Türstation für Einfamilienhaus

Benutzerhandbuch

V1.0.0

Vorwort

Allgemein

Diese Anleitung beschreibt die Konfiguration der Türstation für Einfamilienhäuser (nachfolgend als „VTO“ bezeichnet) über die Weboberfläche.

Sicherheitshinweise

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

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

Änderungsverlauf

Version	Inhaltliche Überarbeitung	Veröffentlichungsdatum
V1.0.0	Erste Veröffentlichung.	Januar 2021

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 Landes aktualisiert. Ausführliche 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 Widersprüchen behalten wir uns das Recht einer endgültigen Erläuterung vor.
- 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.

- Bitte besuchen Sie unsere Website oder wenden Sie sich an Ihren Fachhändler oder an den Kundendienst, wenn Probleme bei der Verwendung des Gerätes auftreten.
- Bei Unklarheiten oder Widersprüchen behalten wir uns das Recht einer endgültigen Erläuterung vor.

Wichtige Sicherheits- und Warnhinweise

Die folgende Beschreibung ist die korrekte Anwendungsmethode der VTO. 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 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 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

- 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

1 VTO initialisieren

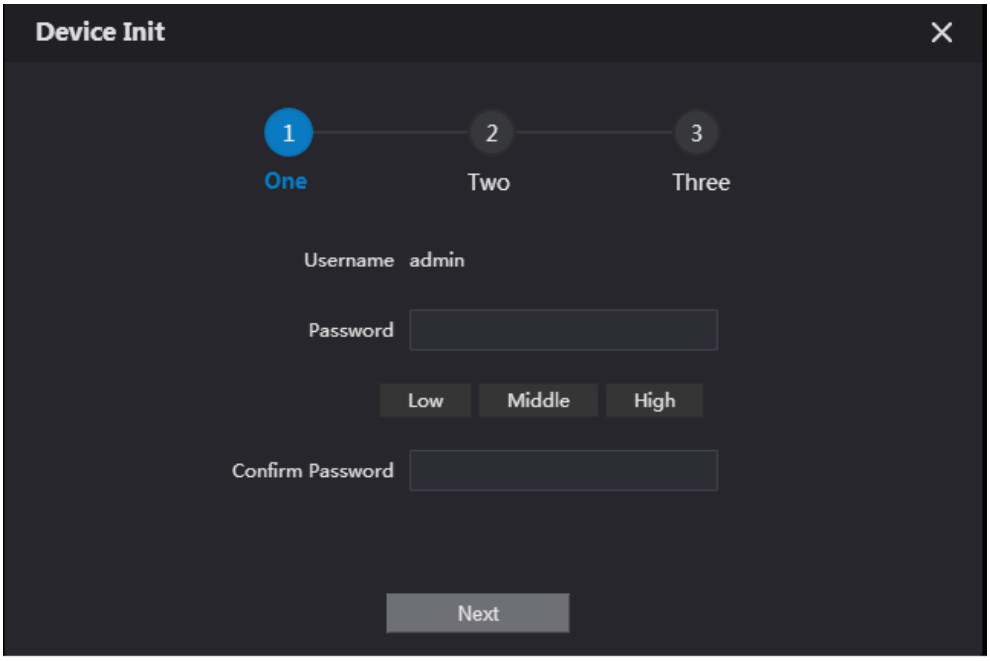
Bei der erstmaligen Anmeldung oder nach der Rücksetzung der VTO müssen Sie sie über die Weboberfläche initialisieren.

Schritt 1: Schalten Sie die VTO ein.

Schritt 2: Rufen Sie die Standard-IP-Adresse (192.168.1.108) der VTO auf.

Achten Sie darauf, dass sich die IP-Adresse Ihres PCs in demselben Netzwerksegment wie die VTO befindet.

Abbildung 1-1 Initialisierung des Geräts



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

Schritt 4: Geben Sie eine E-Mail-Adresse für die Passwortrücksetzung ein.

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

2 Anmelden und Passwort zurücksetzen

2.1 Anmelden

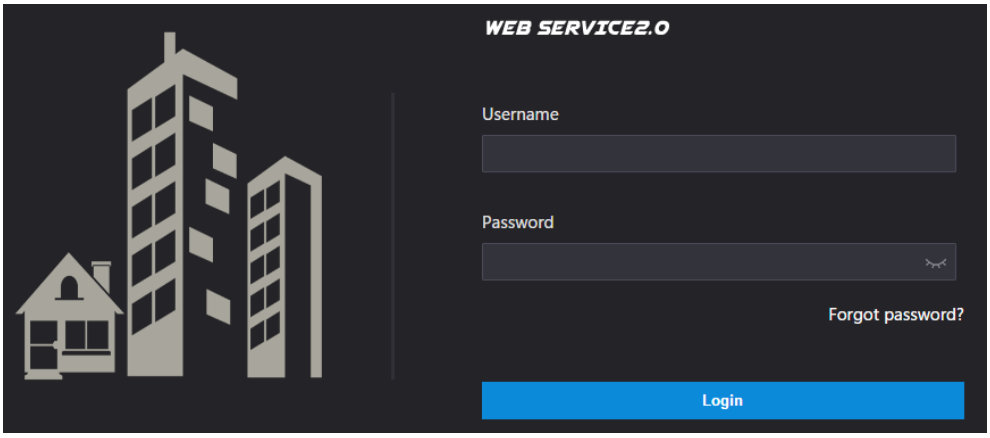
Stellen Sie vor dem Anmelden sicher, dass sich der PC im selben Netzwerksegment wie die VTO befindet.

Schritt 1: 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.

Schritt 2: Geben Sie als Benutzernamen „admin“ und dann das Passwort ein, das Sie bei der Initialisierung festgelegt haben. Klicken Sie anschließend auf **Anmelden** (Login).

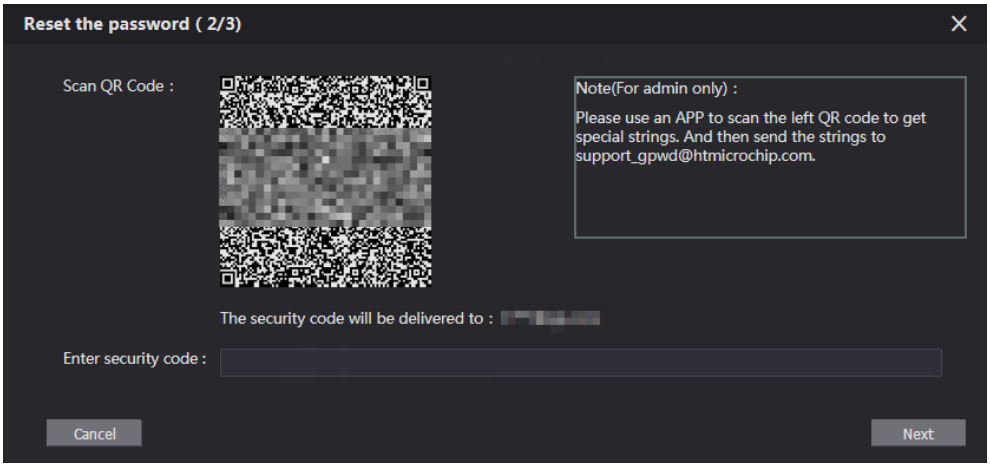
Abbildung 2-1 Anmelden



2.2 Passwort zurücksetzen

Schritt 1: Klicken Sie im Anmeldefenster auf **Passwort vergessen?** (Forgot Password?) und dann auf **Weiter** (Next).

Abbildung 2-2 Passwort zurücksetzen



Schritt 2: Scannen Sie den QR-Code und Sie erhalten einen Zeichenkette aus Ziffern und Buchstaben.

Schritt 3: Senden Sie die Zeichenkette an die E-Mail-Adresse: support_gpwd@htmicrochip.com. Daraufhin wird der Sicherheitscode an die während der Initialisierung konfigurierte E-Mail-Adresse gesendet.

Schritt 4: Geben Sie den Sicherheitscode in das Eingabefeld ein und klicken Sie auf **Weiter** (Next).

- Wenn Sie während der Initialisierung keine E-Mail-Adresse eingerichtet haben, wenden Sie sich für Unterstützung an Ihren Lieferanten oder den Kundendienst.
- Der Sicherheitscode ist nach Empfang nur 24 Stunden lang gültig.
- Wenn Sie 5-mal in Folge den falschen Sicherheitscode eingeben, wird Ihr Konto 5 Minuten lang gesperrt.

Schritt 5: Geben Sie das neue Passwort ein und bestätigen Sie es. Klicken Sie dann auf **OK**.

3 Hauptfenster

Abbildung 3-1 Hauptfenster

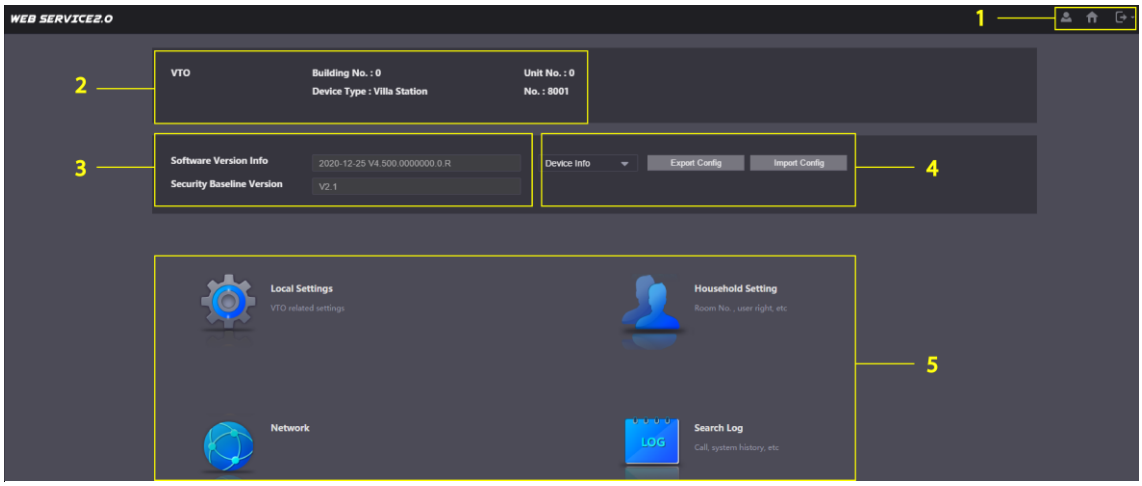


Tabelle 3-1 Einführung in das Hauptfenster

Nr.	Funktion	Beschreibung
1	Allgemeine Funktionen	•  : Zum Ändern des Passwortes und Ihrer E-Mail-Adresse. •  : Zum Aufrufen des Hauptfensters. •  : Zum Abmelden, Neustarten der VTO oder Rücksetzen der VTO auf die Werkseinstellungen.  Falls Sie die VTO auf die Werkseinstellungen zurücksetzen, werden alle Daten mit Ausnahme des externen Speichers gelöscht. Sie können die SD-Karte zum Löschen der darauf befindlichen Daten formatieren.
2	VTO-Informationen	Prüfen Sie Informationen von VTO und System.
3	Systeminformationen	
4	Konfigurationsmanager	Exportieren oder importieren Sie VTO-Konfiguration oder Benutzerinformationen.
5	Funktion	Konfigurieren Sie Parameter für verschiedene Funktionen.  Oberfläche und Funktion können je nach Modell variieren. Das aktuelle Produkt ist maßgeblich.

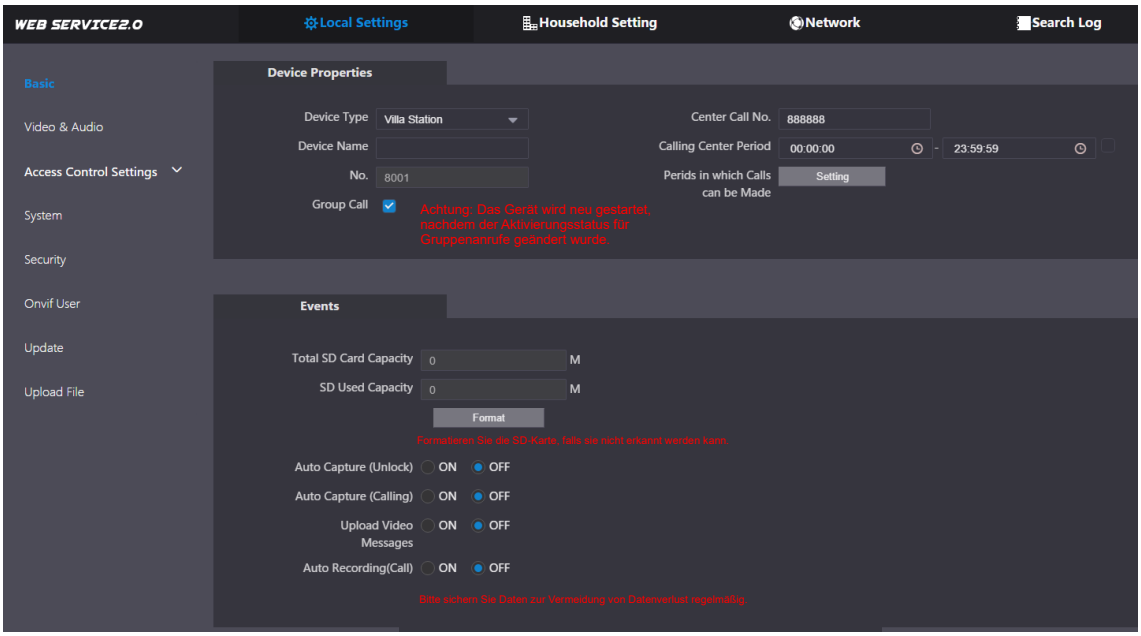
4 Lokale Einstellungen

Dieses Kapitel stellt die detaillierte Konfiguration der VTO vor.

4.1 Allgemein

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

Abbildung 4-1 Allgemein



Schritt 2: Konfigurieren Sie die Parameter.

Tabelle 4-1 Beschreibung der allgemeinen Parameter

Parameter	Beschreibung
Gerätetyp	Wählen Sie **Station für Einfamilienhaus** (Villa Station) oder **Kleine Wohnung** (Small Apartment) wie erforderlich.
Zentrale-Rufnummer	Die Standardtelefonnummer für das Management Center ist 888888, und Sie können sie auf jede Nummer mit bis zu 9 Stellen einstellen.
Gerätename	Wenn andere Geräte diese VTO überwachen, erscheint der Gerätename im Überwachungsbild.
Anrufzeitraum des Zentrums	Zeitraum, in dem das Management Center angerufen werden kann.
Nr.	Dient der Unterscheidung der einzelnen VTOs. Wir empfehlen, dies entsprechend der Einheiten- oder Gebäudenummer einzustellen. Anschließend können Sie VTOs über ihre Nummern dem SIP-Server hinzufügen. Sie können die Nummer der VTO ändern, wenn diese nicht als SIP-Server fungiert.
Zeiträume, in denen	Konfigurieren Sie die Zeit, wenn Sie Anrufe nur während eines bestimmten

Parameter	Beschreibung
Anrufe gemacht werden können	Zeitraums empfangen möchten.
Gruppenruf	Aktivieren Sie dies an der als SIP-Server fungierenden VTO. Wenn ein Haupt-VTH einen Anruf empfängt, erhalten auch alle Erweiterungs-VTHs den Anruf.
Gesamtkapazität der SD-Karte	Zeigt die gesamte und die belegte Kapazität der SD-Karte an. Durch Anklicken von **Formatieren** (Format) werden alle Daten auf der SD-Karte gelöscht.
Belegte SD-Kapazität	
Formatieren	
Automatische Erfassung (Entriegelung)	Wenn die Tür entriegelt wird, erstellt die VTO zwei Schnappschüsse und speichert diese auf der SD-Karte.
Automatische Erfassung (Anruf)	Wenn die VTO anruft, wird ein Schnappschuss erstellt und auf der SD-Karte der VTO gespeichert.
Videonachrichten hochladen	Bei Aktivierung: ● Falls eine SD-Karte in VTH und VTO eingelegt ist, wird die Videonachricht auf den SD-Karten sowohl in VTH als auch in VTO gespeichert. ● Falls nur in VTH oder in VTO eine SD-Karte eingelegt ist, wird die Videonachricht nur auf der SD-Karte in VTH oder VTO gespeichert. ● Falls weder in VTH noch in VTO eine SD-Karte eingelegt ist, wird keine Videonachricht gespeichert.
Automatische Aufzeichnung (Anruf)	Wenn die VTO einen Anruf durchführt, wird eine Aufzeichnung erstellt und auf der SD-Karte der VTO gespeichert.

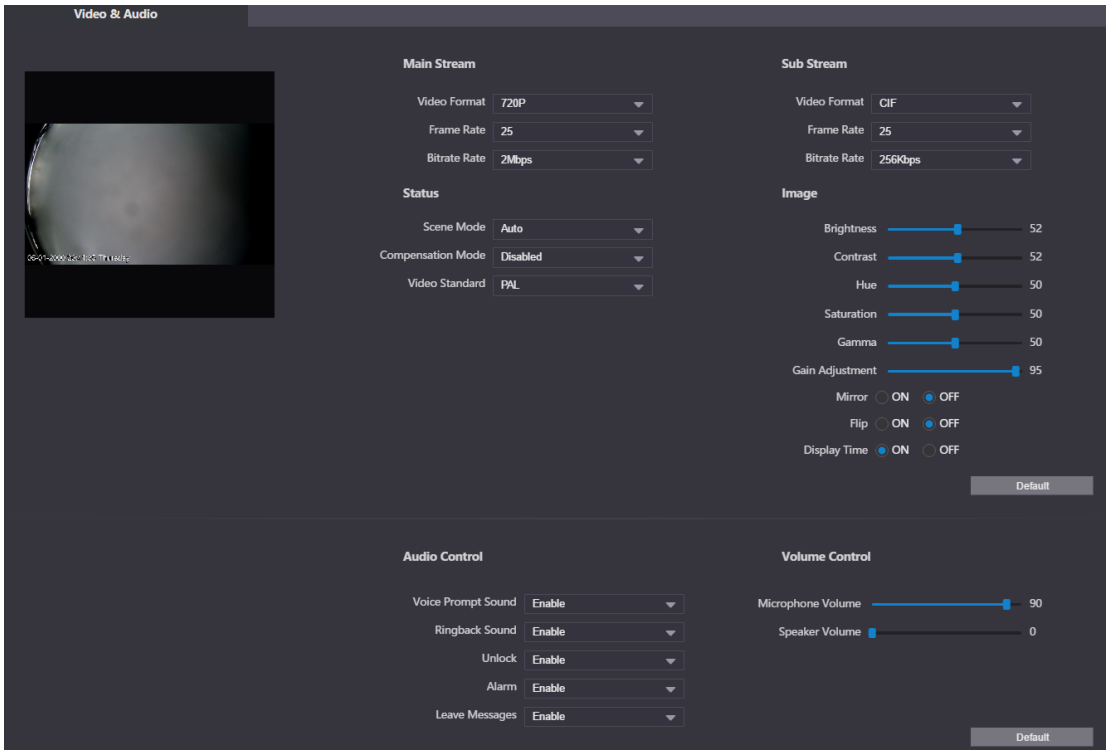
Schritt 3: Klicken Sie auf **Speichern** (Save).

4.2 Video & Audio

Konfigurieren Sie Videoformat und Qualität und Audio der VTO.

Schritt 1: Wählen Sie **Lokale Einstellungen > Video & Audio** (Local Settings > Video & Audio).

Abbildung 4-2 Video und Audio



Schritt 2: Konfigurieren Sie die Parameter, die bei Änderung übernommen werden.

Tabelle 4-2 Beschreibung der Videoparameter

Parameter		Beschreibung
Haupt-/Sub-Stream	Videoformat	Wählen Sie verschiedene Auflösungen wie erforderlich: ● **1080p**: 1920 × 1080. ● **720p**: 1280 × 720. ● **WVGA**: 800 × 480. ● **QVGA**: 320 × 240. ● **D1**: 720 × 480. ● **CIF**: 352 × 288.
	Bildfrequenz	Je höher der Wert ist, desto ruckelfreier ist das Video, doch desto mehr Bandbreite wird benötigt.
	Bitrate	Je höher der Wert ist, desto besser ist die Videoqualität, doch desto mehr Bandbreite wird benötigt.

Parameter		Beschreibung
Status	Szenenmodus	Treffen Sie Ihre Auswahl wie erforderlich entsprechend den Lichtbedingungen. **Auto** ist standardmäßig ausgewählt.
	Kompensationsmodus	• **BLC**: Gegenlichtkompensation. Verbessert die Klarheit des Motivs im Bild. • **WDR**: Breiter Dynamikbereich. Verbessert die Helligkeit dunkler Bereiche und reduziert die Helligkeit heller Bereiche zur Verbesserung des Bildes. • **HLC**: Kompensation intensiven Lichts. Reduziert die Helligkeit heller Flecken zur Verbesserung des Gesamtbildes.
	Video-Standard	Wählen Sie entsprechend Ihrer Region **PAL** oder **NTSC**. **PAL** wird vor allem in China und Europa genutzt, während **NTSC** vorwiegend in den Bereinigten Staaten und Japan verwendet wird.
Bild	Helligkeit	Je höher der Wert ist, desto heller wird das Bild.
	Kontrast	Wählen Sie für mehr Kontrast zwischen hellen und dunklen Bereichen einen höheren Wert.
	Farbton	Machen Sie das Bild heller oder dunkler. Der Standardwert wird durch den Lichtsensor erzeugt und sollte beibehalten werden.
	Sättigung	Je höher der Wert ist, desto satter wird die Farbe.
	Gamma	Ändert die Bildhelligkeit und verbessert den Bilddynamikbereich mit einer nichtlinearen Methode. Je höher der Wert ist, desto heller wird das Bild.
	Verstärkungsanpassung	Verstärkt das Videosignal, um die Bildhelligkeit zu erhöhen. Wenn der Wert zu groß ist, rauscht das Bild stärker.
	Spiegeln	Zeigt das Bild, wobei linke und rechte Seite vertauscht werden.
	Drehen	Zeigt das Bild verkehrt herum.
	Anzeigezeit	Zeigt die aktuelle Uhrzeit und das aktuelle Datum im Videobild.
Audiosteuerung	—	Schalten Sie jeden einzelnen Tontyp ein oder aus.
Lautstärkeregelung	Mikrofonlautstärke	Stellen Sie die Lautstärke nach Bedarf ein.
	Lautsprecherlautstärke	

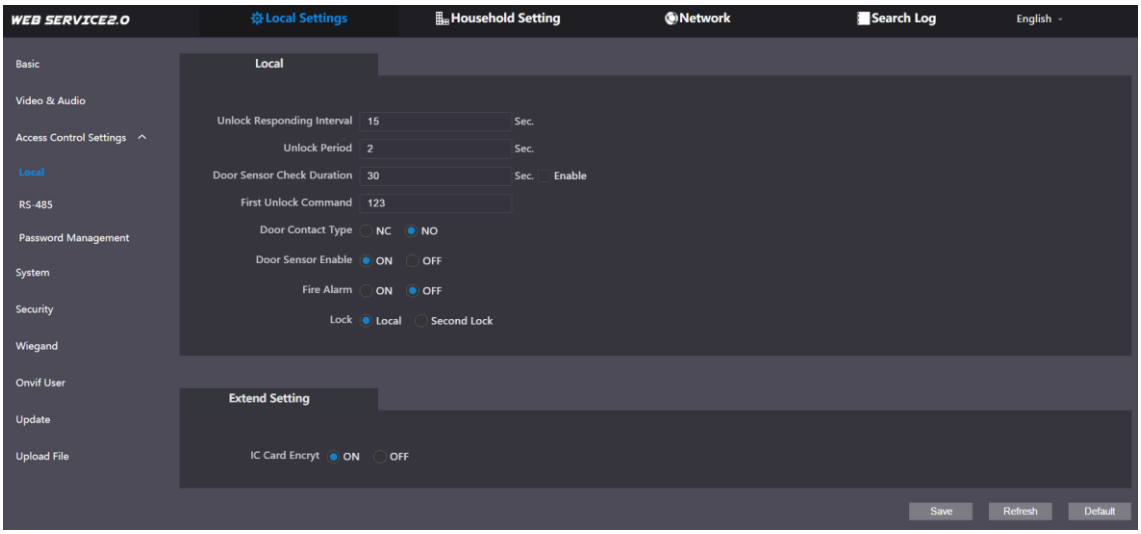
4.3 Zutrittskontrolleinstellungen

Dieser Abschnitt zeigt, wie die zwei mit dem Schloss- oder RS-485-Anschluss verbundenen Schlösser konfiguriert werden.

4.3.1 Lokal

Schritt 1: Wählen Sie **Lokale Einstellungen** > **Zutrittskontrolleinstellungen** (Local Settings > Access Control Settings).

Abbildung 4-3 Lokal



Schritt 2: Konfigurieren Sie die Parameter.

Tabelle 4-3 Beschreibung der Parameter für die lokale Zugangskontrolle

Parameter	Beschreibung
Antwortabstand entriegeln	Die Tür kann erst nach Ablauf des Intervalls erneut entriegelt werden.
Entriegelungsdauer	Die Dauer, wie lange der das Schloss entriegelt bleibt.
Türsensor-Prüfdauer	• Aktivieren Sie dies und die Tür wird erst verriegelt, wenn sich die Türsensoren berühren. Falls die Tür länger als die **Türsensor-Prüfdauer** (Door Sensor Check Duration) entriegelt ist, wird der Türsensor-Alarm ausgelöst und der Alarm wird an das Management Center gesendet. • Deaktivieren Sie ihn und die Tür wird nach der **Entriegelungsdauer** (Unlock Period) verriegelt. Zur Konfiguration dieses Parameters müssen Sie einen Türkontakt installieren.
Erster/zweiter Entriegelungsbefehl	Sie können ein Telefon eines Drittanbieters, z. B. ein SIP-Telefon, mit der VTO verbinden und mit einem Befehl die Tür aus der Ferne öffnen.
Türkontakttyp	• **NC**: Normalerweise geschlossen. • **NO**: Normalerweise offen.
Türkontakt aktivieren	Synchronisieren Sie den Türsensorstatus mit den Innenmonitoren (VTHs).

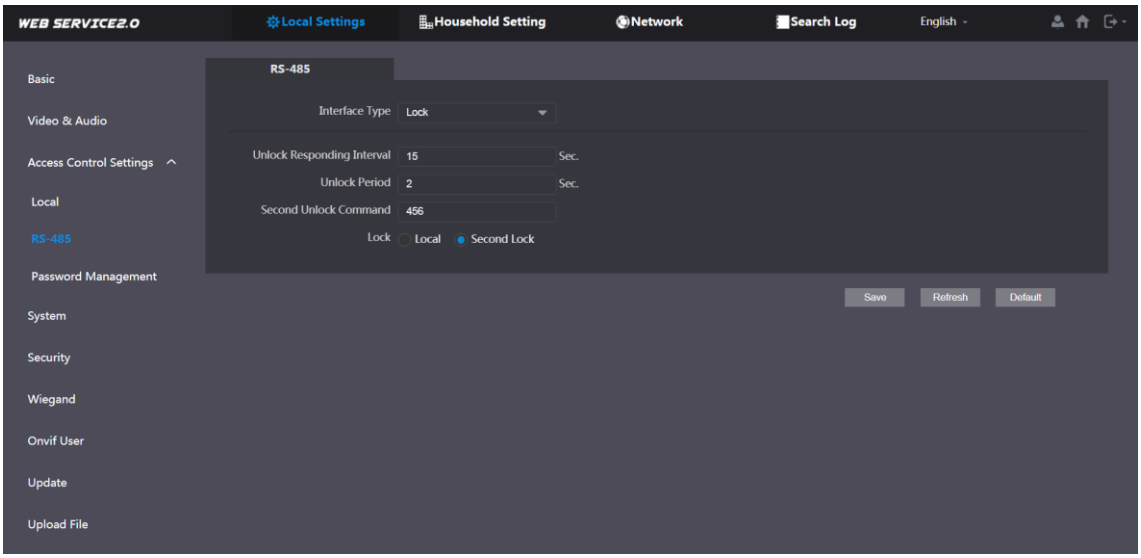
Parameter	Beschreibung
Feueralarm	Wenn diese Option eingeschaltet ist, können Sie ein Alarmgerät mit dem ursprünglich für den Türkontakt vorgesehenen Anschluss verbinden. In diesem Fall können Sie jedoch nicht die Türkontakt-Funktion nutzen.
Schloss	Nicht-externe Methoden wie Passwort oder Karte entriegeln das von Ihnen ausgewählte Schloss.
IC-Karte verschlüsseln	Von der VTO ausgestellte Zutrittskarten werden verschlüsselt und können nicht geklont werden.

Schritt 3: Klicken Sie auf **Speichern** (Save).

4.3.2 RS-485

Wählen Sie **Lokale Einstellungen > Zutrittskontrolleinstellungen** (Local Settings > Access Control Settings), und konfigurieren Sie dann die Parameter des mit dem RS-485-Anschluss verbundenen Schlosses. Siehe Tabelle 4-3 für eine Beschreibung der Parameter.

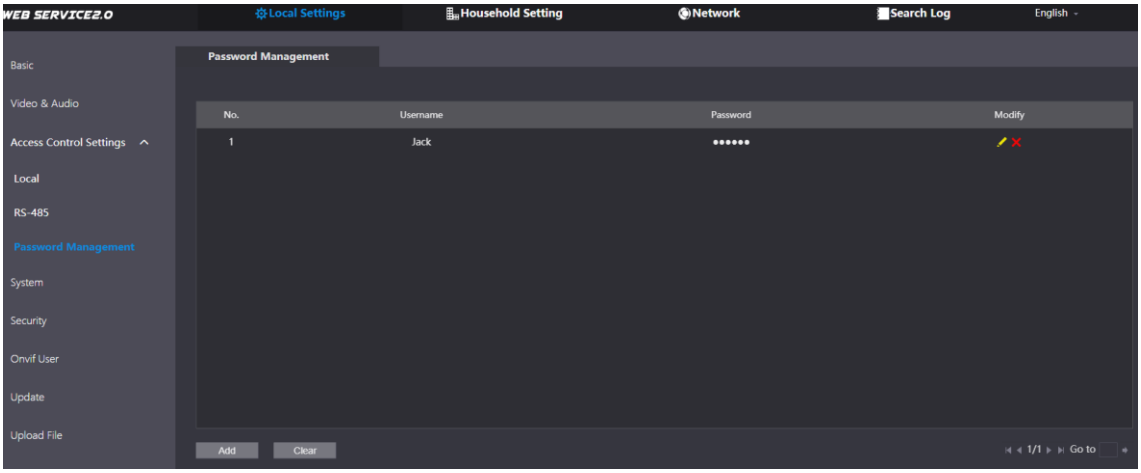
Abbildung 4-4 Über RS-485-Anschluss verbundenes Schloss



4.3.3 Passwortverwaltung

Fügen Sie einen Benutzernamen und ein Passwort zur Entriegelung der Tür hinzu.

Abbildung 4-5 Passwortverwaltung

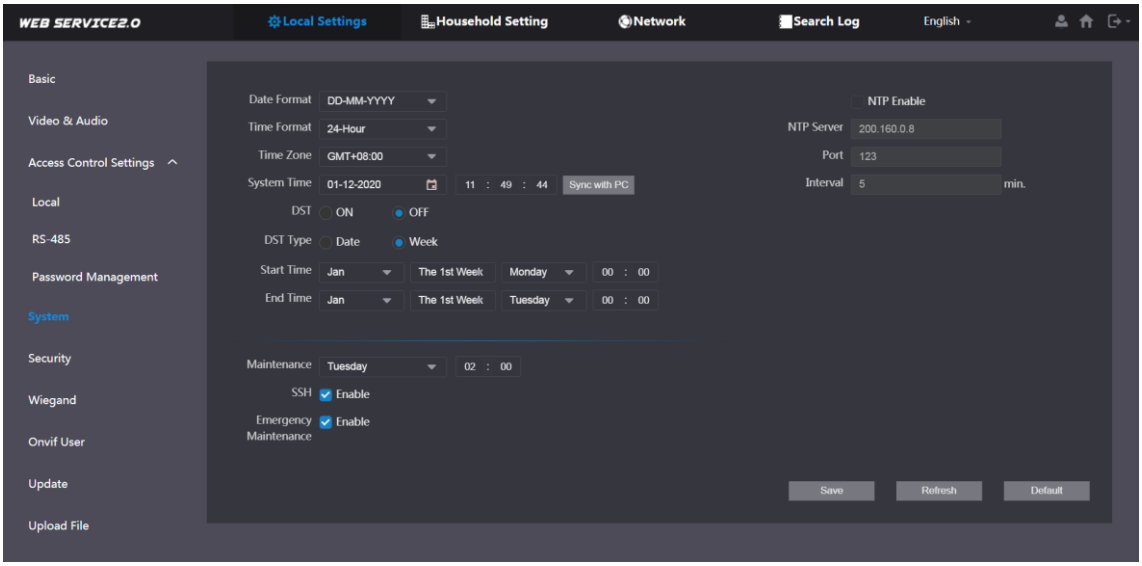


4.4 System

Konfigurieren Sie Zeitparameter, NTP-Server und mehr.

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

Abbildung 4-6 System



Schritt 2: Konfigurieren Sie die Parameter.

Tabelle 4-4 Beschreibung der Systemparameter

Parameter	Beschreibung
Datumformat	Wählen Sie ein Format wie erforderlich.
Zeitformat	
Systemzeit	⚠ Die Änderung der Systemzeit kann Probleme bei Videosuche und Informationsveröffentlichung verursachen. Schalten Sie vor Änderung Videoaufnahme und automatischen Schnappschuss aus.
Zeitzone	Konfigurieren Sie die Zeitzone wie erforderlich.

Parameter	Beschreibung
Mit PC synchronisieren	Synchronisieren Sie die VTO-Systemzeit mit Ihrem PC.
Sommerzeit	Sommerzeitumstellung. Falls in Ihrer Region zwischen Sommer- und Winterzeit unterschieden wird, müssen Sie diese Option aktivieren und den Sommerzeit-Typ, Start- und Endzeit konfigurieren.
Art der Sommerzeit	Wählen Sie wie erforderlich **Datum** (Date) und **Woche** (Week) und konfigurieren Sie den spezifischen Zeitraum.
Startzeit	Konfigurieren Sie die Start- und Endzeit der Sommerzeit.
Endzeit	
NTP aktivieren	Aktivieren Sie NTP und geben Sie die IP-Adresse des NTP-Servers ein. Anschließend synchronisiert die VTO die Zeit automatisch mit dem NTP Server.
NTP-Server	
Port	Portnummer des NTP Servers.
Intervall	Zyklus der VTO-Zeitaktualisierung. Maximal 30 Minuten.
Wartung	Definieren Sie die Zeit, zu welcher die VTO automatisch neu starten soll.
SSH	Sie können Debugging-Geräte über das SSH-Protokoll mit der VTO verbinden. ⚠ Sie sollten dies ausschalten und den Sicherheitsmodus sowie den Schutz ausgehender Dienstinformationen einschalten. Siehe „4.5 Sicherheit“. Andernfalls ist die VTO möglicherweise Sicherheitsrisiken und Datenlecks ausgesetzt.
Notfallwartung	Aktivieren Sie dies für Fehleranalyse und Reparatur. 🕮 Diese Funktion belegt die Ports 8088 und 8087.

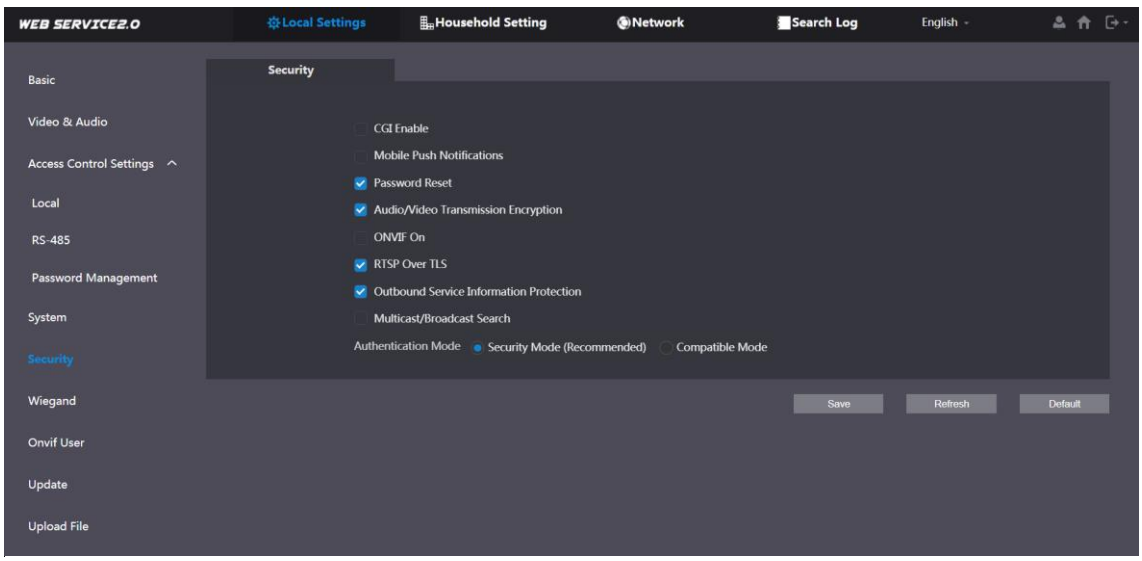
Schritt 3: Klicken Sie auf **Speichern** (Save).

4.5 Sicherheit

Konfigurieren Sie die Funktionen zur Gerätesicherheit.

Schritt 1: Wählen Sie **Lokale Einstellungen > Sicherheit** (Local Settings > Security).

Abbildung 4-7 Sicherheit



Schritt 2: Konfigurieren Sie die Parameter.

Tabelle 4-5 Beschreibung der Sicherheitsparameter

Parameter	Beschreibung
CGI aktivieren	Aktivieren Sie die Nutzung des CGI-Befehls. ⚠ Wir empfehlen, diese Funktion auszuschalten. Andernfalls ist die VTO möglicherweise Sicherheitsrisiken und Datenlecks ausgesetzt.
Mobiltelefon Push-Benachrichtigung	Senden Sie Informationen an die App auf dem Smartphone. ⚠ Wir empfehlen, diese Funktion auszuschalten, wenn Sie sie nicht benötigen. Andernfalls ist die VTO möglicherweise Sicherheitsrisiken und Datenlecks ausgesetzt.
Passwort zurücksetzen	Wenn dies ausgeschaltet ist, können Sie das Passwort nicht zurücksetzen.
Verschlüsselung der Audio-/Videoübertragung	Verschlüsseln Sie alle Daten während Sprach- und Videoanrufen. ⚠ Wir empfehlen, dies einzuschalten. Andernfalls ist die VTO möglicherweise Sicherheitsrisiken und Datenlecks ausgesetzt.
ONVIF ein	Erlauben Sie Drittanbietern, den Videostream der VTO über das ONVIF-Protokoll zu beziehen. ⚠ Wir empfehlen, diese Funktion auszuschalten. Andernfalls ist die VTO möglicherweise Sicherheitsrisiken und Datenlecks ausgesetzt.
RTSP über TSL	Geben Sie verschlüsselten Bitstream über RTSP aus. ⚠ Wir empfehlen, dies einzuschalten. Andernfalls ist die VTO möglicherweise Sicherheitsrisiken und Datenlecks ausgesetzt.
Schutz ausgehender Dienstinformationen	Schützen Sie Ihre Passwörter. ⚠ Wir empfehlen, dies einzuschalten. Andernfalls ist die VTO möglicherweise Sicherheitsrisiken und Datenlecks ausgesetzt.
Multicast-/Broadcast-Suche	Aktivieren Sie dies und die VTO wird von anderen Geräten gefunden. ⚠ Wir empfehlen, diese Funktion auszuschalten. Andernfalls ist die VTO möglicherweise Sicherheitsrisiken und Datenlecks ausgesetzt.

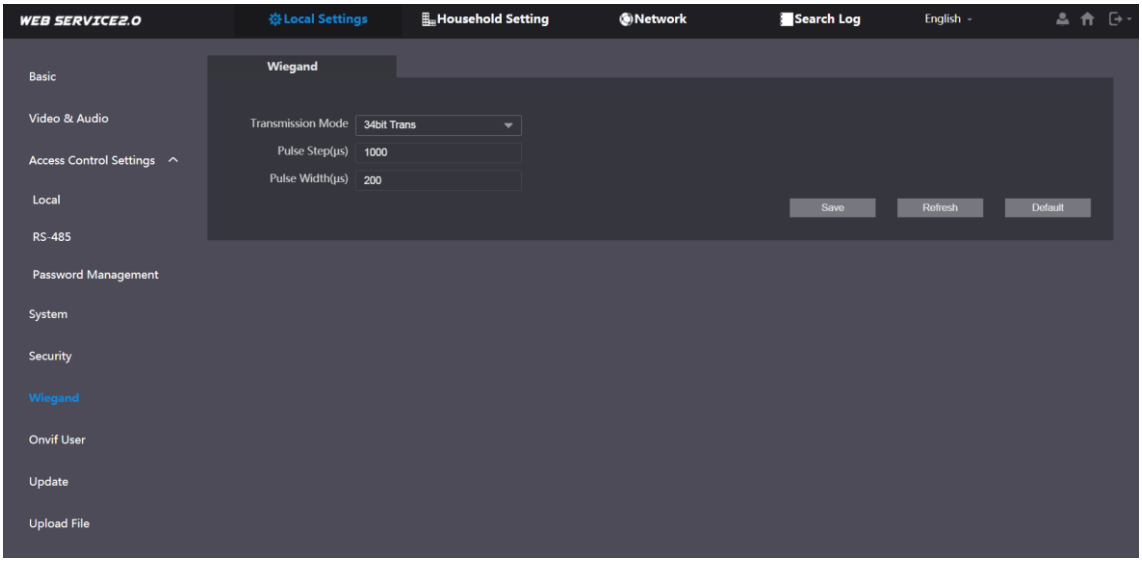
Parameter	Beschreibung
Authentifizierungsmodus	• **Sicherheitsmodus** (Security Mode) (empfohlen): Unterstützt die Anmeldung mit Digest-Authentifizierung. • **Kompatibler Modus** (Compatible Mode)**:** Nutzt die alte Anmeldemethode. ⚠ Wir empfehlen den Sicherheitsmodus. Kompatibler Modus könnte die VTO Sicherheitsrisiken und Datenlecks aussetzen.

Schritt 3: Klicken Sie auf **Speichern** (Save).

4.6 Wiegand

Konfigurieren Sie die Parameter bei Verbindung mit anderen Geräten, wie einem Kartenleser mit Wiegand-Anschluss, wie erforderlich.

Abbildung 4-8 Wiegand



4.7 Onvif-Benutzer

Fügen Sie Konten für Geräte hinzu, um die VTO über das ONVIF-Protokoll zu überwachen.

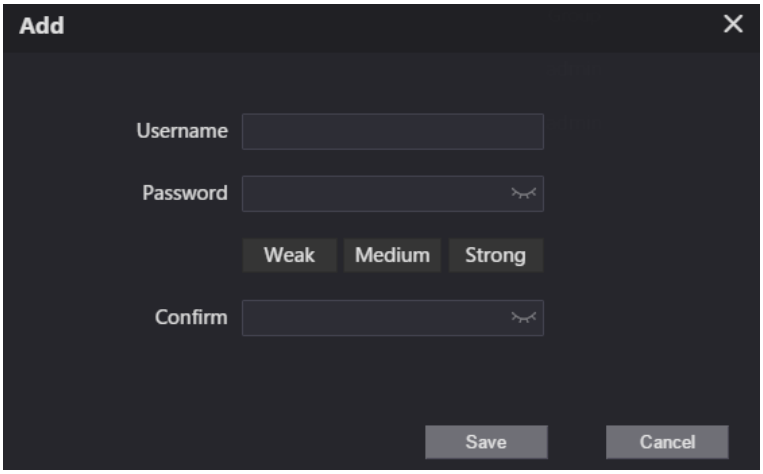
⚠

Wenn Sie ein Konto löschen, kann dies nicht rückgängig gemacht werden.

Schritt 1: Wählen Sie **Lokale Einstellungen > Onvif-Benutzer** (Local Settings > Onvif User).

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

Abbildung 4-9 Einen Onvif-Benutzer hinzufügen

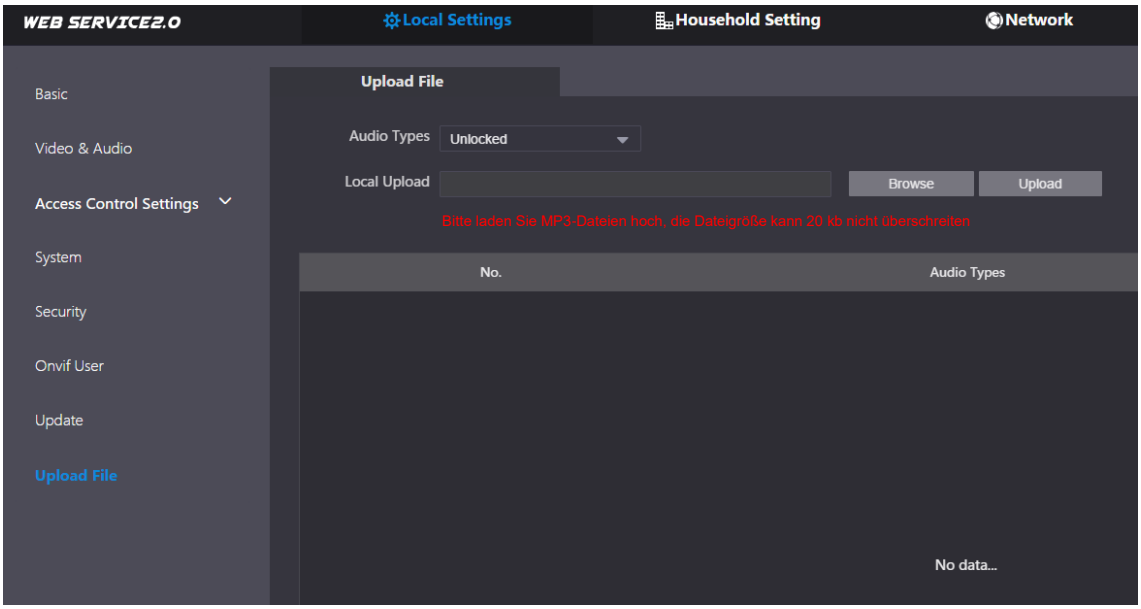


Schritt 3: Geben Sie die Daten ein und klicken Sie auf **Speichern** (Save).
ONVIF-Geräte können die VTO nun über das Konto überwachen. Einzelheiten finden Sie in der Bedienungsanleitung des ONVIF-Gerätes.

4.8 Datei hochladen

Laden Sie die Audiodatei hoch, um den Ton beim Anrufen, Entriegeln der Tür usw. zu ändern.
Schritt 1: Wählen Sie **Lokale Einstellungen > Datei hochladen** (Local Settings > Upload File).
Schritt 2: Wählen Sie einen Audiotyp, klicken Sie dann zur Auswahl der Audiodatei wie erforderlich auf **Durchsuchen** (Browse).

Abbildung 4-10 Tonaufforderung ändern



Schritt 3: Klicken Sie auf **Hochladen** (Upload).

5 Haushaltseinstellung

Dieses Kapitel zeigt, wie VTO, VTH, VTS und IPC hinzugefügt, geändert und gelöscht und Nachrichten vom SIP-Server an VTOs und VTHs gesendet werden können, wenn die VTO als SIP-Server fungiert. Wenn Sie andere Server als SIP-Server verwenden, finden Sie Details zur Konfiguration im entsprechenden Handbuch.

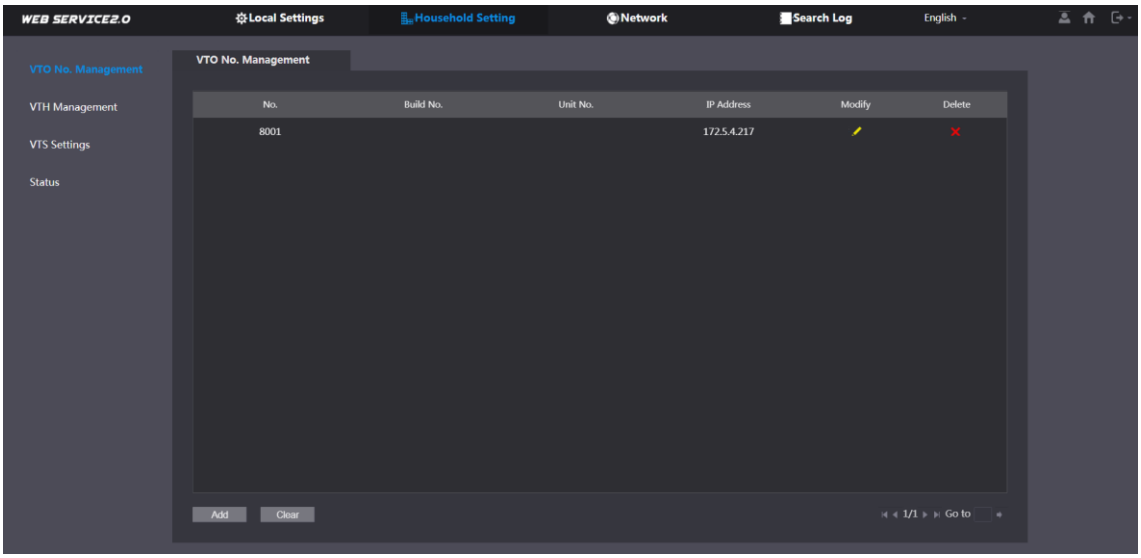
Einzelheiten zur Konfiguration der Parameter des SIP-Servers finden Sie unter „6.3 SIP-Server".

5.1 VTO-Nr.-Verwaltung

Sie können dem SIP-Server VTOs hinzufügen und alle mit demselben SIP-Server verbundenen VTOs können einander anrufen.

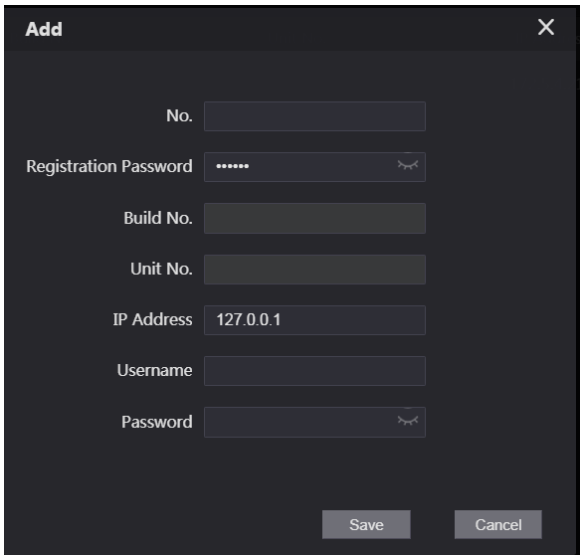
Schritt 1: Melden Sie sich bei der Weboberfläche der als SIP-Server fungierenden VTO an und wählen Sie dann **Haushaltseinstellung** > **VTO-Nr.-Verwaltung** (Household Setting > VTO No. Management).

Abbildung 5-1 VTO-Verwaltung



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

Abbildung 5-2 VTO hinzufügen



Schritt 3: Konfigurieren Sie die Parameter.

Der SIP-Server muss hinzugefügt werden.

Tabelle 5-1 VTO-Konfiguration hinzufügen

Parameter	Beschreibung
Nr.	Die von Ihnen konfigurierte VTO-Nummer. Siehe Tabelle 4-1 für Details.
Registrierungspasswort	Behalten Sie den Standardwert bei.
Gebäudenr.	Nur wenn andere Server als SIP-Server fungieren.
Einheiten-Nr.	
IP-Adresse	IP-Adresse der VTO.
Benutzername	Benutzername und Passwort der VTO zur Anmeldung an der Weboberfläche.
Passwort	

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

Klicken Sie zum Ändern oder Löschen einer VTO auf oder , klicken Sie zum Löschen aller hinzugefügten VTOs auf **Löschen** (Clear). Die VTO, an der Sie sich angemeldet haben, kann jedoch nicht geändert oder gelöscht werden.

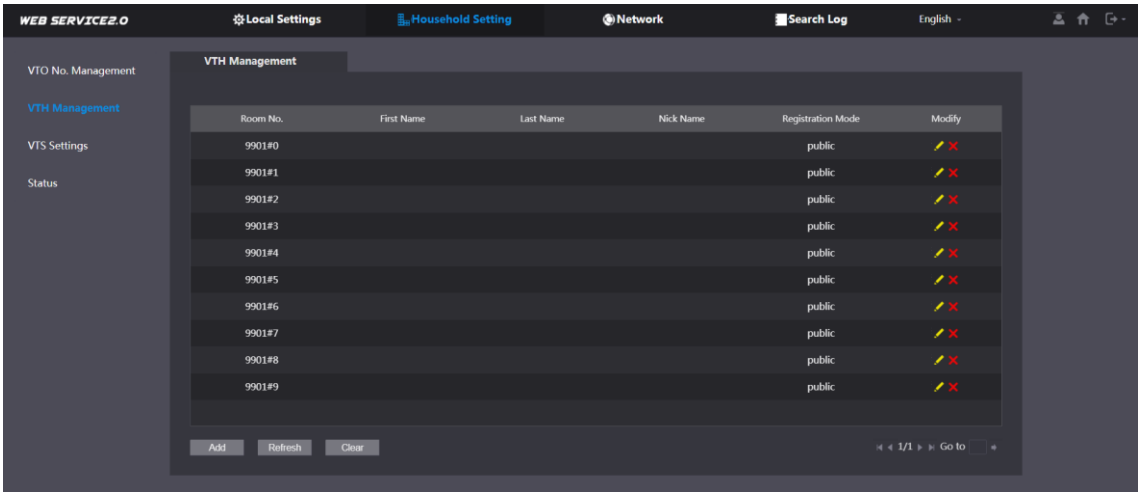
5.2 VTH-Verwaltung

5.2.1 Zimmernummer hinzufügen

Sie können Zimmernummern zum SIP-Server hinzufügen und dann die Zimmernummer auf VTHs konfigurieren, um sie mit dem Netzwerk zu verbinden.

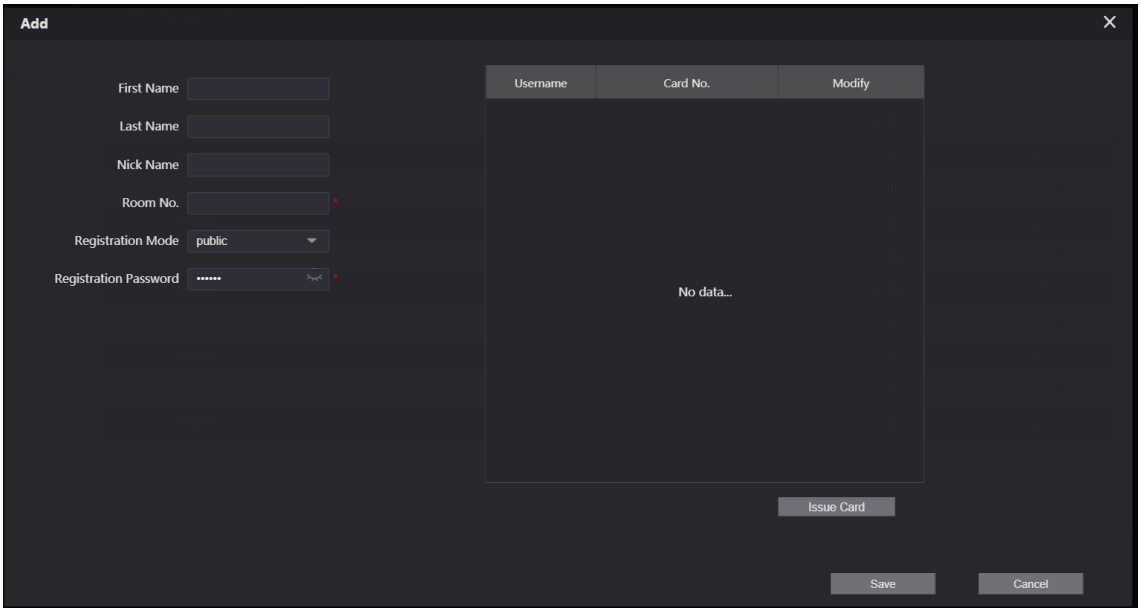
Schritt 1: Melden Sie sich an der Weboberfläche des SIP-Servers an und wählen Sie dann **Haushaltseinstellung > VTH-Verwaltung** (Household Setting > VTH Management**).**

Abbildung 5-3 Zimmernummernverwaltung



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

Abbildung 5-4 Eine Zimmernummer hinzufügen



Schritt 3: Konfigurieren Sie die Parameter.

Tabelle 5-2 Zimmerdaten

Parameter	Beschreibung
Vorname	Geben Sie die Daten ein, die Sie zur Unterscheidung der einzelnen Zimmer benötigen.
Nachname	
Spitzname	
Zimmernr.	Geben Sie eine Zimmernummer ein, konfigurieren Sie dann die Nummer an einem VTH, um ihn mit dem Netzwerk zu verbinden.
Registrierungstyp	Wählen Sie **öffentlich** (public).
Registrierungspasswort	Behalten Sie den Standardwert bei.

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

Klicken Sie zum Ändern oder Löschen einer Zimmernummer auf oder .

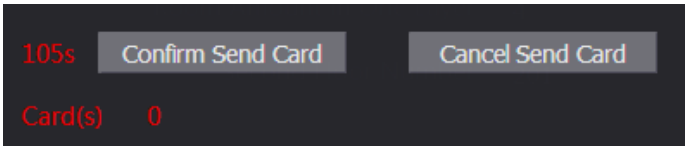
5.2.2 Zugangskarte ausstellen

Stellen Sie eine Zugangskarte aus, um die Tür eines Zimmers zu entriegeln.

Zur Nutzung dieser Funktion muss die VTO über einen Kartenleser verfügen.

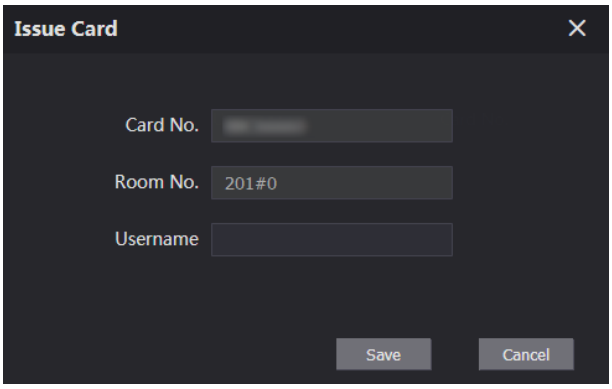
Schritt 1: Wählen Sie **Haushaltseinstellung** > **VTH-Verwaltung** (Household Setting > VTH Management), klicken Sie auf **Hinzufügen** (Add) und dann auf **Karte ausstellen** (Issue Card).

Abbildung 5-5 Countdown-Meldung



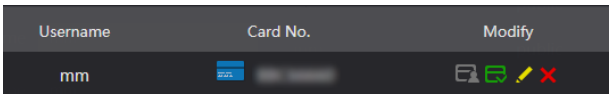
Schritt 2: Ziehen Sie die Karte an der VTO durch.

Abbildung 5-6 Karte ausstellen



Schritt 3: Geben Sie den Benutzernamen ein, klicken Sie auf **Speichern** (Save) und dann auf **Versandkarte bestätigen** (Confirm Send Card).

Abbildung 5-7 Ausgestellte Zugangskarte



Sonstige Operationen

- Klicken Sie auf , um sie als Hauptkarte einzurichten. Das Symbol wechselt zu . Mit der Hauptkarte können Zugangskarten für dieses Zimmer an der VTO ausgestellt werden.
- Klicken Sie auf , um sie als verloren einzustellen. Das Symbol wechselt zu . Eine verlorene Karte kann nicht zum Öffnen der Tür verwendet werden.
- Klicken Sie zum Ändern des Benutzernamens oder zum Löschen der Karte auf oder .

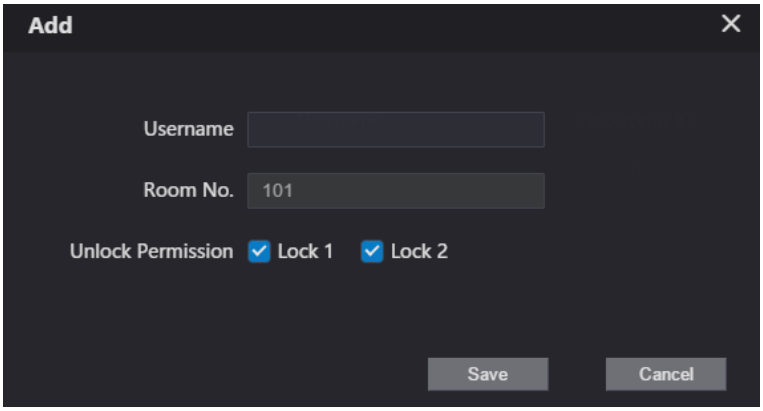
5.2.3 Fingerabdruck ausstellen

Stellen Sie Fingerabdrücke aus, um die Tür eines Zimmers zu entriegeln.

Zur Nutzung dieser Funktion muss die VTO über einen Fingerabdruck-Scanner verfügen.

Schritt 1: Wählen Sie **Haushaltseinstellung > VTH-Verwaltung** (Household Setting > VTH Management), klicken Sie auf **Hinzufügen** (Add) und dann auf **Fingerabdruck ausstellen** (Issue Fingerprint).

Abbildung 5-8 Stellen Sie den Fingerabdruck aus.



Schritt 2: Geben Sie den Benutzernamen ein, weisen Sie wie erforderlich Entriegelungsrechte zu und klicken Sie auf **Speichern** (Save).

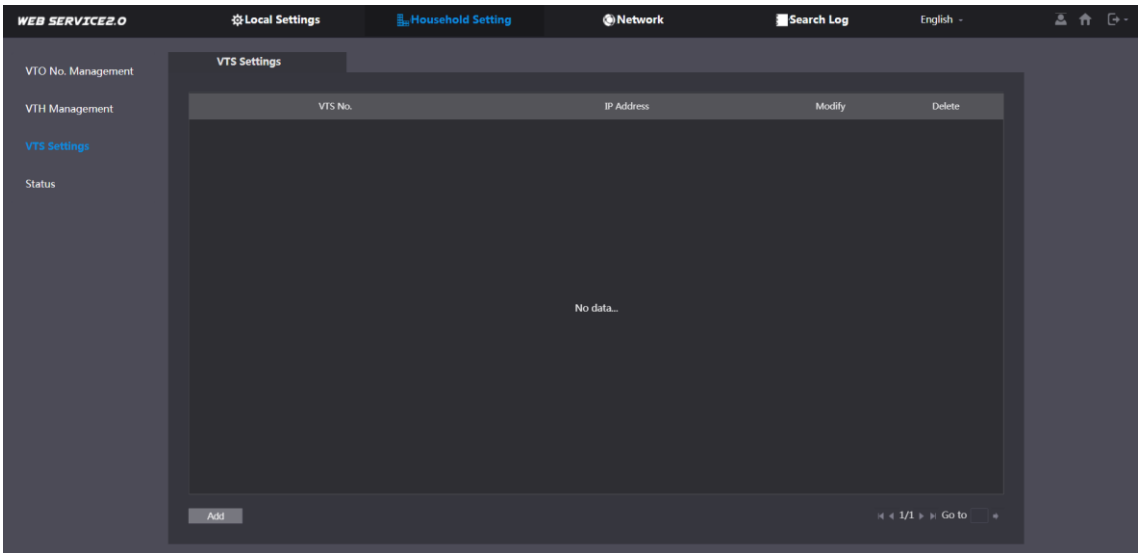
Schritt 3: Drücken Sie Ihren Finger an den Scanner.

5.3 VTS-Verwaltung

Sie können dem SIP-Server einen VTS hinzufügen und dieser kann dann als Verwaltungszentrale verwendet werden. Er dient zudem der Verwaltung, dem Anrufen oder dem Empfangen von Anrufen von allen VTOs und VTHs im Netzwerk. Siehe das entsprechende Benutzerhandbuch für Einzelheiten.

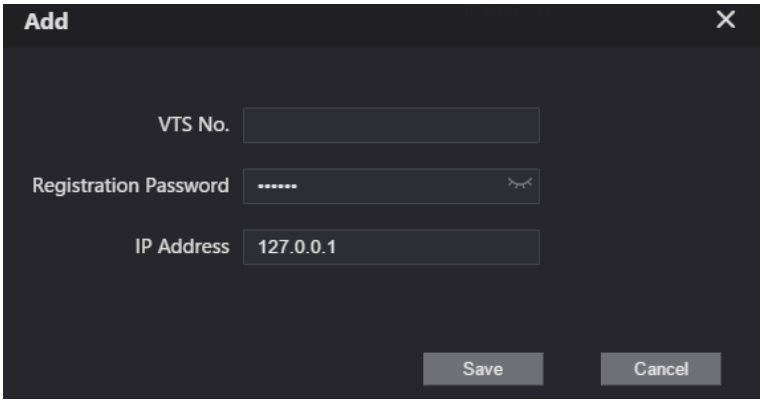
Schritt 1: Melden Sie sich an der Weboberfläche der als SIP-Server fungierenden VTO an und wählen Sie dann **Haushaltseinstellung > VTS-Einstellungen** (Household Setting > VTS Settings).

Abbildung 5-9 VTS-Verwaltung



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

Abbildung 5-10 VTS hinzufügen



Schritt 3: Konfigurieren Sie die Parameter.

Tabelle 5-3 VTS-Konfiguration hinzufügen

Parameter	Beschreibung
VTS-Nr.	Die Nummer des VTS.
Registrierungspasswort	Behalten Sie den Standardwert bei.
IP-Adresse	VTS-IP-Adresse.

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

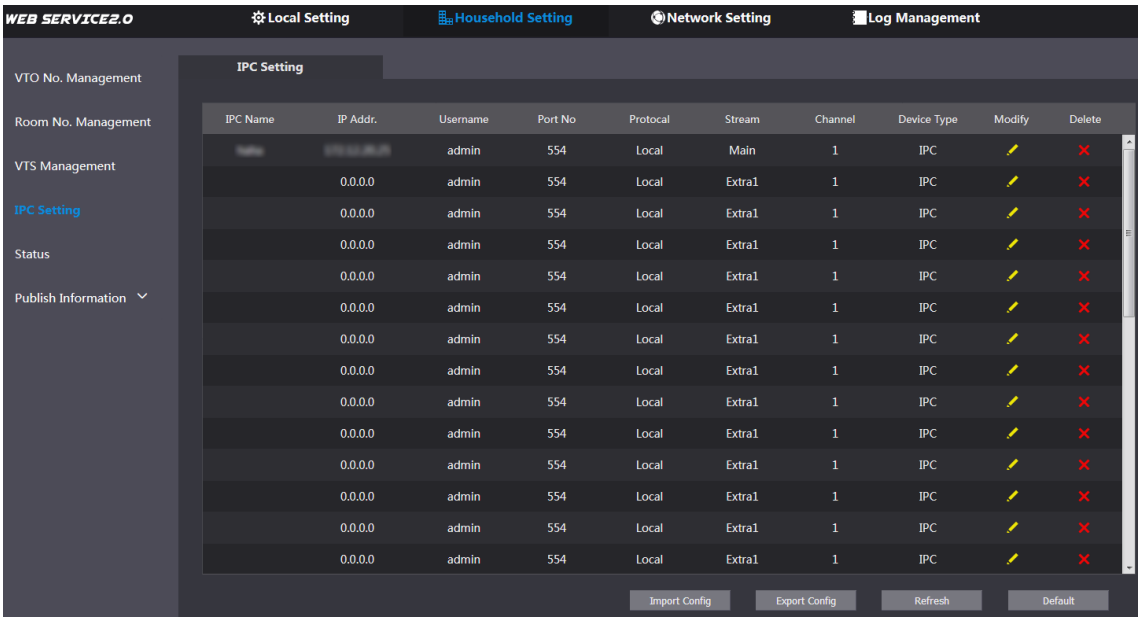
5.4 IPC-Einstellung

Sie können IPC und NVR zu der als SIP-Server fungierenden VTO hinzufügen. Anschließend können alle angeschlossenen VTHs diese überwachen.

Schnittstellen können je nach Produkt variieren. Das Menü ist ausschlaggebend.

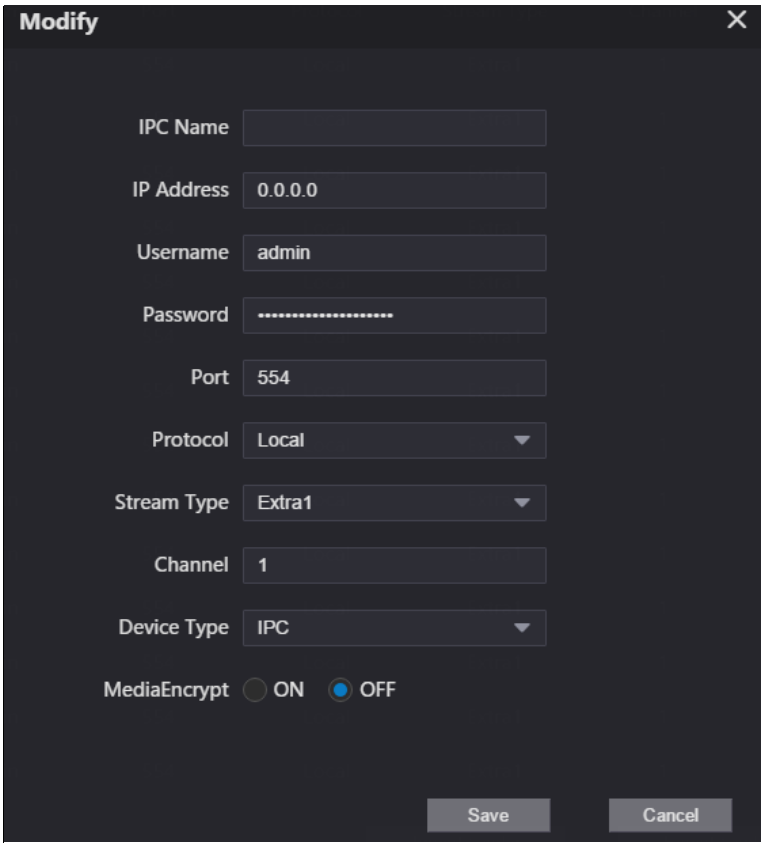
Schritt 1: Melden Sie sich an der Weboberfläche der als SIP-Server fungierenden VTO an und wählen Sie dann **Haushaltseinstellung > IPC-Einstellung** (Household Setting > IPC Setting).

Abbildung 5-11 IPC-Einstellung



Schritt 2: Klicken Sie auf .

Abbildung 5-12 IPC hinzufügen



Schritt 3: Konfigurieren Sie die Parameter.

Tabelle 5-4 IPC-Konfiguration hinzufügen

Parameter	Beschreibung
Name der IPC	Geben Sie den Namen ein, der den IPC identifiziert.
IP-Adresse	IP-Adresse des IPC.
Benutzername	Benutzername und Passwort des Gerätes zur Anmeldung an der Weboberfläche.
Passwort	
Port	Behalten Sie den Standardwert bei.
Protokoll	Wählen Sie **Lokal** (Local) oder **Onvif**.
Stream-Typ	● **Main** (Haupt): Bessere Videoqualität, erfordert aber mehr Bandbreite. ● **Extra1:** Ruckelfreies Video mit schlechterer Qualität, erfordert aber weniger Bandbreite.
Kanal	Die Anzahl Kanäle, die ein Gerät unterstützt.
Gerätetyp	Treffen Sie Ihre Auswahl wie erforderlich.
Medienverschlüsselung	Wählen Sie **Ein** (On), falls der hinzugefügt IPC verschlüsselt ist.

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

Sonstige Operationen

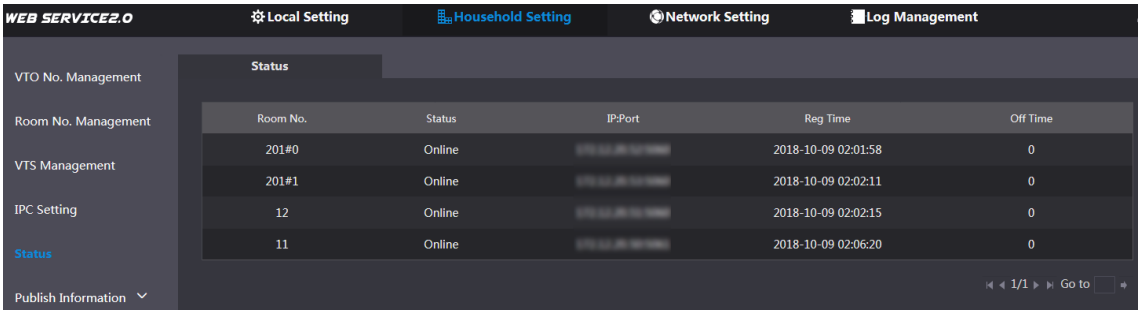
- **Export Konfig (Export Config)**: Exportieren Sie die Geräteinformationen auf Ihren PC.
- **Import Konfig (Import Config)**: Importieren Sie Geräteinformationen.

5.5 Status

Sie können den Online-Status und die IP-Adressen aller angeschlossenen Geräte anzeigen.

Melden Sie sich auf der Weboberfläche des SIP-Servers an und wählen Sie dann **Haushaltseinstellung > Status** (Household Setting > Status).

Abbildung 5-13 Status



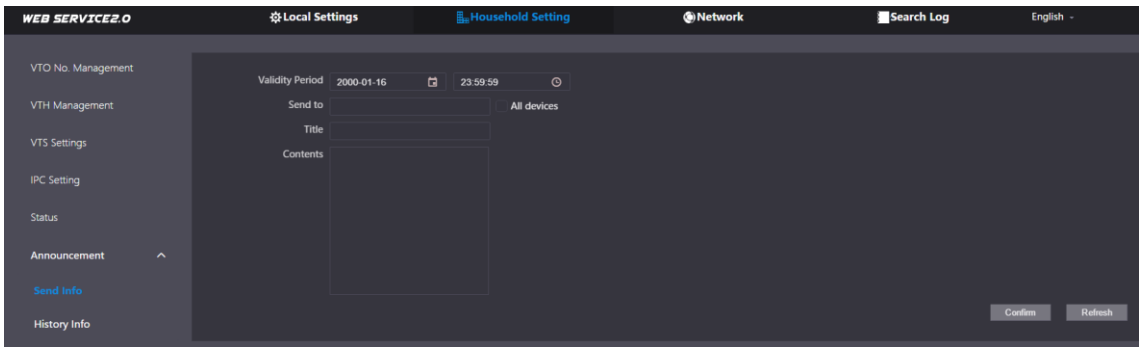
5.6 Info veröffentl

Sie können Nachrichten vom SIP-Server an VTH-Geräte senden und den Nachrichtenverlauf anzeigen.

5.6.1 Info senden

Schritt 1: Melden Sie sich an der Weboberfläche des SIP-Servers an und wählen Sie dann **Haushaltseinstellung > Informationen veröffentlichen > Informationen senden** (Household Setting > Publish Information > Send Info).

Abbildung 5-14 Versandinformationen



Schritt 2: Geben Sie den **Gültigkeitszeitraum** (Validity Period) an, in dem die Nachricht gültig ist.

Schritt 3: Geben Sie die VTO- oder VTH-Nummer ein oder wählen Sie **Alle Geräte** (All devices), um die Nachricht an alle Geräte im Netzwerk zu senden. Geben Sie anschließend den Titel und den Inhalt Ihrer Nachricht ein.

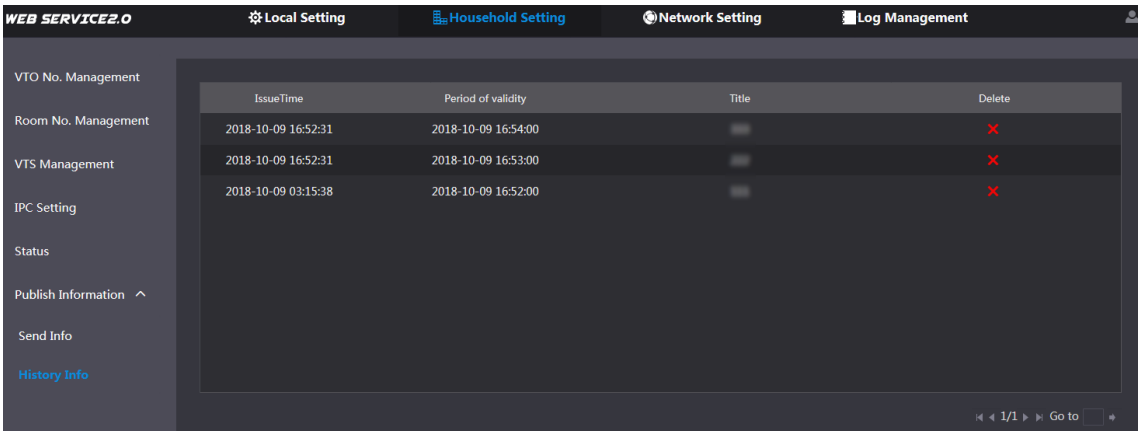
Schritt 4: Klicken Sie auf **Bestätigen** (Confirm).

5.6.2 Verlaufsdaten

Sie können die Informationen gesendeter Nachrichten einsehen.

Melden Sie sich an der Weboberfläche des SIP-Servers an und wählen Sie **Haushaltseinstellung > Informationen veröffentlichen > Verlaufsdaten** (Household Setting > Publish Information > History Info).

Abbildung 5-15 Verlaufsdaten



6 Netzwerk

Dieses Kapitel stellt vor, wie die Netzwerkparameter konfiguriert werden.

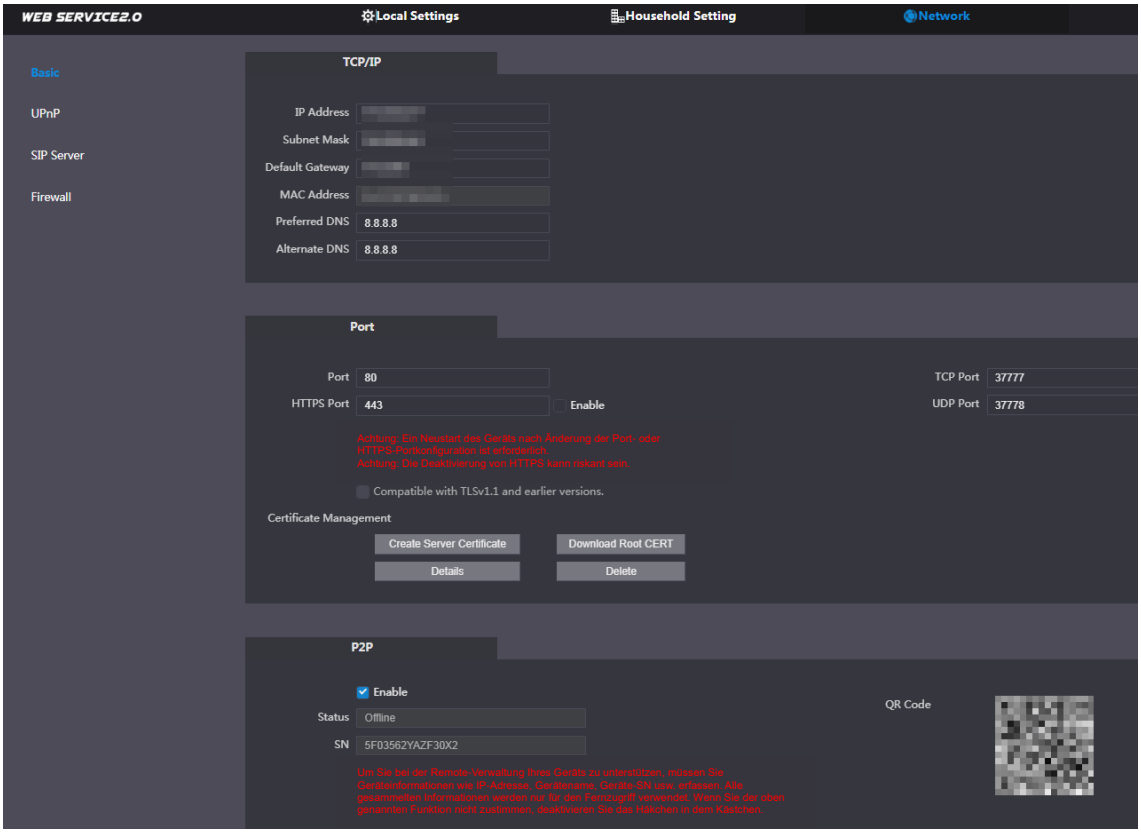
6.1 Allgemein

6.1.1 TCP/IP

Sie können IP-Adresse, Subnetzmaske, Standard-Gateway und DNS der VTO ändern.

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

Abbildung 6-1 TCP/IP und Port



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

Die VTO wird neu gestartet. Sie müssen beim erneuten Anmelden die IP-Adresse Ihres PCs auf dasselbe Netzwerksegment ändern wie das der VTO.

6.1.2 Port

Tabelle 6-1 Beschreibung der Parameter

Parameter	Beschreibung
Port	80 ist Standard. Falls dieser bereits verwendet wird, können Sie wie erforderlich eine Nummer von 1025 bis 65535 wählen. Sie können *http://VTO IP address:Port* zur Anmeldung am VTO eingeben.

Parameter	Beschreibung
HTTPS-Port	Aktivieren Sie es und klicken Sie auf **Speichern** (Save). Nun können Sie *https://VTO IP address:HTTPS Port* zur Anmeldung an der VTO eingeben.
TCP/UDP-Port	Dient dem Zugreifen auf die VTO mit Geräten in anderen Netzwerken. Siehe „6.2 UPnP“ für Details.
Server-Zertifikat erstellen	Die eindeutige digitale Kennung der VTO für das SSL-Protokoll. Bei erstmaliger Verwendung oder nach Änderung der IP-Adresse der VTO müssen Sie diesen Vorgang erneut durchlaufen. ⚠ Wenn Sie das Zertifikat, das erstellt wurde, löschen, kann dies nicht rückgängig gemacht werden.
Stammzertifikat herunterladen	Wenn Sie einen PC verwenden, der sich niemals an der VTO angemeldet hat, müssen Sie das Stammzertifikat herunterladen und es zum Installieren doppelt anklicken. Anschließend können Sie die oben erwähnte HTTPS-Funktion nutzen. ⚠ Wenn Sie das Zertifikat, das installiert wurde, löschen, kann dies nicht rückgängig gemacht werden.

6.1.3 P2P

Aktivieren Sie die Funktion **P2P**. Anschließen können Sie den QR-Code mit Ihrem Telefon scannen, um die VTO der App auf Ihrem Smartphone hinzuzufügen. Einzelheiten finden Sie in der Schnellstartanleitung.

6.2 UPnP

Wenn die VTO als SIP-Server fungiert, können Sie die UPnP-Funktion so konfigurieren, dass sich WAN-Geräte an der VTO anmelden können.

Vorbereitung

- Aktivieren Sie die UPnP-Funktion am Router, konfigurieren Sie dann die WAN-IP-Adresse für den Router.
- Schließen Sie die VTO am LAN-Port des Routers an.

6.2.1 UPnP-Dienste aktivieren

Schritt 1: Wählen Sie **Netzwerk > UPnP** (Network > UPnP).
Schritt 2: Aktivieren Sie die aufgelisteten Dienste wie erforderlich.
Schritt 3: Wählen Sie **Aktivieren** (Enable).
Schritt 4: Klicken Sie auf **Speichern** (Save).

6.2.2 UPnP-Dienste hinzufügen

Schritt 1: Wählen Sie **Netzwerk > UPnP** (Network > UPnP).
Schritt 2: Klicken Sie auf **Hinzufügen** (Add).
Schritt 3: Konfigurieren Sie die Parameter wie erforderlich.

Abbildung 6-2 Einen UPnP-Dienst hinzufügen

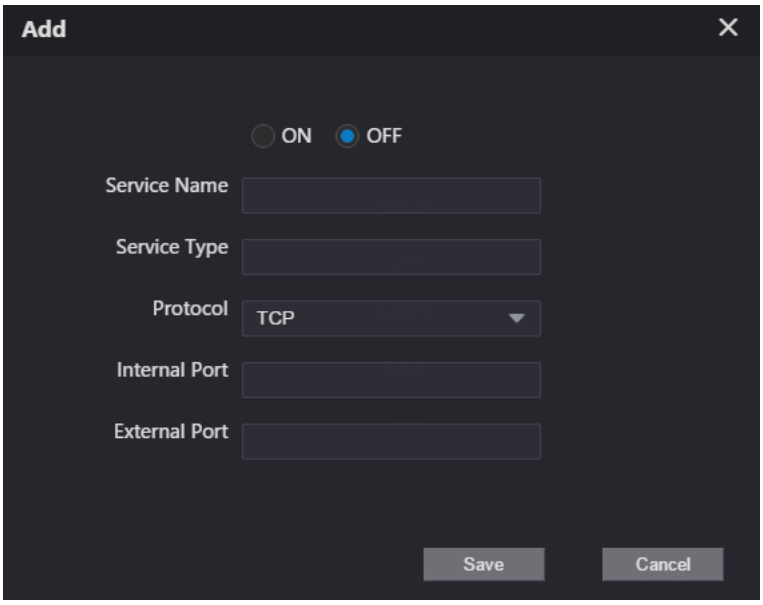


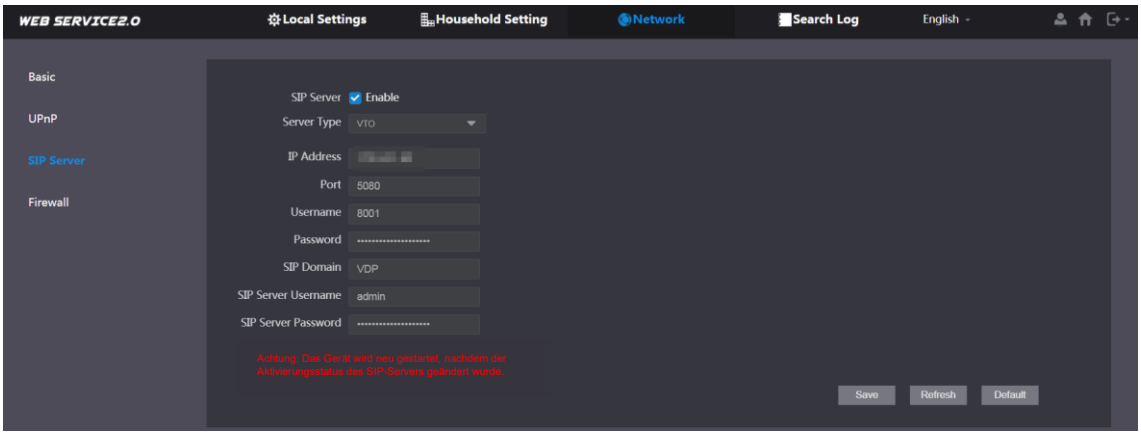
Tabelle 6-2 Beschreibung der Parameter

Parameter	Beschreibung
Dienstname	Geben Sie die Informationen wie erforderlich ein.
Diensttyp	
Protokoll	Wählen Sie **TCP** oder **UDP** wie erforderlich.
Interner Port	Nutzen Sie die Portnummer von 1024 bis 5000.
Externer Port	• Verwenden Sie zur Vermeidung von Konflikten nicht die Portnummern 1 bis 1023. • Wenn Sie diese Funktion für mehrere Geräte konfigurieren müssen, achten Sie darauf, dass die Ports nicht identisch sind. • Die von Ihnen genutzte Portnummer darf nicht belegt sein. • Interne und externe Portnummer müssen identisch sein.

6.3 SIP-Server

Im Netzwerk muss sich ein SIP-Server befinden, damit alle verbundenen VTOs und VTHs einander anrufen können. Sie können eine VTO oder andere Server als SIP-Server verwenden.
Schritt 1: Wählen Sie **Netzwerk > SIP-Server** (Network > SIP Server).

Abbildung 6-3 SIP-Server



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

- Die VTO, an der Sie sich als SIP-Server angemeldet haben:
  Aktivieren Sie **SIP-Server** (SIP Server) und klicken Sie auf **Speichern** (Save). Anschließend startet die VTO neu. Sie können dieser VTO VTOs und VTHs hinzufügen. Einzelheiten finden Sie unter „5 Haushaltseinstellung".
  Falls die VTO, an der Sie sich angemeldet haben, nicht als SIP-Server fungiert, sollten Sie **SIP-Server** (SIP Server) nicht aktivieren. Andernfalls schlägt die Verbindung fehl.
- Falls eine andere VTO als SIP-Server fungiert:
  Aktivieren Sie **SIP-Server** (SIP Server) nicht. Setzen Sie **Server-Typ** (Server Type) auf **VTO,** konfigurieren Sie die Parameter und klicken Sie dann auf **Speichern** (Save).

Tabelle 6-3 SIP-Serverkonfiguration

Parameter	Beschreibung
IP-Adr.	VTO-IP-Adresse.
Port	• 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 der VTO zur Anmeldung an der Weboberfläche.
SIP-Server-Passwort	

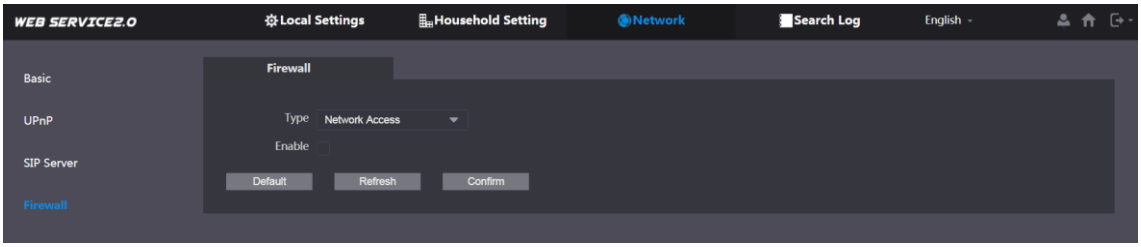
- Wenn andere Server als SIP-Server fungieren:
  Wählen Sie wie erforderlich **Server-Typ** (Server Type), beachten Sie dann die entsprechende Anleitung für Einzelheiten.

6.4 Firewall

Sie können verschiedene Firewall-Typen zur Steuerung des Netzwerkzugriffs auf die VTO aktivieren.

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

Abbildung 6-4 Firewall



Schritt 2: Wählen Sie eine oder mehrere Firewall-Typen und aktivieren Sie sie dann.

Schritt 3: Konfigurieren Sie die Parameter.

Tabelle 6-4 Beschreibung der Firewall-Typen

Typ	Beschreibung
Netzwerkzugriff	Wählen Sie entweder **Weißliste** (Allowlist) oder **Schwarzliste** (Blocklist) und fügen Sie dann eine IP-Adresse oder ein Segment hinzu, die/das (nicht) auf die VTO zugreifen darf.
PING verboten	Die VTO reagiert nicht auf den Ping, um Ping-Angriffe zu vermeiden.
Anti-Semijoin	Schützt die VTO-Leistung durch Blockieren übermäßiger SYN-Pakete.

7 Protokollverwaltung

Wählen Sie **Suchprotokoll** (Search Log). Sie können nach verschiedenen Protokollen suchen und diese wie erforderlich an Ihren PC exportieren.

Falls der Speicher voll ist, werden die ältesten Aufzeichnungen überschritten. Sichern Sie die Aufzeichnungen wie erforderlich.

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.