennung ausgelöst. Je kleiner der Wert ist, desto wahrscheinlicher ist es, dass die Bewegungserkennung ausgelöst wird.
- Wenn die Rasterzahl kleiner als der Schwellenwert ist, erscheint eine grüne Linie; wenn die Rasterzahl größer als der Schwellenwert ist, erscheint eine rote Linie. Siehe Abbildung 4–14.

Schritt 4: Klicken Sie auf **OK**, um die Einstellung zu beenden.

4.6.5 Lautstärke einstellen

Sie können die Lautstärke des Lautsprechers des Zugangs-Controllers einstellen.

Abbildung 4–16 Lautstärkeeinstellung

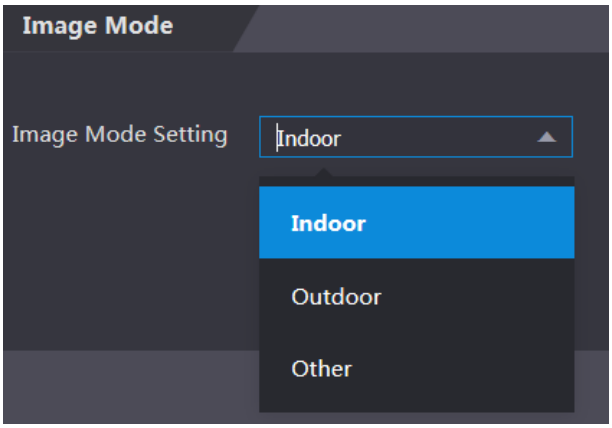


4.6.6 Bildmodus

Es gibt drei Optionen: Innen, Außenbereich und Sonstige. Wählen Sie **Innen** (Indoor), wenn der Zugangs-Controller im Innenbereich installiert ist, wählen Sie **Außenbereich** (Outdoor),

wenn der Zugangs-Controller im Außenbereich installiert ist und wählen Sie **Sonstige** (Other), wenn der Zugangs-Controller an Orten mit Gegenlicht wie Korridoren und Fluren installiert ist.

Abbildung 4–17 Bildmodus

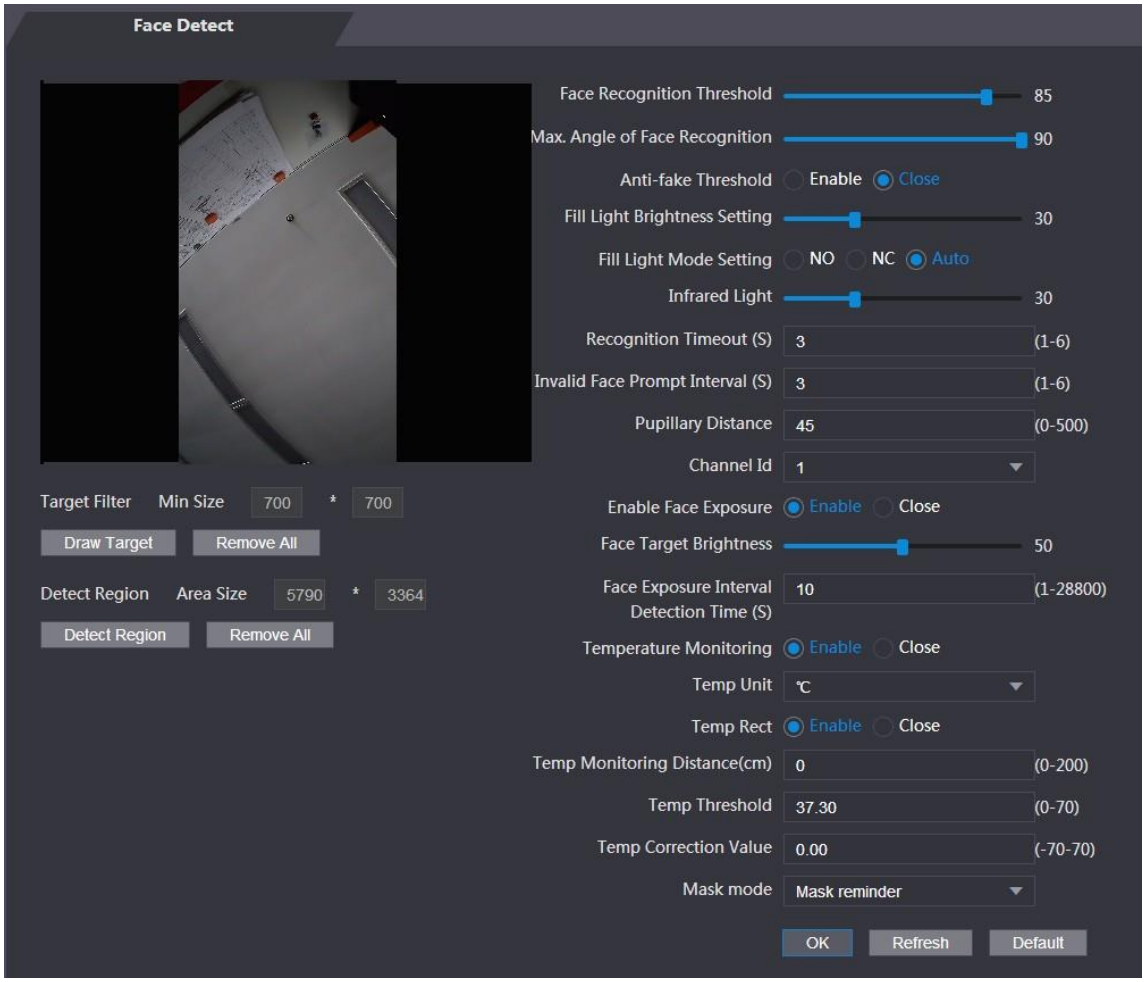


4.7 Gesichtserkennung

Sie können in diesem Menü Parameter für das menschliche Gesicht konfigurieren, um die Genauigkeit der Gesichtserkennung zu erhöhen.

Schritt 1: Wählen Sie **Gesichtserkennung** (Face Detect).

Abbildung 4–18 Gesichtserkennung



Schritt 2: Konfigurieren Sie die Parameter.

Tabelle 4–5 Beschreibung der Gesichtserkennungsparameter

Parameter	Beschreibung
Schwelle der Gesichtserkennung	Je größer der Wert ist, desto höher ist die Genauigkeit.
Max. Winkel der Gesichtserkennung	Je größer der Winkel ist, desto größer ist der Bereich der Profile, der erkannt wird.
Fälschungs-Schwellenwert	Diese Funktion verhindert, dass Personen durch menschliche Gesichtsbilder oder Gesichtsmodelle entriegeln können. Es gibt zwei Optionen: **Aktivieren** (Enable) und **Schließen** (Close).
Einstellung der Helligkeit des Aufhelllichts	Sie können die Helligkeit des Aufhelllichts einstellen.
Aufhelllichtmodus einstellen	Es gibt drei Aufhelllichtmodi. ● NO: Das Aufhelllicht ist normalerweise eingeschaltet. ● NC: Das Aufhelllicht ist normalerweise ausgeschaltet. ● Auto: Das Aufhelllicht wird automatisch eingeschaltet, wenn ein Bewegungserkennungsereignis ausgelöst wird. Wenn **Auto** gewählt wird, ist das Aufhelllicht auch dann nicht eingeschaltet, wenn der Infrarotlicht-Wert größer als 19 ist.
Infrarot-Licht	Stellen Sie die IR-Lichthelligkeit durch Ziehen des Schiebereglers ein.
Zeitüberschreitung bei Erkennung	Wenn eine Person, die nicht über eine Zugangsberechtigung verfügt, vor dem Zugangs-Controller steht und das Gesicht erkannt wird, meldet der Controller, dass die Gesichtserkennung fehlgeschlagen ist. Das Meldeintervall wird als Zeitüberschreitung bei Erkennung bezeichnet.
Meldeintervall ungültiges Gesicht	Wenn ein Gesicht ohne Zugangsberechtigung vor dem Zugangs-Controller steht, meldet der Controller, dass das Gesicht ungültig ist. Das Meldeintervall ist ein ungültiges Gesichtsmeldeintervall.
Pupillenabstand	Der Pupillenabstand ist der Pixelwert des Bildes zwischen den Mittelpunkten der Pupillen in beiden Augen. Sie müssen einen geeigneten Wert einstellen, damit der Zugangs-Controller bei Bedarf Gesichter erkennen kann. Der Wert ändert sich in Abhängigkeit von den Gesichtsgrößen und dem Abstand zwischen den Gesichtern und dem Objektiv. Je näher das Gesicht am Objektiv ist, desto größer sollte der Wert sein. Wenn sich ein Erwachsener 1,5 m vom Objektiv entfernt befindet, kann der Wert für den Pupillenabstand zwischen 50 und 70 liegen.
Gesichtsbelichtung aktivieren	Nachdem die Gesichtsbelichtung aktiviert wurde, ist das menschliche Gesicht klarer, wenn der Zugangs-Controller im Freien installiert ist.
Kanal-ID	Es gibt zwei Optionen: 1 und 2. 1 ist Weißlichtkamera und 2 ist IR-Licht-Kamera.

Parameter	Beschreibung
Ziel zeichnen	Klicken Sie auf **Ziel zeichnen** (Draw Target), um den minimalen Gesichtserfassungsrahmen zu zeichnen. Klicken Sie auf **Alle entfernen** (Remove All), um alle von Ihnen gezeichneten Rahmen zu entfernen.
Erkennungsbereich	Klicken Sie auf **Erkennungsbereich** (Detect Region) und passen Sie mit der Maus den Gesichtserfassungsbereich an. Klicken Sie auf **Alle entfernen** (Remove All), um alle Gesichtserfassungsbereiche zu entfernen.
Gesicht Zielhelligkeit	Der Standardwert ist 50. Stellen Sie die Helligkeit nach Bedarf ein.
Belichtungsintervall Gesicht	Nachdem ein Gesicht erkannt wurde, schaltet der Zugangs-Controller Licht ein, um das Gesicht zu beleuchten, und der Zugangs-Controller schaltet erst wieder Licht ein, wenn das von Ihnen eingestellte Intervall verstrichen ist.
Temperaturüberwachung	Stellen Sie ein, ob die Überwachung der Körpertemperatur aktiviert werden soll. ● Temperatureinheit: Wählen Sie eine Temperatureinheit. ● Temperaturrechteck: Stellen Sie ein, ob die Temperaturüberwachung aktiviert werden soll oder nicht. ● Abstand der Temperaturüberwachung (cm): Der Wert ist standardmäßig 0. Stellen Sie andere Werte ein, um die Temperaturüberwachung innerhalb eines definierten Abstands zu ermöglichen. 80 cm wird empfohlen. ● Temperatur-Schwellenwert (°C): Stellen Sie die Temperaturschwelle ein. Die überwachte Körpertemperatur wird als hohe Temperatur gewertet, wenn sie größer oder gleich dem eingestellten Wert ist. ● Temperatur-Korrekturwert: Dieser Parameter dient Testzwecken. Die Differenz der Temperaturüberwachungsumgebung kann zu einer Temperaturabweichung zwischen der überwachten Temperatur und der Ist-Temperatur führen. Sie können mehrere überwachte Stichproben für Tests auswählen. Entsprechend dem Vergleich zwischen der überwachten Temperatur und der Ist-Temperatur können Sie mit diesem Parameter die Temperaturabweichung korrigieren. Wenn beispielsweise die überwachte Temperatur um 0,5 °C niedriger als die Ist-Temperatur ist, wird der Korrekturwert auf 0,5 °C eingestellt; wenn die überwachte Temperatur um 0,5 °C höher als die Ist-Temperatur ist, wird der Korrekturwert auf -0,5 °C eingestellt. 📖 Nur der Zugangs-Controller mit einer Temperaturüberwachungseinheit unterstützt diesen Parameter.

Parameter	Beschreibung
Masken-Modus	● Nicht erkannt: Maske wird bei der Gesichtserkennung nicht erkannt. ● Maske Erinnerung: Maske wird bei der Gesichtserkennung erkannt. Wenn die Person erkannt wird, ohne eine Maske zu tragen, erinnert das System an die Maske, und der Durchgang wird erlaubt. ● Maske abfangen: Maske wird bei der Gesichtserkennung erkannt. Wenn die Person erkannt wird, ohne eine Maske zu tragen, erinnert das System an die Maske, und der Durchgang wird nicht erlaubt.

Schritt 3: Klicken Sie auf **OK**, um die Einstellung zu beenden.

4.8 Netzwerkeinstellungen

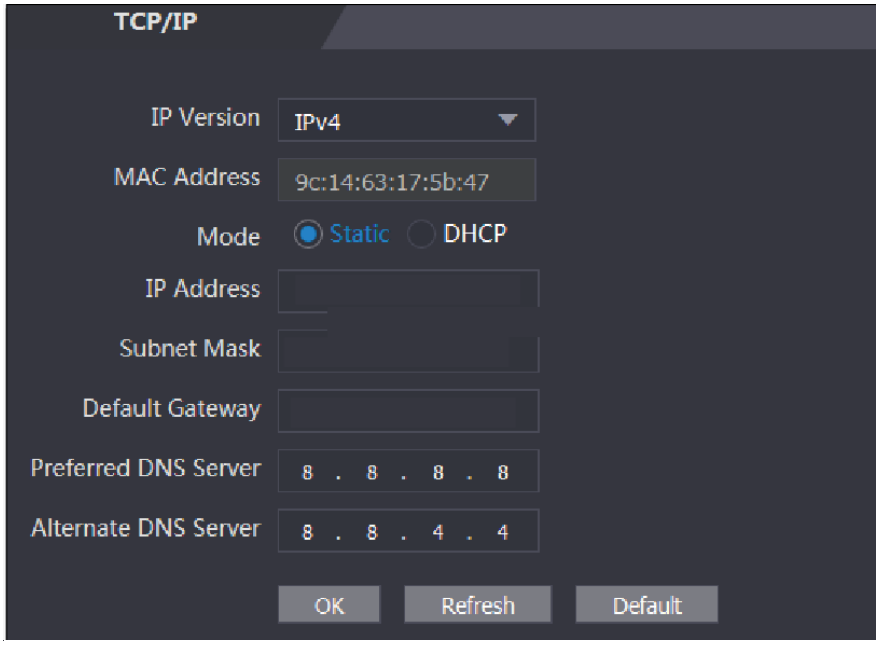
4.8.1 TCP/IP

Sie müssen IP-Adresse und DNS-Server konfigurieren, um zu gewährleisten, dass der Zugangs-Controller mit anderen Geräten kommunizieren kann.

Vergewissern Sie sich, dass der Zugangs-Controller korrekt mit dem Netzwerk verbunden ist.

Schritt 1: Wählen Sie **Netzwerkeinstellungen > TCP/IP** (Network Setting > TCP/IP).

Abbildung 4–19 TCP/IP



Schritt 2: Konfigurieren Sie die Parameter.

Tabelle 4–6 TCP/IP

Parameter	Beschreibung
IP-Version	Es gibt eine Option: IPv4.
MAC-Adresse	Die MAC-Adresse des Zugangs-Controllers wird angezeigt.
Modus	● Statisch Stellen Sie IP-Adresse, Subnetzmaske und Gateway-Adresse manuell ein. ● DHCP ◇ Nachdem DHCP aktiviert wurde, können IP-Adresse, Subnetzmaske und Gateway-Adresse nicht konfiguriert werden. ◇ Wenn DHCP wirksam ist, werden IP-Adresse, Subnetzmaske und Gateway-Adresse automatisch angezeigt; wenn DHCP nicht wirksam ist, sind IP-Adresse, Subnetzmaske und Gateway-Adresse leer. ◇ Wenn Sie die Standard-IP sehen möchten, wenn DHCP wirksam ist, müssen Sie DHCP deaktivieren.
IP-Adresse	Geben Sie die IP-Adresse ein und konfigurieren Sie dann die Subnetzmaske und die Gateway-Adresse. IP-Adresse und Gateway-Adresse müssen sich im gleichen Netzwerksegment befinden.
Subnetzmaske	
Standardgateway	
Bevorzugter DNS-Server	Stellen Sie die IP-Adresse des bevorzugten DNS-Servers ein.
Alternativer DNS-Server	Stellen Sie die IP-Adresse des alternativen DNS-Servers ein.

Schritt 3: Klicken Sie auf **OK**, um die Einstellung zu beenden.

4.8.2 Port

Stellen Sie die Höchstzahl der Verbindungs-Clients, mit denen der Zugangs-Controller verbunden werden kann, und Portnummern ein.

Schritt 1: Wählen Sie **Netzwerkeinstellungen > Port** (Network Setting > Port).

Das Menü **Port** wird angezeigt.

Schritt 2: Konfigurieren Sie die Portnummern. Siehe nachstehende Tabelle.

Mit Ausnahme der Höchstzahl der Verbindungen müssen Sie den Zugangs-Controller neu starten, damit die Konfiguration nach der Änderung von Werten wirksam wird.

Tabelle 4–7 Beschreibung der Ports

Parameter	Beschreibung
Höchstzahl der Verbindungen	Sie können die Höchstzahl der Verbindungen von Clients festlegen, mit denen der Zugangs-Controller verbunden werden kann. Plattform-Clients wie Smart PSS werden nicht mitgezählt.
TCP-Port	Der Standardwert ist 37777.

Parameter	Beschreibung
HTTP-Port	Der Standardwert ist 80. Wenn ein anderer Wert als Portnummer verwendet wird, müssen Sie diesen Wert beim Anmelden über Browser hinter der Adresse hinzufügen.
HTTPS-Port	Der Standardwert ist 443.
RTSP-Port	Der Standardwert ist 554.

Schritt 3: Klicken Sie auf **OK**, um die Einstellung zu beenden.

4.8.3 Registrieren

Wenn der Zugangs-Controller mit einem externen Netzwerk verbunden ist, meldet er seine Adresse an den Server, den der Benutzer bestimmt hat, damit Clients auf den Zugangs-Controller zugreifen können.

Schritt 1: Wählen Sie **Netzwerkeinstellungen > Autom. Registrierung** (Network Setting > Auto Register).

Das Menü **Autom. Registrierung** (Auto Register) wird angezeigt.

Schritt 2: Wählen Sie **Aktivieren** (Enable) und geben Sie Host-IP, Port und Unter-Geräte-ID ein.

Tabelle 4–8 Beschreibung Automatische Registrierung

Parameter	Beschreibung
Host-IP	Server IP-Adresse oder Server-Domänenname.
Port	Für die automatische Registrierung verwendeter Server-Port.
Unter-Geräte-ID	Vom Server zugewiesene Zugangs-Controller-ID.

Schritt 3: Klicken Sie auf **OK**, um die Einstellung zu beenden.

4.8.4 P2P

Peer-to-Peer-Computing oder Networking ist eine verteilte Anwendungsarchitektur, die Aufgaben oder Arbeitslasten zwischen Kollegen (Peers) aufteilt. Sie können eine mobile Anwendung herunterladen, indem Sie den QR-Code scannen und dann ein Konto registrieren, sodass mehr als ein Zugangs-Controller auf der mobilen Anwendung verwaltet werden kann. Sie müssen keine dynamischen Domänennamen verwenden, Port-Mapping durchführen und Sie benötigen nicht den Transit-Server.

Wenn Sie P2P verwenden möchten, müssen Sie den Zugangs-Controller mit einem externen Netzwerk verbinden, anderenfalls kann der Zugangs-Controller nicht verwendet werden.

Abbildung 4–20 P2P

Schritt 1: Wählen Sie **Netzwerkeinstellungen > P2P** (Network Setting > P2P).
Das Menü **P2P** wird angezeigt.
Schritt 2: Wählen Sie **Aktivieren** (Enable), um die P2P-Funktion zu aktivieren.
Schritt 3: Klicken Sie auf **OK**, um die Einstellung zu beenden.

Scannen Sie den QR-Code auf Ihrer Web-Oberfläche, um die Seriennummer des Zugangs-Controllers zu erhalten.

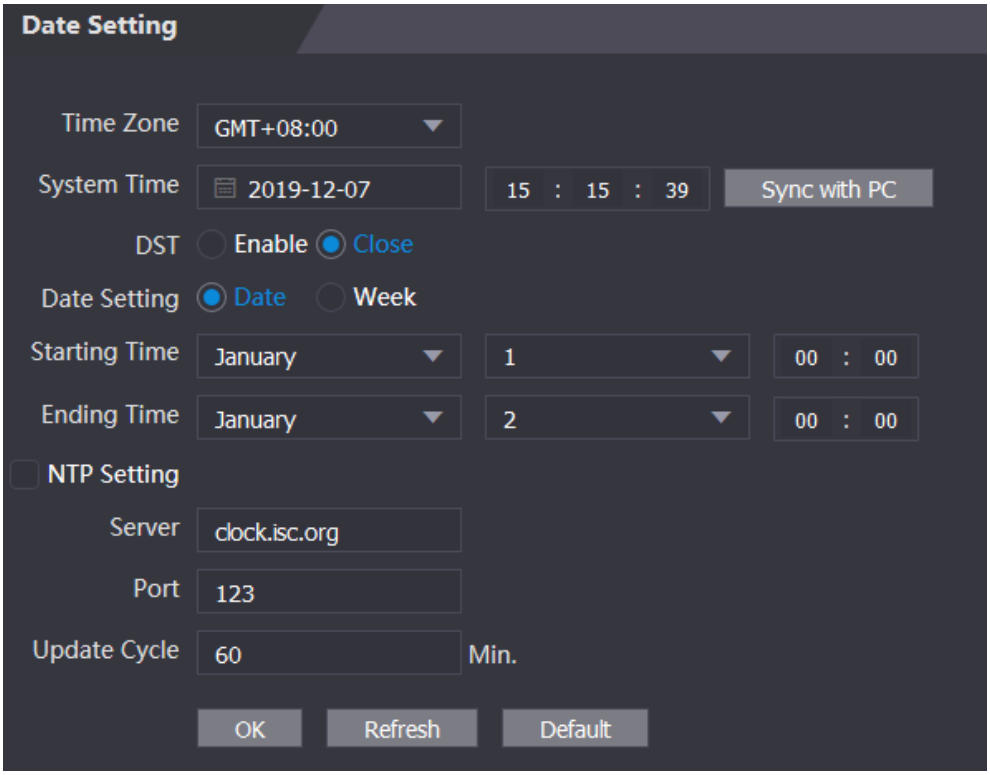
4.9 Datum einstellen

Sie müssen Zeitzone, Uhrzeit, Sommerzeit und NTP für den Zugangs-Controller einstellen.

Diese Funktion wird nur von bestimmten Modellen unterstützt.

Schritt 1: Wählen Sie **Datum einstellen** (Date Setting).
Das Menü **Datum einstellen** (Date Setting) wird angezeigt. Siehe Abbildung 4–21

Abbildung 4–21 Datum einstellen



Schritt 2: Stellen Sie die Parameter ein.

Tabelle 4–9 Datum einstellen

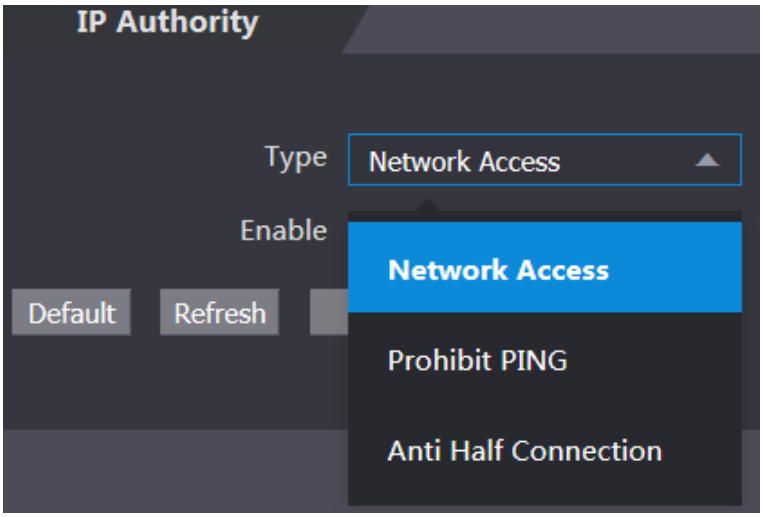
Parameter	Beschreibung
Zeitzone	Wählen Sie Ihre Zeitzone.
Systemzeit	Sie können die Systemzeit manuell einstellen oder Sie klicken auf **Mit PC synchronisieren** (Sync with PC), um die Zeit des Zugangs-Controllers mit der Computerzeit zu synchronisieren.
Sommerzeit	1. Sommerzeit aktivieren. 2. Wählen Sie **Datum** (Date) oder **Woche** (Week) in **Datum einstellen** (Date Setting). 3. Stellen Sie die **Startzeit** (Starting Time) und die **Endzeit** (Ending Time) ein.
NTP-Einstellung	1. **NTP-Einstellung** (NTP Setting) aktivieren. 2. Konfigurieren Sie die Parameter. ◇ Server: Geben Sie den Domänennamen des NTP-Servers ein. Die Zeit des Zugangs-Controllers wird mit dem NTP-Server synchronisiert. ◇ Port: Geben Sie die Portnummer des NTP-Servers ein. ◇ Aktualisierungszyklus: Stellen Sie einen Aktualisierungszyklus ein, damit wird die Zugangs-Controller-Zeit entsprechend aktualisiert. 3. Klicken Sie auf **OK**.

4.10 Sicherheitsmanagement

4.10.1 IP-Verwaltung

Wählen Sie einen Cyber-Sicherheitsmodus.

Abbildung 4–22 IP-Verwaltung



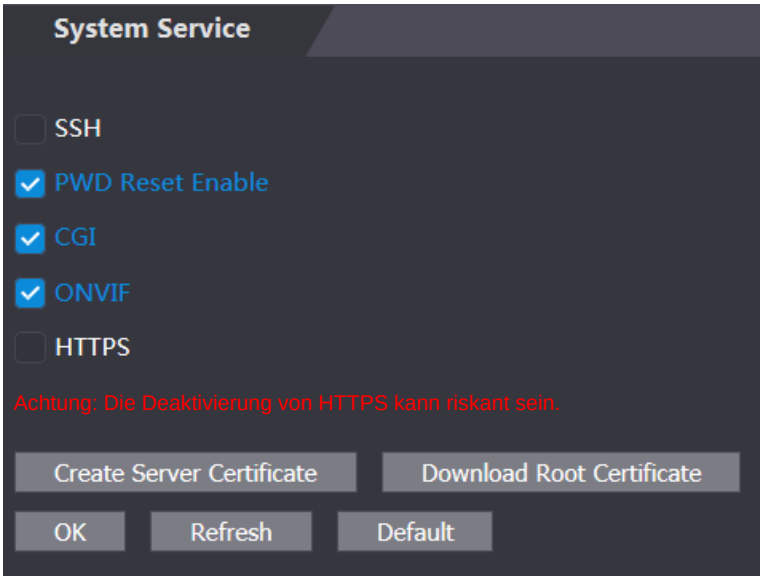
4.10.2 Systeme

4.10.2.1 Systemdienst

Es gibt vier Optionen: SSH, Passwort-Rücksetzung aktivieren, CGI und HTTPS. Siehe „3.12 Funktionen“ um eine oder mehrere auszuwählen.

Die auf der Web-Oberfläche vorgenommene Konfiguration des Systemdienstes und die Konfiguration im Menü **Funktionen** (Features) des Zugangs-Controller wird synchronisiert.

Abbildung 4–23 Systemdienst



4.10.2.2 Server-Zertifikat erstellen

Klicken Sie auf **Server-Zertifikat erstellen** (Create Server Certificate), geben Sie die erforderlichen Daten ein, klicken Sie auf **Speichern** (Save), damit startet der Zugangs-Controller neu.

4.10.2.3 Stammzertifikat herunterladen

Schritt 1: Klicken Sie auf **Stammzertifikat herunterladen** (Download Root Certificate).
Wählen Sie im Dialogfenster **Datei speichern** (Save File) einen Pfad zum Speichern des Zertifikats.
Schritt 2: Doppelklicken Sie auf das heruntergeladene **Stammzertifikat** (Root Certificate), um es zu installiren. Folgen Sie den Anweisungen auf dem Bildschirm, um das Zertifikat zu installieren.

4.11 Benutzerverwaltung

Sie können Benutzer hinzufügen und löschen, Benutzer-Passwörter ändern und eine E-Mail-Adresse zum Zurücksetzen des Passworts eingeben, wenn Sie Ihr Passwort vergessen haben.

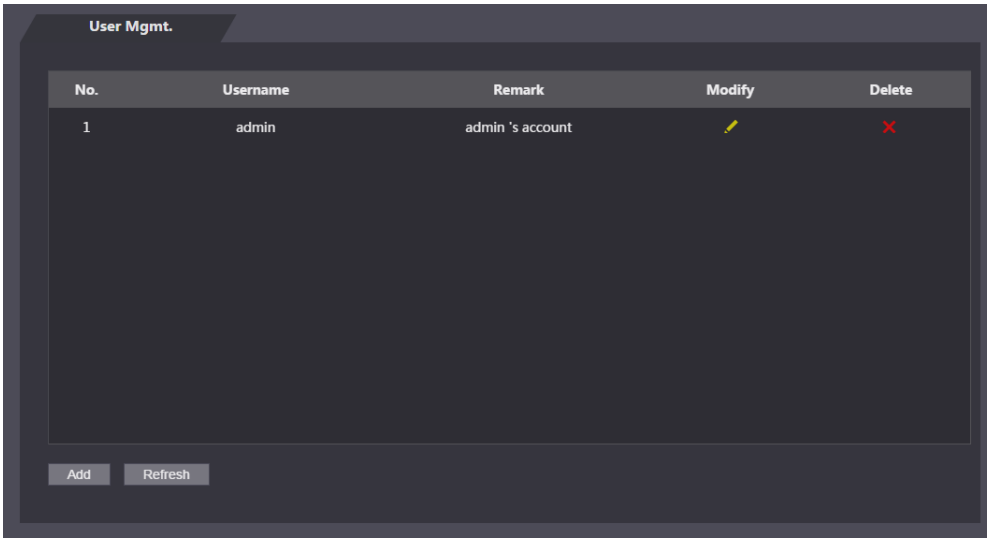
4.11.1 Benutzer hinzufügen

Klicken Sie auf **Hinzufügen** (Add) im Menü **Benutzerverwaltung** (User Mgmt.), um Benutzer hinzuzufügen, dann geben Sie Benutzername und Passwort ein, bestätigen das Passwort und schreiben Bemerkungen. Klicken Sie auf **OK**, um das Hinzufügen von Benutzern zu beenden.

4.11.2 Benutzerdaten modifizieren

Sie können Benutzerdaten modifizieren, indem Sie auf im Menü **Benutzerverwaltung** (User Mgmt.) klicken. Siehe Abbildung 4–24.

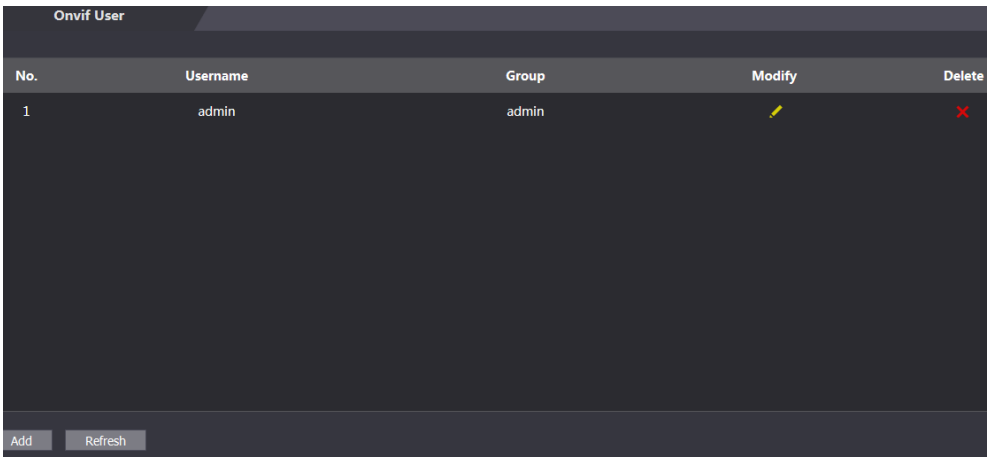
Abbildung 4–24 Benutzerverwaltung



4.11.3 ONVIF-Benutzer

Open Network Video Interface Forum (ONVIF) ist ein globales und offenes Industrieforum mit dem Ziel, die Entwicklung und Nutzung eines globalen offenen Standards für die Schnittstelle von physischen IP-basierten Sicherheitsprodukten zu erleichtern. Bei der Verwendung von ONVIF haben Administrator, Betreiber und Benutzer unterschiedliche Berechtigungen des ONVIF-Servers. Erstellen Sie nach Bedarf ONVIF-Benutzer.

Abbildung 4–25 ONVIF-Benutzer

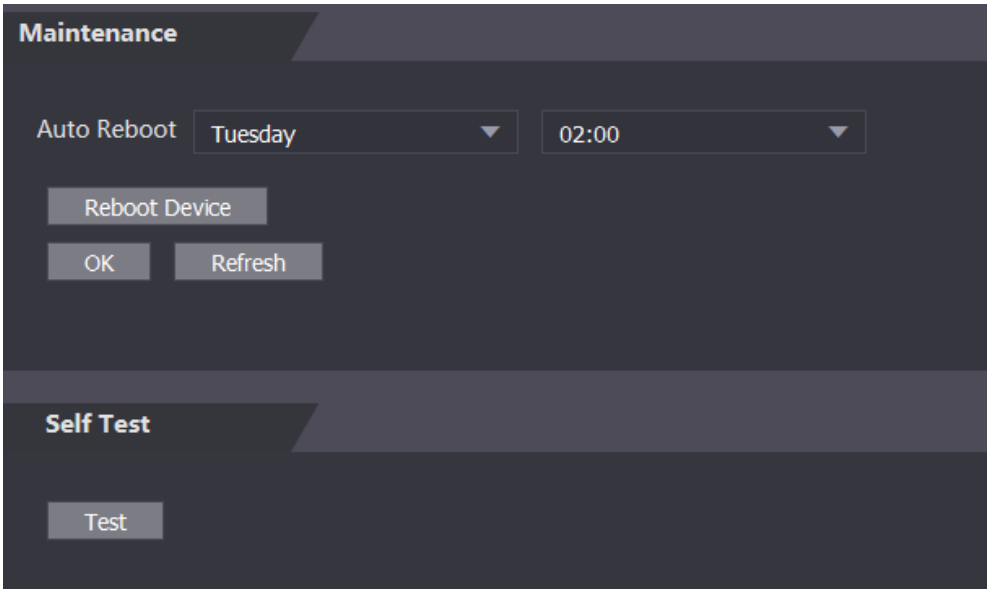


4.12 Wartung

Sie können den Zugangs-Controller in Ruhezeiten neu starten, um seine Laufgeschwindigkeit zu verbessern. Sie müssen die Zeit und das Datum für den automatischen Neustart einstellen.

Die Standard-Neustartzeit ist Dienstags um 2 Uhr morgens. Klicken Sie auf **Gerät neu starten** (Reboot Device), damit startet der Zugangs-Controller sofort neu. Klicken Sie auf **OK**, damit startet der Zugangs-Controller jeden Dienstag um 2 Uhr morgens neu. Siehe Abbildung 4–26.

Abbildung 4–26 Wartung



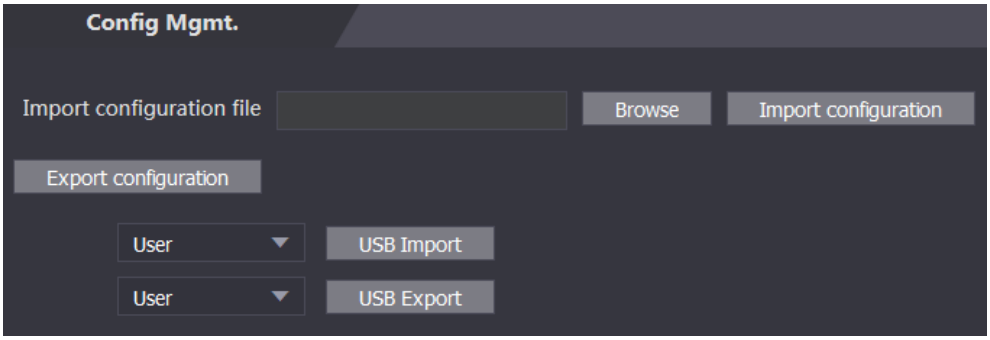
4.13 Konfigurationsverwaltung

Sie müssen die Konfigurationsverwaltung durchführen, Ergebnisrückmeldung freischalten, sowie Wiegand- und serielle Einstellungen für den Zugangs-Controller wählen.

4.13.1 Konfigurationsverwaltung

Wenn mehr als ein Zugangs-Controller die gleiche Konfiguration benötigt, können Sie Parameter für sie konfigurieren, indem Sie Konfigurationsdateien importieren oder exportieren. Siehe Abbildung 4–27.

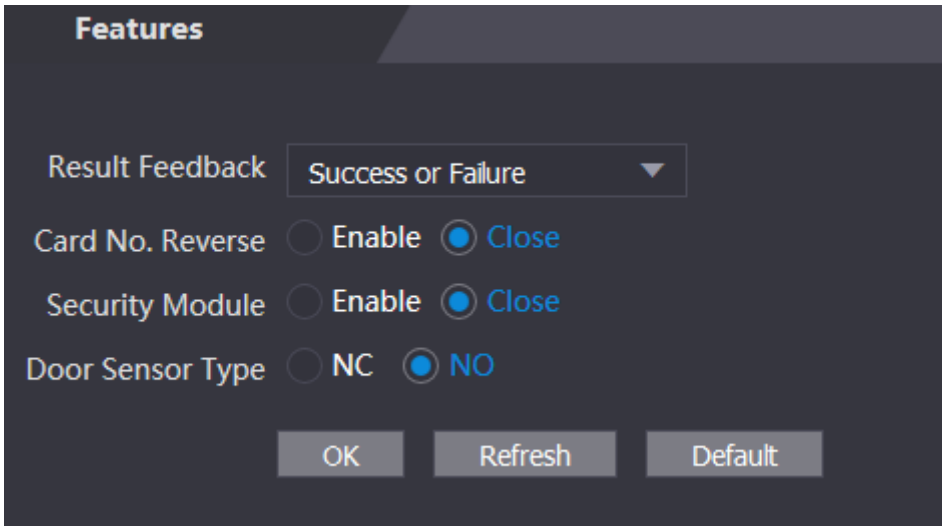
Abbildung 4–27 Konfigurationsverwaltung



4.13.2 Schlüsselmerkmale

Wählen Sie bei Bedarf Ergebnisrückmeldung. Für Details siehe „3.12.2 Ergebnisrückmeldung“.

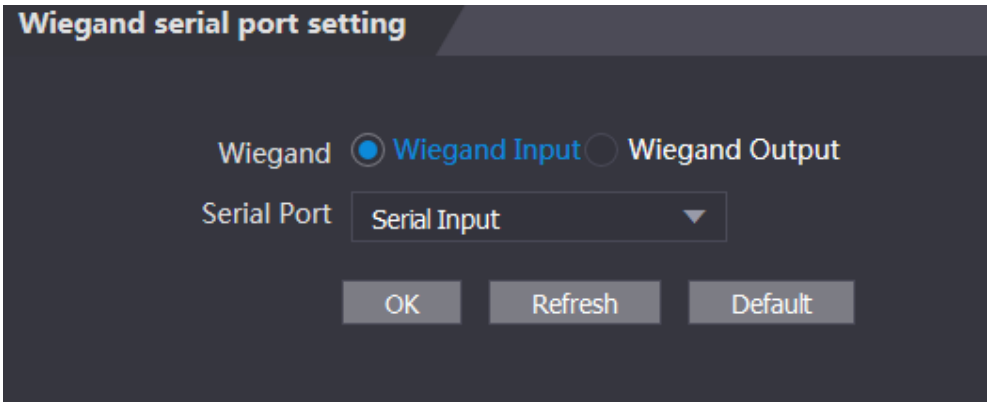
Abbildung 4–28 Funktionen



4.13.3 Wiegand seriellen Port einstellen

Wählen Sie Wiegand/seriellen Port einstellen. Einzelheiten finden Sie in den Abschnitten „3.9.2 Serielle Schnittstellen einstellen“ und „3.9.3 Wiegand-Konfiguration“.

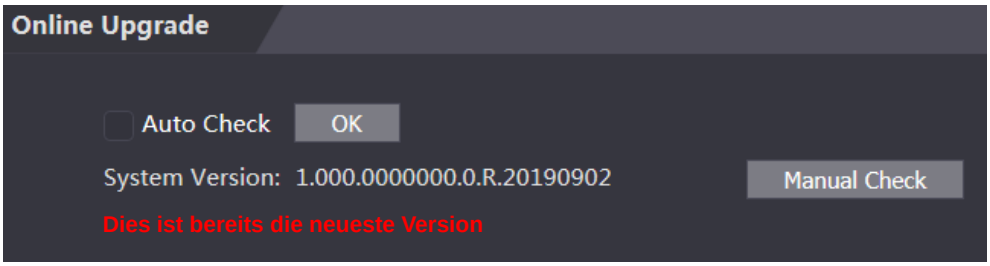
Abbildung 4–29 Wiegand seriellen Port einstellen



4.14 Aktualisieren

Wählen Sie **Autom. überprüfen** (Auto Check), um das System automatisch zu aktualisieren. Alternativ wählen Sie **Manuell überprüfen** (Manual Check), um das System manuell zu aktualisieren.

Abbildung 4–30



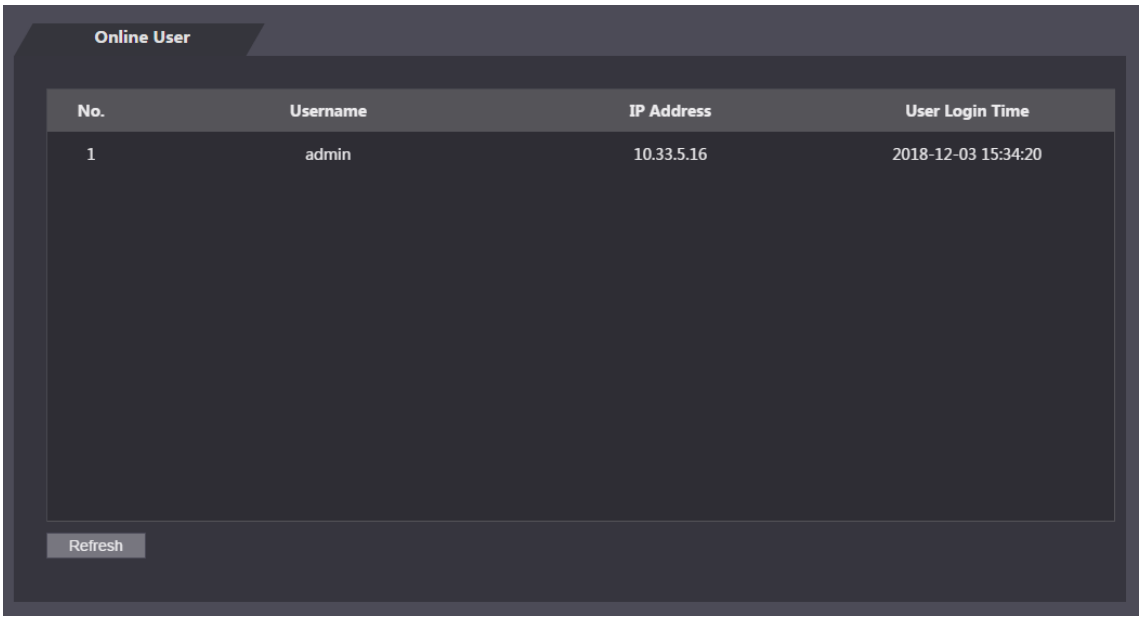
4.15 Versionsinformationen

Sie können Informationen wie MAC-Adresse, Seriennummer, MCU-Version, Web-Version, Sicherheits-Grundversion und Systemversion anzeigen.

4.16 Online-Benutzer

Sie können Benutzername, IP-Adresse und Benutzer-Anmeldezeit im Menü **Online-Benutzer** (Online User) anzeigen. Siehe Abbildung 4–31.

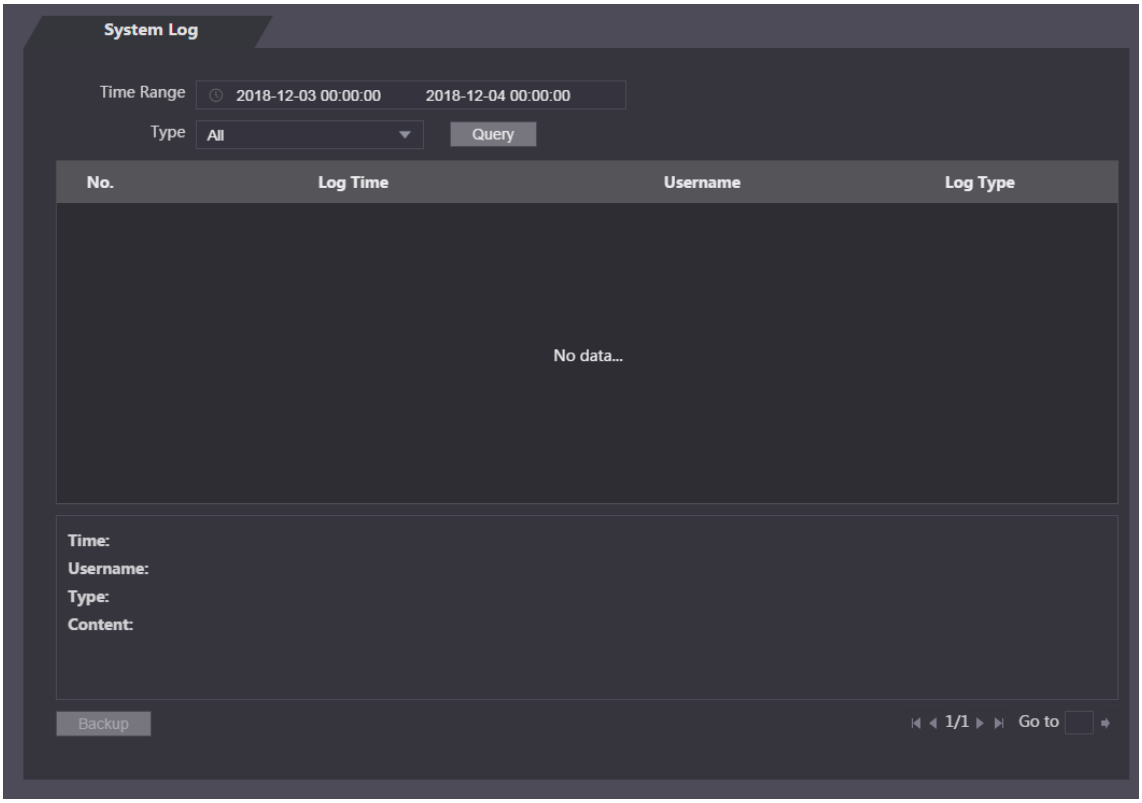
Abbildung 4–31 Online-Benutzer



4.17 Systemprotokoll

Sie können das Systemprotokoll im Menü **Systemprotokoll** (System Log) anzeigen und sichern.

Abbildung 4–32 Systemprotokoll



4.17.1 Protokolle abfragen

Wählen Sie einen Zeitbereich und seinen Typ und klicken Sie auf **Abfrage** (Query), damit werden die entsprechenden Protokolle angezeigt.

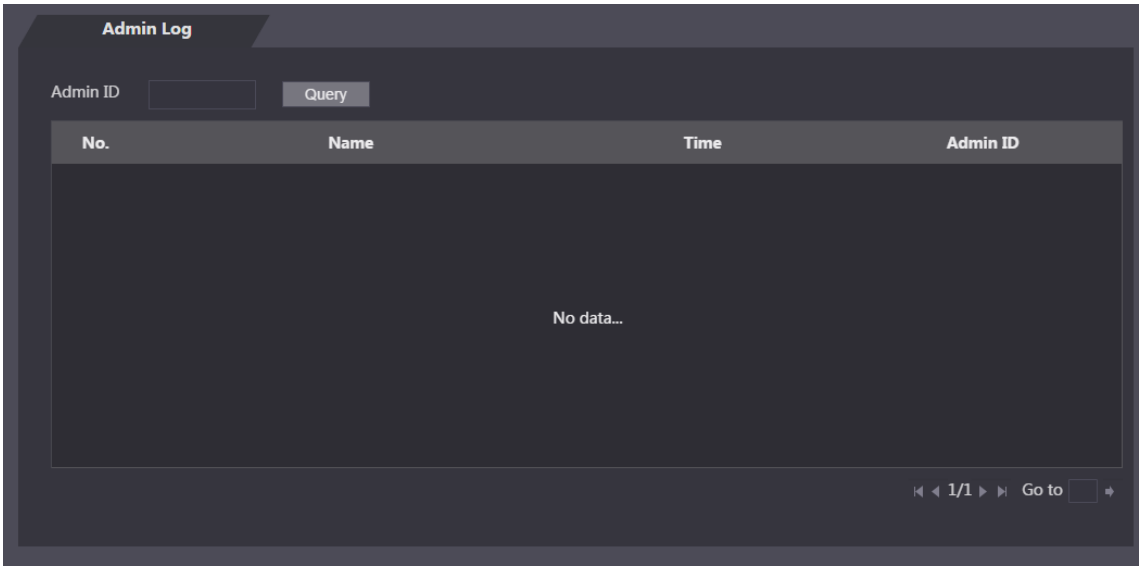
4.17.2 Protokolle sichern

Klicken Sie auf **Backup**, um die angezeigten Protokolle zu sichern.

4.17.3 Administrator-Protokoll

Geben Sie die Administrator-ID im Menü **Administrator-Protokoll** (Admin Log) ein und klicken Sie auf **Abfrage** (Query), um die Betriebsaufzeichnungen des Administrators anzuzeigen.

Abbildung 4–33 Administrator-Protokoll



Fahren Sie mit der Maus über , damit sehen Sie die detaillierten Informationen des aktuellen Benutzers.

4.18 Verlassen

Klicken Sie auf und dann auf **OK**, um sich in der Web-Oberfläche abzumelden.

5 FAQ

1 **Der Zugangs-Controller startet nach dem Einschalten nicht.**

Prüfen Sie, ob die 12-V-Stromversorgung korrekt angeschlossen ist und ob die Ein/Aus-Taste gedrückt wurde.

2 **Gesichter können nach dem Einschalten des Zugangs-Controllers nicht erkannt werden.**

Vergewissern Sie sich, dass Gesicht im Entriegelungsmodus gewählt ist. Siehe „3.8.2 Entsperren“.

Vergewissern Sie sich, dass Gesicht unter Zugang > Entriegelungsmodus > Gruppenkombination (Access > Unlock Mode > Group Combination) als Entsperrmodus gewählt ist. Siehe „3.8.2.3 Gruppenkombination“.

3 **Es gibt kein Ausgabesignal, wenn der Zugangs-Controller und der externe Controller am Wiegand-Port angeschlossen sind.**

Überprüfen Sie, ob die Massekabel des Zugangs-Controllers und des externen Controllers verbunden sind.

4 **Nachdem Administrator und Passwort vergessen wurden, können keine Konfigurationen mehr vorgenommen werden.**

Löschen Sie Administratoren über die Plattform oder wenden Sie sich an den technischen Support, um den Zugangs-Controller aus der Ferne zu entsperren.

5 **Benutzerdaten und Gesichtsbilder können nicht in den Zugangs-Controller importiert werden.**

Prüfen Sie, ob Namen von XML-Dateien und Titel von Tabellendateien geändert wurden, da das System die Dateien anhand ihrer Titel identifiziert.

6 **Das Gesicht eines Benutzers wird erkannt, aber die Daten anderer Benutzer werden angezeigt.**

Vergewissern Sie sich beim Importieren von Gesichtern, dass keine anderen Personen in der Nähe sind. Löschen Sie das Originalgesicht und importieren Sie es erneut.

Anhang 1 Hinweise zur Temperaturüberwachung

- Wärmen Sie die Temperaturüberwachungseinheit nach dem Einschalten für mehr als 20 Minuten auf, damit sie das thermische Gleichgewicht erreichen kann.
- Installieren Sie die Temperaturüberwachungseinheit in einer windstillen Innenumgebung, und halten Sie die Innentemperatur auf 15 °C bis 32 °C.
- Vermeiden Sie direkte Sonneneinstrahlung auf die Temperaturüberwachungseinheit.
- Vermeiden Sie die Installation der Temperaturüberwachungseinheit gegenüber einer Lichtquelle und einer Fensterscheibe.
- Halten Sie die Temperaturüberwachungseinheit von thermischen Störquellen fern.
- Faktoren wie Sonnenlicht, Wind, Kaltluft sowie kalte und warme Luft aus Klimaanlagen beeinflussen die Oberflächentemperatur des menschlichen Körpers, was zu einer Temperaturabweichung zwischen der überwachten Temperatur und der tatsächlichen Temperatur führt.
- Schwitzen ist ebenfalls eine Möglichkeit für den Körper, sich automatisch abzukühlen und Wärme abzuleiten, was ebenfalls eine Temperaturabweichung zwischen der überwachten und der tatsächlichen Temperatur verursacht.
- Warten Sie die Temperaturüberwachungseinheit regelmäßig (alle 2 Wochen). Verwenden Sie ein weiches Staubtuch, um den Staub auf der Oberfläche des Temperatursensors und des Abstandssensors vorsichtig abzuwischen, um ihn sauber zu halten.

Anhang 2 Hinweise zur Gesichtsaufnahme/Vergleich

Vor der Registrierung

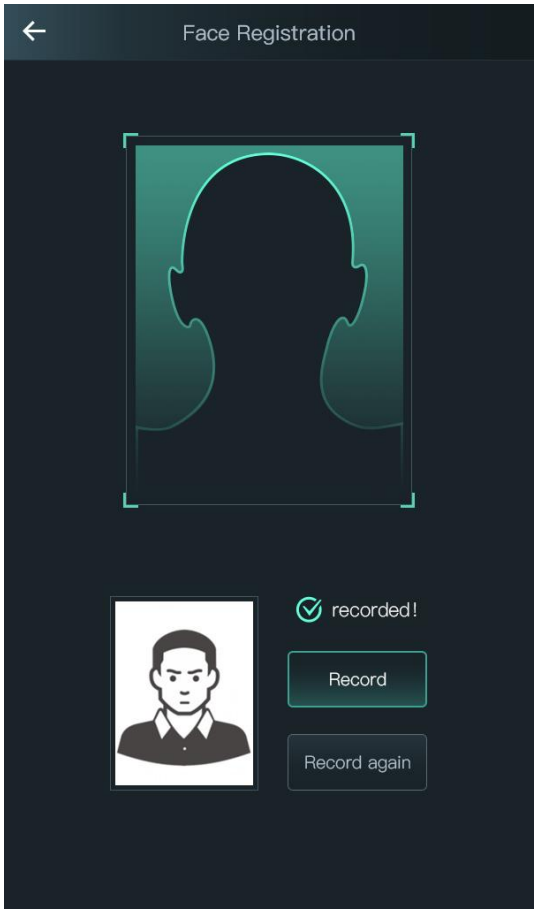
- Brillen, Hüte und Bärte können die Gesichtserkennung beeinflussen.
- Bedecken Sie beim Tragen eines Huts nicht Ihre Augenbrauen.
- Verändern Sie Ihren Bartstil nicht stark, wenn Sie das Gerät verwenden, da sonst die Gesichtserkennung fehlschlagen könnte.
- Halten Sie Ihr Gesicht sauber.
- Halten Sie das Gerät mindestens zwei Meter von einer Lichtquelle und mindestens drei Meter von Fenstern oder Türen entfernt, anderenfalls können Gegenlicht und direkte Sonneneinstrahlung die Gesichtserkennung des Geräts beeinträchtigen.

Während der Registrierung

Sie können Gesichter über den Zugangs-Controller oder über die Plattform registrieren. Zur Registrierung über die Plattform siehe Benutzerhandbuch der Plattform.

Richten Sie Ihren Kopf mittig mit dem Fotorahmen aus. Ein Foto Ihres Gesichts wird automatisch aufgenommen.

Anhang Abbildung 2-1 Registrierung

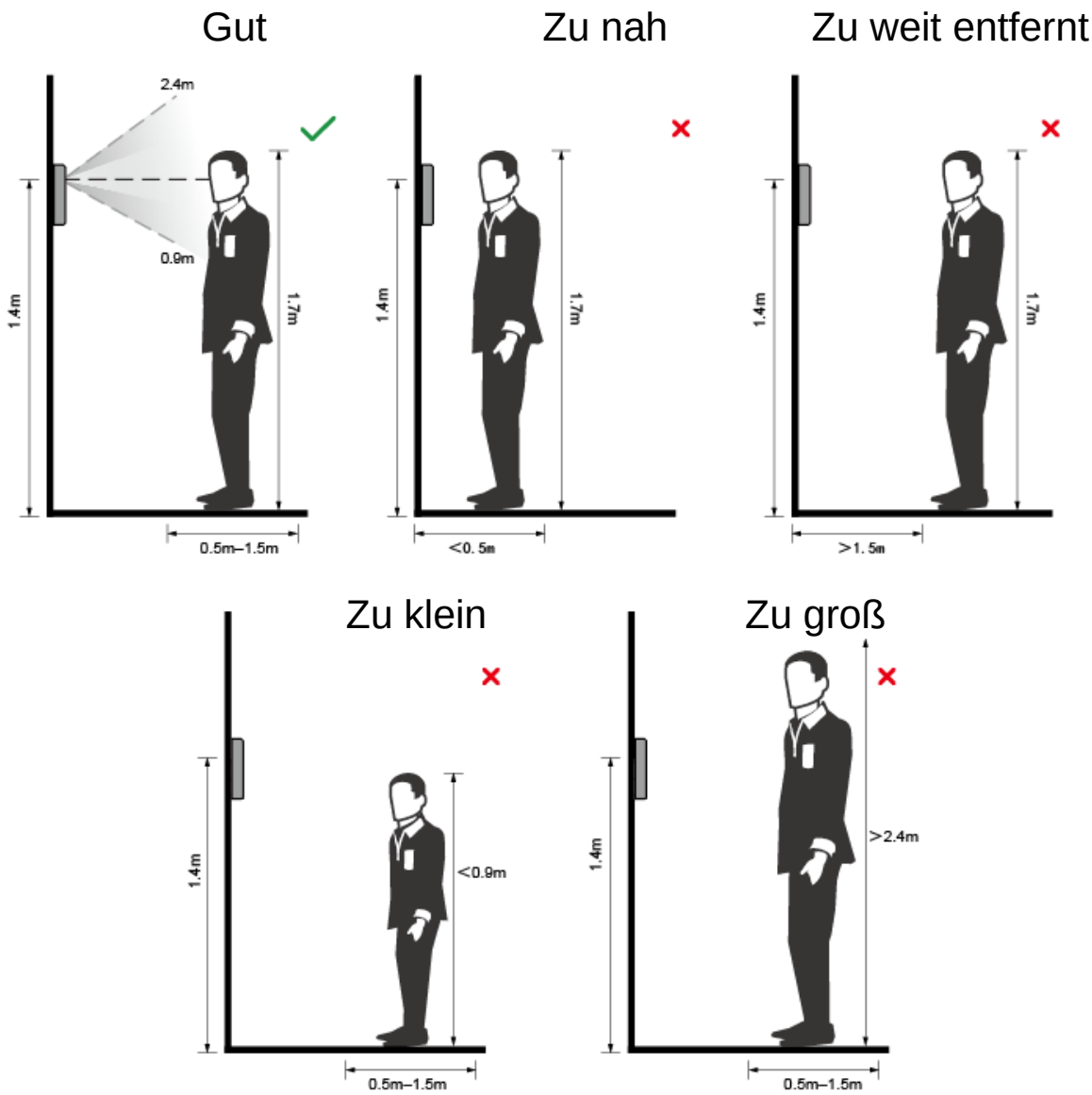


- Bewegen Sie weder Kopf noch Körper, anderenfalls kann die Registrierung fehlschlagen.
- Vermeiden Sie, dass zwei Gesichter gleichzeitig im Aufnahmerahmen erscheinen.

Gesichtsposition

Wenn sich Ihr Gesicht nicht in der korrekten Position befindet, wird die Gesichtserkennung möglicherweise beeinträchtigt.

Anhang Abbildung 2-2 Angemessene Gesichtsposition

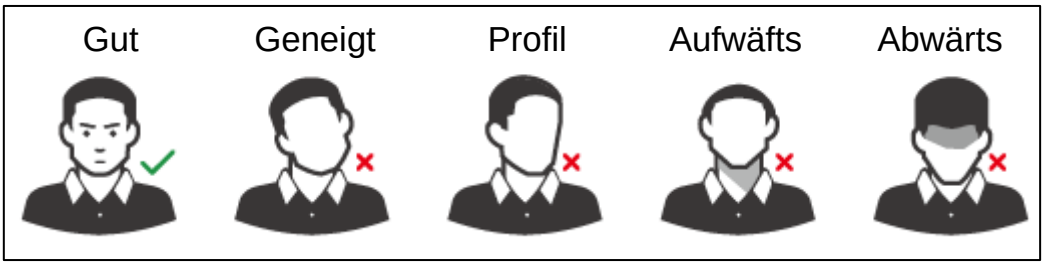


Anforderungen an Gesichter

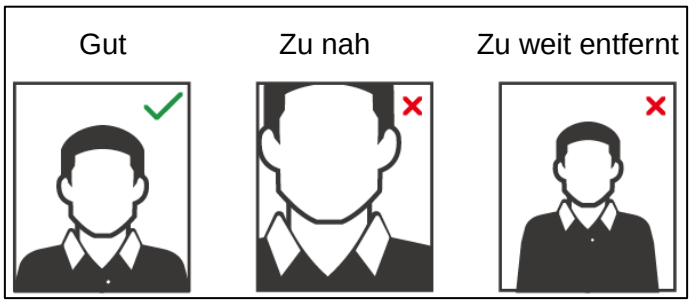
- Achten Sie darauf, dass das Gesicht sauber und die Stirn nicht von Haaren bedeckt ist.
- Tragen Sie keine Brille, Hut, Vollbart oder andere Gesichtsornamente, die die Aufnahme von Gesichtsbildern beeinflussen.
- Richten Sie Ihr Gesicht mit geöffneten Augen und ohne Gesichtsausdruck auf die Mitte der Kamera.

- Halten Sie Ihr Gesicht bei der Gesichtserkennung nicht zu nahe an oder zu weit von der Kamera entfernt, wenn Sie Ihr Gesicht aufnehmen.

Anhang Abbildung 2-3 Kopfhaltung



Anhang Abbildung 2-4 Abstand des Gesichts



- Beim Importieren von Gesichtsbildern über die Verwaltungsplattform ist darauf zu achten, dass die Bildauflösung im Bereich 150 × 300 bis 600 × 1200 liegt, die Bildpixel größer als 500 × 500 sind, die Bildgröße kleiner als 75 KB ist und Bildname und Personen-ID übereinstimmen.
- Achten Sie darauf, dass das Gesicht nicht 2/3 der gesamten Bildfläche einnimmt und das Seitenverhältnis nicht größer als 1:2 ist.

Anhang 3 Empfehlungen zur Cybersicherheit

Cybersicherheit ist mehr als nur ein Schlagwort: Es ist etwas, das sich auf jedes Gerät bezieht, das mit dem Internet verbunden ist. Die IP-Videoüberwachung ist nicht immun gegen Cyberrisiken, aber grundlegende Maßnahmen zum Schutz und zur Stärkung von Netzwerken und vernetzten Geräten machen sie weniger anfällig für Angriffe. Nachstehend finden Sie einige Tipps und Empfehlungen, wie Sie ein sichereres Sicherheitssystem schaffen können.

Verbindliche Maßnahmen, die zur Netzwerksicherheit der Grundausstattung zu ergreifen sind:

1. **Verwenden Sie sichere Passwörter**

   Sehen Sie sich die folgenden Vorschläge an, um Passwörter festzulegen:

   - Die Länge muss mindestens 8 Zeichen betragen;
   - Verwenden Sie mindestens zwei Zeichenarten. Zu den Zeichenarten gehören Groß- und Kleinbuchstaben, Zahlen und Symbole;
   - Fügen Sie nicht den Kontonamen oder den Kontonamen in umgekehrter Reihenfolge ein;
   - Verwenden Sie keine fortlaufenden Zeichen wie 123, abc usw.;
   - Verwenden Sie keine gleichen Zeichen wie 111, aaa usw.;

2. **Aktualisieren Sie Firmware und Client-Software rechtzeitig**

   - Gemäß dem Standardverfahren in der Technikbranche empfehlen wir, die Firmware Ihrer Geräte (wie NVR, DVR, IP-Kamera usw.) auf dem neuesten Stand zu halten, damit das System mit den neuesten Sicherheitspatches und -Fixes aktualisiert ist. Wenn das Gerät an ein öffentliches Netzwerk angeschlossen ist, empfehlen wir, die Funktion „Nach Updates suchen“ zu aktivieren, um rechtzeitig Informationen zu Firmware-Aktualisierungen zu erhalten, die vom Hersteller veröffentlicht wurden.
   - Wir empfehlen, die neueste Version der Client-Software herunterzuladen und zu verwenden.

„Nice to have“-Empfehlungen zur Verbesserung der Netzwerksicherheit Ihrer Geräte:

1. **Physischer Schutz**

   Wir empfehlen, dass Sie Geräte, insbesondere Speichergeräte, physisch schützen. Stellen Sie das Gerät beispielsweise in einem speziellen Computerraum und -schrank auf und implementieren Sie gute Zugriffsrechte und Schlüsselverwaltung, um zu verhindern, dass unbefugte Personen physische Verbindungen herstellen können, wie schädigende Hardware, unbefugten Anschluss von Wechselmedien (z. B. USB-Flashlaufwerken, serielle Schnittstelle) usw.

2. **Passwörter regelmäßig ändern**

   Wir empfehlen, die Passwörter regelmäßig zu ändern, um das Risiko zu verringern, erraten oder geknackt zu werden.

3. **Passwörter einstellen und rechtzeitig aktualisieren**

   Das Gerät unterstützt die Funktion Passwortrücksetzung. Richten Sie rechtzeitig entsprechende Daten für das Zurücksetzen des Passworts ein, einschließlich der Fragen zur Mailbox und zum Passwortschutz des Endbenutzers. Wenn sich die Daten ändern, ändern Sie diese bitte rechtzeitig. Bei der Einstellung von Fragen zum Passwortschutz empfehlen wir, keine Fragen zu verwenden, die leicht zu erraten sind.

4. **Kontosperre aktivieren**

   Die Kontosperrfunktion ist standardmäßig aktiviert und wir empfehlen, sie eingeschaltet zu lassen, um die Kontosicherheit zu gewährleisten. Versucht sich ein Angreifer mehrmals mit dem falschen Passwort anzumelden, wird das entsprechende Konto und die Quell-IP-Adresse gesperrt.

5. **Standard HTTP und andere Dienstports ändern**

   Wir empfehlen, den Standard-HTTP- und andere Dienst-Ports zu einem Nummer-Set zwischen 1024 und 65535 zu ändern, um das Risiko zu verringern, dass Außenstehende erraten können, welche Ports Sie verwenden.

6. **HTTPS aktivieren**

   Wir empfehlen, HTTPS zu aktivieren, damit Sie den Webdienst über einen sicheren Kommunikationskanal besuchen können.

7. **Weißliste aktivieren**

   Wir empfehlen, die Weißlistenfunktion so zu aktivieren, dass jeder, mit Ausnahme derjenigen mit den angegebenen IP-Adressen, vom Zugriff auf das System ausgeschlossen wird. Achten Sie daher darauf, dass Sie die IP-Adresse Ihres Computers und die IP-Adresse des Begleitgeräts in die Weißliste aufnehmen.

8. **MAC-Adressenverknüpfung**

   Wir empfehlen, die IP- und MAC-Adresse des Gateways mit dem Gerät zu verknüpfen, um das Risiko von ARP-Spoofing zu reduzieren.

9. **Konten und Privilegien sinnvoll zuordnen**

   Gemäß den Geschäfts- und Verwaltungsanforderungen sollten Sie Benutzer sinnvoll hinzufügen und ihnen ein Minimum an Berechtigungen zuweisen.

10. **Unnötige Dienste deaktivieren und sichere Modi wählen**

    Falls nicht erforderlich, empfehlen wir, einige Dienste wie SNMP, SMTP, UPnP usw. zu deaktivieren, um Risiken zu reduzieren.

    Falls erforderlich, wird dringend empfohlen, dass Sie sichere Modi verwenden, einschließlich, aber nicht darauf beschränkt, die folgenden Dienste:

    - SNMP: Wählen Sie SNMP v3 und richten Sie starke Verschlüsselungs- und Authentifizierungspasswörter ein.
    - SMTP: Wählen Sie TLS, um auf den Mailbox-Server zuzugreifen.
    - FTP: Wählen Sie SFTP, und richten Sie starke Passwörter ein.
    - AP-Hotspot: Wählen Sie den WPA2-PSK-Verschlüsselungsmodus und richten Sie starke Passwörter ein.

11. **Audio- und Video-verschlüsselte Übertragung**

    Wenn Ihre Audio- und Videodateninhalte sehr wichtig oder sensibel sind, empfehlen wir, eine verschlüsselte Übertragungsfunktion zu verwenden, um das Risiko zu verringern, dass Audio- und Videodaten während der Übertragung gestohlen werden.

    Zur Erinnerung: Die verschlüsselte Übertragung führt zu einem Verlust der Übertragungseffizienz.

12. **Sichere Auditierung**

    - Online-Benutzer überprüfen: Wir empfehlen, die Online-Benutzer regelmäßig zu überprüfen, um zu sehen, ob ein Gerät ohne Berechtigung angemeldet ist.
    - Geräteprotokoll prüfen: Durch die Anzeige der Protokolle können Sie die IP-Adressen, mit denen Sie sich bei Ihren Geräten angemeldet haben und deren wichtigste Funktionen erkennen.

13. **Netzwerkprotokoll**

    Aufgrund der begrenzten Speicherkapazität der Geräte sind gespeicherte Protokolle begrenzt. Wenn Sie das Protokoll über einen längeren Zeitraum speichern müssen, empfehlen wir, die Netzwerkprotokollfunktion zu aktivieren, um zu gewährleisten, dass die kritischen Protokolle mit dem Netzwerkprotokollserver für die Rückverfolgung synchronisiert werden.

14. **Aufbau einer sicheren Netzwerkumgebung**

    Um die Sicherheit der Geräte besser zu gewährleisten und mögliche Cyberrisiken zu reduzieren, empfehlen wir:

    - Deaktivieren Sie die Port-Mapping-Funktion des Routers, um einen direkten Zugriff auf die Intranet-Geräte aus dem externen Netzwerk zu vermeiden.
    - Das Netzwerk muss entsprechend dem tatsächlichen Netzwerkbedarf partitioniert und isoliert werden. Wenn es keine Kommunikationsanforderungen zwischen zwei Subnetzwerken gibt, empfehlen wir, VLAN, Netzwerk-GAP und andere Technologien zur Partitionierung des Netzwerks zu verwenden, um den Netzwerkisolationseffekt zu erreichen.
    - Einrichtung des 802.1x Zugangsauthentifizierungssystems, um das Risiko eines unbefugten Zugriffs auf private Netzwerke zu reduzieren.
    - Wir empfehlen, die Firewall- oder Blacklist- und Whitelist-Funktion Ihres Geräts zu aktivieren, um das Risiko eines Angriffs auf Ihr Gerät zu verringern.