Zugangs-Controller mit Gesichtserkennung

Kurzanleitung

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
GEFAHR	Weist auf ein hohes Gefahrenpotential hin, das, wenn es nicht vermieden wird, zum Tod oder zu schweren Verletzungen führt.
WARNUNG	Weist auf eine mittlere bis geringe Gefahr hin, die zu leichten oder mittelschweren Verletzungen führen kann, wenn sie nicht vermieden wird.
VORSICHT	Weist auf eine potenziell gefährliche Situation hin, die, wenn sie nicht vermieden wird, zu Schäden am Gerät, Datenverlust, Leistungsminderung oder unerwarteten Ergebnissen führen kann.
TIPPS	Bietet Methoden, die helfen können, ein Problem zu lösen oder Zeit zu sparen.
HINWEIS	Bietet zusätzliche Informationen als Hervorhebung oder Ergänzung zum Text.

Änderungsverlauf

Version	Inhaltliche Überarbeitung	Veröffentlichungsdatum
V1.0.0	Erste Veröffentlichung	April 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 Anleitungen 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.
- 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 Abmessungen und Komponenten

Abbildung 1–1 Abmessungen und Komponenten (mm [Zoll])

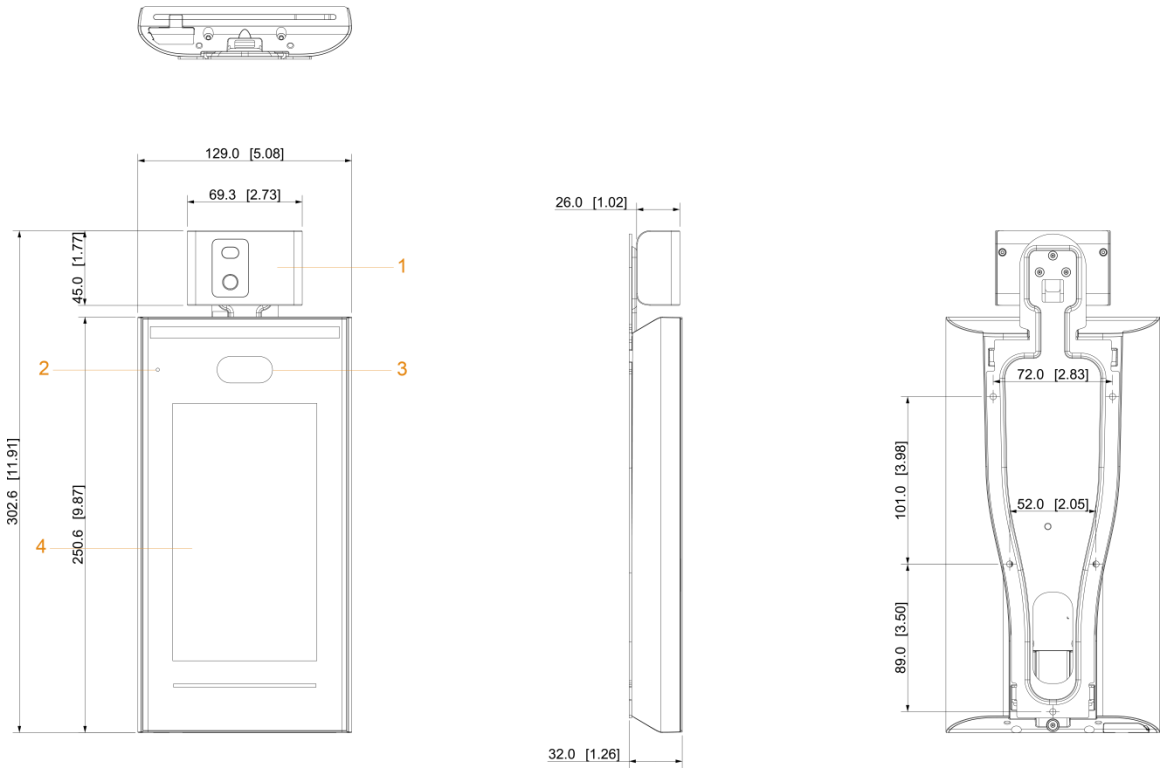


Tabelle 1-1 Beschreibung der Komponenten

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

2 Anschluss und Installation

2.1 Kabel anschließen

- Überprüfen Sie, ob das Sicherheitsmodul der Zugriffskontrolle unter **Funktion > Sicherheitsmodul** (Function > Security Module) aktiviert ist. Wenn es aktiviert ist, müssen Sie das Zugriffskontroll-Sicherheitsmodul separat erwerben. Das Sicherheitsmodul benötigt eine separate Stromversorgung.
- Sobald das Sicherheitsmodul aktiviert ist, sind die Ausgangstaste, die Schlosssteuerung und die Feuerlöschverbindung ungültig.

Abbildung 2–1 Kabelanschluss

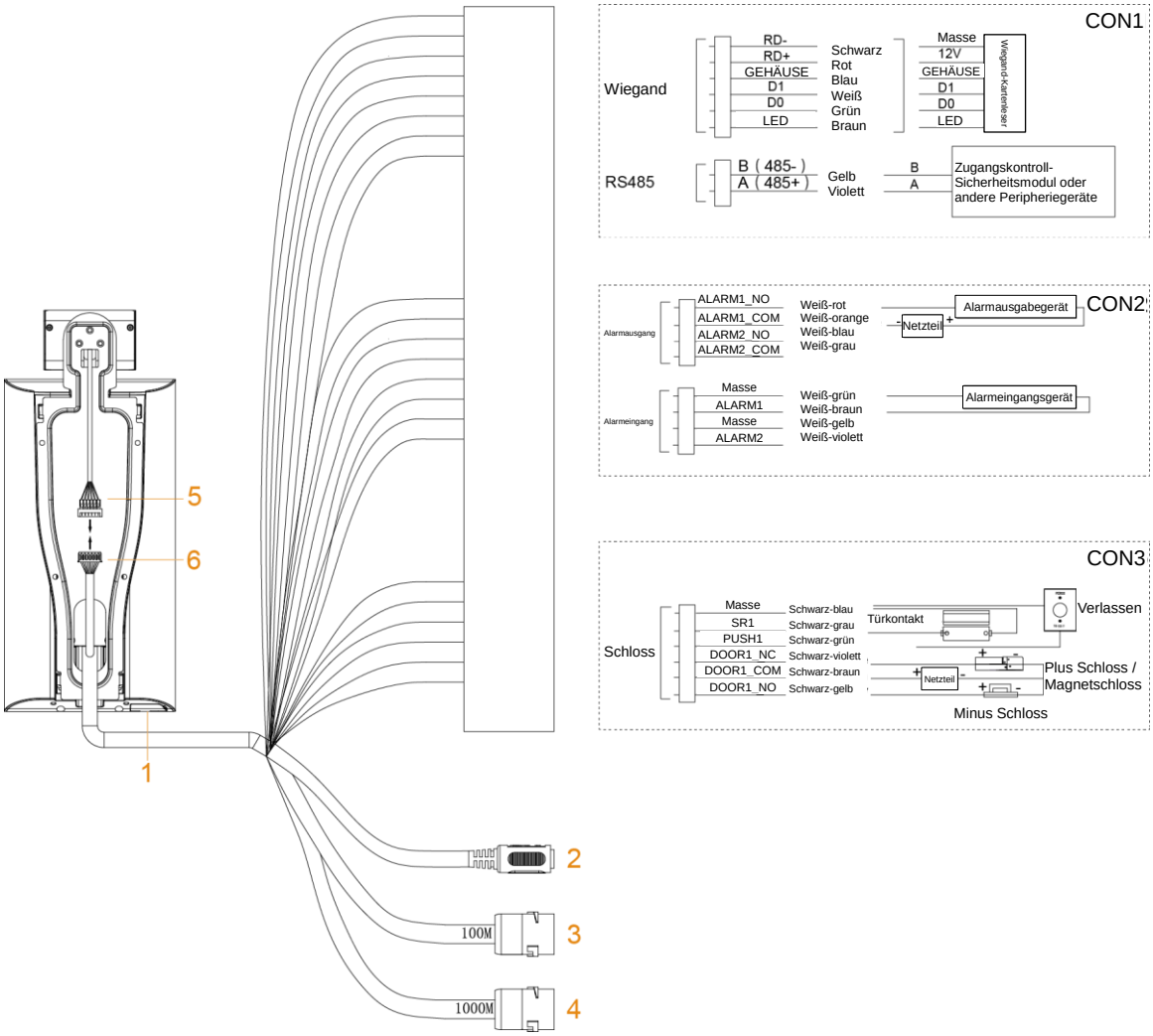


Tabelle 2–1 Beschreibung der Komponenten

Nr.	Name
1	USB-Anschluss
2	Stromanschluss
3	100M Netzwerkanschluss
4	1000M Netzwerkanschluss
5, 6	Anschlüsse für die Temperaturüberwachungseinheit

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 2–2 Anforderungen an die Umgebungsbeleuchtung

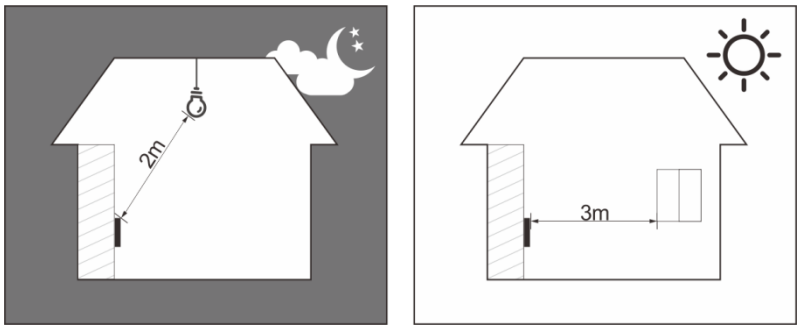
Kerze: 10 Lux Glühbirne: 100 Lux - 850 Lux Sonnenlicht: ≥1200 Lux

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.

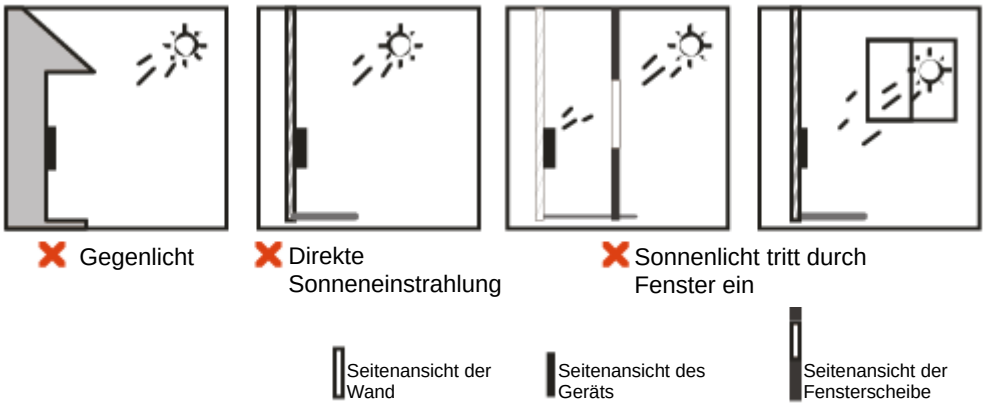
Empfohlene Orte

Abbildung 2–3 Empfohlene Orte



Nicht empfohlene Orte

Abbildung 2–4 Nicht empfohlene Orte



2.3 Installation

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

Abbildung 2–5 Installationshöhe

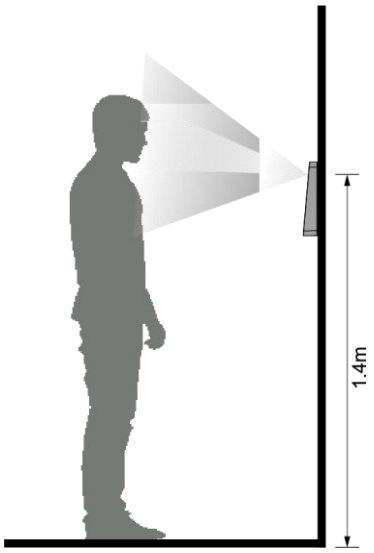
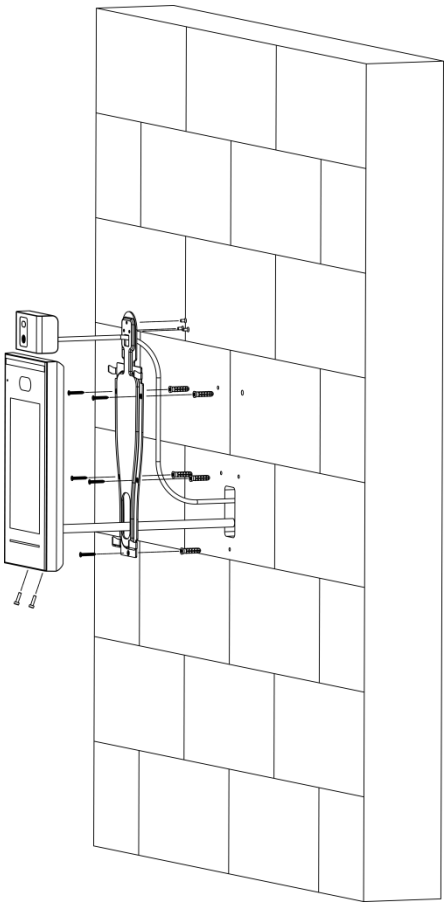


Abbildung 2–6 Montageschema



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 fünf Montagelöchern der Halterung anbringen.

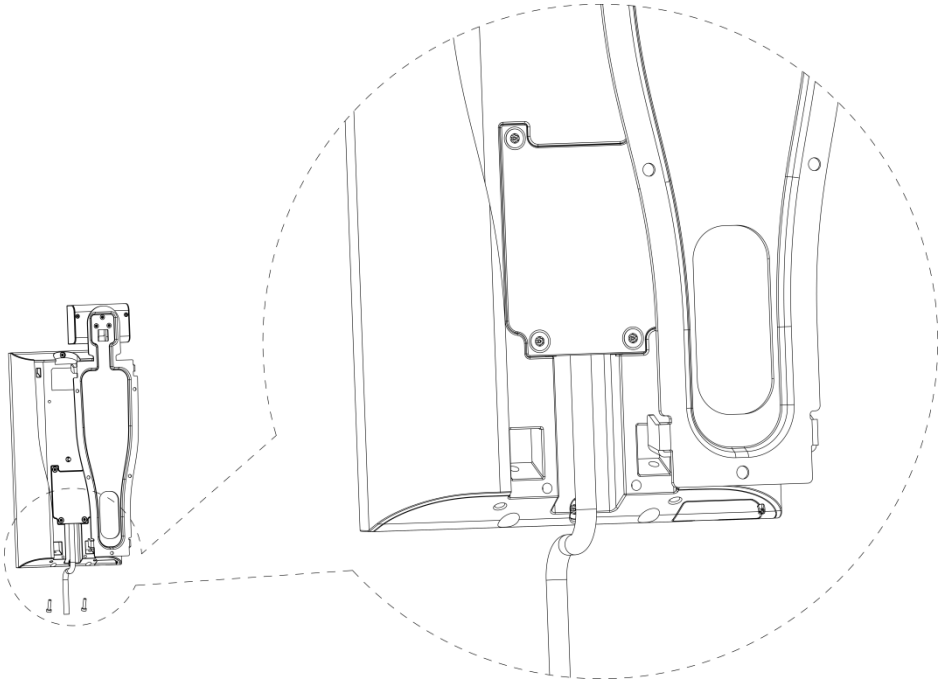
Schritt 4: Schließen Sie die Kabel für den Zugangs-Controller an. Siehe „2.1 Kabel anschließen“.

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 2–7 Silikondichtmittel aufbringen



3 Systembetrieb

3.1 Initialisierung

Das Administrator-Passwort und eine E-Mail-Adresse müssen beim ersten Einschalten des Zugangs-Controllers eingerichtet werden, anderenfalls kann der Zugangs-Controller nicht verwendet werden.

Abbildung 3–1 Initialisierung

- Das Administrator-Passwort kann über die von Ihnen eingegebene E-Mail-Adresse zurückgesetzt werden, falls Sie es vergessen haben.
- 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 ' " ; : &).
- Zugangs-Controller ohne Touchscreen initialisieren Sie über die Web-Oberfläche. Siehe Benutzerhandbuch für Einzelheiten.

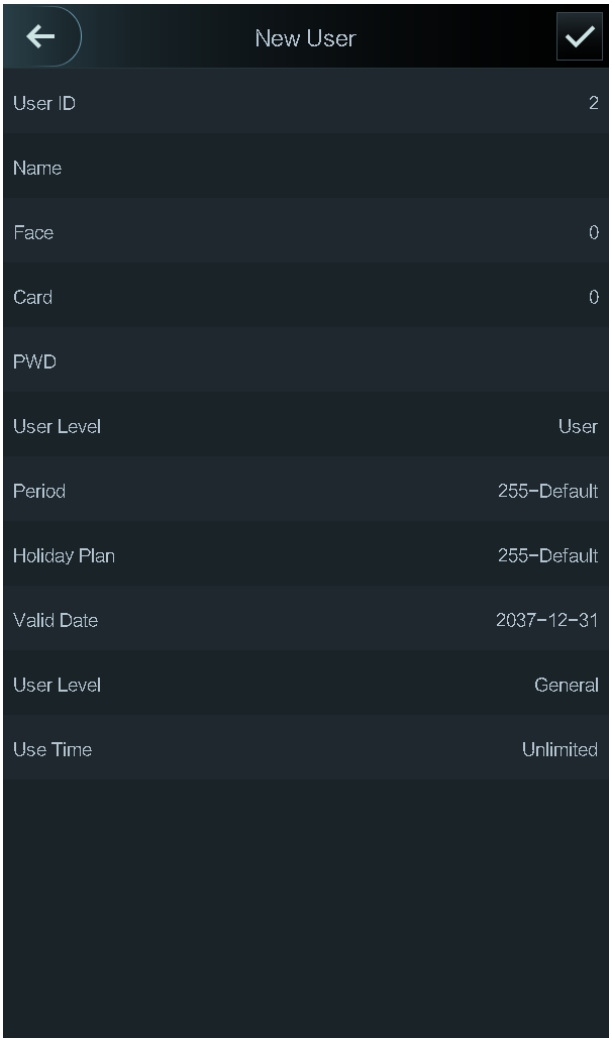
3.2 Neue Benutzer hinzufügen

Sie können neue Benutzer hinzufügen, indem Sie Benutzer-IDs und Namen eingeben, Fingerabdrücke, Gesichtsbilder und Passwörter importieren und Benutzerebenen wählen.

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

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

Abbildung 3–2 Neuer Benutzer



Schritt 2: Konfigurieren Sie die Parameter im Menü.

Tabelle 3-1 Neuer Benutzer Beschreibung der Parameter

Parameter	Beschreibung
Benutzer-ID	Geben Sie Benutzer-IDs ein. Die IDs bestehen aus 32 Zeichen (einschließlich Zahlen und Buchstaben) und 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 auf dem Bildaufnahmerahmen zentriert ist, dann wird automatisch ein Bild Ihres Gesichts aufgenommen. Einzelheiten zur Gesichtsbildaufnahme finden Sie unter „Anhang 2 Hinweise zur Gesichtsaufnahme/Vergleich“.
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. Wenn der Zugangs-Controller kein Kartenlesemodul hat, müssen Sie das Gerät an peripheren Kartenlesern anschließen.

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.
Ebene	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. Falls Sie das Administrator-Passwort vergessen sollten, legen Sie besser mehr als einen Administrator an.
Zeitraum	Der Zeitraum, in dem der Benutzer die Tür entriegeln kann. Detaillierte Einstellungen für den Zeitraum finden Sie im Benutzerhandbuch.
Urlaubsplan	Sie können einen Urlaubsplan festlegen, in dem der Benutzer die Tür entriegeln kann. Ausführliche Informationen zu den Einstellungen des Urlaubsplans finden Sie im Benutzerhandbuch.
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 bestimmte Male in bestimmten Zeiträumen die Tür entriegeln. Sobald sie die maximale Anzahl und Zeiträume 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** (Guest) ist, können Sie die Höchstanzahl festlegen, an denen der Gast die Tür entriegeln kann.

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

4 Web-Bedienung

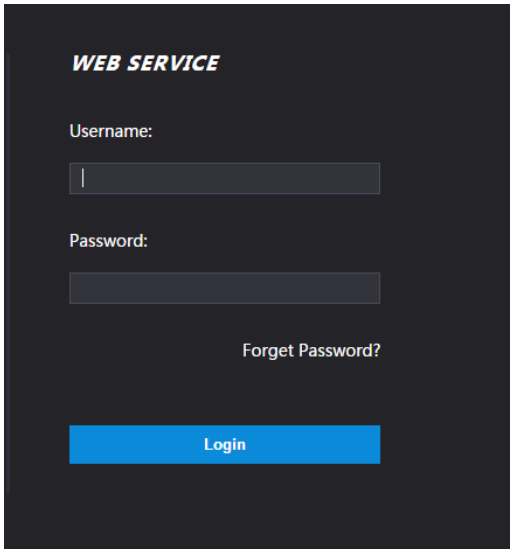
Der Zugangs-Controller kann über die Web-Oberfläche konfiguriert und bedient werden. Über die Web-Oberfläche können Sie Parameter einstellen, darunter Netzwerkparameter, Videoparameter und Zugangs-Controller-Parameter; außerdem können Sie das System warten und aktualisieren. Einzelheiten finden Sie im Benutzerhandbuch. Hier wird nur der Anmeldevorgang beschrieben.

Sie müssen ein Passwort und eine E-Mail-Adresse einrichten, bevor Sie sich zum ersten Mal an der Web-Oberfläche anmelden. Das von Ihnen festgelegte Passwort wird für die Anmeldung an der Web-Oberfläche verwendet und die E-Mail-Adresse dient dem Zurücksetzen von Passwörtern.

Schritt 1: Öffnen Sie den Webbrowser, geben Sie die IP-Adresse des Zugangs-Controllers in die Adressleiste ein und drücken Sie dann die Eingabetaste.

- Vergewissern Sie sich, dass der Computer, der zur Anmeldung an der Web-Oberfläche verwendet wird, sich im gleichen LAN wie das Gerät befindet.
- Der Zugangs-Controller verfügt über 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 Anmeldung



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

- Der Standard-Benutzername des Administrators ist admin und das Passwort ist das Anmelde-Passwort 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?** (Forget Password?), um es zurückzusetzen. Siehe Benutzerhandbuch.

Schritt 3: Klicken Sie auf **Anmelden** (Login).

Die Startseite der Web-Oberfläche wird angezeigt.

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

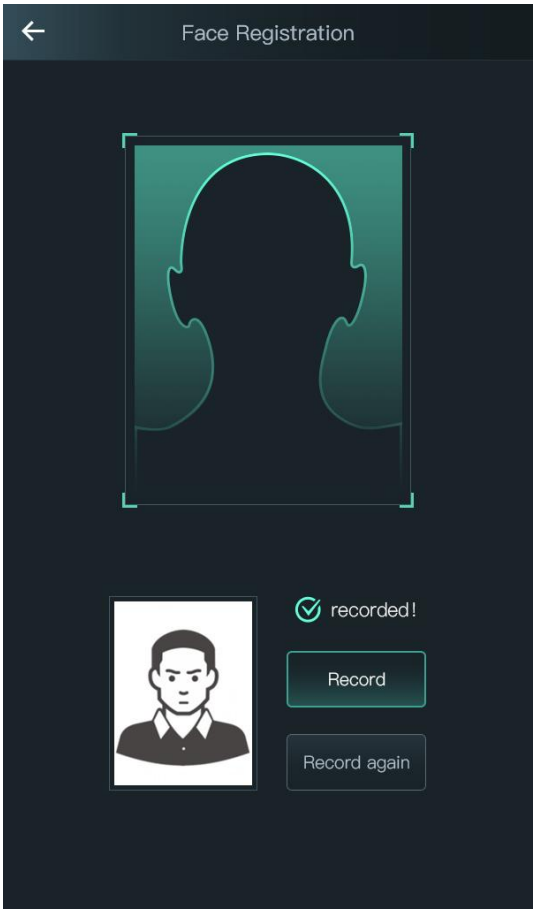
- Brillen, Hüte und Bärte können die Gesichtserkennung beeinflussen.
- Bedecken Sie beim Tragen eines Huts nicht Ihre Augenbrauen.
- Verändern Sie Ihren Bartstil nicht stark, wenn Sie das Gerät verwenden, da sonst die Gesichtserkennung fehlschlagen könnte.
- Halten Sie Ihr Gesicht sauber.
- Halten Sie 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

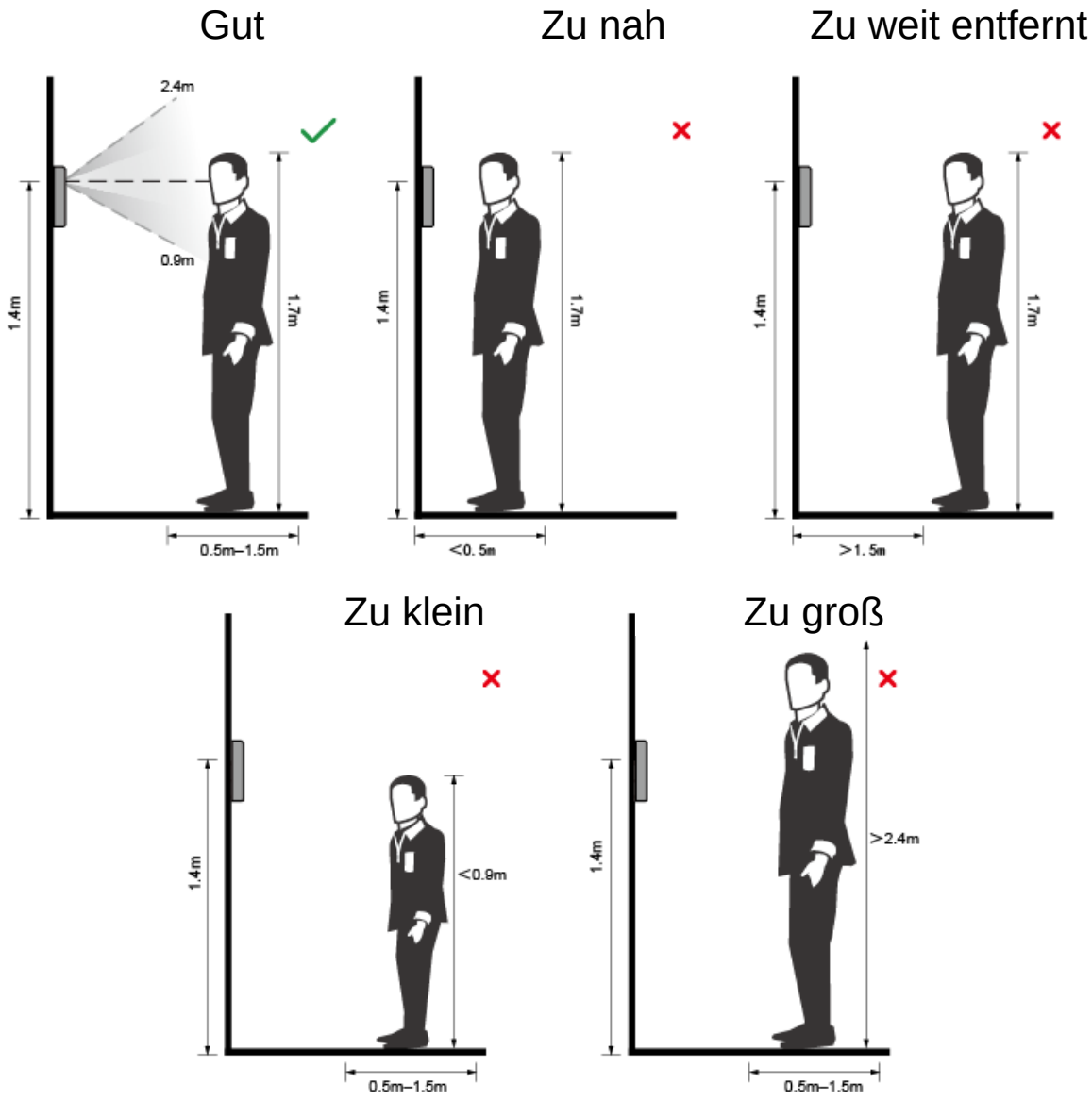


- Bewegen Sie weder Kopf noch Körper, anderenfalls kann die Registrierung fehlschlagen.
- Vermeiden Sie, dass zwei Gesichter gleichzeitig im Aufnahmerahmen erscheinen.

Gesichtsposition

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

Anhang Abbildung 2-2 Angemessene Gesichtsposition

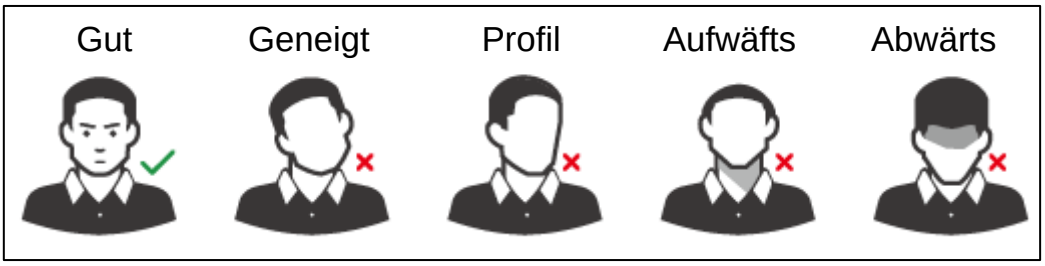


Anforderungen an Gesichter

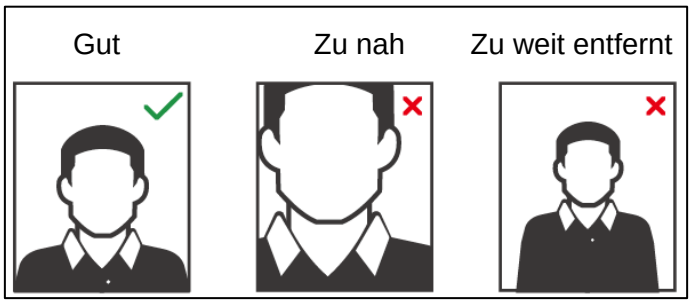
- Achten Sie darauf, dass das Gesicht sauber und die Stirn nicht von Haaren bedeckt ist.
- Tragen Sie keine Brille, Hut, Vollbart oder andere Gesichtsornamente, die die Aufnahme von Gesichtsbildern beeinflussen.
- Richten Sie Ihr Gesicht mit geöffneten Augen und ohne Gesichtsausdruck auf die Mitte der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