

Türstation für Einfamilienhaus (Version 4.5)

Kurzanleitung








Vorwort

Allgemein

Diese Anleitung stellt Aufbau, Montageverfahren und grundlegende Konfiguration der Türstation für Einfamilienhaus (nachfolgend als „VTO“ bezeichnet) vor.

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.	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

Verwenden Sie das Gerät nur wie beschrieben. Bitte lesen Sie das Handbuch vor dem Gebrauch des Geräts sorgfältig durch, um Gefahren und Sachschäden zu vermeiden. Halten Sie sich während des Gebrauchs strikt an das Handbuch und bewahren Sie es für späteres 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 waagrecht an einem stabilen Ort, 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 einem gut belüfteten Ort 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

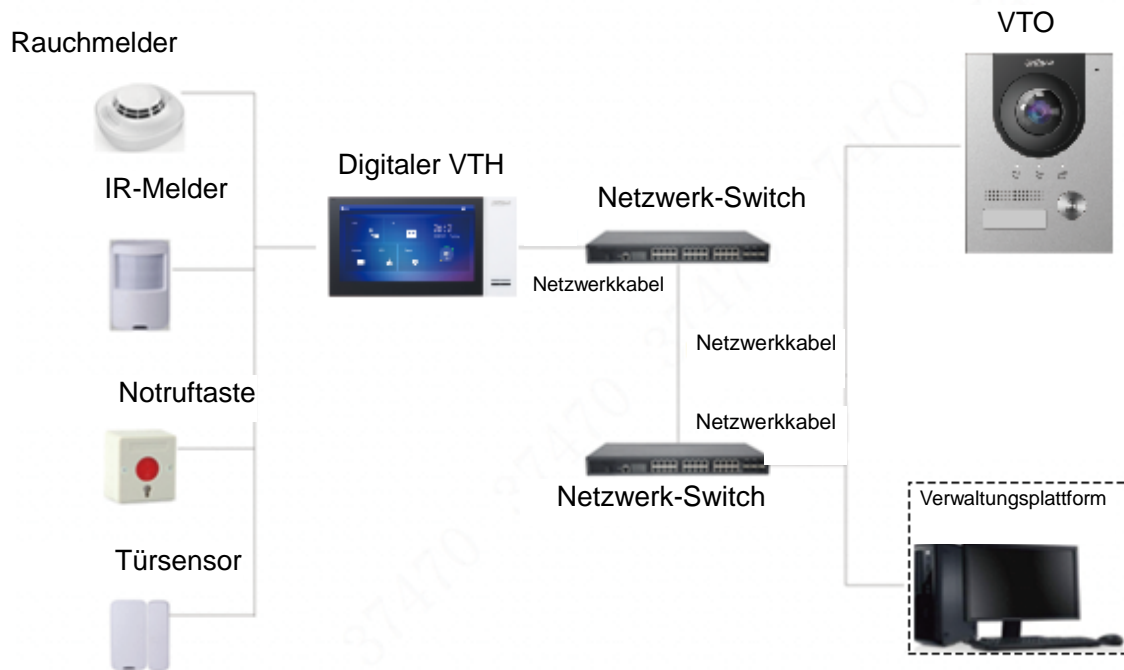
- Das Produkt muss Stromkabel verwenden, die Ihren lokalen Anforderungen entsprechen.
- Verwenden Sie ein Netzteil, das den SELV-Anforderungen (Safety Extra Low Voltage) entspricht, und schließen Sie es an einer Nennspannung gemäß IEC60950-1 an. Informationen zu bestimmten Anforderungen an die Stromversorgung finden Sie auf den Geräteetiketten.
- Der Gerätestecker dient als Trennvorrichtung. Der Stecker muss während des Betriebs jederzeit frei zugänglich sein.

Inhaltsverzeichnis

Vorwort	I
Wichtige Sicherheits- und Warnhinweise	III
1 Netzwerkdiagramm	1
2 Erscheinungsbild	2
2.1 VTO2101E-P.....	2
2.1.1 Frontblende	2
2.1.2 Geräterückseite.....	3
2.2 VTO2202F-P-S2/ VTO2202F-P/VTO2202F/VTO2201F-P	4
2.2.1 Frontblende	4
2.2.2 Geräterückseite.....	5
2.3 VTO2111D-P-S2/VTO1101D-P	6
2.3.1 Frontblende	6
2.3.2 Geräterückseite.....	7
2.4 VTO3211D-P-S2.....	8
2.4.1 Frontblende	8
2.4.2 Geräterückseite.....	9
2.5 VTO3221E-P/VTO6221E-P	10
2.5.1 Frontblende	10
2.5.2 Geräterückseite.....	11
2.6 VTO2211G-P/VTO1201G-P.....	12
2.6.1 Frontblende	12
2.6.2 Geräterückseite.....	13
3 Montage	15
4 Konfiguration	16
4.1 Vorgehensweise.....	16
4.2 Konfigurationswerkzeug	16
4.3 VTO konfigurieren.....	16
4.3.1 Initialisierung.....	16
4.3.2 VTO-Nummer konfigurieren	17
4.3.3 Netzwerkparameter konfigurieren	18
4.3.4 SIP-Server konfigurieren	19
4.3.5 Rufnummer und Gruppenruf konfigurieren.....	20
4.3.6 VTOs hinzufügen.....	20
4.3.7 Zimmernummer hinzufügen.....	22
4.4 Inbetriebnahme.....	24
4.4.1 VTO ruft VTH an	24
4.4.2 VTH überwacht VTO.....	24
5 App installieren und Gerät hinzufügen	26
5.1 Durch Kabelnetzwerk hinzufügen (wird nur von Modell mit Station für Einfamilienhaus unterstützt)	26
5.2 Durch Soft-Zugangspunkt hinzufügen (wird nur von Modell mit Station für Einfamilienhaus unterstützt)	28
Anhang 1 Empfehlungen zur Cybersicherheit	34

1 Netzwerkdiagramm

Abbildung 1-1 Netzwerkdiagramm



In bestimmten Anwendungen wie Einfamilienhäusern ist ein Management Center/eine Managementplattform üblicherweise unnötig.

2 Erscheinungsbild

2.1 VTO2101E-P

2.1.1 Frontblende

Abbildung 2-1 VTO2101E-P

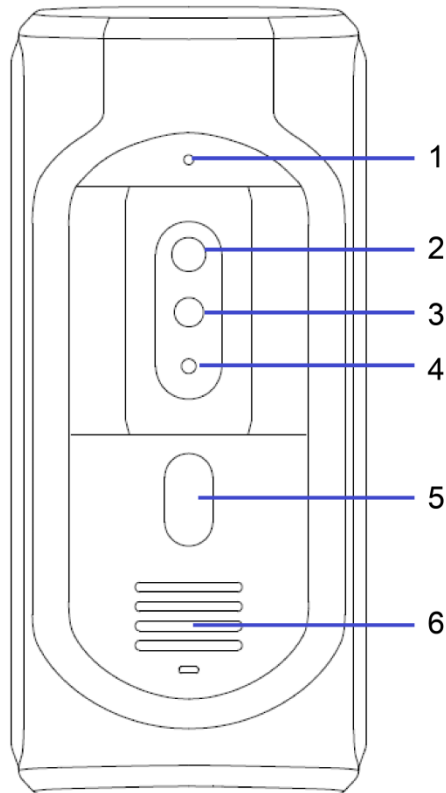


Tabelle 2-1 Beschreibung der Frontplatte

Nr.	Name	Beschreibung
1	Mikrofon	—
2	Kamera	—
3	IR-Ausleuchtungslicht	Liefert bei Dunkelheit zusätzliches IR-Licht für die Kamera.
4	Lichtsensoren	Erkennt Umgebungslichtbedingungen.
5	Klingelknopf	Zum Anrufen der VTHs oder des Management Center.
6	Lautsprecher	—

2.1.2 Geräterückseite

Abbildung 2-2 VTO2101E-P

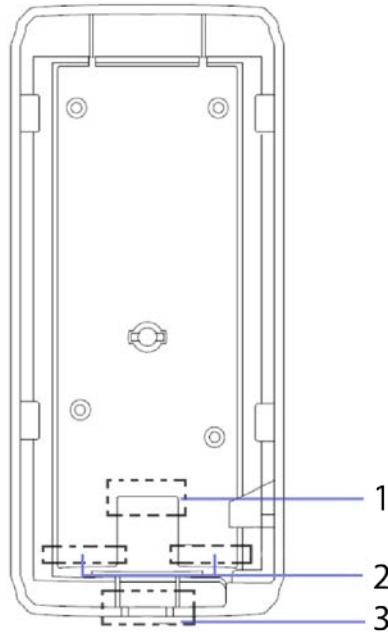
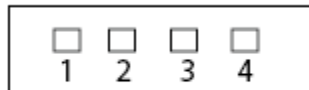


Tabelle 2-2 Beschreibung der Geräterückseite

Nr.	Name	Beschreibung
1	Netzwerkanschluss	Hier wird das Netzkabel angeschlossen.
2	RS-485-Anschlüsse	Beachten Sie die nachstehende Abbildung und Tabelle.
3	Kabelausgang	Führen Sie die Kabel hier hindurch.

Abbildung 2-3 Kabel anschließen



TÜR



STROMVERSORGUNG / 485

Tabelle 2-3 Port Beschreibung

TÜR		STROMVERSORGUNG / 485	
Nr.	Name	Nr.	Name
1	NEIN	1	+12 V
2	NC	2	Erde
3	COM	3	RS-485A
4	Alarめingang oder Entriegelung (Standard)	4	RS-485B

2.2 VTO2202F-P-S2/ VTO2202F-P/VTO2202F/VTO2201F-P

2.2.1 Frontblende

Abbildung 2-4 Frontblende

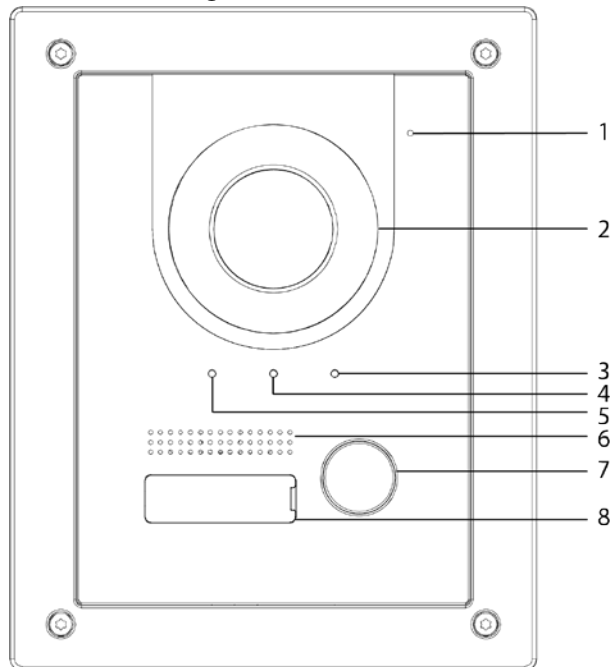


Tabelle 2-4 Beschreibung der Frontplatte

Nr.	Name	Beschreibung
1	Mikrofon	—
2	Kamera	—
3	Anzeige	Ein: Tür entriegelt.
4		Ein: Anruf erfolgt.
5		Ein: Telefonieren.
6	Lautsprecher	—
7	Klingelknopf	Zum Anrufen anderer VTHs oder des Management Center.
8	Namensschild	Host-Name.

2.2.2 Geräterückseite

Abbildung 2-5 Geräterückseite

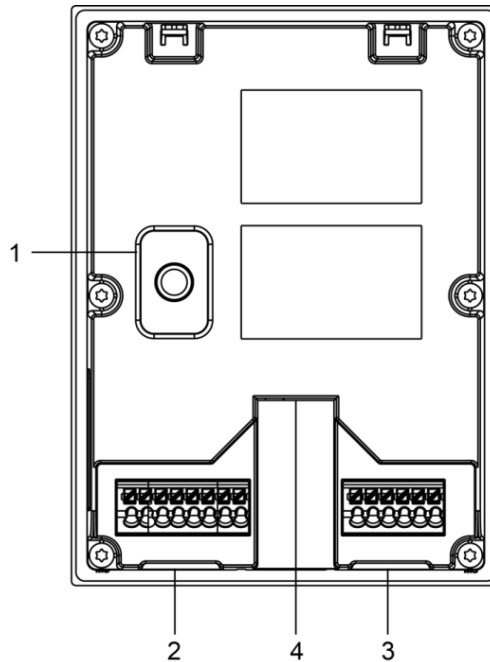



Tabelle 2-5 Beschreibung der Geräterückseite

NEI N	Name	Beschreibung
1	Sabotagekontakt	Wenn die VTO gewaltsam von der Wand entfernt wird, wird ein Alarm ausgelöst und Alarminformationen werden an das Management Center gesendet.
2	Port	Von links nach rechts: Erde +12-V-AUSGANG RS485_B RS485_A ALARM_NO ALARM_COM VTO2202F-P-S2: 2-adrig + (48 V); VTO2202F-P und VTO2202F: EOC1 (+12V); VTO2201F: +24 V. VTO2202F-P-S2: 2-adrig - (Erde); VTO2202F-P und VTO2202F: EOC2 (Erde); VTO2201F: Erde.
3		Von links nach rechts: DOOR_BUTTON DOOR_FB Erde DOOR_NC DOOR_COM DOOR_NO
4	Ethernet-Port	Verbindung mit dem Netzwerk über Ethernet-Kabel.  Nur Modelle mit „P“ unterstützen PoE.

2.3 VTO2111D-P-S2/VTO1101D-P

2.3.1 Frontblende

Abbildung 2-6 Frontblende

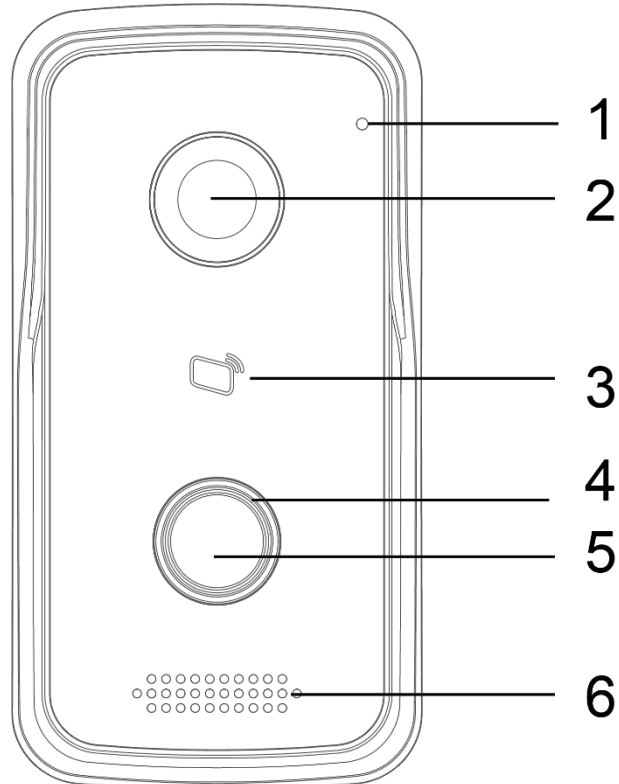


Tabelle 2-6 Beschreibung der Frontplatte

Nr.	Name	Beschreibung
1	Mikrofon	—
2	Kamera	—
3	Bereich zum Lesen der Karte	Zum Entriegeln oder Ausstellen einer Karte durchziehen.
4	Anzeige	<ul style="list-style-type: none">● Leuchtet blau: Standby-Modus.● Blinkt blau: Anruf oder es gibt kein Netzwerk.
5	Klingelknopf	Zum Anrufen der VTHs oder des Management Center.
6	Lautsprecher	—

2.3.2 Geräterückseite

Abbildung 2-7 Geräterückseite

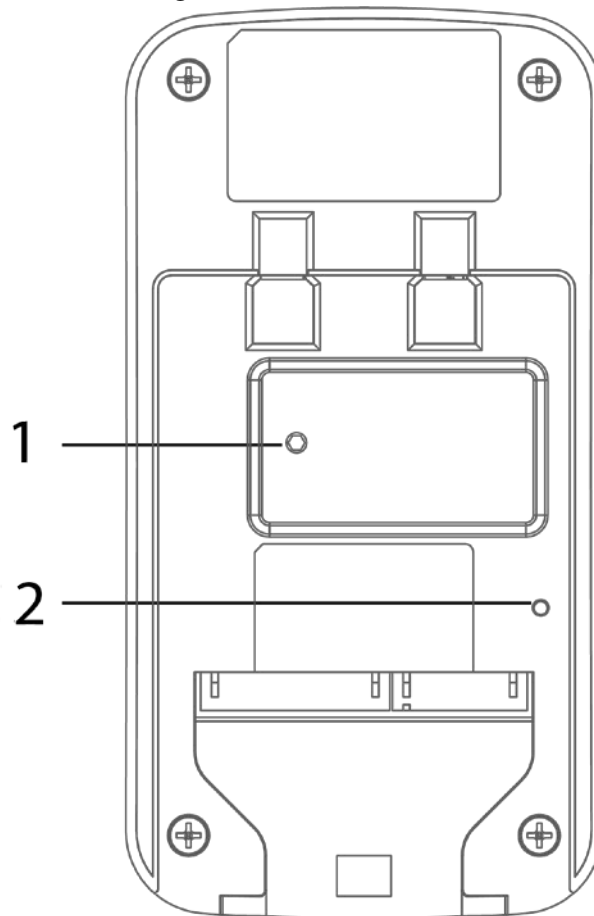


Tabelle 2-7 Beschreibung der Geräterückseite

Nr.	Name	Beschreibung
1	Sabotagekontakt	Wenn die VTO gewaltsam von der Wand entfernt wird, wird ein Alarm ausgelöst und Alarminformationen werden an das Management Center gesendet.
2	Reset	Halten Sie sie zum Reset aller Einstellungen 10 Sekunden gedrückt.

Abbildung 2-8 Kabel anschließen

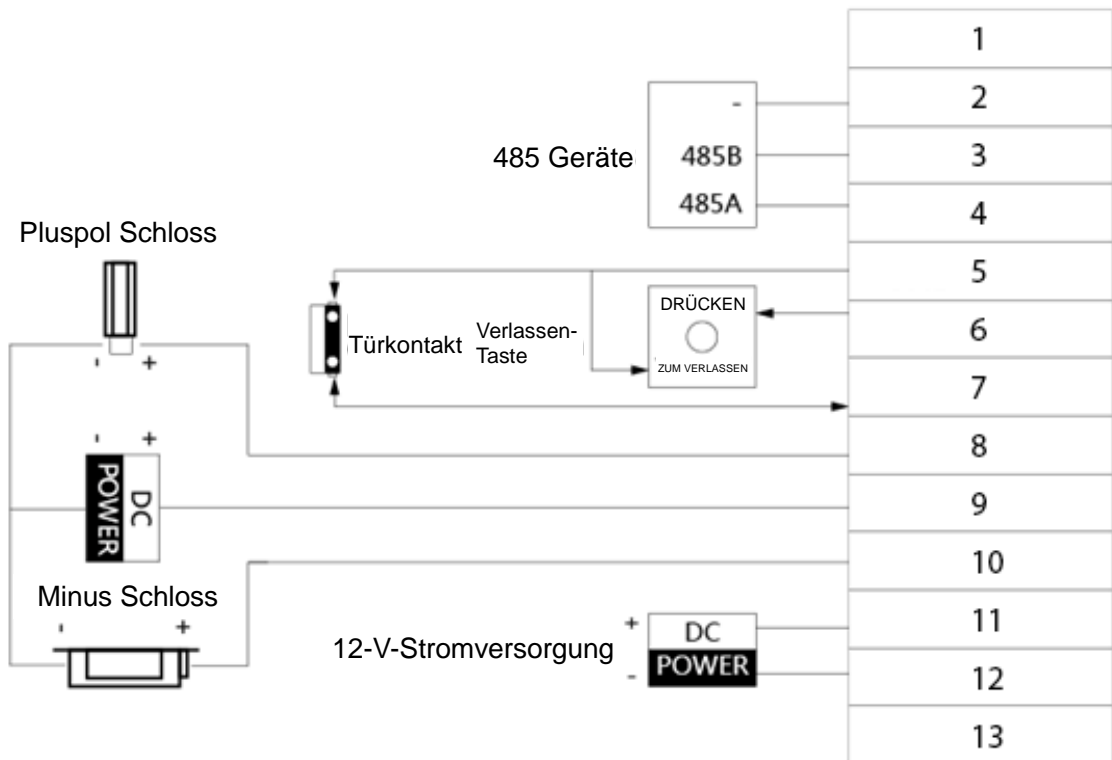


Tabelle 2-8 Port Beschreibung

Nr.	Beschreibung	Nr.	Beschreibung
1	Entfällt	8	NC
2	Erde	9	COM
3	485_B	10	NEIN
4	485_A	11	Erde
5	Erde	12	12 V
6	ENTRIEGELN	13	NETZ
7	FEEDBACK	—	—

2.4 VTO3211D-P-S2

2.4.1 Frontblende

Die Anzahl der Tasten auf der Frontblende variiert je nach Modell. VTO3211D-P-S2 hat eine Taste, VTO3211D-P2-S2 hat zwei Tasten und VTO3211D-P4-S2 hat vier Tasten. Hier nehmen wir VTO3211D-P4-S2 als Beispiel.

Abbildung 2-9 VTO3211D-P4-S2

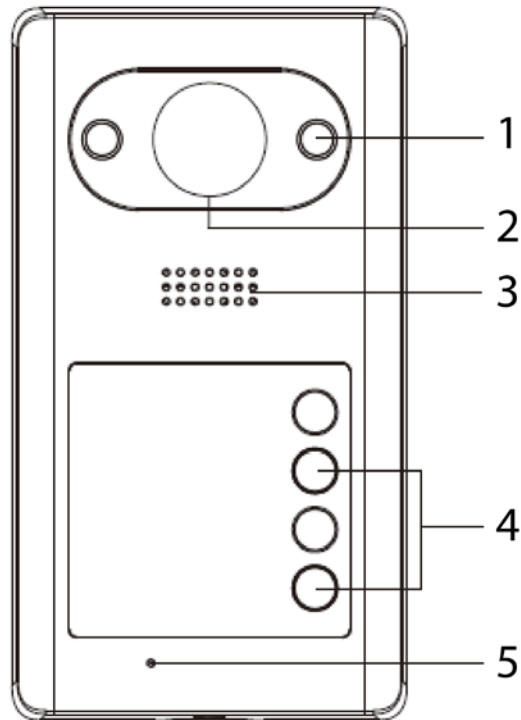


Tabelle 2-9 Beschreibung der Frontplatte

Nr.	Name	Beschreibung
1	IR-Beleuchtung	Liefert bei Dunkelheit zusätzliches IR-Licht für die Kamera.
2	Kamera	—
3	Lautsprecher	—
4	Klingelknopf	Zum Anrufen der VTHs oder des Management Center.
5	Mikrofon	—

2.4.2 Geräterückseite

Abbildung 2-10 VTO3211D-P4

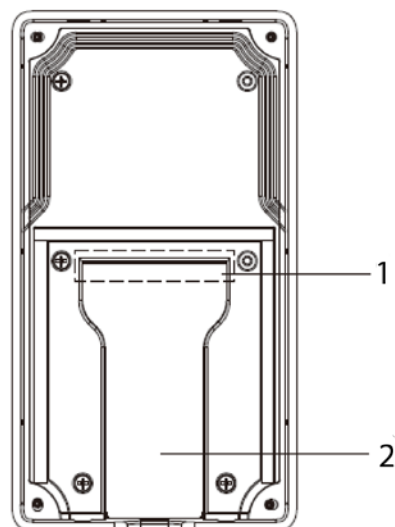


Tabelle 2-10 Beschreibung der Geräterückseite

Nr.	Name	Beschreibung
1	Kabelanschlüsse	Beachten Sie die nachstehende Abbildung und Tabelle.
2	Kabelausgang	Führen Sie die Kabel hier hindurch.

Abbildung 2-11 Kabel anschließen

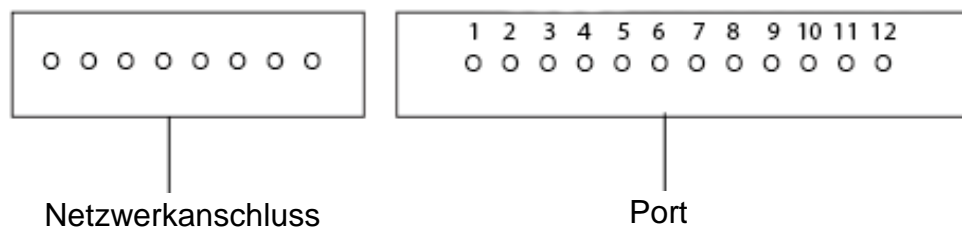


Tabelle 2-11 Kabelstecker

Nr.	Name	Nr.	Name
1	ALM_COM	7	DOOR_FEED
2	ALM_NO	8	DOOR_NC
3	ALM_IN	9	DOOR_COM
4	RS485B	10	DOOR_NO
5	RS485A	11	Erde
6	DOOR_OPEN	12	DC 12 V

2.5 VTO3221E-P/VTO6221E-P

2.5.1 Frontblende

Abbildung 2-12 VTO3221E-P/VTO6221E-P

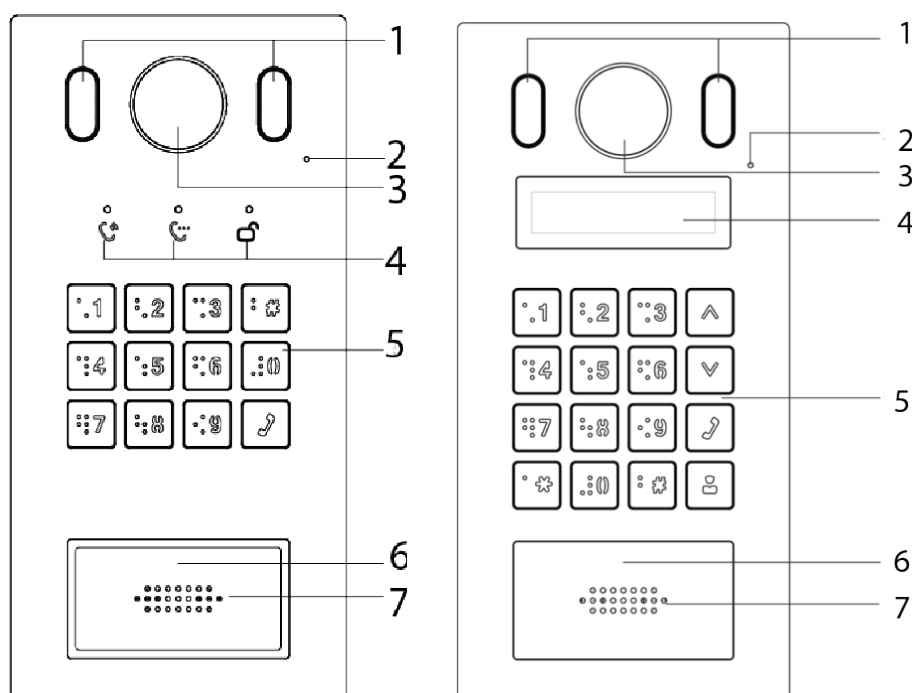


Tabelle 2-12 Beschreibung der Frontplatte von VTO3221E-P und VTO6221E-P

Nr.	Name	Beschreibung
1	Beleuchtung	Liefert bei Dunkelheit zusätzliches Licht für die Kamera.
2	Mikrofon	—
3	Kamera	—
4	VTO3221E-P: Kontrollleuchten	Zeigt den Status zu Anruf, Gespräch und Entriegelung.
	VTO6221E-P: Bildschirm	—
5	Tastenfeld	—
6	Bereich zum Lesen der Karte	Ziehen Sie die Karte hier durch, um die Tür zu entriegeln.
7	Lautsprecher	—

2.5.2 Geräterückseite

Abbildung 2-13 VTO3221E-P

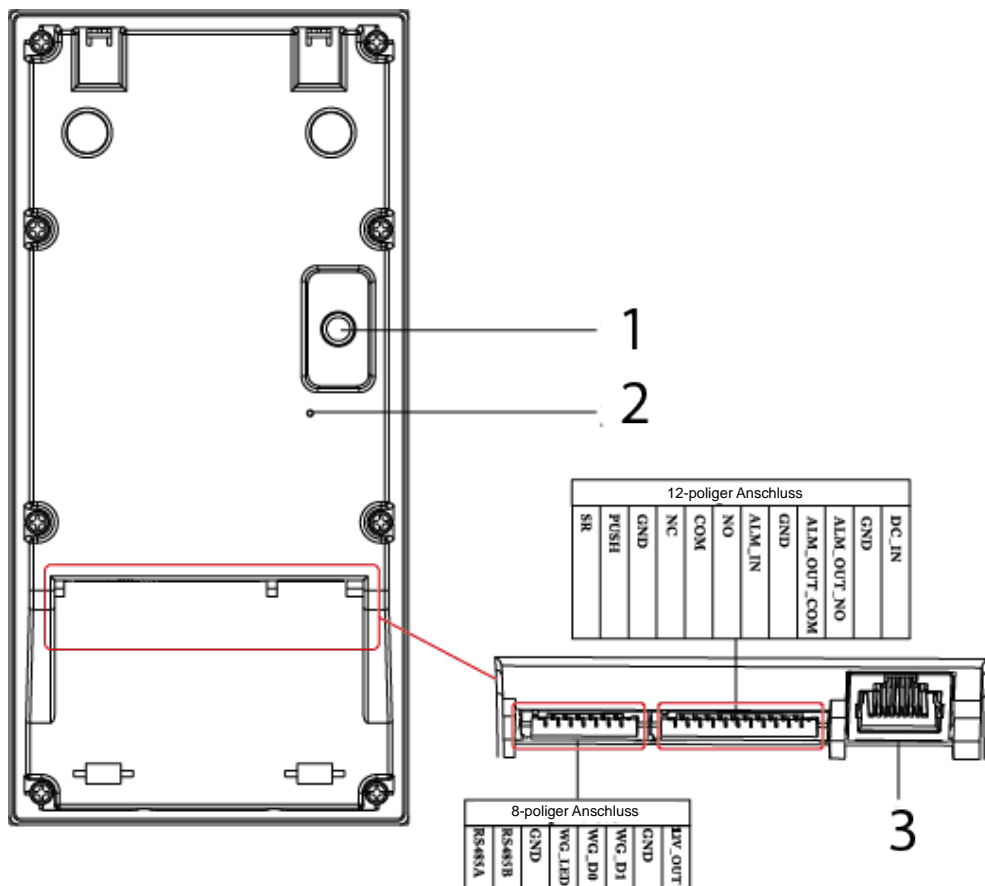


Tabelle 2-13 Beschreibung der Geräterückseite

Nr.	Name	Beschreibung
1	Sabotagekontakt	Wenn die VTO gewaltsam von der Wand entfernt wird, wird ein Alarm ausgelöst und Alarminformationen werden an das Management Center gesendet.
2	Rücksetztaste	Halten Sie sie zum Reset aller Einstellungen 10 s gedrückt.
3	Ethernet-Port	Schließen Sie hier ein Ethernetkabel an.

2.6 VTO2211G-P/VTO1201G-P

2.6.1 Frontblende

Abbildung 2-14 Frontblende von VTO2211G/VTO1201G

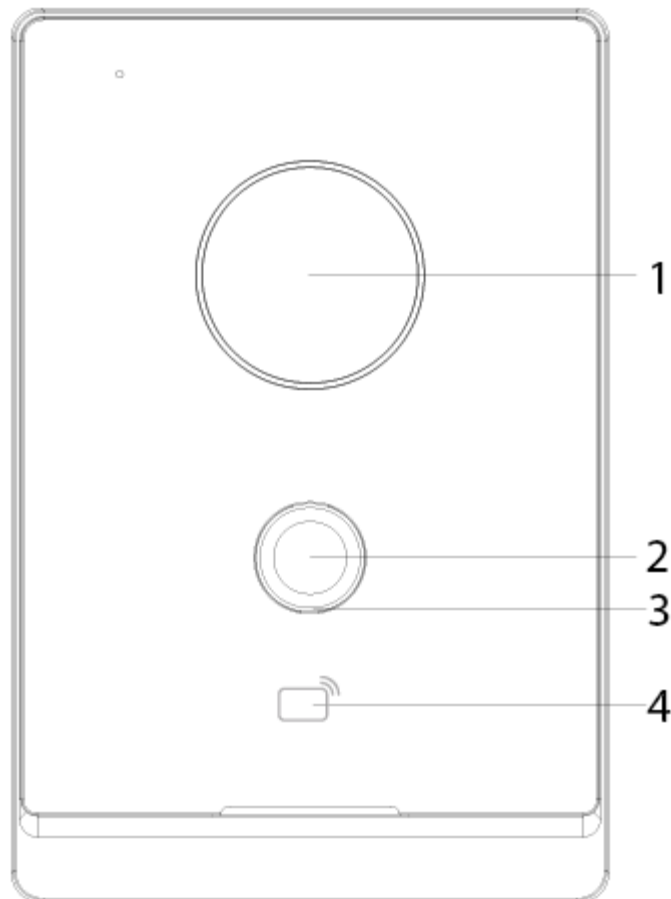


Tabelle 2-14 Beschreibung der Frontplatte

Nr.	Name	Beschreibung
1	Kamera	—
2	Klingelknopf	Zum Anrufen der VTHs oder des Management Center.
3	Anzeige	<ul style="list-style-type: none">● Aus : Das Gerät befindet sich im Bereitschaftsmodus.● Grün leuchtend: Ein Anruf erfolgt.● Leuchtet blau: Anruf erfolgt.● Gelb/grün: Tür entriegelt durch VTH, während die VTO einen Anruf absetzt.● Rot/blau: Tür entriegelt durch VTH, wenn an der VTO ein Anruf erfolgt.● Blau atmend: Netzwerk getrennt.
4	Bereich zum Lesen der Karte	Ziehen Sie die Karte hier durch, um die Tür zu entriegeln (nur bei VTO2211G-P).

2.6.2 Geräterückseite

Abbildung 2-15 Rückplatte von VTO2211G-P/VTO1201G-P

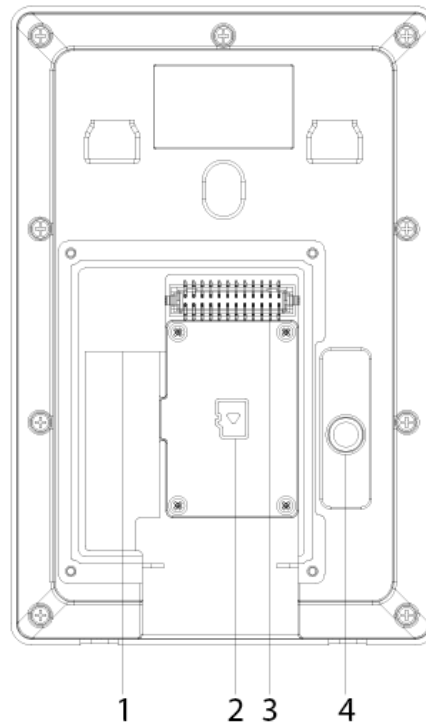
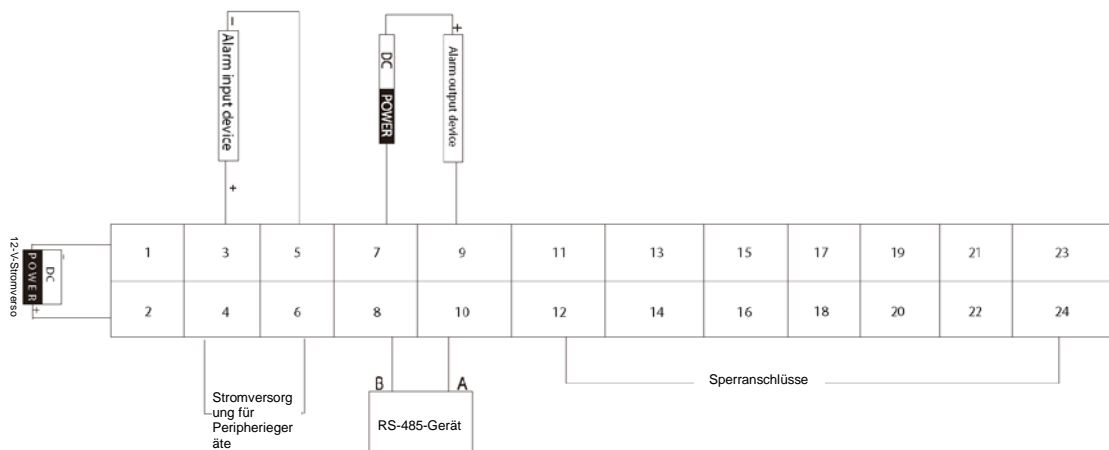


Tabelle 2-15 Beschreibung der Geräterückseite

Nr.	Beschreibung	Nr.	Beschreibung
1	Netzwerkanschluss	3	Ports
2	Abdeckung SD-Karte	4	Sabotagekontakt

Abbildung 2-16 VTO2211G-P-Kabelanschluss



Ports 12, 14, 16, 18, 20, 22 und 24 dienen der Verbindung mit Schlössern.

Tabelle 2-16 Port Beschreibung

Nr.	Name	Nr.	Name
1	DC_IN-	13	Nicht verfügbar
2	DC_IN+	14	DOOR1_COM

Nr.	Name	Nr.	Name
3	ALARM_IN	15	Nicht verfügbar
4	+12-V-AUSGANG	16	DOOR1_NO
5	Erde	17	Nicht verfügbar
6	Erde	18	Erde
7	ALARM_NO	19	Nicht verfügbar
8	RS485B	20	DOOR1_FB
9	ALARM_COM	21	Nicht verfügbar
10	RS485A	22	Erde
11	Nicht verfügbar	23	Nicht verfügbar
12	DOOR1_NC	24	DOOR1_PUSH

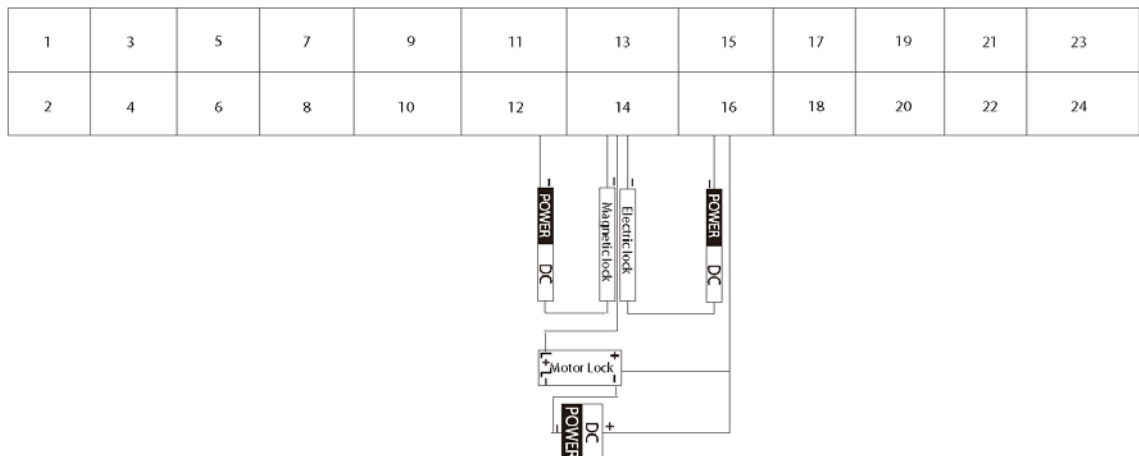
Abbildung 2-17 VTO1201G-P-Kabelanschluss



Tabelle 2-17 Port Beschreibung

Nr.	Name
1	DC_IN-
2	DC_IN+
3-24	Reservierte Funktion

Abbildung 2-18 Schlosskabelanschluss

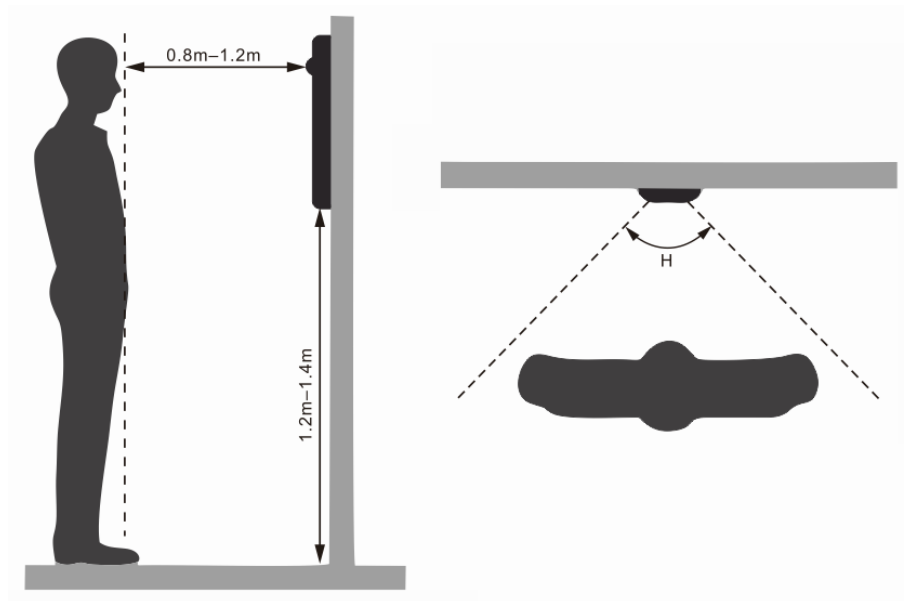


Sie können je nach Bedarf ein magnetisches oder elektrisches Schloss anschließen. Regeln zum Anschließen des Ports entnehmen Sie bitte der obigen Abbildung.

3 Montage

- Installation und Konfiguration müssen von Fachkräften durchgeführt werden. Wenden Sie sich an den technischen Support, falls Sie das Gerät reparieren lassen müssen.
- Die Installationsposition entnehmen Sie bitte der nachstehenden Abbildung. Der horizontale Betrachtungswinkel des Gerätes variiert je nach Modell und das menschliche Gesicht sollte auf die Mitte des Gerätes ausgerichtet sein.

Abbildung 3-1 Installationsverfahren



4 Konfiguration

Dieses Kapitel stellt die grundlegende Konfiguration von VTO- und VTH-Geräten vor. Siehe Benutzerhandbuch für Einzelheiten.



Schnittstellen können je nach Software-Version variieren. Das Menü ist ausschlaggebend.

4.1 Vorgehensweise



Überprüfen Sie jedes Gerät vor der Konfiguration und stellen Sie sicher, dass die Verdrahtung keine Kurzschlüsse oder Unterbrechungen aufweist.

Schritt 1: Planen Sie IP und Nummer (fungiert als Telefonnummer) für jedes Gerät.

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

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

Schritt 4: Prüfen Sie, ob alle Einstellungen stimmen. Siehe „4.4 Inbetriebnahme“.

4.2 Konfigurationswerkzeug

Sie können das Konfigurationswerkzeug „VDPConfig“ herunterladen und zur Konfiguration und Aktualisierung mehrerer Geräte nutzen. Ausführliche Einzelheiten finden Sie im entsprechenden Benutzerhandbuch.

4.3 VTO konfigurieren

Schließen Sie den VTO mit einem Netzkabel an Ihren PC an. Für die erstmalige Verwendung müssen Sie ein neues Anmeldepasswort für die Weboberfläche erstellen.

4.3.1 Initialisierung

Stellen Sie sicher, dass sich der PC im selben Netzwerksegment befindet.

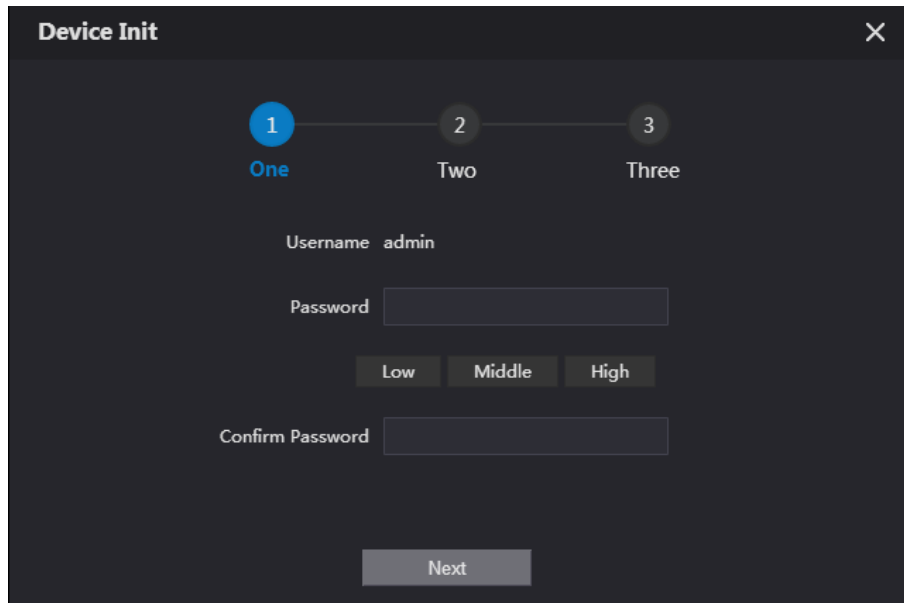
Schritt 1: Schalten Sie die VTO ein.

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 4-1 Initialisierung des Geräts

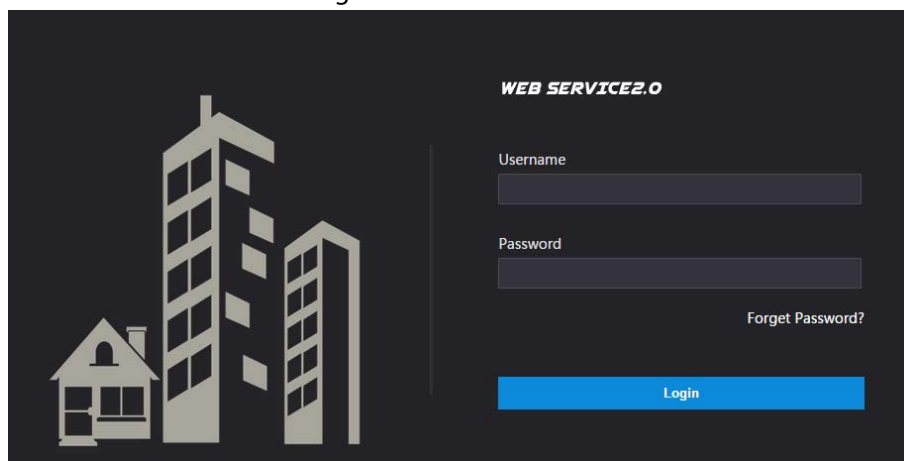


Schritt 3: Geben Sie Ihr neues Passwort ein und bestätigen Sie es. Klicken Sie dann auf **Weiter** (Next).

Schritt 4: Wählen Sie **E-Mail** (Email) und geben Sie die E-Mail-Adresse zur Passwortrücksetzung ein.

Schritt 5: Klicken Sie auf **Weiter** (Next), klicken Sie dann zum Aufrufen des Anmeldefensters auf **OK**.

Abbildung 4-2 Anmeldefenster



4.3.2 VTO-Nummer konfigurieren

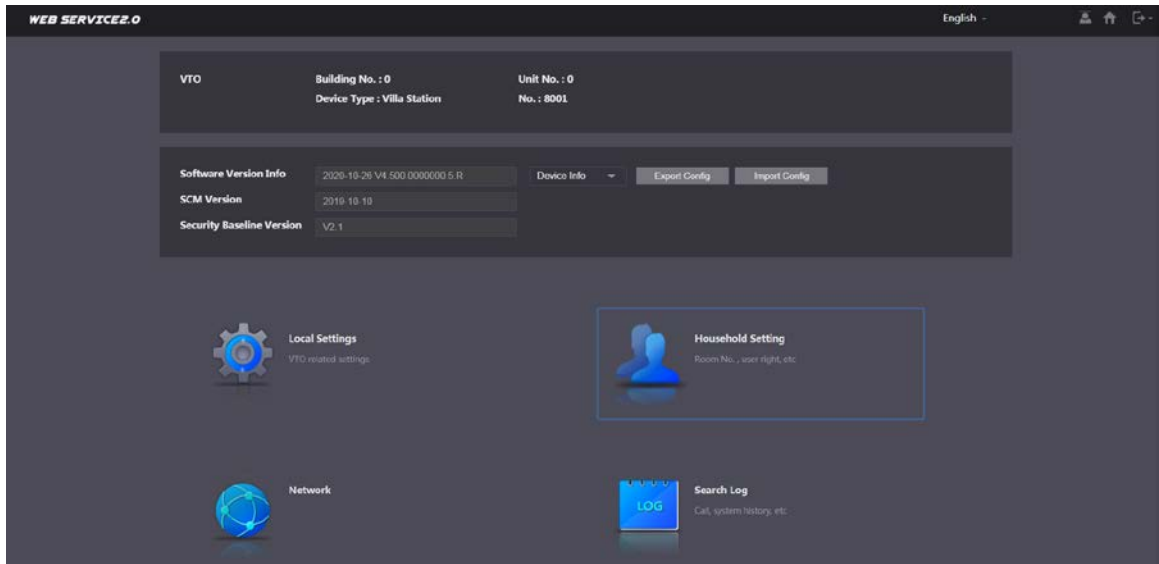
Nummern können zur Unterscheidung der einzelnen VTOs verwendet werden und sollten entsprechend der Einheiten- oder Gebäudennummer eingestellt werden.



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

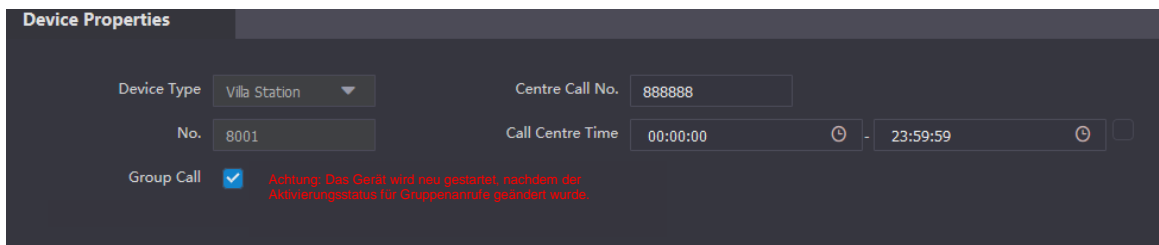
Schritt 1: Melden Sie sich bei der VTO-Weboberfläche an.

Abbildung 4-3 Hauptfenster



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

Abbildung 4-4 Geräteeigenschaften

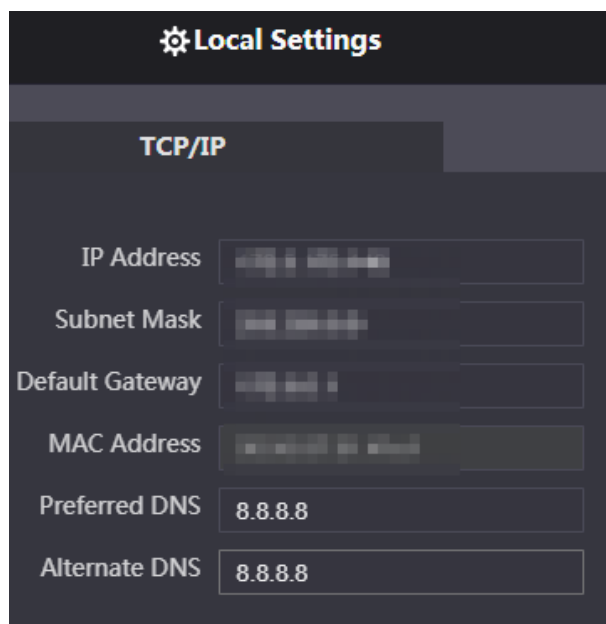


Schritt 3 Geben Sie die Nummer unter **Nr.** (No.), klicken Sie dann auf **Bestätigen** (Confirm).

4.3.3 Netzwerkparameter konfigurieren

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

Abbildung 4-5 TCP/IP-Informationen



Schritt 2: Geben Sie die jeweiligen Parameter ein, klicken Sie dann auf **Speichern** (Save).

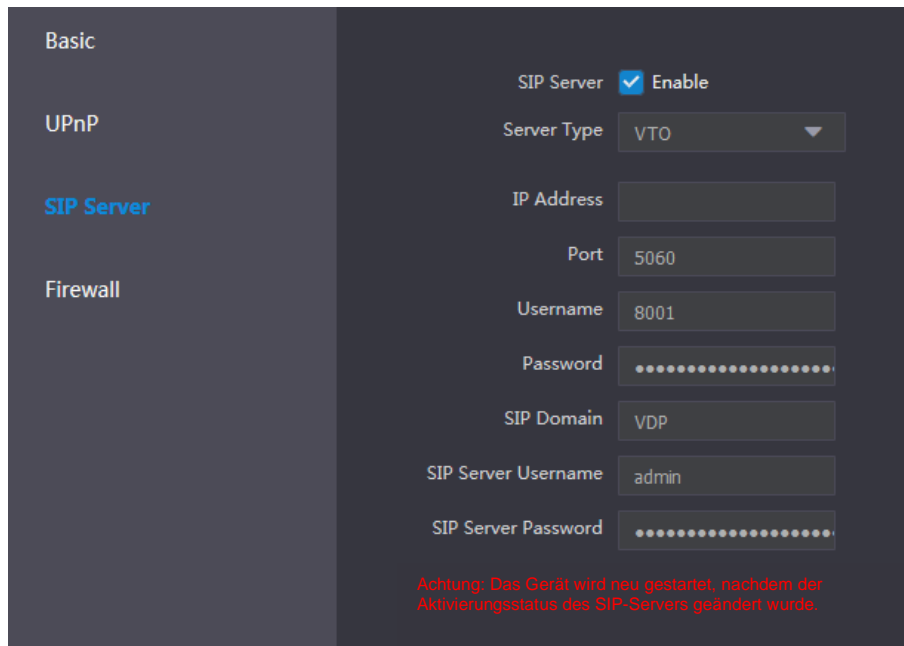
Die VTO startet automatisch neu. Sie müssen beim erneuten Anmelden die IP-Adresse Ihres PCs demselben Netzwerksegment hinzufügen wie die VTO.

4.3.4 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.

Schritt 1: Wählen Sie **Netzwerk > SIP-Server** (Network > SIP Server).

Abbildung 4-6 SIP-Server



Schritt 2: Wählen Sie den Server-Typ wie erforderlich.

- Falls die aktuelle VTO als SIP-Server fungiert, aktivieren Sie **SIP-Server** (SIP Server) und klicken Sie dann auf **Speichern** (Save).

Die VTO startet automatisch neu, anschließend können Sie dieser VTO weitere VTOs und VTHs hinzufügen. Siehe „4.3.6 VTOs hinzufügen und 4.3.7 Zimmernummer hinzufügen“.



Falls die aktuelle VTO nicht als SIP-Server fungiert, aktivieren Sie **SIP-Server** (SIP Server) nicht. Andernfalls schlägt die Verbindung mit dieser VTO fehl.

- Falls andere VTOs als SIP-Server fungieren, stellen Sie **Server-Typ** (Server Type) auf VTO ein, konfigurieren Sie dann die Parameter.

Tabelle 4-1 SIP-Serverkonfiguration

Parameter	Beschreibung
IP-Adr.	Die IP-Adresse der VTO, die als SIP-Server fungiert.
Port	<ul style="list-style-type: none"> 5060 ist der Standard, wenn VTO als SIP-Server fungiert. 5080 ist der Standard, wenn die Plattform als SIP-Server fungiert.
Benutzername	Behalten Sie den Standardwert bei.
Passwort	
SIP-Domäne	VDP.
SIP-Server-Benutzername	Benutzername und Passwort zur Anmeldung an der Weboberfläche des VTO-Servers.
SIP-Server-Passwort	

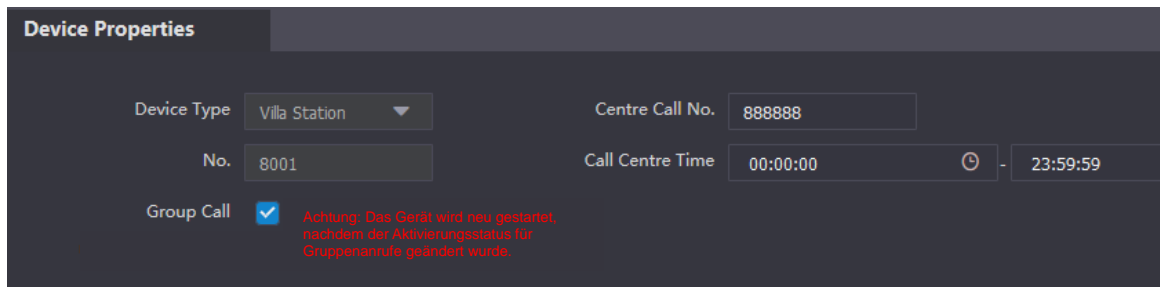
- Falls andere Server als SIP-Server fungieren, stellen Sie **Server-Typ** (Server Type) wie erforderlich ein. Beachten Sie dann die entsprechende Anleitung für weitere Einzelheiten.

4.3.5 Rufnummer und Gruppenruf konfigurieren

Zum Anwählen oder Anrufen einer VTO müssen Sie die Rufnummer jeder VTO, die als Telefonnummer fungiert, konfigurieren.

Schritt 1: Wählen Sie **Lokale Einstellungen > Grundlegend** (Local Settings > Basic).

Abbildung 4-7 Geräteeigenschaften



Schritt 2: Geben Sie im Eingabefeld **Nr.** (No.) die Zimmernummer ein, die Sie anrufen müssen und klicken Sie zum Speichern auf **Bestätigen** (Confirm). Wiederholen Sie diesen Vorgang an der Weboberfläche jeder Türstation für Einfamilienhäusern (VTO).

Am SIP-Server können Sie die Gruppenruf-Funktion aktivieren. Beim Anrufen einer Haupt-VTH empfangen auch alle Erweiterungs-VTHs den Anruf.



Die VTO startet nach Aktivierung oder Deaktivieren der Gruppenanruf-Funktion neu.

Schritt 3: Melden Sie sich an der Weboberfläche des SIP-Servers an und wählen Sie dann **Lokale Einstellungen > Grundlegend** (Local Settings > Basic).

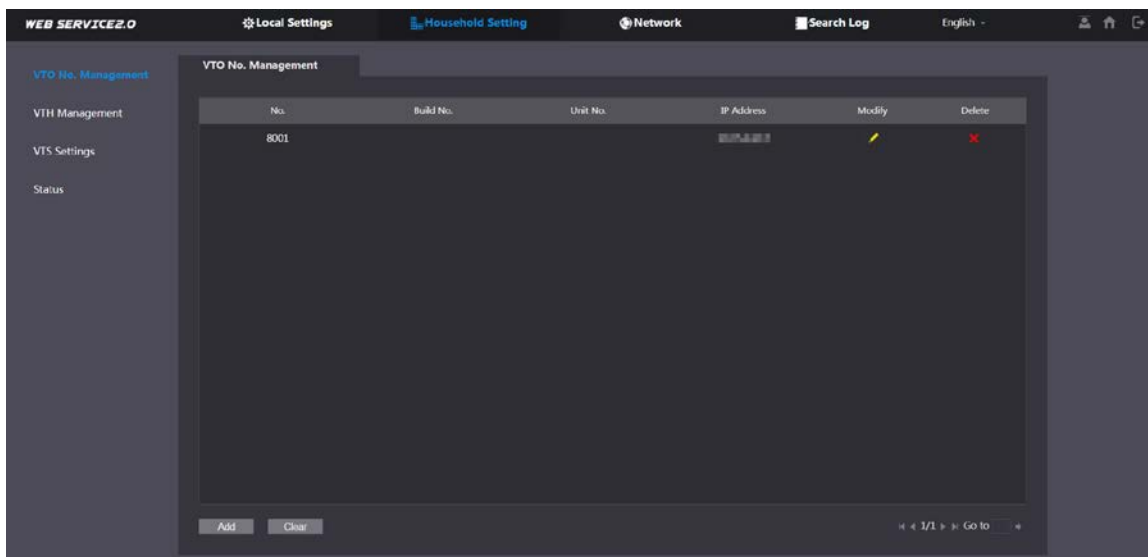
Schritt 4: Aktivieren Sie **Gruppenanruf** (Group Call) und klicken Sie auf **Bestätigen** (Confirm). Anschließend startet die VTO neu.

4.3.6 VTOs hinzufügen

Sie können dem SIP-Server VTOs hinzufügen und alle mit demselben SIP-Server verbundenen VTOs können Videoanrufe untereinander durchführen. Dieser Abschnitt bezieht sich auf den Zustand, in dem ein VTO 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 4-8 VTO-Nr.-Verwaltung



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

Abbildung 4-9 VTO hinzufügen

Schritt 3: Konfigurieren Sie die Parameter.



Der SIP-Server muss hinzugefügt werden.

Tabelle 4-2 Türstationen (VTO) hinzufügen

Parameter	Beschreibung
Datensatznr.	VTO-Nummer. Siehe „4.3.2 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).

4.3.7 Zimmernummer hinzufügen

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



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

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

Abbildung 4-10 Zimmernummernverwaltung


Room No.	First Name	Last Name	Nick Name	Registration Mode	Modify
9901#0				public	
9901#1				public	
9901#2				public	
9901#3				public	
9901#4				public	
9901#5				public	
9901#6				public	
9901#7				public	
9901#8				public	
9901#9				public	

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



Abbildung 4-11 Eine einzelne Zimmernummer hinzufügen

Schritt 3: Zimmerdaten konfigurieren.

Tabelle 4-3 Zimmerdaten

Parameter	Beschreibung
Vorname	Informationen zur Differenzierung einzelner Zimmer.
Nachname	
Spitzname	
Zimmernr.	Zimmernummer.  <ul style="list-style-type: none"> • Wenn mehrere VTHs vorhanden sind, sollte die Zimmernummer für die Haupt-VTH mit #0 enden und die Zimmernummern für Erweiterungs-VTHs mit #1, #2 usw. • Sie können bis zu 9 Erweiterungs-VTHs für einen Haupt-VTH konfigurieren.
Registrierungsmodus	Wählen Sie öffentlich (public).
Registriertes Passwort	Behalten Sie den Standardwert bei.

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

Klicken Sie auf , um die Zimmerdaten zu ändern und klicken Sie auf , um das Zimmer zu löschen.

4.4 Inbetriebnahme

4.4.1 VTO ruft VTH an

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


Schritt 2: Tippen Sie auf  an der VTH, um den Anruf anzunehmen.

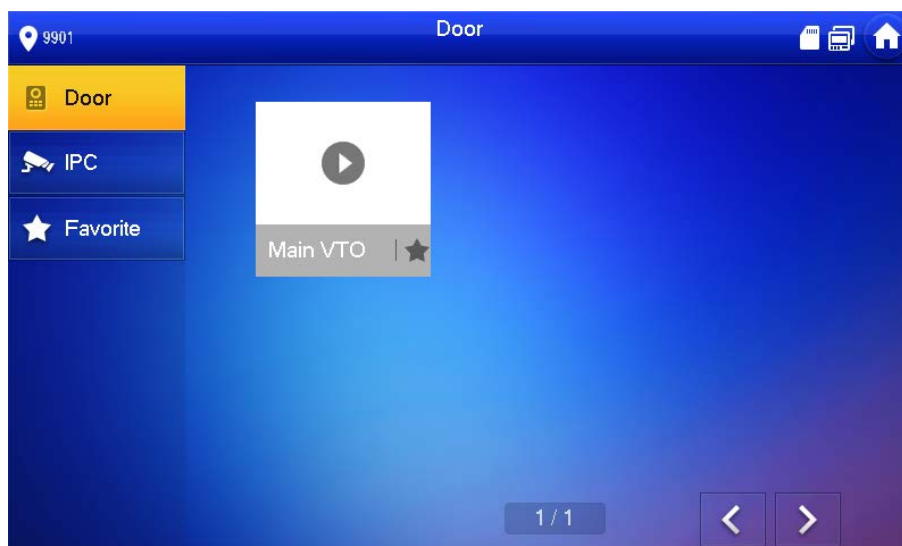
Abbildung 4-12 Anrufbildschirm



4.4.2 VTH überwacht VTO

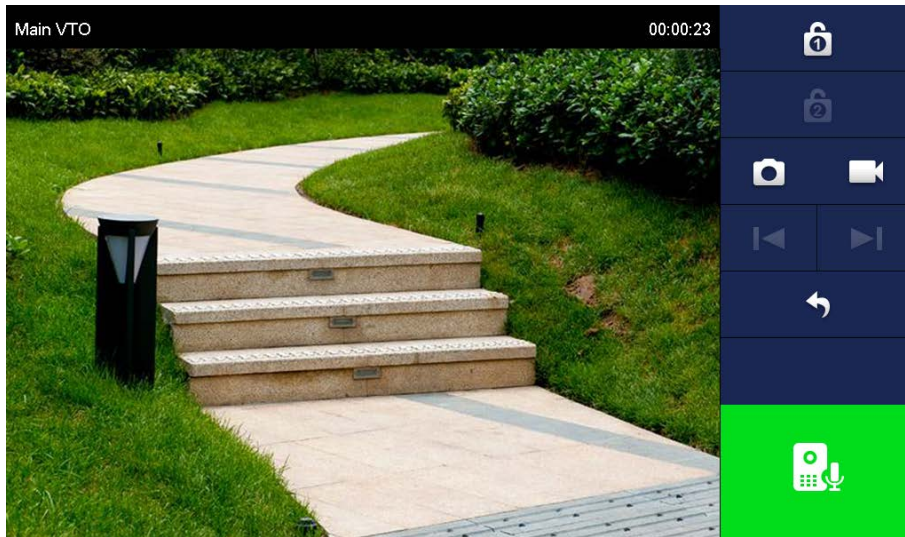
Schritt 1: Wählen Sie auf der Hauptoberfläche des VTH **Monitor > Tür** (Monitor > Door) aus.

Abbildung 4-13 Tür



Schritt 2: Wählen Sie eine VTO.

Abbildung 4-14 Video überwachen




5 App installieren und Gerät hinzufügen

Mit der DMSS-App können Sie Geräte verwalten, Videos wiedergeben, Türen entriegeln und mehr.


Bevor Sie DMSS die VTO hinzufügen, müssen Sie die VTO per WLAN mit dem Router verbinden oder die VTO über einen Switch mit dem Router verbinden und dann manuell die IP-Adresse der VTO so ändern, dass sie sich in demselben Netzwerk wie der Router befindet, falls DHCP nicht unterstützt wird.

Schritt 1: Suchen Sie im App Store nach „DMSS“ und installieren Sie es.

Schritt 2: Tippen Sie an Ihrem Smartphone auf , und befolgen Sie dann die Bildschirmanweisungen, bis das Fenster zur Auswahl der Region angezeigt wird.

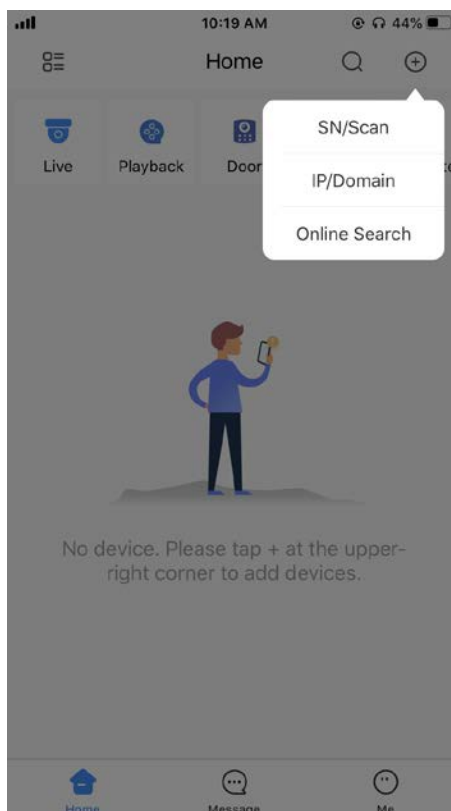
Schritt 3: Wählen Sie einen Region.

Schritt 4: Tippen Sie oben rechts im Fenster auf **Fertig** (Done).

Schritt 5: Tippen Sie links oben auf .

Schritt 6: Tippen Sie auf .

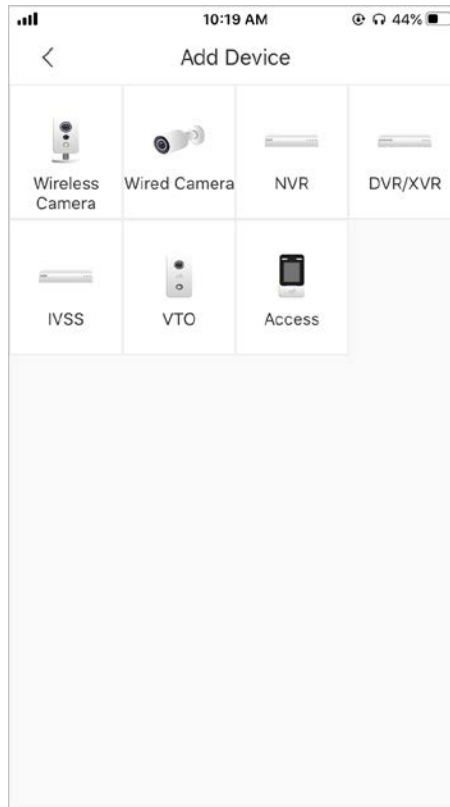
Abbildung 5-1 Ausgangsstellung



5.1 Durch Kabelnetzwerk hinzufügen (wird nur von Modell mit Station für Einfamilienhaus unterstützt)

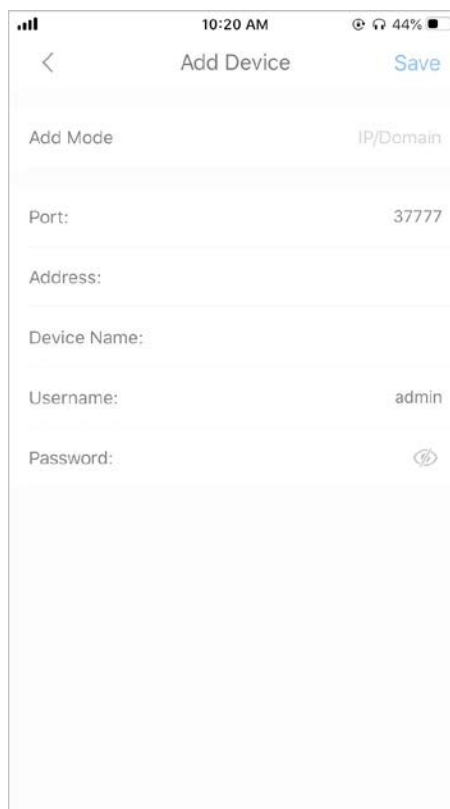
Schritt 1: Tippen Sie auf **IP/Domäne** (IP/Domain). Siehe Abbildung 5-1 .

Abbildung 5-2 Gerät hinzufügen



Schritt 2: Tippen Sie auf **VTO**.

Abbildung 5-3 Gerät hinzufügen



Schritt 1: Geben Sie die Parameter ein.

Schritt 2: Tippen Sie auf **Speichern** (Save).

Das VTO-Gerät wird hinzugefügt. Nun können Sie Videos von der VTO betrachten, die VTO anrufen, Türen während Anrufen entriegeln und mehr.

Abbildung 5-4 Tür



5.2 Durch Soft-Zugangspunkt hinzufügen (wird nur von Modell mit Station für Einfamilienhaus unterstützt)

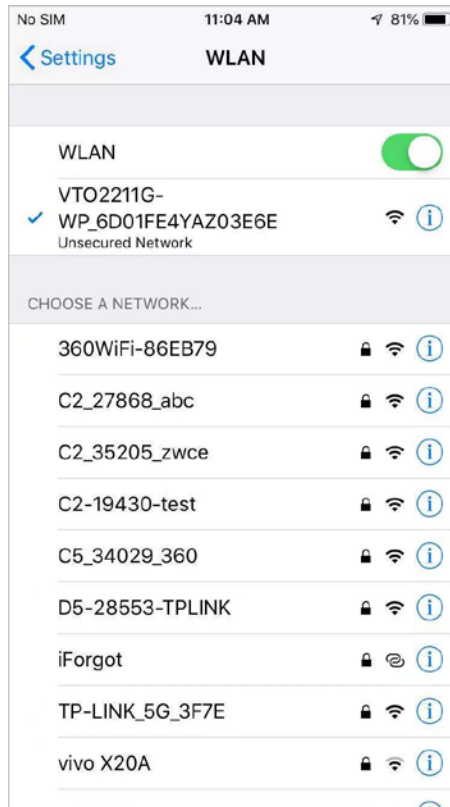
Schritt 1: Schalten Sie die VTO ein.

Schritt 2: Rufen Sie das Fenster **WLAN** an Ihrem Smartphone auf.

Schritt 3: Halten Sie die Ruftaste an der VTO länger als 5 Sekunden gedrückt, bis Sie einen Signalton hören.

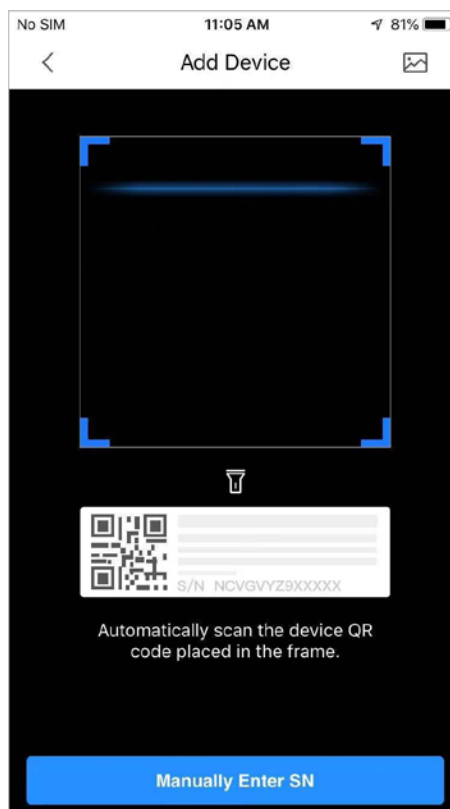
Schritt 4: Verbinden Sie Ihr Smartphone mit dem Netzwerk namens **VTO2211G-WP_6D01FE...** (Seriennummer der VTO).

Abbildung 5-5 Smartphone-WLAN



Schritt 5: Tippen Sie im Fenster **Startseite** (Home) auf **SN/Scan**.

Abbildung 5-6 Scannen Sie den QR-Code



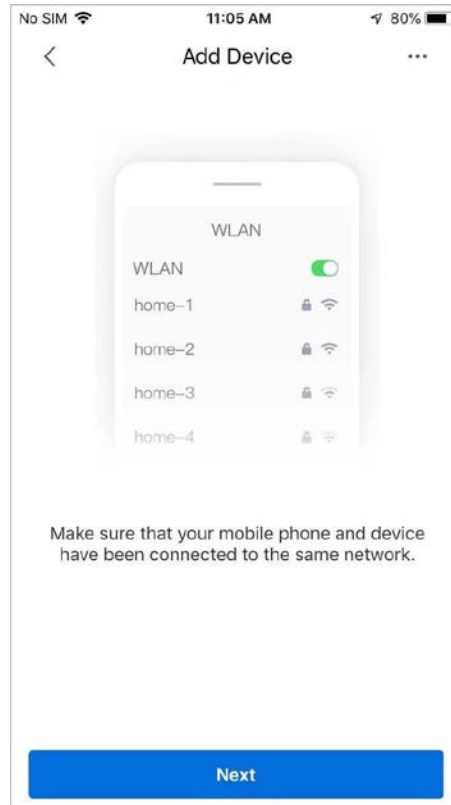
Schritt 6: Scannen Sie den QR-Code an der rückseitigen Abdeckung der VTO.



Der QR-Code kann auch unter **Netzwerk > Grundlegend > P2P** (Network > Basic > P2P) auf der Weboberfläche gefunden werden.

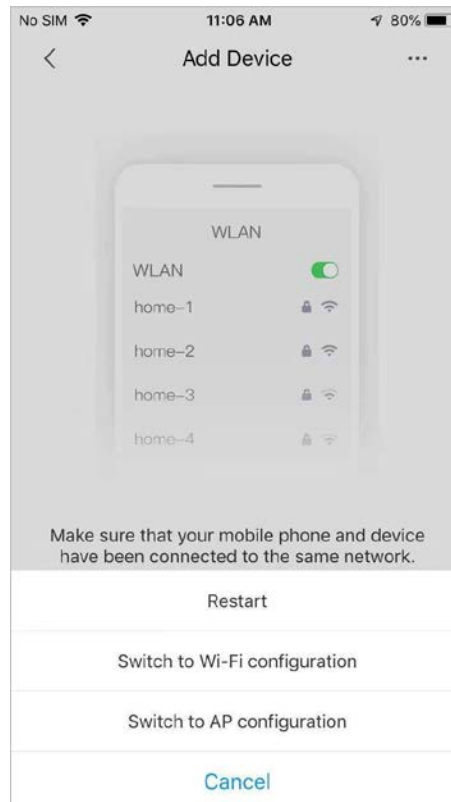
Schritt 7: Tippen Sie auf **Weiter** (Next).

Abbildung 5-7 Gerät hinzufügen



Schritt 8: Tippen Sie rechts oben auf **...**

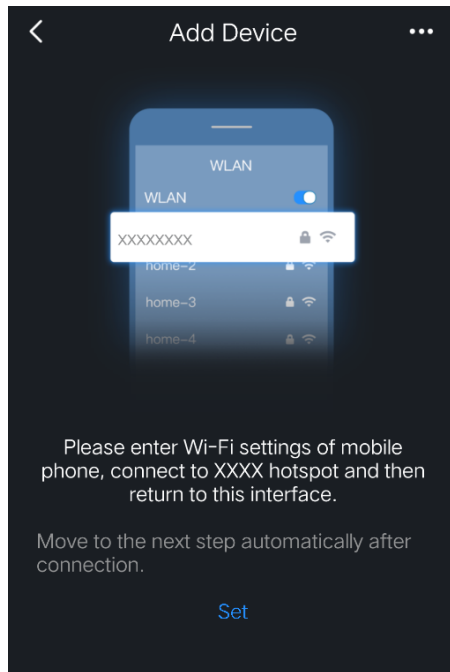
Abbildung 5-8 Wählen Sie einen Netzwerkkonfigurationsmodus



Schritt 9: Wählen Sie **Auf AP-Konfiguration umschalten** (Switch to AP configuration).

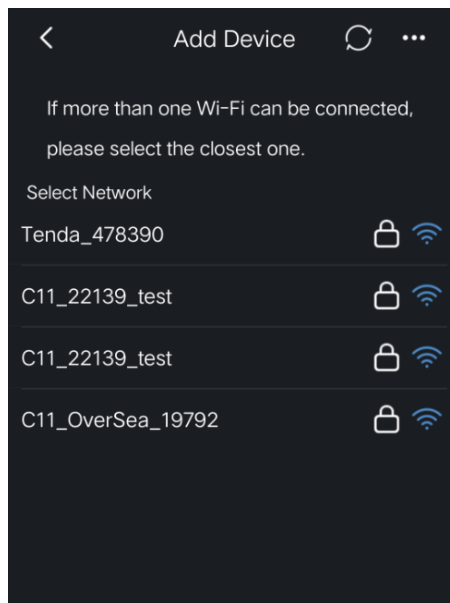
Schritt 10: Tippen Sie auf **Weiter > Einstellen** (Next > Set).

Abbildung 5-9 Stellen Sie das Telefonnetzwerk ein



Schritt 11: Tippen Sie auf einen WLAN-Namen.

Abbildung 5-10 Wählen Sie ein WLAN



Schritt 12: Geben Sie das WLAN-Passwort ein.

Schritt 13: Tippen Sie auf **Weiter** (Next).

Abbildung 5-11 Gerät hinzufügen

The screenshot displays the 'Add Device' interface. At the top, there is a navigation bar with a back arrow, the title 'Add Device', and a 'Save' button. Below this, the 'Add Mode' is set to 'P2P'. The 'SN' field contains the value '8D01F541A28388E'. The 'Device Name' field is empty. The 'Username' field is set to 'admin'. A warning message at the bottom reads: 'Wrong username or password will result in failure to add.' with a 'View Reasons' link. The top status bar shows 'No SIM', '11:10 AM', and '79%' battery.

Schritt 14: Geben Sie den Gerätenamen und das Gerätepasswort (Passwort zur Anmeldung an der VTO-Weboberfläche) ein.

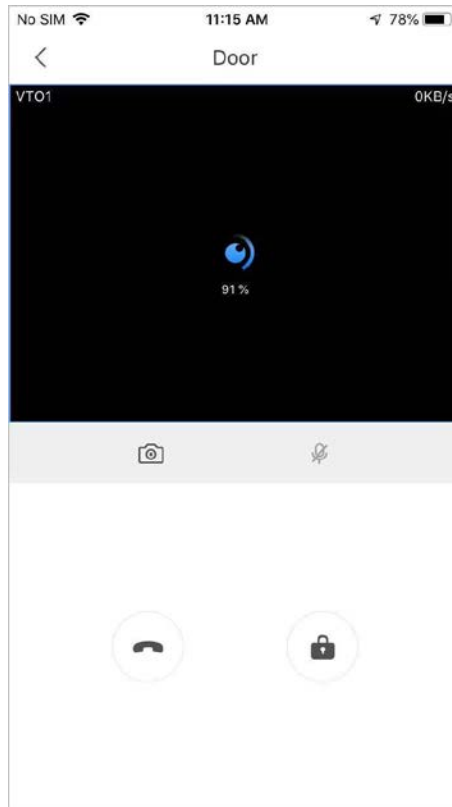
Schritt 15: Tippen Sie auf .

Die Türstation (VTO) wird hinzugefügt. Nun können Sie Videos von der VTO betrachten, die VTO anrufen, Türen während Anrufen entriegeln und mehr.



Nach dem Hinzufügen von VTOs zur Anwendung müssen Sie Nachrichten abonnieren, damit Push-Benachrichtigungen an Ihr Smartphone gesendet werden können.

Abbildung 5-12 Tür



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 Reset 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.