

# **Modulare Türstation**

## **Kurzanleitung**



# Vorwort

## Allgemein

In diesem Dokument werden hauptsächlich die Produktfunktion, die Struktur, die Vernetzung, der Montageprozess, der Debugging-Prozess und die Weboperationen der modularen Türstation (nachfolgend als „VTO“ bezeichnet) vorgestellt.

## Modelle






VTO4202F-MK, VTO4202F-MB1, VTO4202F-MB2, VTO4202F-MB5, VTO4202F-MR, VTO4202F-MS, VTO4202F-MF, VTO4202F-ML, VTO4202F-MA, VTO4202F-P und VTO4202F-P-S2.

## Gerät aktualisieren

Die Stromversorgung kann erst unterbrochen werden, nachdem das Gerät das Upgrade abgeschlossen und neu gestartet hat.

## Sicherheitshinweise

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

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

## Änderungsverlauf

Version	Inhaltliche Überarbeitung	Veröffentlichungsdatum
V1.0.0	Erste Veröffentlichung.	Dezember 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

Die folgende Beschreibung ist die korrekte Anwendungsmethode der VTO. Lesen Sie das Handbuch vor Gebrauch sorgfältig durch, um Gefahren und Sachschäden zu vermeiden. Halten Sie sich während des Gebrauchs strikt an das Handbuch und bewahren Sie zum künftigen Nachschlagen auf.

## Betriebsanforderungen

- Setzen Sie das Gerät weder direktem Sonnenlicht noch Hitzequellen aus.
- Installieren Sie das Gerät nicht an feuchten oder staubigen Orten.
- Installieren Sie das Gerät horizontal an stabilen Orten, damit es nicht herunterfällt.
- Achten Sie darauf, dass keine Flüssigkeiten auf das Gerät tropfen oder spritzen. Stellen Sie keine mit Flüssigkeiten gefüllten Gefäße auf das Gerät.
- Installieren Sie das Gerät an gut belüfteten Orten und blockieren Sie nicht seine Lüftungsöffnung.
- Verwenden Sie das Gerät nur innerhalb des Nenneingangs- und -ausgangsbereichs.
- Nehmen Sie das Gerät nicht selbst auseinander.
- Transportieren, verwenden und lagern Sie das Gerät innerhalb des zulässigen Luftfeuchtigkeits- und Temperaturbereichs.

## Stromanforderungen

- Verwenden Sie in Ihrer Region empfohlene Stromkabel, beachten Sie die angegebenen Spezifikationen.
- Verwenden Sie ein Netzteil, das den SELV-Anforderungen (Safety Extra Low Voltage) entspricht, und schließen Sie es an einer Nennspannung gemäß IEC60950-1 an. Spezifische Anforderungen an die Stromversorgung können Sie dem Typenschild am Gerät entnehmen.
- Der Gerätestecker dient als Trennvorrichtung. Der Stecker muss während des Betriebs jederzeit frei zugänglich sein.

# Inhaltsverzeichnis

<b>Vorwort</b> .....	<b>I</b>
<b>Wichtige Sicherheits- und Warnhinweise</b> .....	<b>III</b>
<b>1 Überblick</b> .....	<b>1</b>
1.1 Beschreibung.....	1
1.2 Funktionen .....	1
<b>2 Aufbau</b> .....	<b>2</b>
2.1 Kameramodul.....	2
2.2 Indikatormodul.....	3
2.3 Audiomodul .....	4
2.4 Tastenmodul .....	5
2.5 Tastaturmodul (mit Braille-Schrift) .....	6
2.6 Kartenmodul.....	6
2.7 Fingerabdruck-Modul.....	7
2.8 Anzeigemodul.....	7
2.9 Leermodul.....	8
2.10 Kaskadenschaltung .....	8
<b>3 Konfiguration und Inbetriebnahme</b> .....	<b>9</b>
3.1 Vorgehensweise.....	9
3.2 VTO konfigurieren.....	9
3.2.1 Initialisierung.....	9
3.2.2 VTO-Nummer konfigurieren .....	10
3.2.3 Netzwerkparameter konfigurieren .....	11
3.2.4 SIP-Server konfigurieren .....	11
3.2.5 VTO hinzufügen.....	13
3.2.6 Zimmernummer hinzufügen.....	14
3.2.7 Modul konfigurieren.....	18
3.3 Inbetriebnahme.....	20
3.3.1 VTO ruft VTH an .....	20
3.3.2 VTH überwacht VTO.....	21
<b>Anhang 1 Empfehlungen zur Cybersicherheit</b> .....	<b>22</b>

# 1 Überblick

## 1.1 Beschreibung

Sie können die modulare VTO mit verschiedenen Modulen, darunter Kameramodul, Indikatormodul, Tastenmodul, Tastaturmodul, Kartenmodul, Fingerabdruck-Modul, Audiomodul und Anzeigemodul, einrichten. Kamera- und Audiomodule sind unverzichtbar und die anderen können nach Bedarf hinzugefügt werden.

## 1.2 Funktionen

- Videoanruf: Zum Absetzen von Anrufen an Innenmonitore (VTHs).
- Gruppenruf: Zum Anrufen mehrerer VTHs gleichzeitig.
- Videoüberwachung: Bis zu 6 VTHs können das Überwachungsbild dieser VTO gleichzeitig betrachten.
- Notruf: Zum Anrufen des Management Center während eines Notfalls.
- Entriegeln: Karte, Fingerabdruck, Passwort und Fernentsperrung.
- Alarm: Sabotagealarm, Türkontakt-Alarm und Alarm zum Entsperren des Passworts. Alarminformationen werden an das Management Center gesendet.
- Aufnahmesuche: Anruflisten, Alarmlisten und Entriegelungslisten.

# 2 Aufbau

## 2.1 Kameramodul

Abbildung 2-1 Frontblende

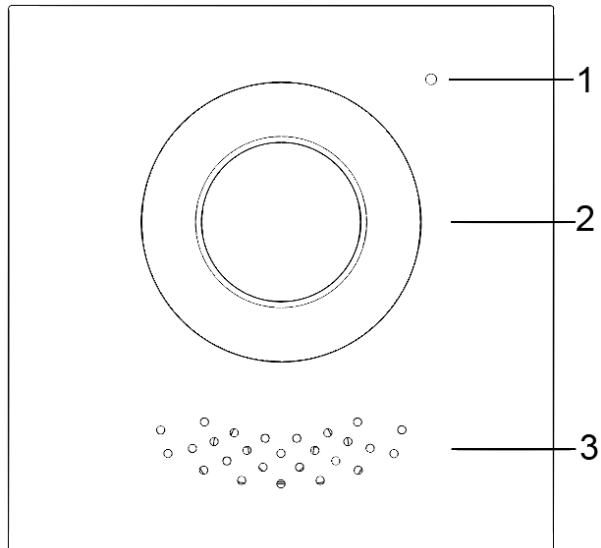


Tabelle 2-1 Beschreibung der Frontplatte

Nr.	Name
1	Mikrofon
2	Kamera
3	Lautsprecher

Abbildung 2-2 Geräterückseite

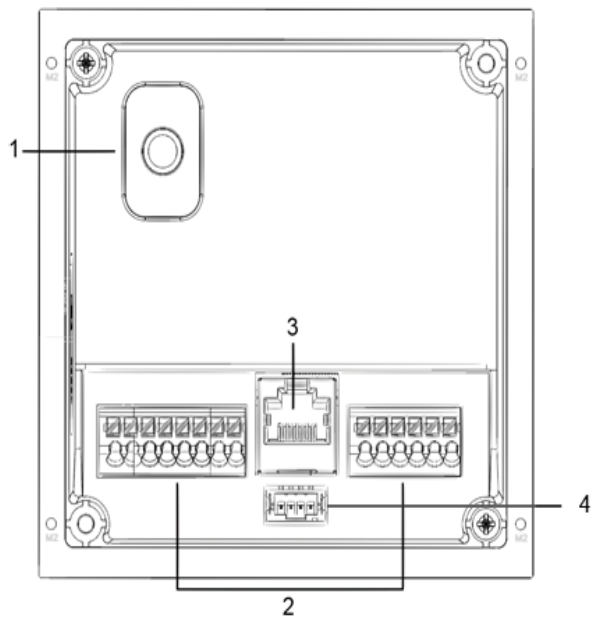


Tabelle 2-2 Beschreibung der Geräterückseite

Nr.	Name	Beschreibung
1	Antimanipulationsschalter	Wenn die VTO gewaltsam von der Wand entfernt wird, wird ein Alarm ausgelöst und Alarminformationen werden an das Management Center gesendet.
2	Ports	Zum Herstellen einer Verbindung zu Stromversorgung, elektrischem Schloss, Solenoid-Schloss und Verlassen-Taste.
3	Ethernet-Port	Zum Anschließen von Netzwerkkabeln.
4	Kaskadier-Anschluss	Zum Verbinden mit anderen Modulen.

Abbildung 2-3 Anschlussbeschreibung

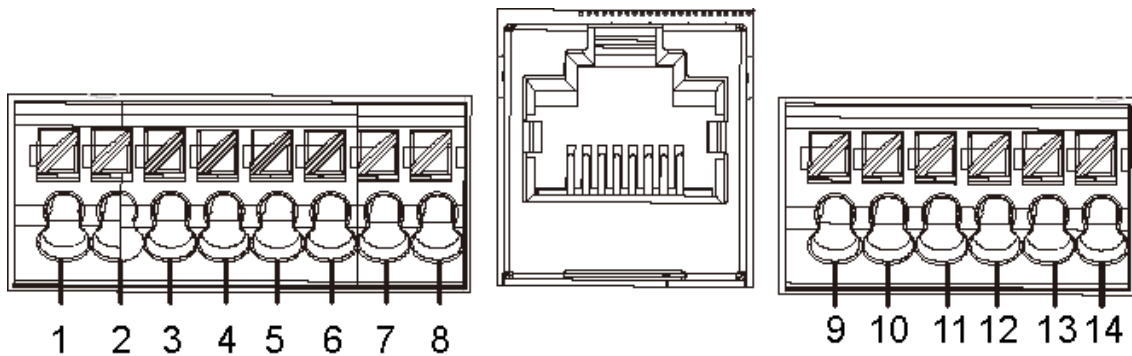


Tabelle 2-3 Port Beschreibung

Nr.	Beschreibung	Nr.	Beschreibung
1	Erde	8	EOC1 (2-adrig - (Erde) für 2-adriges Kameramodul)
2	+12-V-AUSGANG	9	DOOR_BUTTON
3	RS-485_B	10	DOOR_FEEDBACK
4	RS-485_A	11	Erde
5	ALARM_NO	12	DOOR_NC
6	ALARM_COM	13	DOOR_COM
7	EOC2 (2-adrig +(48 V) für 2-adriges Kameramodul)	14	DOOR_NO

## 2.2 Indikatormodul

Abbildung 2-4 Frontblende

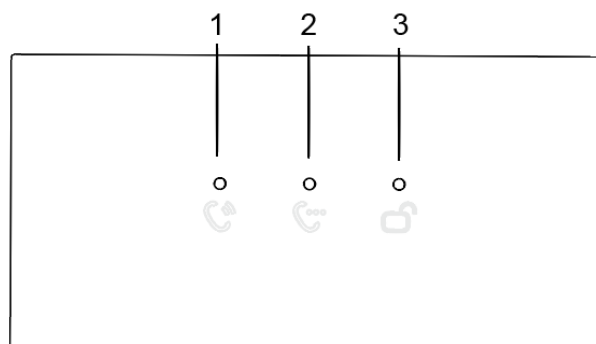




Tabelle 2-4 Indikatormodul-Beschreibung (1)

Nr.	Name	Beschreibung
1	Klingelanzeige	Aktivitätsstatus.
2	Sprechanzeige	
3	Anzeige entsperren	

Abbildung 2-5 Rückplatte des Indikatormoduls

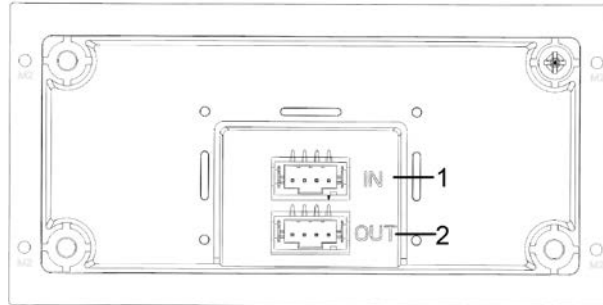


Tabelle 2-5 Indikatormodul-Beschreibung (2)

Nr.	Name	Beschreibung
1	Kaskadeneingang	Zum Verbinden mit anderen Modulen.
2	Kaskadenausgang	

## 2.3 Audiomodul



Die Rückplatte des Audiomoduls entspricht der des Kameramoduls.

Abbildung 2-6 Audiomodul

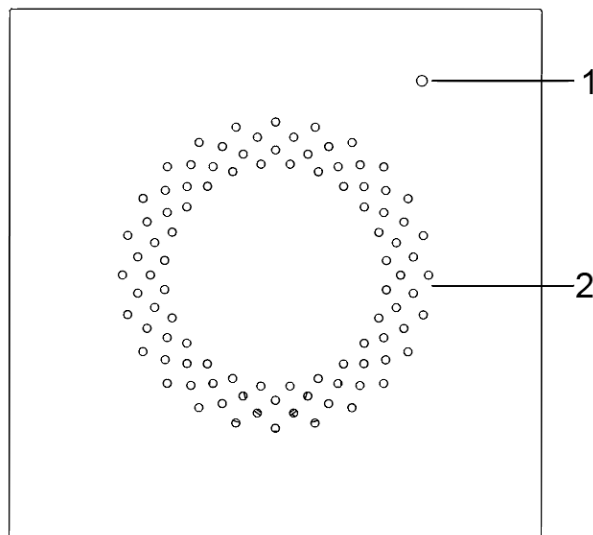


Tabelle 2-6 Audiomodulbeschreibung

Nr.	Name
1	Mikrofon
2	Lautsprecher

## 2.4 Tastenmodul

Ein-Tasten-Modul, Zwei-Tasten-Modul und Fünf-Tasten-Modul sind mit derselben Funktion verfügbar. Hier nutzen wir das Fünf-Tasten-Modul als Beispiel.

Abbildung 2-7 Fünf-Tasten-Modul des Fünf-Tasten-Moduls

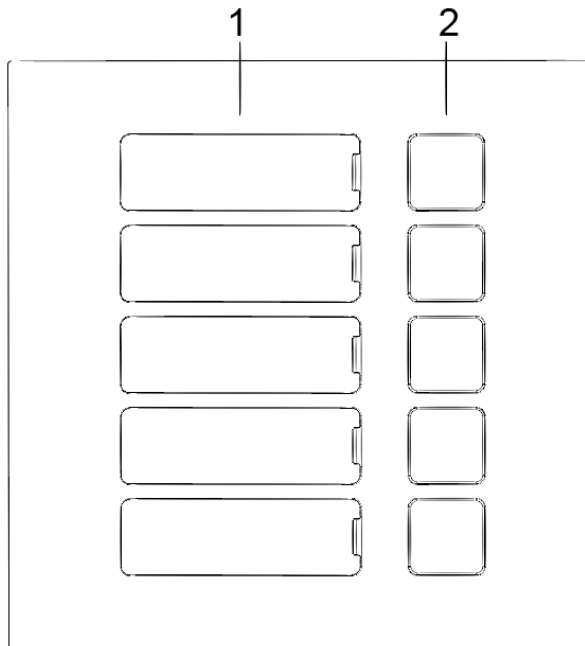


Tabelle 2-7 Beschreibung der Frontplatte


Nr.	Name	Beschreibung
1	Benutzerverzeichnis	Platzieren Sie hier die Namenskarten.
2	Ruftasten	Zum Anrufen anderer VTHs oder des Management Center.  Konfigurieren Sie zunächst relevante Parameter auf der Weboberfläche.

Abbildung 2-8 Rückplatte des Fünf-Tasten-Moduls

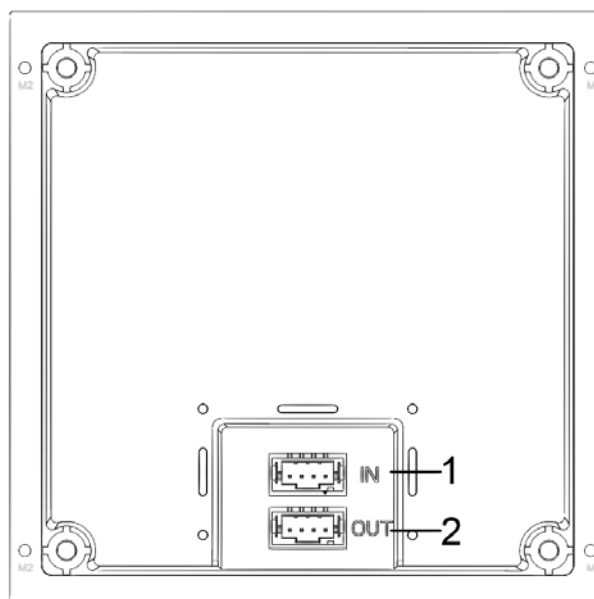


Tabelle 2-8 Beschreibung der Geräterückseite

Nr.	Name
1	Kaskadeneingang
2	Kaskadenausgang

## 2.5 Tastaturmodul (mit Braille-Schrift)



Die Rückplatte des Tastaturmoduls entspricht der des Tastenmoduls.

Abbildung 2-9 Tastaturmodul

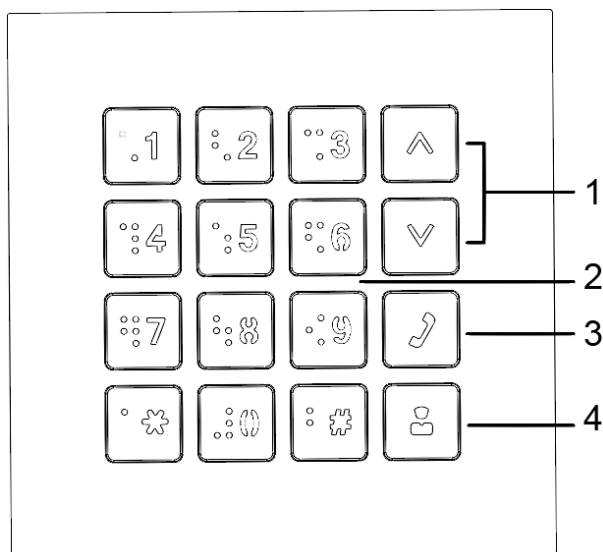


Tabelle 2-9 Beschreibung des Tastaturmoduls

Nr.	Name	Beschreibung
1	Auswahl	—
2	Ziffern	Zur Eingabe von Passwort oder VTH-Nummern.
3	Anruf	Ruft den VTH.
4	Ruft die Verwaltungszentrale	—

## 2.6 Kartenmodul

Ziehen Sie Ihre Karte nahe dem Symbol durch.



Die Rückplatte des Kartenmoduls entspricht der des Tastenmoduls.

Abbildung 2-10 Kartenmodul



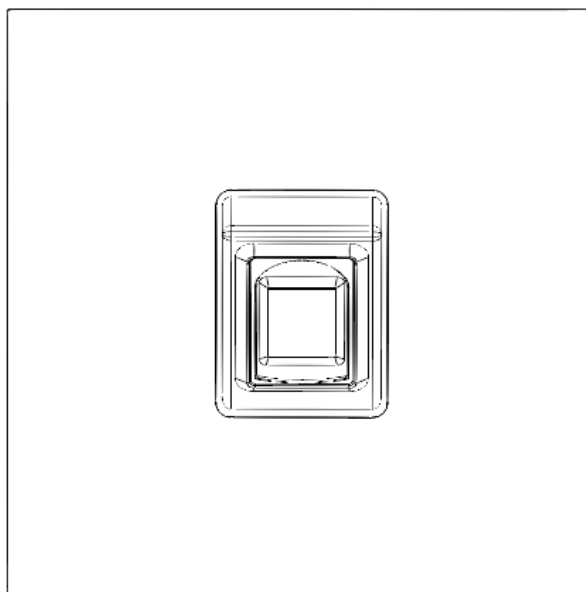
## 2.7 Fingerabdruck-Modul

Erfasst und verifiziert Fingerabdrücke.



Die Rückplatte des Fingerabdruck- und des Tastenmoduls sind in Bezug auf die Anordnung der Anschlüsse unterschiedlich, die Funktionen der Anschlüsse ist jedoch identisch.

Abbildung 2-11 Fingerabdruck-Modul



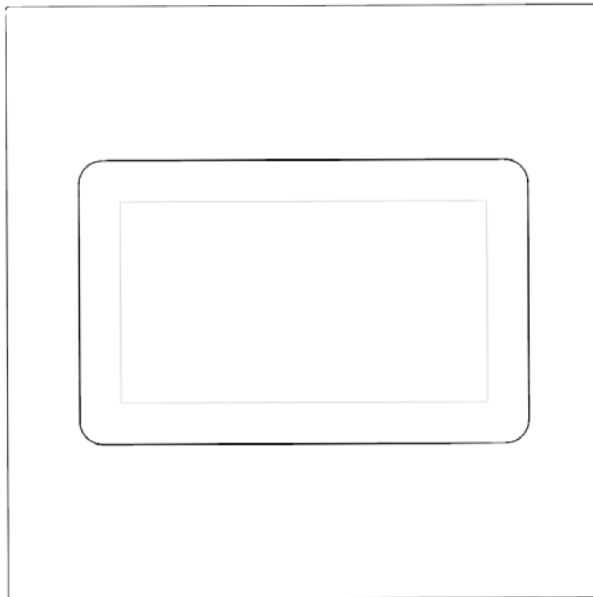
## 2.8 Anzeigemodul

Zeigt die Benutzerinformationen an.



Die Rückseiten des Anzeigemoduls und des Tastenmoduls haben unterschiedliche Anschlusspositionen, die Anschlussfunktionen sind jedoch gleich.

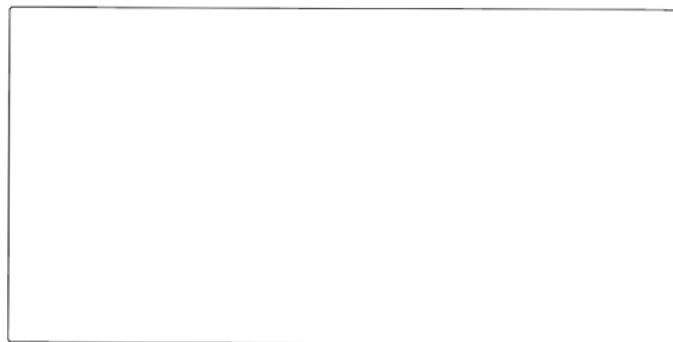
Abbildung 2-12 Anzeigemodul



## 2.9 Leermodul

Verwenden Sie für ein ansprechenderes Aussehen das Leermodul, falls es zusätzlichen Platz beim Zusammenstellen von Modulen gibt.

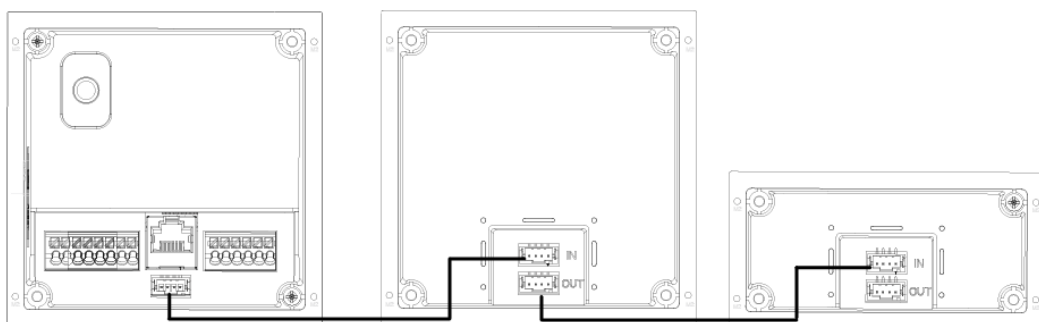
Abbildung 2-13 Leermodul



## 2.10 Kaskadenschaltung

Kaskadenschaltung ist erforderlich, damit alle Module zusammenarbeiten können.

Abbildung 2-14 Beispiel für Kaskadenschaltung



# 3 Konfiguration und Inbetriebnahme

Dieses Kapitel stellt die grundlegende Konfiguration von VTO- und VTH-Geräten vor.



Oberfläche und Funktion können je nach dem für die VTO konfigurierten Gerätetyp variieren. Es gelten die tatsächliche Oberfläche und Funktion.

## 3.1 Vorgehensweise



Überprüfen Sie vor der Konfiguration, dass die Verdrahtung keine Kurzschlüsse oder Unterbrechungen aufweist.

Schritt 1: Planen Sie IP und Einheiten-/Zimmernummer (fungiert als Telefonnummer) für jedes Gerät.

Schritt 2: Konfigurieren Sie die VTO. Siehe „3.2 VTO konfigurieren“.

Schritt 3: Konfigurieren Sie VTH. Siehe das VTH-Benutzerhandbuch.

Schritt 4: Prüfen Sie, ob alle Einstellungen stimmen. Siehe „3.3 Inbetriebnahme“.

## 3.2 VTO konfigurieren

Schließen Sie den VTO mit einem Netzkabel an Ihren PC an. Für die erstmalige Anmeldung müssen Sie ein neues Kennwort für die Webschnittstelle erstellen.

### 3.2.1 Initialisierung

Schritt 1: Schalten Sie die VTO ein.

Schritt 2: Rufen Sie die IP-Adresse der VTO im Browser auf.



Geben Sie zur erstmaligen Anmeldung die Standard-IP (192.168.1.108) ein. Falls Sie mehrere VTOs haben, sollten Sie die Standard-IP-Adresse (**Netzwerk > Grundlegend** (Network > Basic)) zur Vermeidung von Konflikten ändern.

Abbildung 3-1 Initialisierung des Geräts

The screenshot shows a dark-themed 'Device Init' window. At the top, there are three numbered steps: 1 (highlighted in blue), 2, and 3. Below the steps, the text 'One', 'Two', and 'Three' is displayed. The main form contains the following elements: 'Username admin', a 'Password' input field, a password strength indicator with three buttons labeled 'Low', 'Middle', and 'High', a 'Confirm Password' input field, and a 'Next' button at the bottom.

Schritt 3: Geben Sie das Passwort ein und bestätigen Sie es. Klicken Sie dann auf **Weiter** (Next).

Schritt 4: Wählen Sie **E-Mail** (Email), geben Sie eine E-Mail-Adresse für die Passwortrücksetzung ein und klicken Sie dann auf **Weiter** (Next).

Schritt 5: Klicken Sie auf **OK**. Das System ruft das Anmeldefenster auf.

### 3.2.2 VTO-Nummer konfigurieren

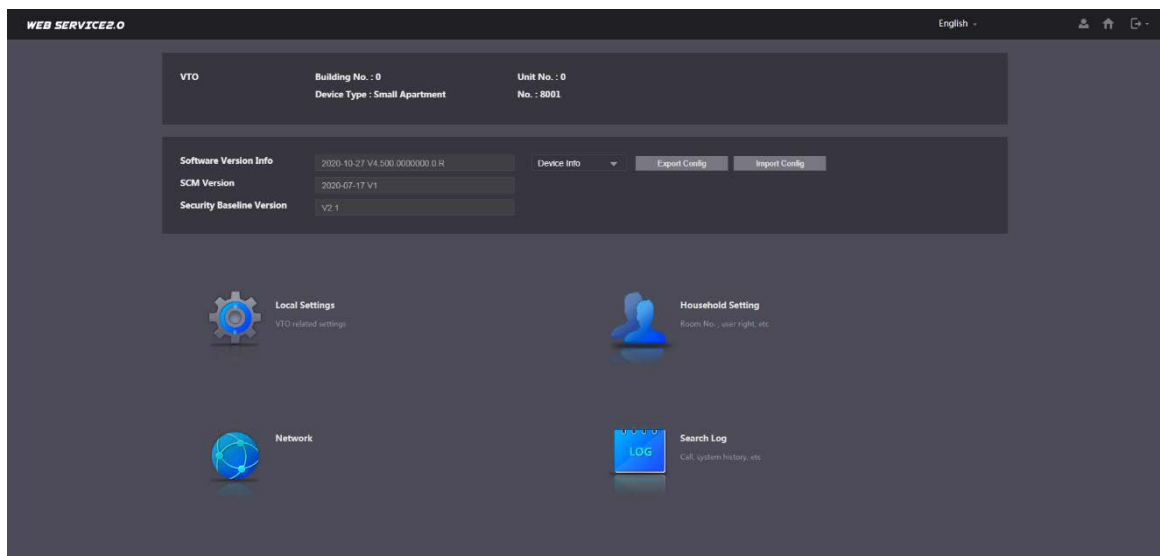
Nummern können zur Unterscheidung der einzelnen VTOs verwendet werden und sollten entsprechend der Einheiten- oder Gebäudennummer eingestellt werden.



Sie können die Nummer einer VTO ändern, wenn diese nicht als SIP-Server arbeitet. Eine VTO-Nummer darf max. 5 Ziffern enthalten und darf mit keiner Zimmernummer identisch sein.

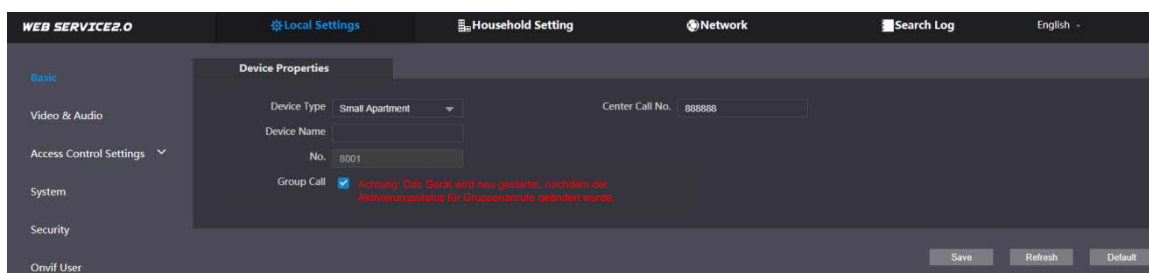
Schritt 1: Melden Sie sich bei der VTO-Weboberfläche an.

Abbildung 3-2 Hauptfenster



Schritt 2: Wählen Sie **Lokale Einstellungen** > **Grundlegend** (Local Settings > Basic).

Abbildung 3-3 Geräteeigenschaften

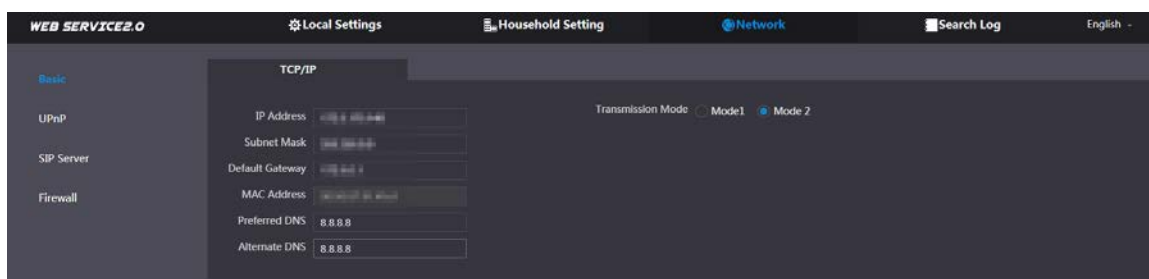


Schritt 3: Geben Sie die Nummer unter **Nr. (No.)**, klicken Sie dann auf **Speichern (Save)**.

### 3.2.3 Netzwerkparameter konfigurieren

Schritt 1: Wählen Sie **Netzwerk > Grundlegend (Network > Basic)**.

Abbildung 3-4 TCP/IP-Informationen



Schritt 2: Bearbeiten Sie die Parameter und klicken Sie auf **Speichern (Save)**.

Die VTO startet automatisch neu. Sie müssen beim erneuten Anmelden die IP-Adresse Ihres PCs auf dasselbe Netzwerksegment ändern, das auch der VTO entspricht.

### 3.2.4 SIP-Server konfigurieren

Bei Verbindung mit demselben SIP-Server können alle VTOs und VTHs einander anrufen. Sie können eine VTO oder andere Server als SIP-Server verwenden.



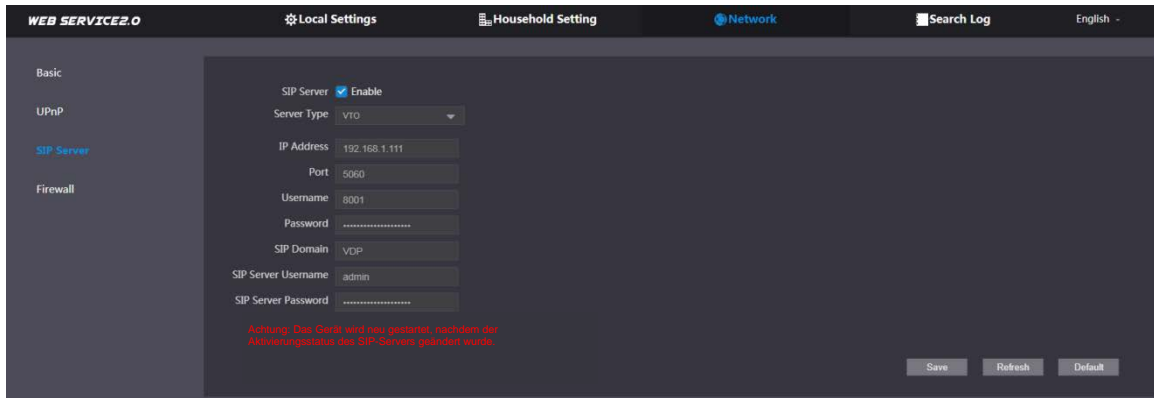
- Wenn die aktuelle VTO der SIP-Server ist, werden die **Gebäudenummer (Building No.)** und die **Einheitennummer (Unit No.)** nicht in den **Geräteeigenschaften (Device Properties)** angezeigt.
- Falls Sie **Netzwerkeinstellung > SIP-Server (Network Setting > SIP Server)** aufrufen, aktivieren Sie **Alternativer Server (Alternate Sever)** und melden Sie sich erneut an der Weboberfläche an. **Gebäudenummer (Building No.)** und **Einheitennummer (Unit No.)** werden im Fenster **Geräteeigenschaften (Device Properties)** angezeigt.

Schritt 1: Melden Sie sich bei der Weboberfläche an.

Schritt 2: Wählen Sie **Netzwerk > SIP-Server (Network > SIP Server)**.




Abbildung 3-5 SIP-Server



**Schritt 3:** Wählen Sie einen SIP-Server.

- VTO als SIP-Server: Dies ist nur auf ein Gebäude anwendbar.
  - 1) Aktivieren Sie **SIP-Server** (SIP Server).
  - 2) Wählen Sie bei **Server-Typ** (Server Type) die Option **VTO**.
  - 3) Konfigurieren Sie die Parameter. Siehe Tabelle 3-1 .
  - 4) Klicken Sie auf **Speichern** (Save). Der VTO wird automatisch neu gestartet.
- Plattform (Express / DSS) als SIP-Server: Dies ist auf mehrere Gebäude oder Einheiten anwendbar. Falls Sie keine Plattform haben, nutzen Sie eine VTO als SIP-Server.
  - 1) Deaktivieren Sie den **SIP-Server** (SIP Server).
  - 2) Setzen Sie **Server-Typ** (Server Type) auf **Express/DSS**.
  - 3) Konfigurieren Sie die Parameter.

Tabelle 3-1 Beschreibung der SIP-Serverparameter

Parameter	Beschreibung
IP-Adresse	IP-Adresse des SIP-Servers.  Falls <b>Alternativer Server</b> (Alternate Server) nicht aktiviert ist, kann die VTO den VTS nicht anrufen.
Port	<ul style="list-style-type: none"> <li>● 5060 ist der Standard, wenn VTO als SIP-Server fungiert.</li> <li>● 5080 ist der Standard, wenn die Plattform als SIP-Server fungiert.</li> </ul>
Benutzername/Passwort	Behalten Sie den Standardwert bei.
SIP-Domäne	<ul style="list-style-type: none"> <li>● Muss VDP sein , wenn der VTO als SIP-Server fungiert.</li> <li>● Bei Null oder beim Standard belassen, wenn die Plattform als SIP-Server fungiert.</li> </ul>
SIP-Server-Benutzername/-Passwort	Zur Anmeldung beim SIP-Server.
Alternative IP-Adresse	IP-Adresse des alternativen Servers.
Alternativer Benutzername	Anmelde-Benutzername und -Passwort des alternativen Servers.
Alternatives Passwort	
Alternative VTS-IP-Adresse	IP-Adresse des alternativen VTS.

Alternativer Server	<ul style="list-style-type: none"> <li>• Nachdem Sie die alternative IP-Adresse, den Benutzernamen, das Kennwort und die VTS-IP-Adresse eingegeben haben, müssen Sie <b>Alternativer Server</b> (Alternate Server) aktivieren.</li> <li>• Nachdem Sie <b>Alternativer Server</b> (Alternate Server) aktiviert haben, können Sie nur die VTS-IP-Adresse eingeben, und die VTO wird neu gestartet.</li> </ul>
---------------------	---

Schritt 4: Klicken Sie auf **OK**, und die VTO startet automatisch neu.



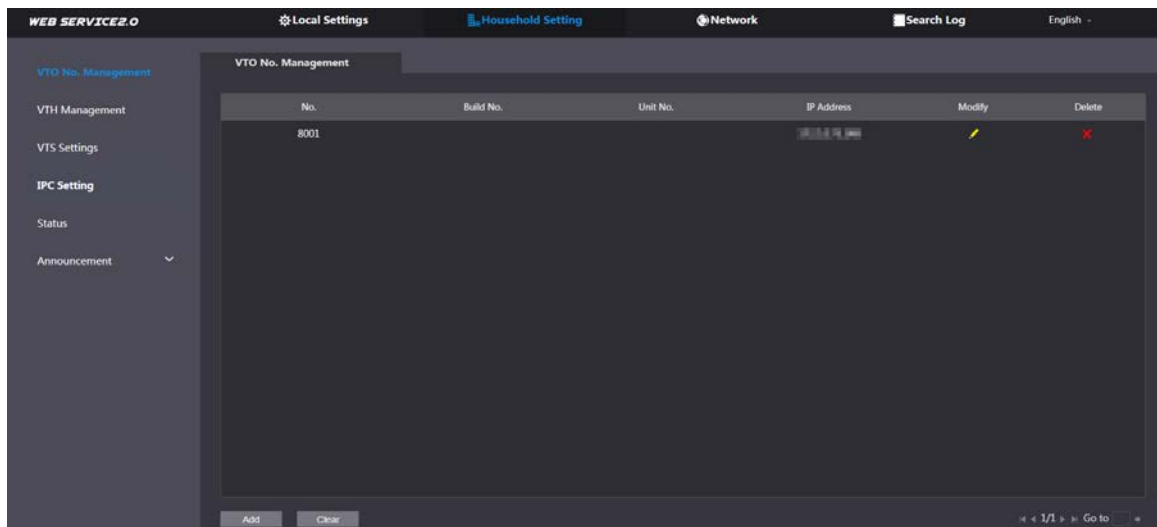
Wenn eine Plattform als SIP-Server fungiert, aktivieren Sie zunächst **Unterstützungsgebäude** (Support Building) und **Unterstützungseinheit** (Support Unit), falls dies zur Einrichtung der Gebäude- und Einheitennummer erforderlich ist.

### 3.2.5 VTO hinzufügen

Sie können dem SIP-Server VTO-Geräte hinzufügen und alle mit demselben SIP-Server verbundenen VTO-Geräte können untereinander Videoanrufe tätigen. Dieser Abschnitt bezieht sich auf den Zustand, in dem ein VTO-Gerät als SIP-Server fungiert. Wenn Sie andere Server als SIP-Server verwenden, finden Sie in den entsprechenden Handbüchern eine detaillierte Konfiguration.

Schritt 1: Melden Sie sich bei der Weboberfläche des SIP-Servers an und wählen Sie dann **Haushaltseinstellung > VTO-Nr. Verwaltung** (Household Setting > VTO No. Management).

Abbildung 3-6 VTO-Nummernverwaltung



Schritt 2: Klicken Sie auf **Hinzufügen** (Add).

Abbildung 3-7 VTO hinzufügen

Schritt 3: Konfigurieren Sie die Parameter.



Der SIP-Server muss hinzugefügt werden.

Tabelle 3-2 VTO hinzufügen

Parameter	Beschreibung
Datensatznr.	VTO-Nummer. Siehe „3.2.2 VTO-Nummer konfigurieren“.
PW registrieren	Behalten Sie den Standardwert bei.
Gebäudenr.	Nur wenn andere Server als SIP-Server fungieren.
Einheiten-Nr.	
IP-Adresse	VTO-IP-Adresse.
Benutzername	Benutzername und Passwort zur Anmeldung an der VTO-Weboberfläche.
Passwort	

Schritt 4: Klicken Sie auf **Speichern** (Save).

### 3.2.6 Zimmernummer hinzufügen

Sie können die vorgesehene Zimmernummer zum SIP-Server hinzufügen und dann die Zimmernummer auf VTH-Geräten konfigurieren, um sie mit dem Netzwerk zu verbinden. Dieser Abschnitt bezieht sich auf den Zustand, in dem die VTO als SIP-Server fungiert. Wenn Sie andere Server als SIP-Server verwenden, finden Sie in den entsprechenden Handbüchern der Server detaillierte Konfiguration.

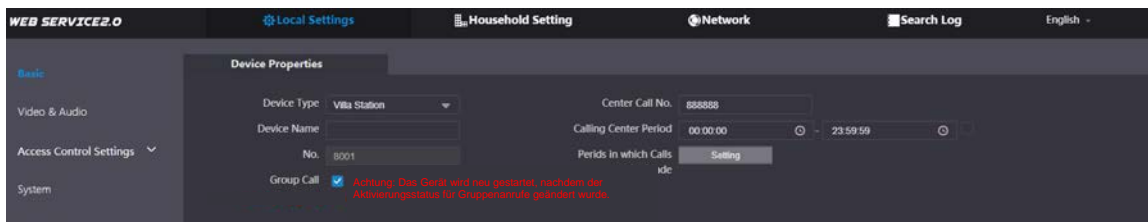


Die Zimmernummer darf höchstens 6 Ziffern, Buchstaben oder deren Kombination enthalten. Sie darf nicht mit einer VTO-Nummer identisch sein.

### Die VTO in einem Einfamilienhaus verwenden

Schritt 1: Melden Sie sich an der Weboberfläche des SIP-Servers an und wählen Sie dann **Lokale Einstellungen > Grundlegend** (Local Settings > Basic).

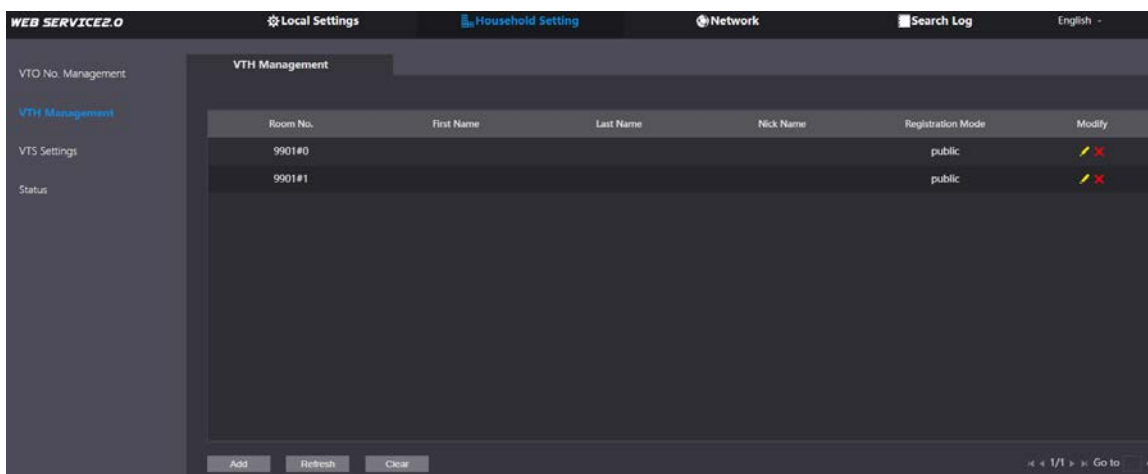
Abbildung 3-8 Geräteeigenschaften



Schritt 2: Setzen Sie **Gerätetyp** (Device Type) auf **Station für Einfamilienhaus** (Villa Station) und klicken Sie auf **Speichern** (Save).

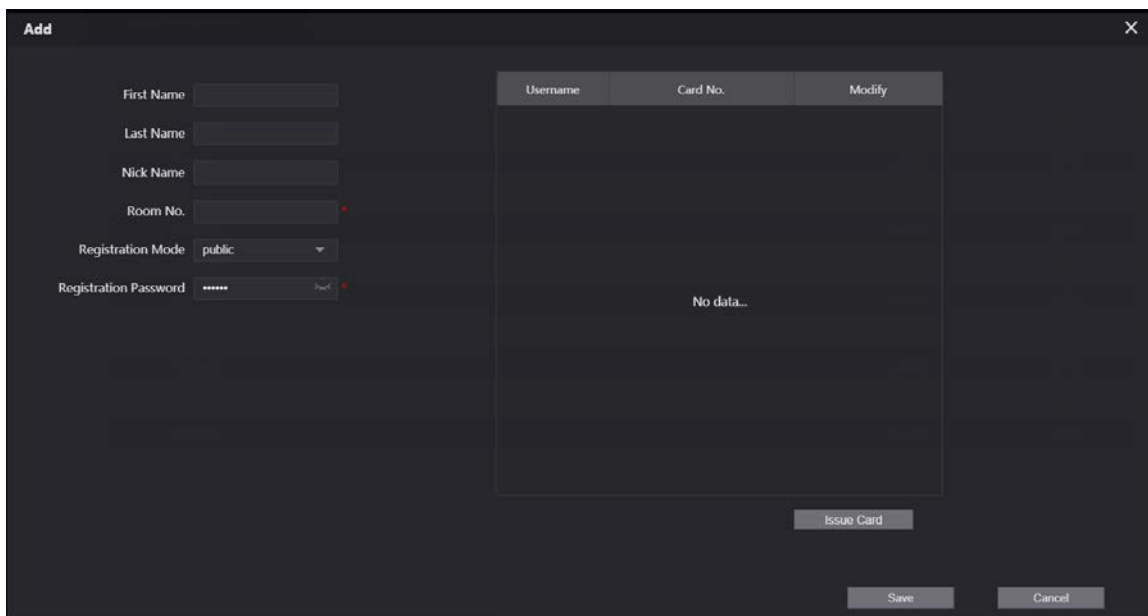
Schritt 3: Wählen Sie **Haushaltseinstellung** > **VTH-Verwaltung** (Household Setting > VTH Management).

Abbildung 3-9 Zimmernummernverwaltung



Schritt 4: Klicken Sie auf **Hinzufügen** (Add).

Abbildung 3-10 Eine einzelne Zimmernummer hinzufügen





Schritt 5: Konfigurieren Sie die Informationen auf der linken Seite.

Tabelle 3-3 Zimmerdaten

Parameter	Beschreibung
Vorname	Informationen zur Differenzierung einzelner Zimmer.
Nachname	
Spitzname	
Zimmernr.	<ul style="list-style-type: none"> <li>• Wenn mehrere VTHs vorhanden sind, sollte die Zimmernummer für die Haupt-VTH mit #0 enden und die Zimmernummern für Sub-VTHs mit #1, #2 usw.</li> <li>• Sie können bis zu 10 Sub-VTHs für einen Haupt-VTH haben.</li> </ul>
Registrierungstyp	Wählen Sie <b>öffentlich</b> (public).
Registrierungspasswort	Behalten Sie den Standardwert bei.

**Schritt 6:** Klicken Sie auf **Speichern** (Save).

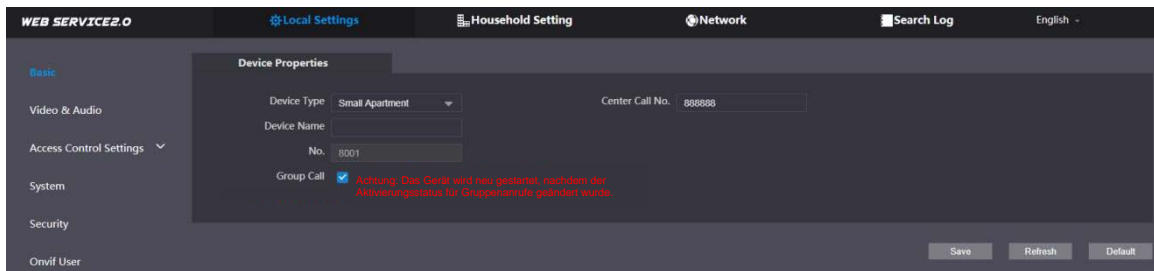


- Klicken Sie zum Ändern oder Löschen einer Zimmernummer auf  oder .
- Klicken Sie zum Löschen aller Zimmernummern auf **Löschen** (Clear).

## Die VTO in einer kleinen Wohnung verwenden

**Schritt 1:** Melden Sie sich an der Weboberfläche des SIP-Servers an und wählen Sie dann **Lokale Einstellungen > Grundlegend** (Local Settings > Basic).

Abbildung 3-11 Geräteeigenschaften

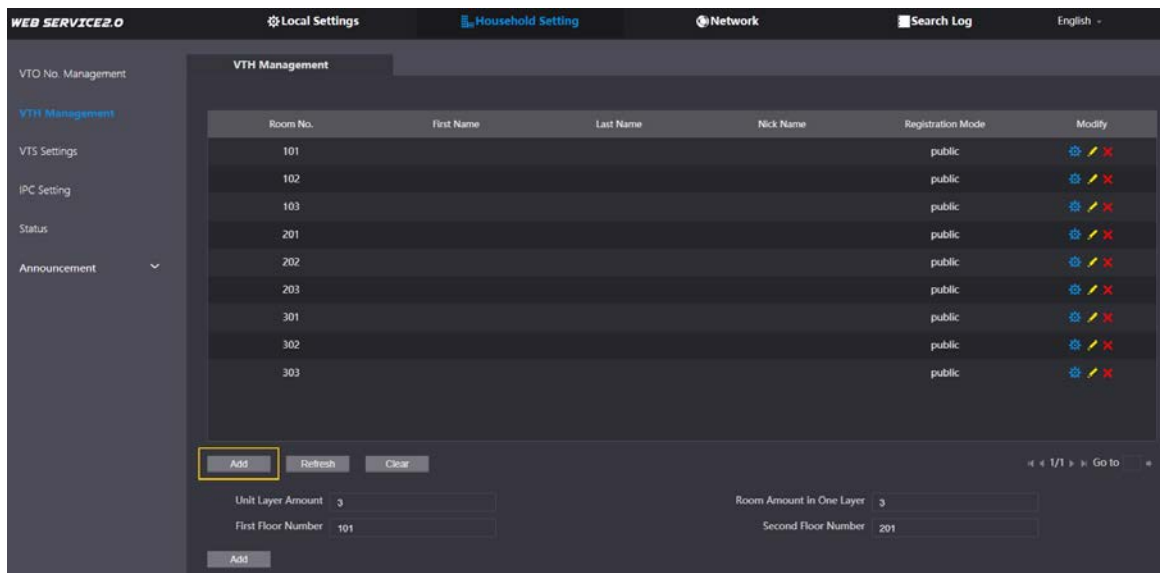


**Schritt 2:** Setzen Sie **Gerätetyp** (Device Type) auf **Kleine Wohnung** (Small Apartment) und klicken Sie auf **Speichern** (Save).

**Schritt 3:** Wählen Sie **Haushaltseinstellung > VTH-Verwaltung** (Household Setting > VTH Management). Sie können eine einzelne Zimmernummer oder Zimmernummern stapelweise hinzufügen .

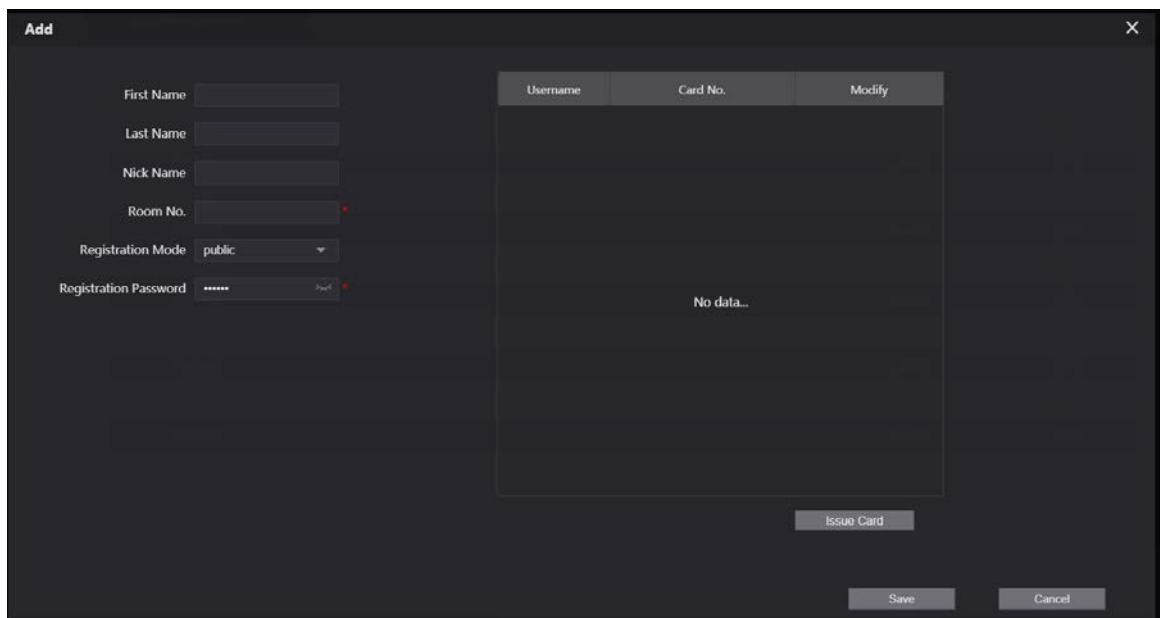
- Fügen Sie eine einzelne Zimmernummer hinzu.

Abbildung 3-12 Zimmernummern hinzufügen



- 1) Klicken Sie auf **Hinzufügen** (Add).

Abbildung 3-13 Eine einzelne Zimmernummer hinzufügen





- 2) Konfigurieren Sie die Informationen auf der linken Seite. Siehe Tabelle 3-3 für Details.

- 3) Klicken Sie auf **Speichern** (Save).
- Fügen Sie mehrere Zimmernummern hinzu.

Abbildung 3-14 Zimmernummern stapelweise hinzufügen

- 1) Konfigurieren Sie die Informationen.
  - ◇ **Einheit Ebenenzahl** (Unit Layer Amount): Die Anzahl der Ebenen in der Wohnung.
  - ◇ **Zimmeranzahl pro Ebene** (Room Amount in One Layer): Die Anzahl Zimmer auf einer Ebene.
  - ◇ **Erste Ebene Nummer** (First Floor Number): Die erste Zimmernummer auf der ersten Ebene.
  - ◇ **Zweite Ebene Nummer** (Second Floor Number): Die erste Zimmernummer auf der zweiten Ebene.
- 2) Klicken Sie auf **Hinzufügen** (Add), klicken Sie dann zur Anzeige des aktuellsten Status auf **Aktualisieren** (Refresh).



- Klicken Sie zum Ändern oder Löschen einer Zimmernummer auf  oder .
- Klicken Sie zum Löschen aller Zimmernummern auf **Löschen** (Clear).

## 3.2.7 Modul konfigurieren

Das Kameramodul ist standardmäßig hinzugefügt. Alle anderen Module müssen vor der Verwendung im Fassadenlayout hinzugefügt werden.

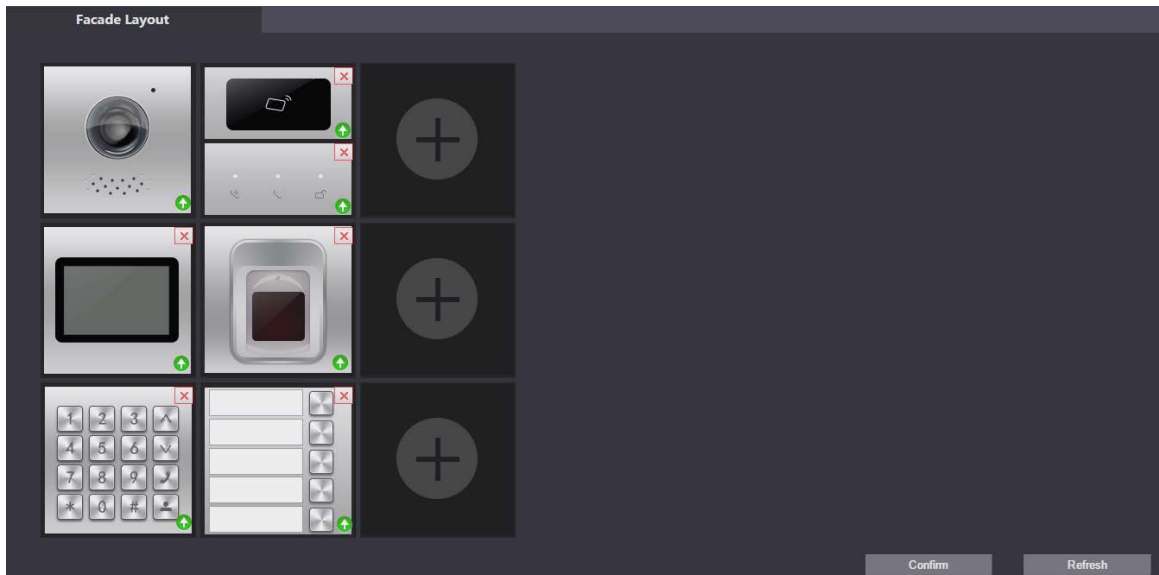



Die VTO kann bis zu 9 funktionale Module haben. Bei Fingerabdruck-Modul, Kartenmodul und Tastaturmodul können Sie nur eines je Typ hinzufügen. Bei anderen Modulen können Sie beliebig viele hinzufügen.

### 3.2.7.1 Module hinzufügen

Schritt 1: Wählen Sie **Lokale Einstellungen** > **Grundlegend** > **Fassadenlayout** (Local Setting > Basic > Façade Layout).

Abbildung 3-15 Fassadengestaltung



**Schritt 2:** Klicken Sie auf  und verfügbare Module werden angezeigt.



Tastaturmodul, Kartenmodul und Fingerabdruckmodul werden nicht angezeigt, wenn sie hinzugefügt wurden.

**Schritt 3:** Wählen Sie Module gemäß der tatsächlichen Gestaltung der VTO aus.



Die Anordnung muss von oben nach unten und von links nach rechts erfolgen.

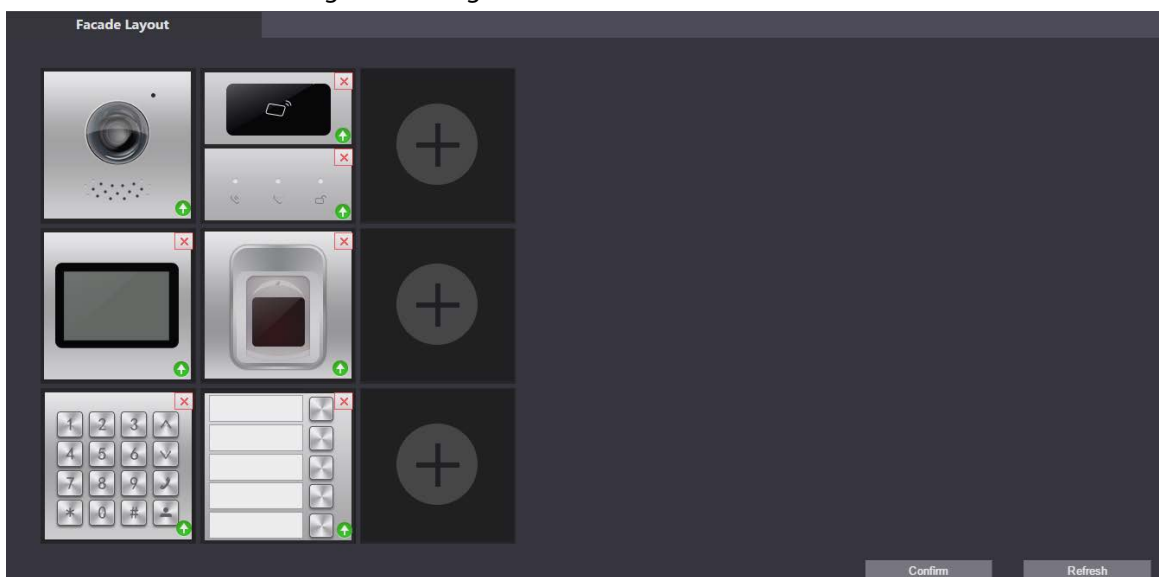
**Schritt 4:** Klicken Sie auf **Bestätigen** (Confirm), starten Sie dann den Browser zur Anwendung der Änderungen neu.

### 3.2.7.2 Module konfigurieren

Sie müssen Zimmernummern für das Tastenmodul konfigurieren.

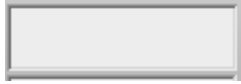
**Schritt 1:** Wählen Sie **Lokale Einstellungen** > **Grundlegend** > **Fassadenlayout** (Local Setting > Basic > Façade Layout).

Abbildung 3-16 Konfigurationen Sie das Tastenmodul



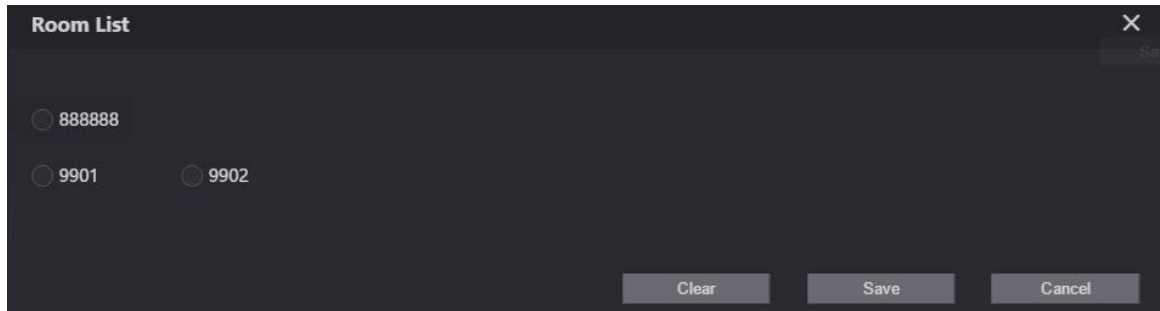


Schritt 2: Klicken Sie auf



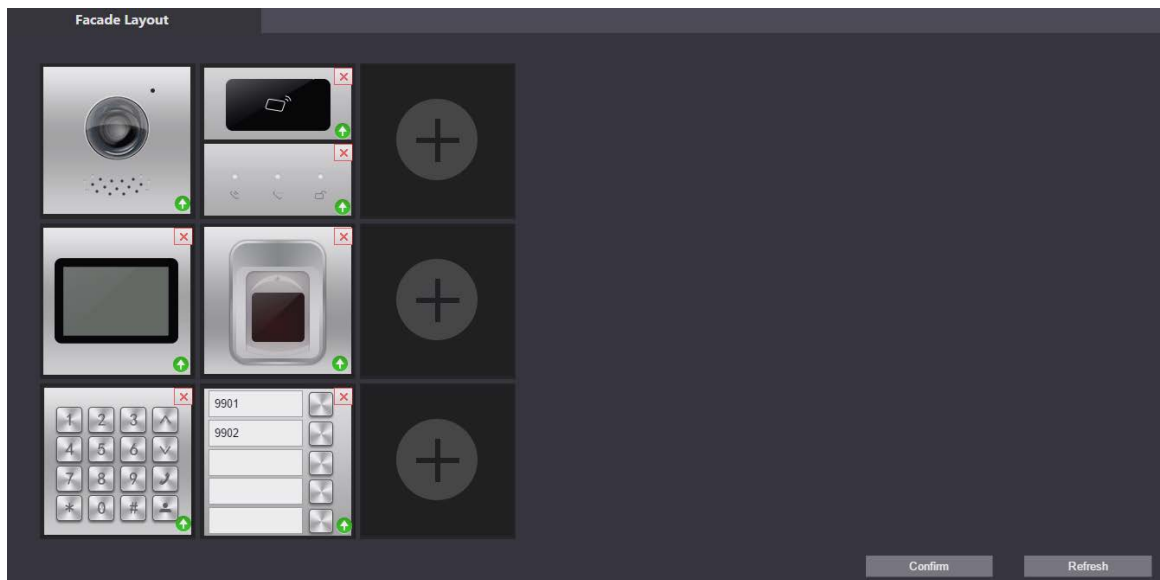
Die auf der Oberfläche angezeigte Zimmernummer entspricht jener der hinzugefügten VTH. „888888“ ist die Nummer des Management Center.

Abbildung 3-17 Zimmerliste



Schritt 3: Wählen Sie die Zimmernummer, klicken Sie dann auf **Speichern** (Save).

Abbildung 3-18 Informationen zur Zimmernummer



Schritt 4: Klicken Sie auf **Bestätigen** (Confirm), starten Sie dann den Browser zur Anwendung der Änderungen neu.

## 3.3 Inbetriebnahme

### 3.3.1 VTO ruft VTH an

Schritt 1: Wählen Sie eine Zimmernummer an der VTO an.

Schritt 2: Drücken Sie .


Schritt 3: Tippen Sie auf  an der VTH, um den Anruf anzunehmen.

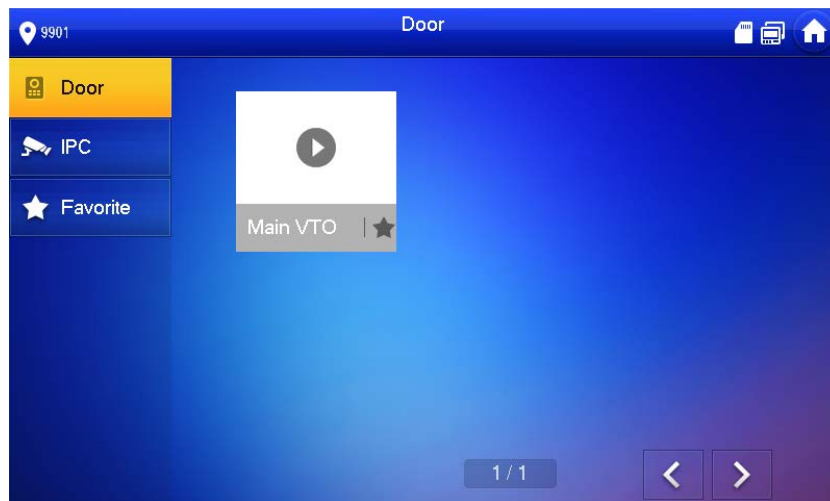
Abbildung 3-19 Anrufbildschirm



### 3.3.2 VTH überwacht VTO

Schritt 1: Wählen Sie an der VTH **Überwachen** > **Tür** (Monitor > Door).

Abbildung 3-20 Tür



Schritt 2: Wählen Sie die VTO, die Sie überwachen möchten.

Abbildung 3-21 Video überwachen



# Anhang 1 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 des Basisgerätes zu ergreifen sind:**

### **1. Verwenden Sie sichere Passwörter**

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

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

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

- Gemäß dem in der Tech-Industrie üblichen Verfahren empfehlen wir, die Firmware Ihrer Geräte (wie NVR, DVR, IP-Kamera usw.) auf dem neuesten Stand zu halten, um zu gewährleisten, dass das System mit den neuesten Sicherheitspatches und -fixes ausgestattet ist. Wenn das Gerät mit dem öffentliche Netzwerk verbunden ist, empfehlen wir, die Funktion „Automatische Überprüfung auf Aktualisierungen“ (Auto-Check for Updates) zu aktivieren, um aktuelle Informationen über vom Hersteller freigegebene Firmware-Aktualisierungen zu erhalten.
- 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 die Geräte beispielsweise in einen speziellen Computerraum und -schrank und implementieren Sie eine gut durchdachte Zutrittskontrollberechtigung und Schlüsselverwaltung, um unbefugte Mitarbeiter davon abzuhalten, physische Kontakte wie beschädigte Hardware, unbefugten Anschluss von Wechseldatenträgern (z.B. USB-Stick, serielle Schnittstelle) usw. durchzuführen.

### **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. Kontosperrfunktion 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, die Standard-HTTP- und andere Dienstports in einen beliebigen Zahlensatz zwischen 1024 - 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. MAC-Adressenverknüpfung**

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

#### **8. Konten und Privilegien sinnvoll zuordnen**

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

#### **9. 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 Verschlüsselungsmodus WPA2-PSK und richten Sie starke Passwörter ein.

#### **10. 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.

#### **11. 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.

#### **12. 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.

#### **13. Aufbau einer sicheren Netzwerkumgebung**

Um die Sicherheit der Geräte besser zu gewährleisten und mögliche Cyberisiken 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 Zugangssystem, um das Risiko eines unbefugten Zugriffs auf private Netzwerke zu reduzieren.
- Aktivieren Sie die IP/MAC-Adressfilterfunktion, um den Bereich der Hosts einzuschränken, die auf das Gerät zugreifen dürfen.