2-Draht-Switch

Benutzerhandbuch

V1.0.0

Vorwort

Allgemein

Dieses Benutzerhandbuch stellt den Aufbau und die Installation des 2-Draht-Switch (im Folgenden als „Switch“ 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

Wichtige Sicherheits- und Warnhinweise

In diesem Kapitel werden die Inhalte zum sachgerechten Umgang mit dem Switch, zur Gefahrenabwehr und zur Vermeidung von Sachschäden vorgestellt. Lesen Sie diese Inhalte vor der Benutzung des Switch aufmerksam durch, beachten Sie sie bei der Verwendung und bewahren Sie die Anleitung für späteres Nachschlagen auf.

Betriebsanforderungen

- Ändern Sie das Standard-Passwort, nachdem der Switch aktiviert wurde.
- Setzen Sie den Switch nicht direkter Sonneneinstrahlung oder einer Wärmequelle aus.
- Setzen Sie den Switch nicht Nässe oder Staub aus.
- Installieren Sie den Switch eben oder an einem stabilen Ort, damit er nicht herunterfallen kann.

- Lassen Sie keine Flüssigkeit auf den Switch tropfen oder spritzen und stellen Sie keine mit Flüssigkeit gefüllten Gegenstände auf den Switch.
- Installieren Sie den Switch an einem gut belüfteten Ort und blockieren Sie die Lüftungsöffnungen nicht.
- Verwenden Sie den Switch innerhalb des Nennbereichs, der Leistungsaufnahme und -ausgabe.
- Nehmen Sie das Gerät nicht selbst auseinander.
- Verwenden Sie das mitgelieferte Netzgerät.
- Lesen und verstehen Sie den Aufbau, bevor Sie Kabel anschließen. Siehe „2 Aufbau“ für Details.
- Vergewissern Sie sich vor dem Einschalten, dass alle Kabel korrekt angeschlossen sind.
- Wenn nach dem Einschalten die Betriebsanzeige dauerhaft rot leuchtet und die RUN-Anzeige grün blinkt, arbeitet der Switch ordnungsgemäß.
- Vergewissern Sie sich vor dem Abziehen des Netzkabels, dass der Netzschalter auf „AUS“ steht.
- Für eine optimale Leistung muss bei einer Kaskadierung mehrerer Switches nur der erste Switch mit dem Ethernet verbunden werden.
- Montieren Sie die Switche nicht übereinander.

Anforderungen an die Stromversorgung

- Der Switch muss mit Stromkabeln betrieben werden, die den örtlichen Anforderungen entsprechen und innerhalb ihrer Nenndaten liegen.
- Verwenden Sie das mit dem Switch gelieferte Netzteil, anderenfalls kann es zu Verletzungen und Schäden am Gerät kommen.
- Verwenden Sie ein Netzteil, das den SELV-Anforderungen (Safety Extra Low Voltage) entspricht, und schließen Sie es an einer Nennspannung gemäß IEC60950-1 an. Die spezifischen Anforderungen an die Stromversorgung finden Sie auf dem Etikett des Switch.
- Verwenden Sie für Geräte vom Typ I eine geerdete Steckdose.
- Der Gerätestecker ist die Trennvorrichtung. Der Stecker muss während des Betriebs jederzeit frei zugänglich sein, wenn Sie ihn verwenden.

Inhaltsverzeichnis

1 Beschreibung

1.1 Produktübersicht

Der Switch verfügt über einen 2-Draht-P-Port, zwei 2-Draht-Kaskadierungs-Ports und zwei RJ-45-Ports. Sie können bis zu 10 Switches miteinander verbinden, um bis zu 200 Geräte in das Netzwerk zu bringen. Dies ist für eine Wohnanlage geeignet, in der es viele Mieter gibt. Wenn sie über den Switch mit dem Netzwerk verbunden sind, können 2-Draht-Innenraummonitore (VTH) Anrufe tätigen, Türen entriegeln und überwachen.

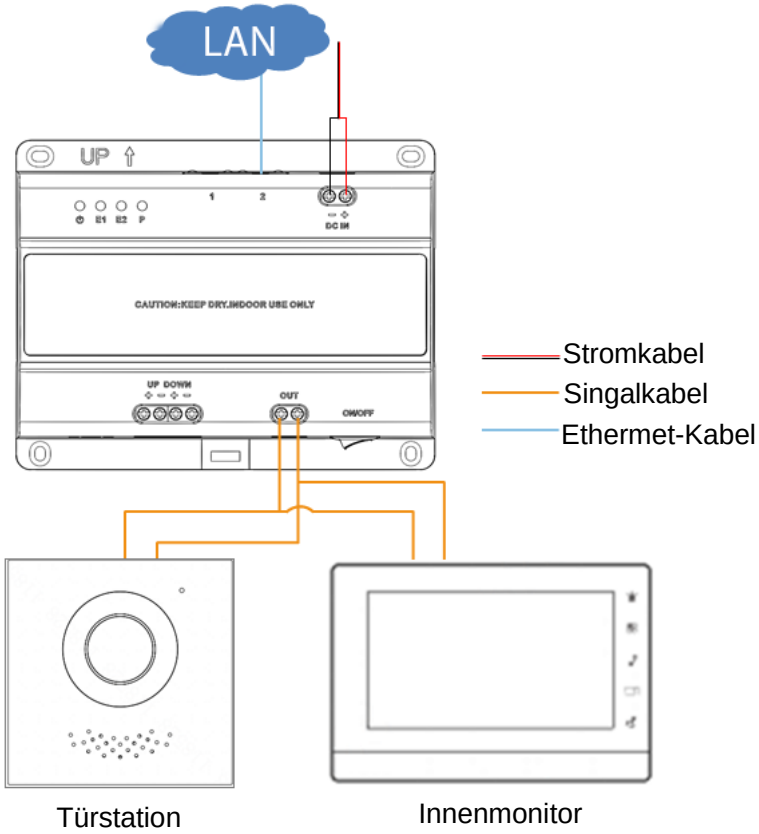
1.2 Anwendung

An einen einzigen 2-Draht-Switch können maximal 20 VTHs und 2 Türstationen (VTOs) angeschlossen werden. Basierend auf der Gesamtzahl der Geräte haben wir Einfamilienhaus und Wohnung.

Einfamilienhaus

Wenn es nicht mehr als 20 VTHs und 2 VTOs gibt, können sie am selben Switch angeschlossen werden.

Abbildung 1-1 Einfamilienhaus Netzwerkdiagramm

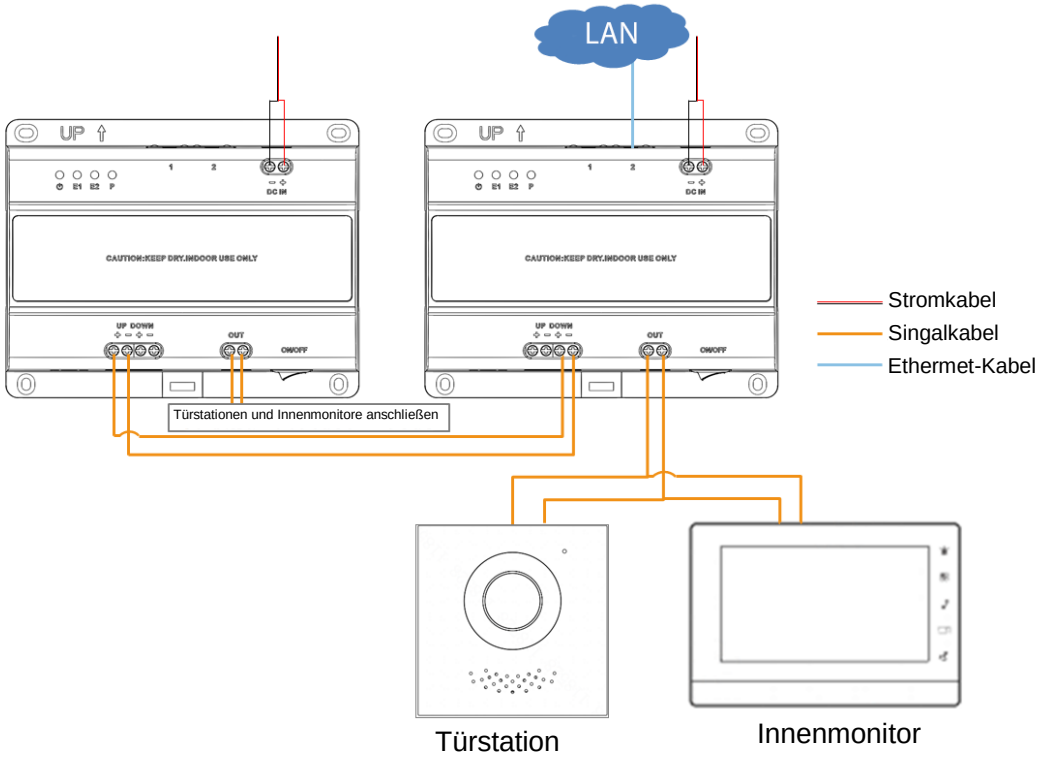


Wohnung

Wenn mehr als 20 VTHs und 2 VTOs vorhanden sind, benötigen Sie mehr als einen Switch, um sie alle mit dem Netzwerk zu verbinden. Verwenden Sie die 2-Draht-Kaskadierungs-Ports oder RJ-45-Ports, um die Switches nach Bedarf zu verbinden und achten Sie darauf, dass alle Switches mit demselben Netzwerk verbunden sind. Nehmen Sie die Kaskadierung mit den 2-Draht-Kaskadierungs-Ports als Beispiel.

Der Kabelanschluss bei der Kaskadierung mit RJ-45-Ports ist derselbe wie beim Einfamilienhaus.

Abbildung 1-2 Netzwerkdiagramm Wohnung mit 2-Draht-Kaskadierungs-Ports



Beachten Sie bei der Auswahl der korrekten Signalkabel für die Anzahl der Geräte die folgende Anleitung:

R (Gesamtwiderstand) = 6 V/die Anzahl der VTHs/0,1 A (der durchschnittliche Strom für jeden VTH)

Zum Beispiel muss der Gesamtwiderstand der Kabel für 5 VTHs kleiner als 6 V/5/0,1 A = 12 Ω sein.

Tabelle 1-1 Verwendung verschiedener Kabel

Kabeltyp für Kaskadierung	**Unterstützte Geräteanzahl**	**Maximale Entfernung**
2-adriges Kabel 4-adriges Kabel	20 VTHs und 2 VTOs.	50 m: ● Zwischen 2 Switches. ● Zwischen 1 Switch und 1 VTH/VTO.
Ethernetkabel	12 VTHs und 2 VTOs.	● 50 m. Zwischen 2 Switches. ● 30 m. Zwischen Switch und VTO, wenn nur 1 VTO vorhanden ist. ● 5 m und 30 m. Der Abstand zwischen den 2 VTOs und dem Switch.

⚠

Wenn Sie mehrere Switches verwenden, achten Sie darauf, dass jeder Switch mindestens 3 m von den anderen entfernt ist.

2 Aufbau

2.1 Frontblende

Abbildung 2-1 Aufbau der Frontplatte

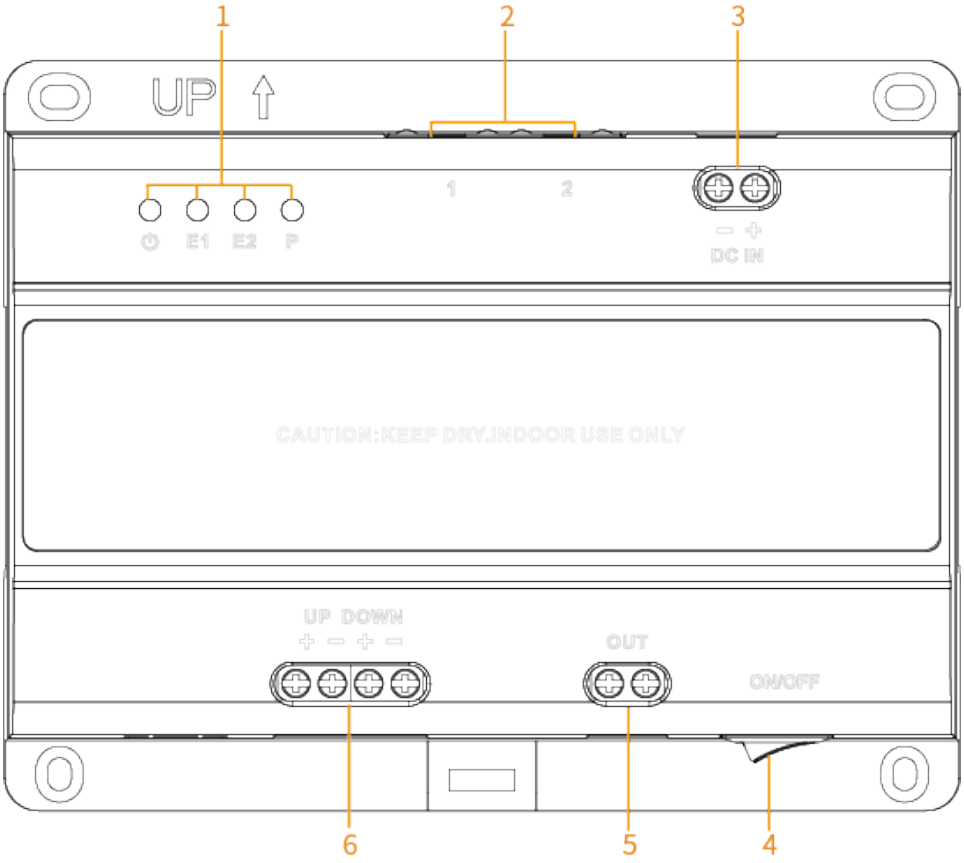


Tabelle 2-1 Aufbau

Nr.	Teil	Beschreibung
1	Anzeige	Von links nach rechts: • STROMVERSORGUNG. ◇ Rot: Eingeschaltet. ◇ Aus: Kein Strom. • E1. ◇ Blinkt grün: Das Gerät ist ordnungsgemäß mit dem Uplink-Port verbunden. ◇ Grün leuchtend: Kein Signal vom Uplink-Port. ◇ Aus: Das Gerät ist ausgeschaltet oder hat eine Fehlfunktion. • E2. ◇ Blinkt grün: Das Gerät ist ordnungsgemäß mit dem Downlink-Port verbunden. ◇ Grün leuchtend: Kein Signal vom Downlink-Port. ◇ Aus: Das Gerät ist ausgeschaltet oder hat eine Fehlfunktion. • P. ◇ Blinkt grün: Empfangenes PLC-Signal, dass entweder VTH oder VTO ordnungsgemäß am Switch angeschlossen ist. ◇ Grün leuchtend: Alle VTHs und VTOs sind nicht ordnungsgemäß angeschlossen. ◇ Aus: Die Geräte sind ausgeschaltet oder haben eine Fehlfunktion.
2	Netzwerk	2 RJ-45-Ports.
3	Stromanschluss	Verwenden Sie eine 48-V/DC-Stromversorgung.
4	AUS/EIN	Netzschalter.
5	2-Draht-Ports	Schließen Sie bis zu 20 VTHs und 2 VTOs ohne positive oder negative Pole an.
6	Uplink- und Downlink-Anschlüsse	• UPLINK. Verbinden Sie den positiven Pol mit dem des Downlink-Port des vorherigen Switch, Gleiches gilt für den negativen Pol. • DOWNLINK. Verbinden Sie den positiven Pol mit dem des Uplink-Port des nachfolgenden Switch, Gleiches gilt für den negativen Pol. Unter bestimmten Bedingungen können diese beiden Ports mit dem EOC-Port einer VTO verbunden werden; Sie müssen ebenfalls die beiden positiven Pole miteinander verbinden und Gleiches gilt für die negativen Pole.

Schalten Sie den Switch vor dem Anschließen von Kabeln aus, um Schäden zu vermeiden.

2.2 Geräterückseite

Abbildung 2-2 Aufbau der Rückwand

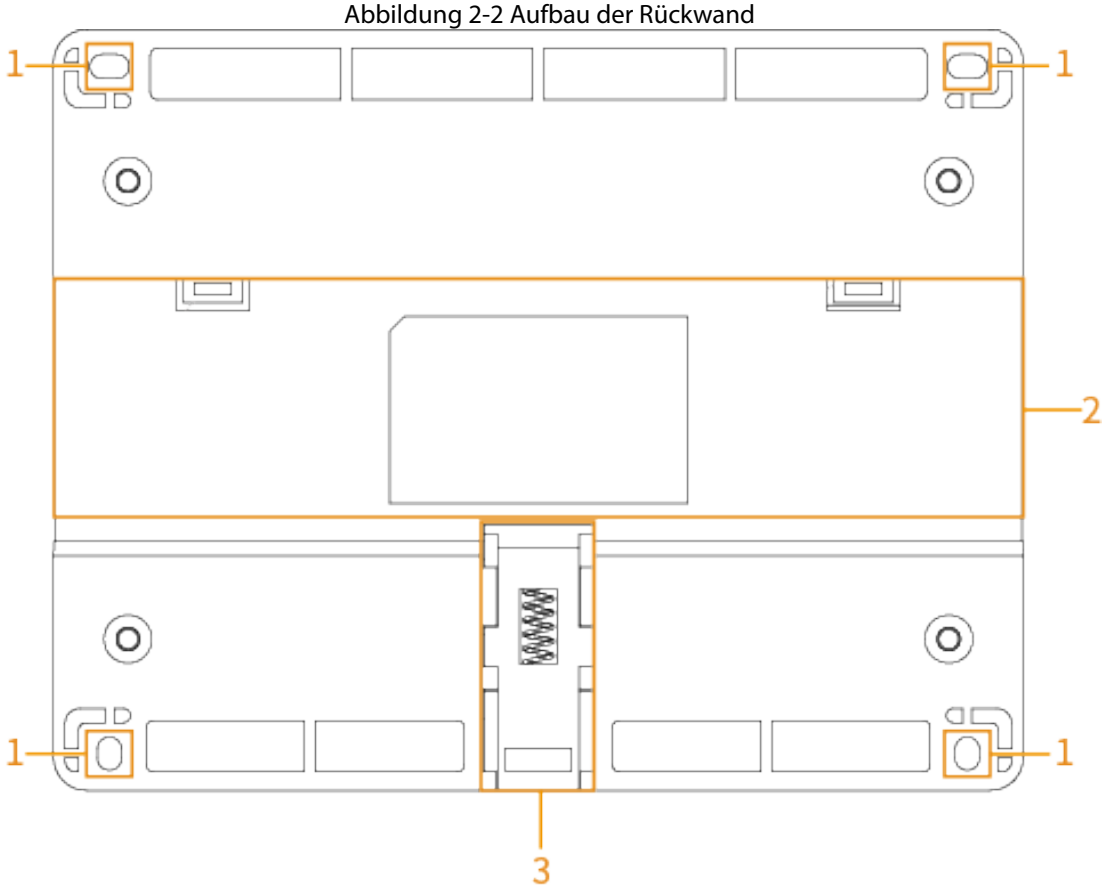


Tabelle 2-2 Aufbau

Nr.	Teil	Beschreibung
1	Schraubenlöcher	Verwenden Sie vier ST3 × 18-SUS, um den Switch zu installieren. Siehe „4.1 Installation mit Schrauben“.
2	Hutschiene	Verwenden Sie eine Hutschiene, um den Switch zu installieren. Siehe „4.2 Installaion mit Hutschiene“.
3	Unterer Haken	Montieren Sie den Switch mit einer 35mm Hutschiene.

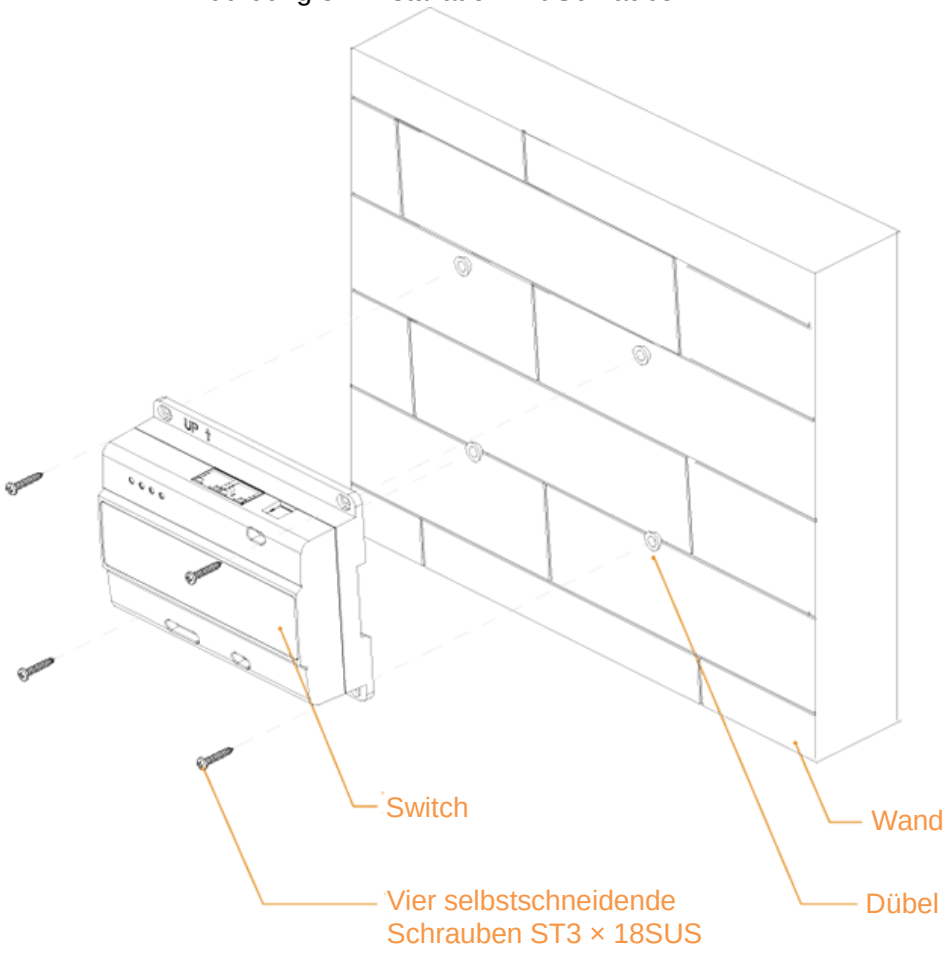
3 Montage

In diesem Kapitel erfahren Sie, wie Sie den Switch mit Schrauben oder einer Hutschiene an der Wand montieren.

3.1 Installation mit Schrauben

Verwenden Sie Schrauben, um den Switch an einer geeigneten Stelle an der Wand zu befestigen.

Abbildung 3-1 Installation mit Schrauben



3.2 Installation mit Hutschiene

Vorbereitung

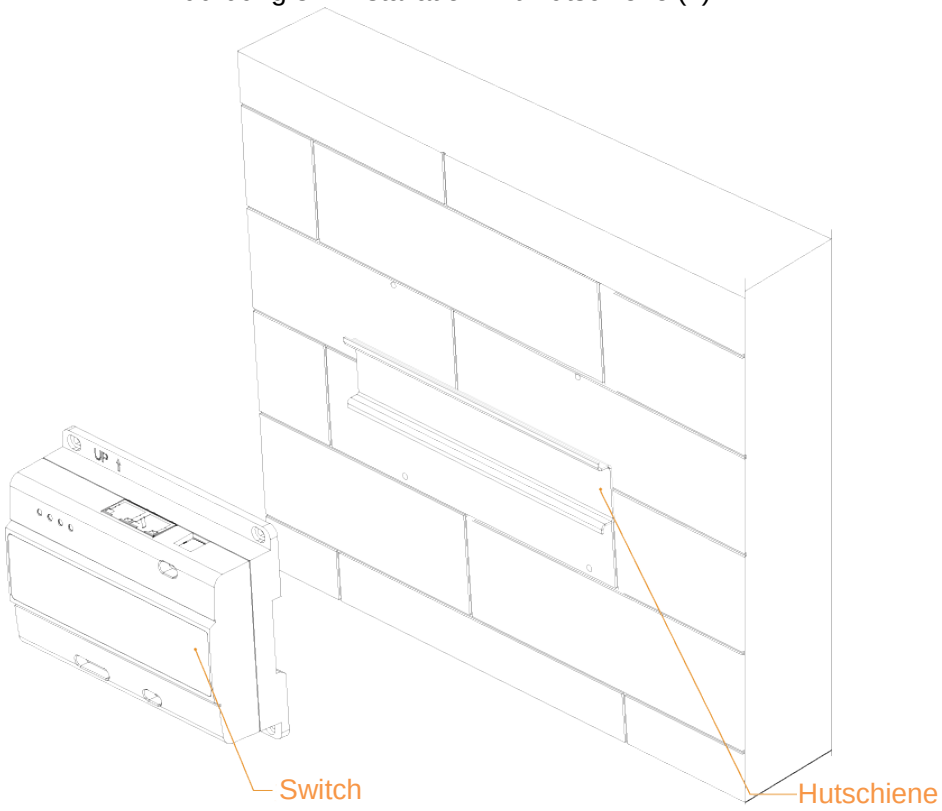
Bereiten Sie eine Standard-35-mm-Hutschiene vor.

Der Switch wird nicht mit einer Hutschiene geliefert.

Vorgehensweise

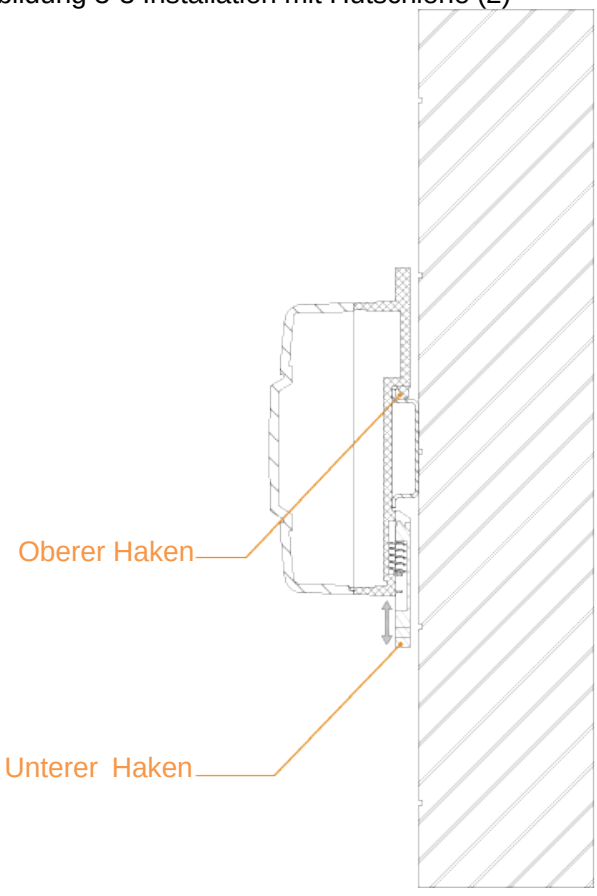
Schritt 1: Befestigen Sie die Hutschiene an einer geeigneten Stelle an der Wand.

Abbildung 3-2 Installation mit Hutschiene (1)



Schritt 1: Hängen Sie die oberen Haken in den Schlitz der Hutschiene ein.
Schritt 2: Ziehen Sie den unteren Haken nach unten und drücken Sie den Switch an die Führungsschiee an.
Schritt 3: Lassen Sie den unteren Haken los.

Abbildung 3-3 Installation mit Hutschiene (2)



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.