Digitaler VTH

Kurzanleitung

V1.0.0

Vorwort

Allgemein

Dieses Dokument stellt hauptsächlich Aufbau, Installation und Konfiguration des Produkts 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.	August 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 an einem stabilen, ebenen Ort, damit es nicht herunterfallen kann.
- Lassen Sie keine Flüssigkeiten auf das Gerät tropfen oder spritzen und stellen Sie keine mit Flüssigkeiten gefüllten Gegenstände 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.
- Das Gerät muss mit geschirmtem Netzwerkkabel betrieben werden.

Stromanforderungen

- Das Gerät muss mit den für diesen Bereich empfohlenen elektrischen Leitungen (Stromkabeln) betrieben werden, die innerhalb ihrer Nennspezifikation verwendet werden müssen.
- 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 entnehmen Sie den Geräteetiketten.
- Der Gerätestecker dient als Trennvorrichtung. Der Stecker muss während des Betriebs jederzeit frei zugänglich sein.

Gerät aktualisieren

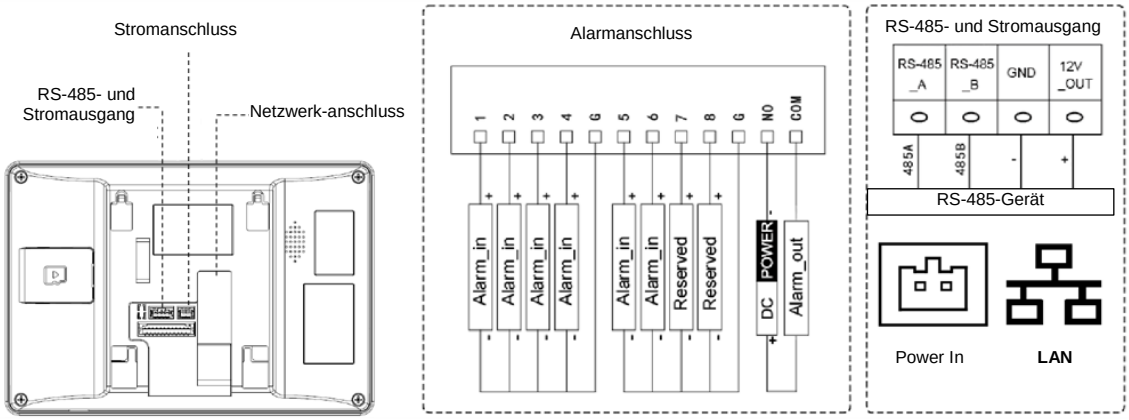
Unterbrechen Sie die Stromversorgung nicht während einer Geräteaktualisierung. Die Stromversorgung darf erst dann unterbrochen werden, wenn das Gerät die Aktualisierung abgeschlossen hat und neu gestartet wurde.

Inhaltsverzeichnis

1 Anschluss auf der Rückseite

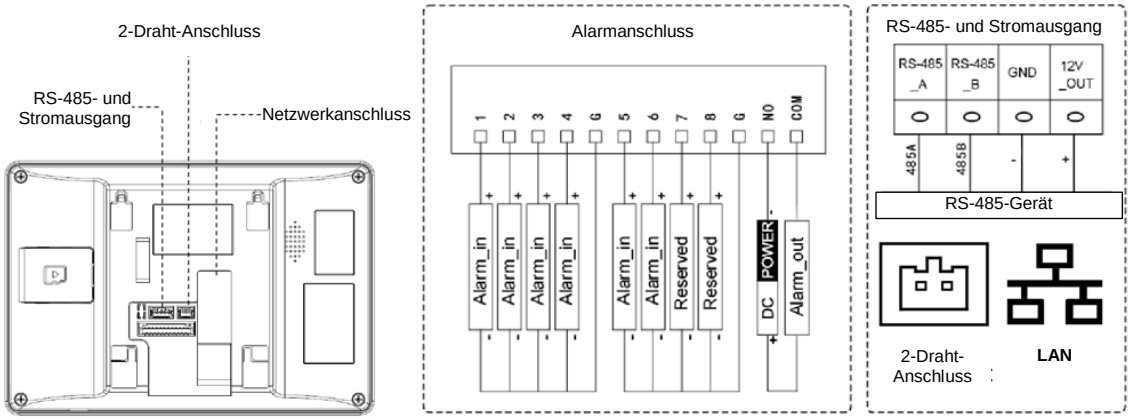
1.1 VTH5421H

Abbildung 1-1 Rückwand VTH5421H



1.2 VTH5422H

Abbildung 1-2 Rückwand VTH5422H



2 Installation und Inbetriebnahme

2.1 Montage

⚠

- Installieren Sie den VTH nicht in widriger Umgebung mit Kondensation, hohen Temperaturen, Staub, korrosiven Substanzen und direkter Sonneneinstrahlung.
- Im Fall einer Störung nach dem Einschalten ziehen Sie sofort das Netzwerkkabel ab und unterbrechen Sie die Stromzufuhr. Schalten Sie das Gerät nach der Fehlerbehebung ein.
- Installation und Fehlersuche müssen durch Fachkräfte durchgeführt werden. Nehmen Sie das Gerät nicht selbst auseinander oder reparieren Sie das Gerät im Fall eines Defekts nicht selbst. Wenden Sie sich an den Kundendienst.
- Die Höhe des Gerätemittelpunkts sollte 1,4 m - 1,6 m über den Boden (OKFF) liegen (das Gerät ist nur für die Montage in einer Höhe ≤ 2 m geeignet).

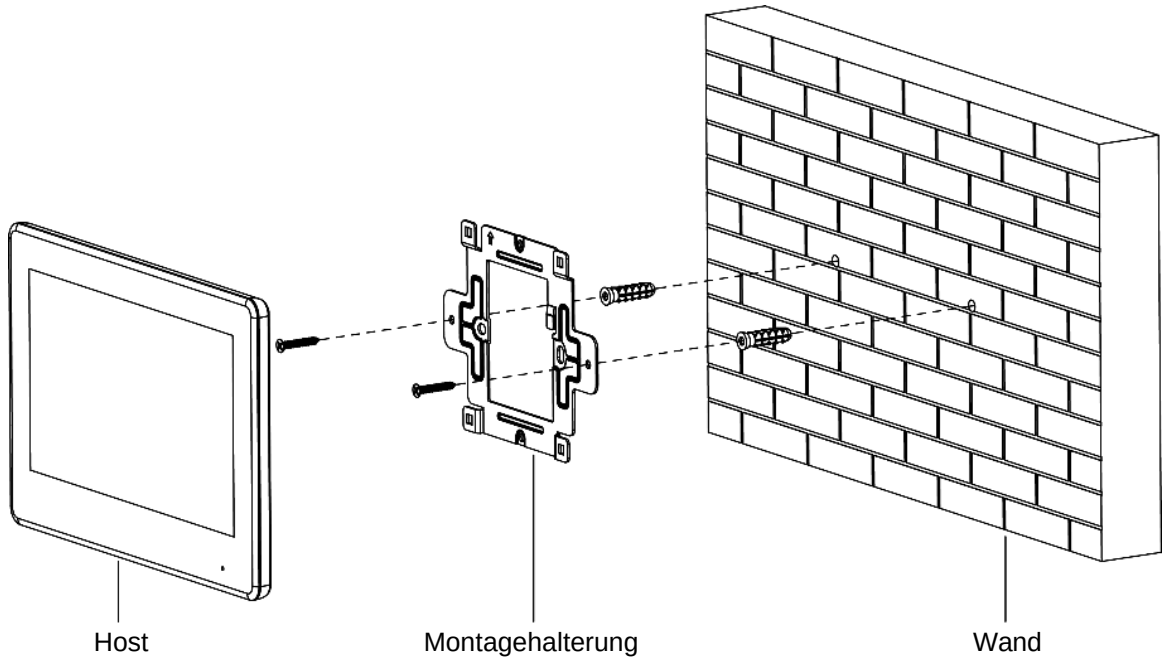
Montieren Sie das Gerät mit einer Halterung direkt an einer Wand, die für alle Gerätetypen geeignet ist.

Schritt 1: Bohren Sie Löcher in die Wand entsprechend der Lochpositionen des Montagewinkels.

Schritt 2: Befestigen Sie den Montagewinkel mit Schrauben an der Wand.

Schritt 3: Setzen Sie das Gerät von oben nach unten in die Montagehalterung ein.

Abbildung 2-1 Aufputzinstallation



2.2 Vorbereitung

Prüfen Sie vor der Inbetriebnahme, ob die folgenden Arbeiten abgeschlossen sind.

- Schalten Sie das Gerät nur ein, wenn kein Kurzschluss und keine Unterbrechung vorliegt.
- Planen Sie IP und Nummer (funktioniert wie eine Telefonnummer) für jede VTO und jeden VTH.

- Bestätigen Sie den Standort des SIP-Servers.
- Scannen Sie den QR-Code auf dem Gehäuse für Details.
- Stellen Sie die VTO- und VTH-Informationen auf der Web-Oberfläche für jede VTO ein und stellen Sie VTH-Informationen, Netzwerk-Informationen und VTO-Informationen an jedem VTH ein.

VTH-Einstellungen

Bei erstmaliger Verwendung muss ein Passwort eingerichtet und eine E-Mail verknüpft werden. Das Passwort dient dazu, den Bildschirm zur Projekteinstellung aufzurufen, während die E-Mail-Adresse dazu dient, Ihr Passwort abzurufen, wenn Sie es vergessen haben.

Schritt 1: Schalten Sie das Gerät ein, wählen Sie Region und Sprache, und tippen Sie auf **OK.**

Abbildung 2-2 Region und Sprache wählen

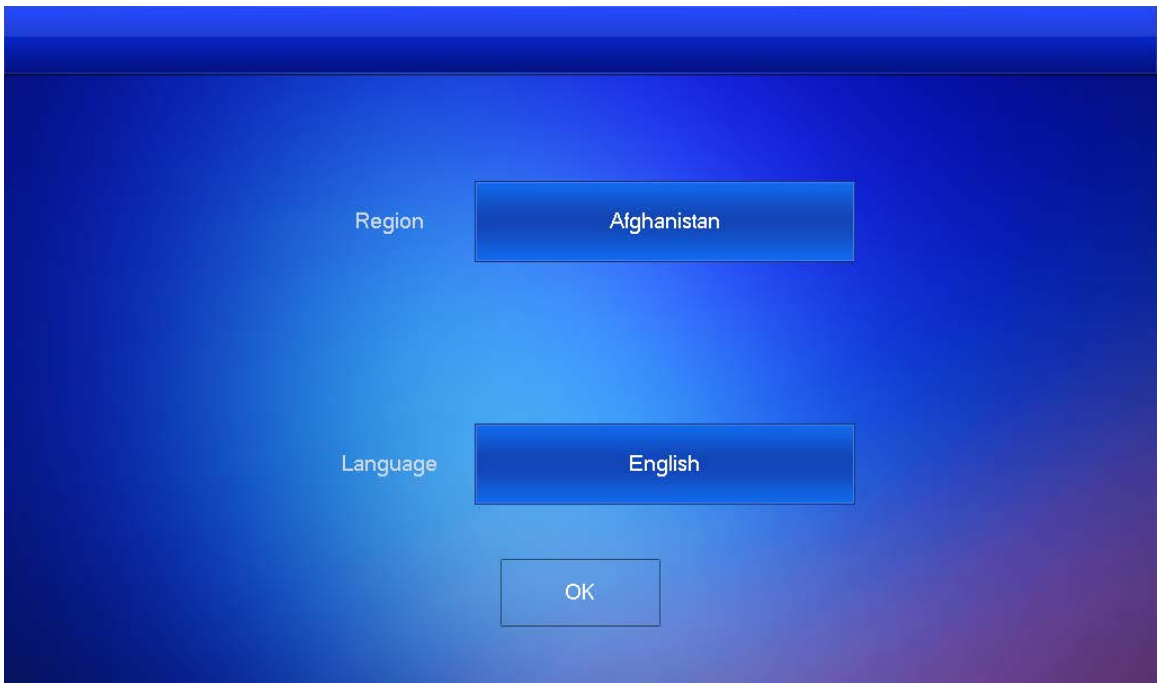


Abbildung 2-3 Passwort für VTH einstellen

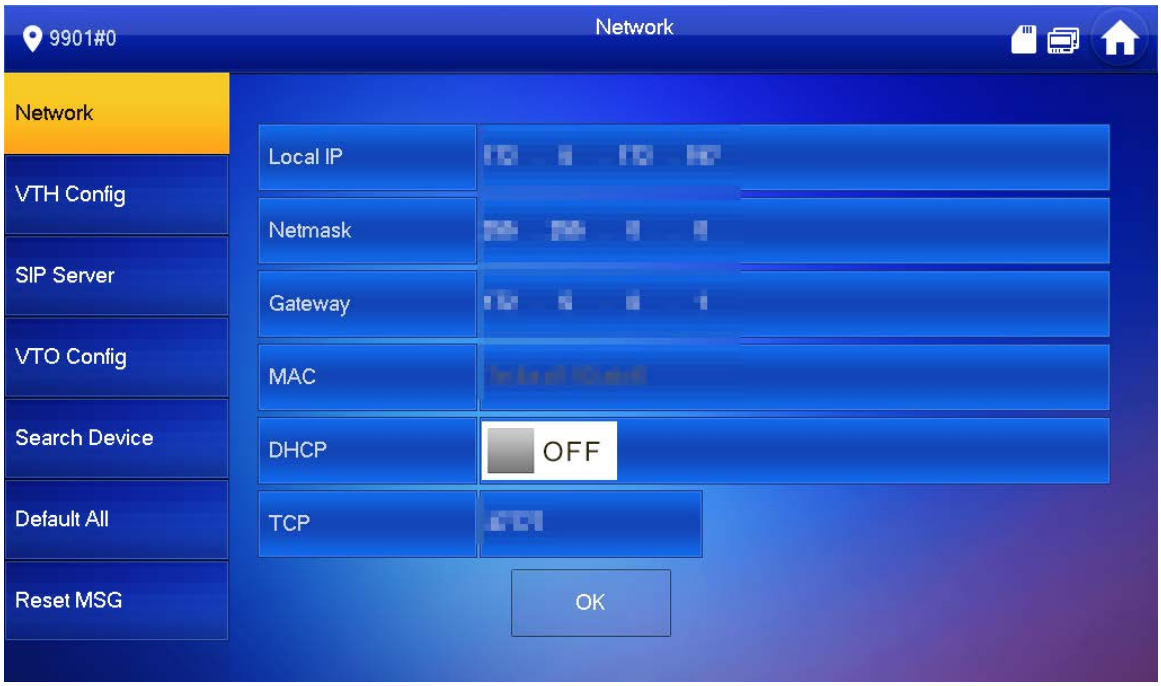
Schritt 2: Geben Sie das Passwort ein und bestätigen Sie es, geben Sie die E-Mail ein, und tippen Sie auf **Weiter** (Next).

Schritt 3: Halten Sie auf **Einstellung** (Setting) für mehr als 6 Sekunden gedrückt, geben Sie das gerade eingestellt Passwort ein und tippen Sie auf **OK.**

Schritt 4: Tippen Sie auf **Netzwerk** (Network). Geben Sie lokale IP, Netzmaske und Gateway ein und tippen Sie dann auf **OK** oder tippen Sie auf OFF, um die DHCP-Funktion zu aktivieren, um IP-Daten automatisch zu beziehen.

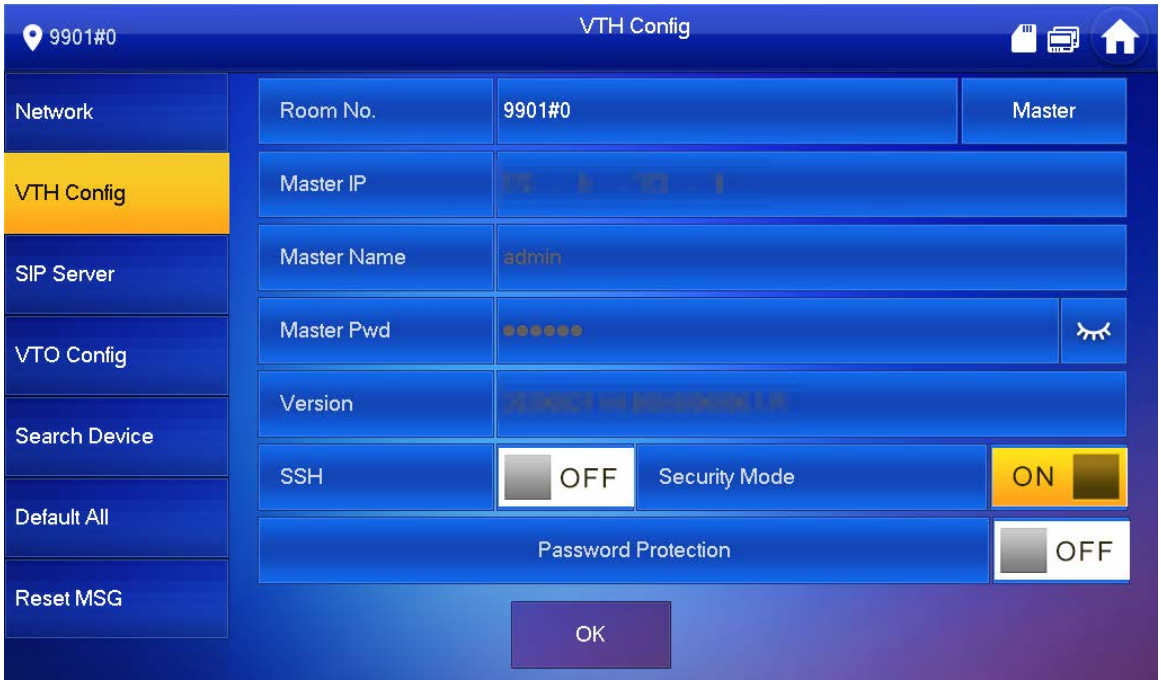
Die IP-Adressen von VTH und VTO müssen sich im gleichen Netzwerksegment befinden. Anderenfalls kann der VTH nach der Konfiguration keine Daten von der VTO erhalten.

Abbildung 2-4 Netzwerk



Schritt 5: Tippen Sie auf VTH-Konfiguration (VTH Config).

Abbildung 2-5 VTH-Konfiguration



- Als Haupt-VTH verwenden.

Geben Sie die Zimmernummer ein (z. B. 9901 oder 101#0) und tippen Sie auf **OK.**

Die Zimmernummer muss mit der VTH-Kurznummer übereinstimmen, die beim Hinzufügen des VTH auf der Web-Oberfläche eingestellt wurde. Sonst kann er keine Verbindung zum VTO herstellen.

Wenn es einen Nebenstellen-VTH gibt, muss die Zimmernummer mit #0 enden. Sonst kann er keine Verbindung zum VTO herstellen.

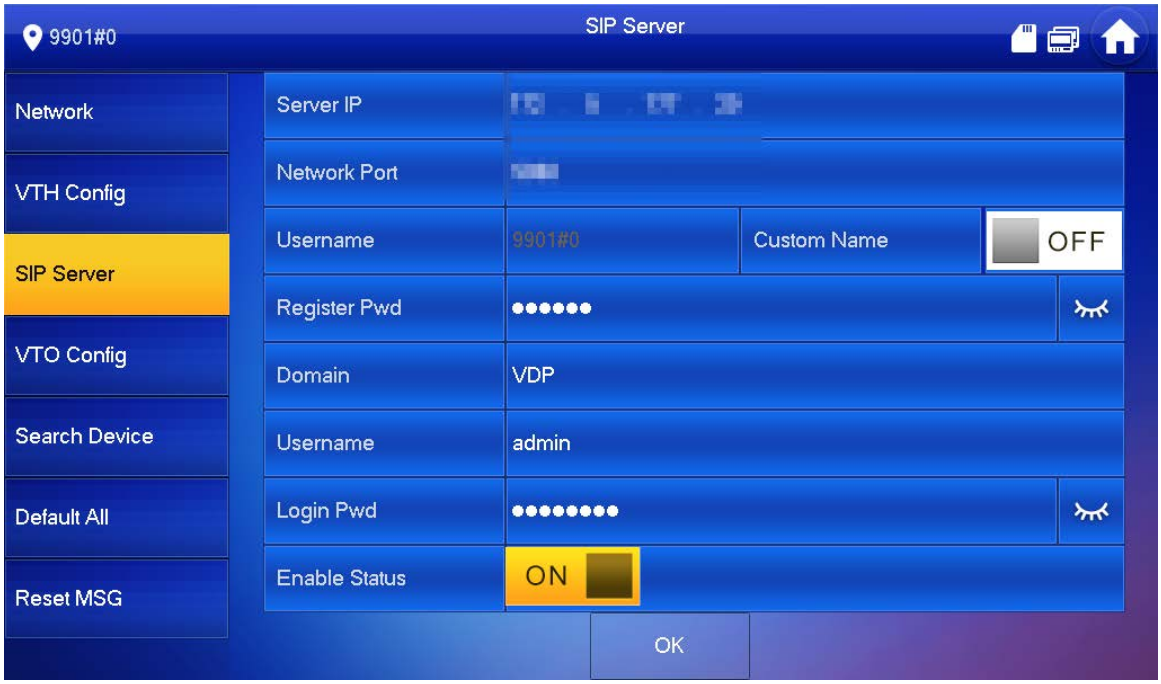
- Als Nebenstellen-VTH verwenden.

1) Tippen Sie auf **Haupt** (Master), damit wechselt das Symbol zu **Nebenstelle** (Extension).
2) Geben Sie die Zimmernummer (z. B. 101#1) und die IP-Adresse des Haupt-VTH ein. Haupt-Name und Haupt-Passwort sind der Benutzername und das Passwort des Haupt-VTH. Der Standard-Benutzername lautet **admin** und das Passwort wurde im vorherigen Schritt eingestellt.

   Sicherheitsmodus ist standardmäßig **An** (On) und Sie können den Standardstatus beibehalten.
3) Tippen Sie auf **OK**, um die Einstellungen zu speichern.

Schritt 6: Tippen Sie auf **SIP-Server** (SIP Server).

Abbildung 2-6 SIP-Server



1) Legen Sie die Einstellungen des **SIP-Servers** (SIP Server) gemäß Tabelle 2-1 fest.

Tabelle 2-1 SIP-Server

Parameter	**Beschreibung**
Server-IP	• Wenn die Plattform als SIP-Server fungiert, ist die Server-IP die IP-Adresse der Plattform. • Wenn der VTO als SIP-Server fungiert, ist die Server-IP die IP-Adresse des VTO.
Netzwerkanschluss	• Wenn die Plattform als SIP-Server fungiert, ist der Netzwerk-Port 5080. • Wenn der VTO als SIP-Server fungiert, ist der Netzwerk-Port 5060.
Benutzername PW registrieren	Standardwert verwenden.
Domäne	Registrierungsdomäne des SIP-Servers, die leer sein kann. Wenn der VTO als SIP-Server fungiert, muss die Registrierungsdomäne des SIP-Servers VDP sein.
Benutzername Anmelde-PW	Benutzername und Passwort zum Anmelden am SIP-Server.

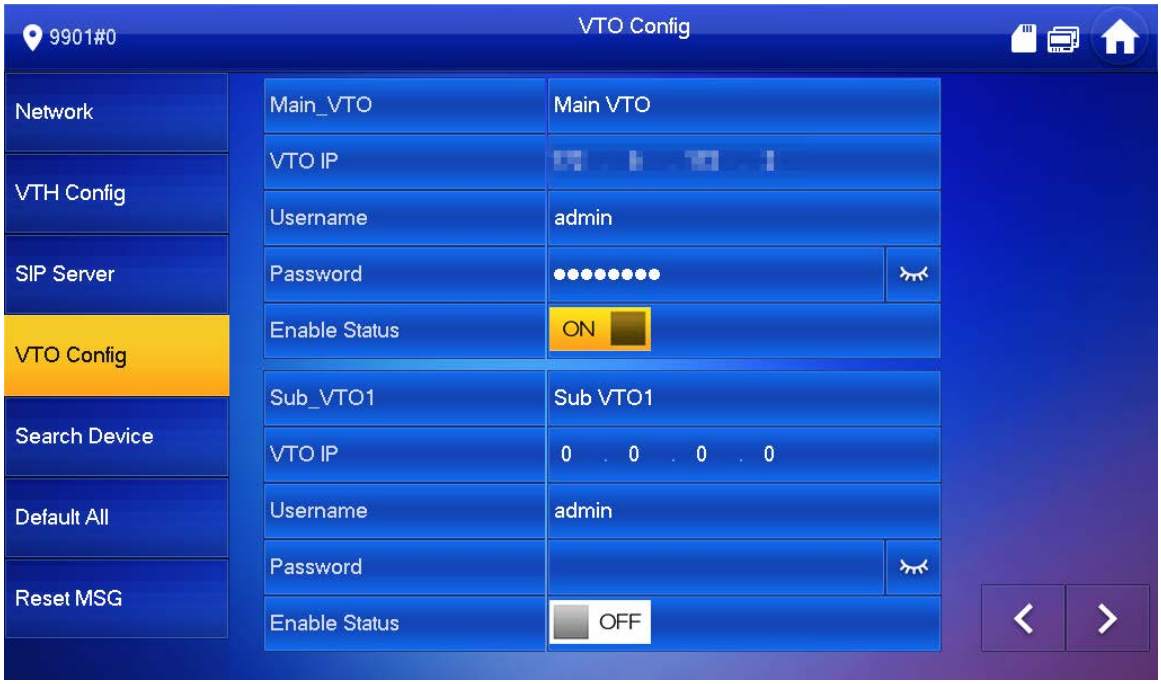
2) Stellen Sie **Status aktivieren** (Enable Status) auf 

ein.

3) Tippen Sie auf **OK**.

Schritt 7: Tippen Sie auf VTO-Konfiguration (VTO Config).

Abbildung 2-7 VTO-Konfiguration



Schritt 8: VTO hinzufügen.

- Fügen Sie einen Haupt-VTO hinzu.

1) Geben Sie den Haupt-VTO-Namen, die VTO-IP-Adresse, den Benutzernamen und das Passwort ein.

2) Stellen Sie **Status aktivieren** (Enable Status) auf ON ein.

Benutzername (Username) und **Passwort** (Password) müssen mit dem Anmeldenamen der Web-Oberfläche und Passwort der VTO übereinstimmen. Sonst kann er keine Verbindung herstellen.

- Fügen Sie einen Neben-VTO hinzu.

1) Geben Sie den Namen und die IP-Adresse der Sub-VTO, den Benutzernamen und das Passwort ein.

2) Stellen Sie **Status aktivieren** (Enable Status) auf ON ein.

Tippen Sie auf < / >, um umzublättern und weitere Sub-VTOs hinzuzufügen.

2.3 Inbetriebnahme

2.3.1 VTO ruft VTH an

Wählen Sie die VTH-Zimmernummer (z. B. 101) an der VTO, um den VTH anzurufen. Der VTH blendet Überwachungsvideo und Bediensymbole ein. Siehe Abbildung 2-8.

Die folgende Abbildung bedeutet, dass sich eine SD-Karte im VTH befindet. Ist keine SD-Karte eingelegt, sind die Symbole für Aufnahme und Foto ausgegraut.

Abbildung 2-8 VTH von VTO naufrufen

2.3.2 VTH überwacht VTO

VTH ist in der Lage, VTO oder IPC zu überwachen. Nehmen Sie VTO als Beispiel.

Wählen Sie **Überwachen > Tür** (Monitor > Door). Siehe Abbildung 2-9. Wählen Sie die VTO, um das Überwachungsvideo aufzurufen. Siehe Abbildung 2-10.

Die folgende Abbildung bedeutet, dass sich eine SD-Karte im VTH befindet. Ist keine SD-Karte eingelegt, sind die Symbole für Aufnahme und Foto ausgegraut.

Abbildung 2-9 Tür

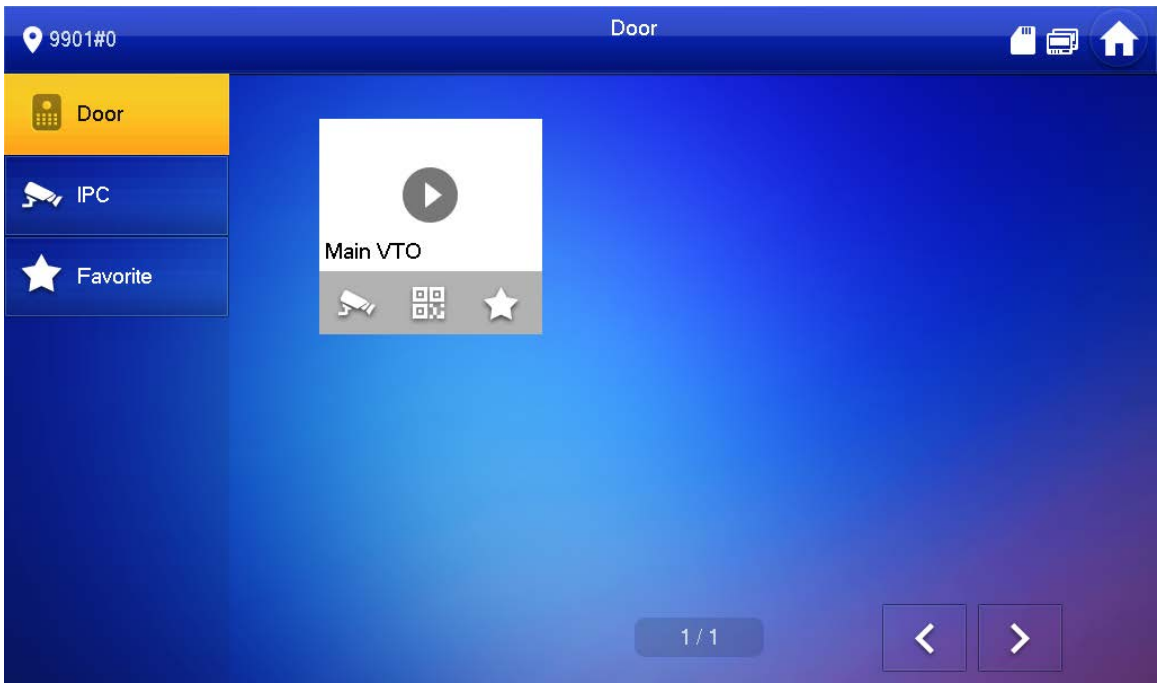
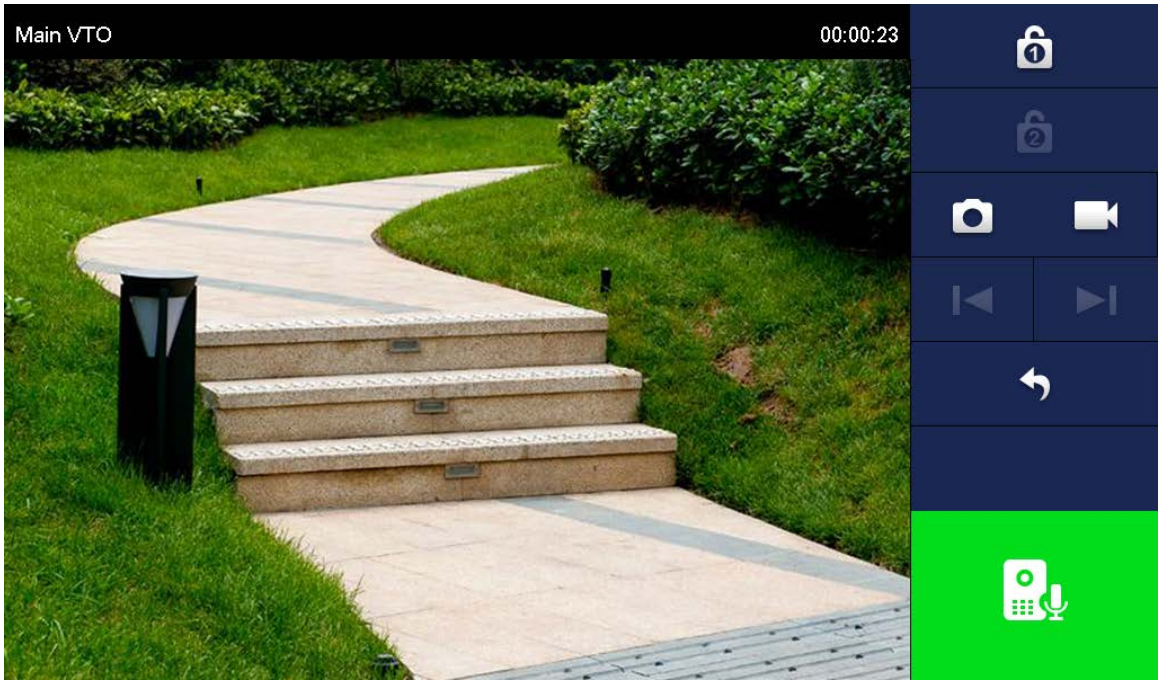


Abbildung 2-10 Video überwachen



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. **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, 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 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.
- Aktivieren Sie die IP/MAC-Adressfilterfunktion, um den Bereich der Hosts einzuschränken, die auf das Gerät zugreifen dürfen.