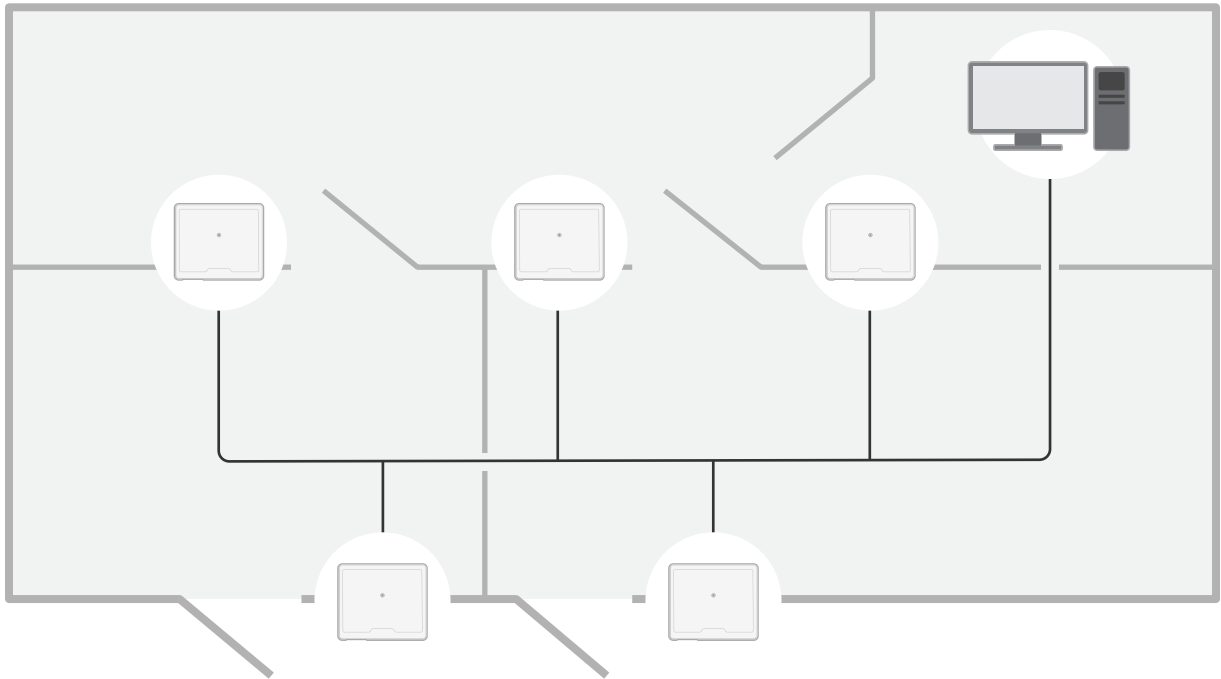


**AXIS A1210 Network Door Controller**

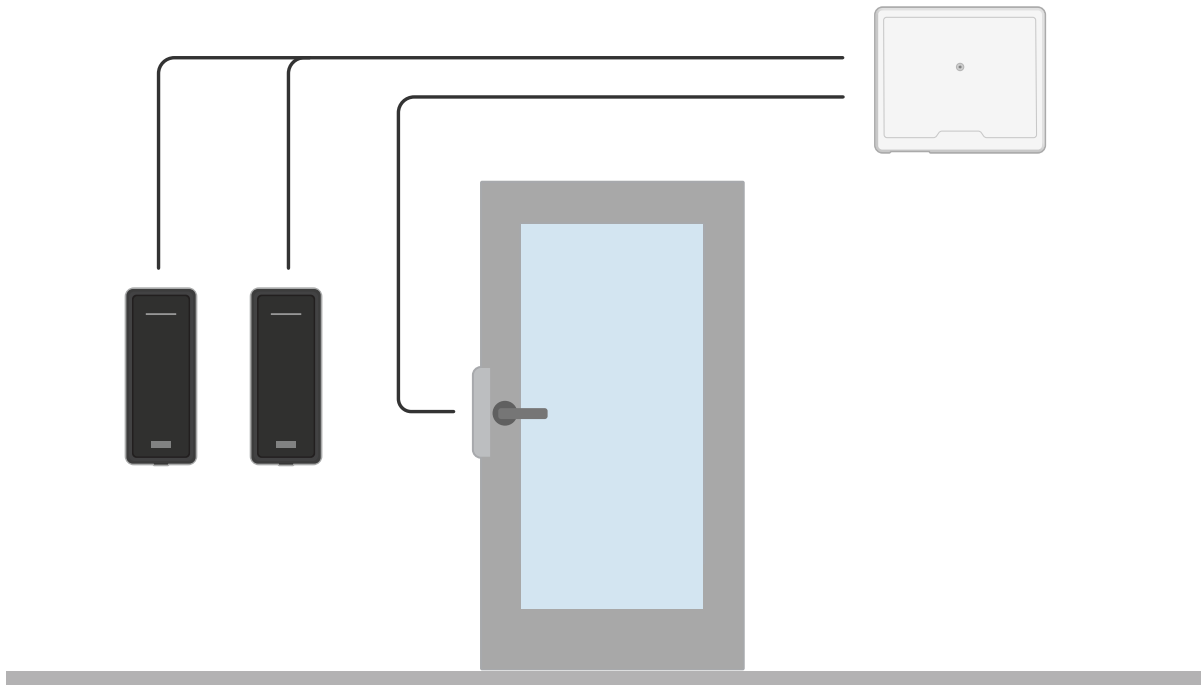
**AXIS A1210-B Network Door Controller**

<b>Lösungsübersicht</b> .....	3
<b>Installation</b> .....	5
<b>Erste Schritte</b> .....	6
Das Gerät im Netzwerk ermitteln .....	6
Weboberfläche des Geräts öffnen .....	6
Erstellen Sie ein Administratorenkonto .....	6
Sichere Kennwörter .....	6
Stellen Sie sicher, dass keiner die Firmware manipuliert hat. ....	7
Übersicht über die Weboberfläche .....	7
<b>Ihr Gerät konfigurieren</b> .....	8
<b>Die Weboberfläche</b> .....	9
Status .....	9
Zutrittskontrolle .....	10
System .....	10
Wartung .....	20
<b>Weitere Informationen</b> .....	22
Cybersicherheit .....	22
<b>Technische Daten</b> .....	23
Produktübersicht .....	23
LED-Anzeigen .....	23
Tasten .....	24
Anschlüsse .....	24
<b>Fehlerbehebung</b> .....	31
Zurücksetzen auf die Werkseinstellungen .....	31
Firmware-Optionen .....	31
Aktuelle Firmware überprüfen .....	31
Firmware aktualisieren .....	31
Technische Fragen, Hinweise und Lösungen .....	32
Support .....	33

### Lösungsübersicht



Der Netzwerk-Türcontroller kann einfach an ein bestehendes IP-Netzwerk angeschlossen und darüber mit Strom versorgt werden. Besondere Kabel sind nicht erforderlich.



Netzwerk-Türcontroller sind mit intelligenten Funktionen ausgestattete Geräte, die einfach in Türnähe angebracht werden können. Sie können bis zu zwei Lesegeräte mit Strom versorgen und steuern.

### Installation



Rufen Sie zur Wiedergabe dieses Videos die Webversion dieses Dokuments auf.

*[help.axis.com/?&pid=74266&section=solution-overview](http://help.axis.com/?&pid=74266&section=solution-overview)*

### Erste Schritte

#### Das Gerät im Netzwerk ermitteln

Mit AXIS IP Utility und AXIS Device Manager die Axis Geräte im Netzwerk ermitteln und ihnen unter Windows® IP-Adressen zuweisen. Beide Anwendungen sind kostenlos und können von [axis.com/support](http://axis.com/support) heruntergeladen werden.

Weitere Informationen zum Zuweisen von IP-Adressen finden Sie unter *Zuweisen von IP-Adressen und Zugreifen auf das Gerät*.

#### Unterstützte Browser

Das Gerät kann mit den folgenden Browsern verwendet werden:

	Chrome™	Firefox®	Edge™	Safari®
Windows®	empfohlen	empfohlen	✓	
macOS®	empfohlen	empfohlen	✓	✓
Linux®	empfohlen	empfohlen	✓	
Andere Betriebssysteme	✓	✓	✓	✓*

\*Um die Weboberfläche von AXIS OS mit iOS 15 oder iPadOS 15 zu verwenden, deaktivieren Sie unter **Settings (Einstellungen) > Safari > Advanced (Erweitert) > Experimental Features (Experimentelle Funktionen)** die Option *NSURLSession Websocket*.

Weitere Informationen zu empfohlenen Browsern finden Sie im *AXIS OS Portal*.

#### Weboberfläche des Geräts öffnen

1. Öffnen Sie einen Browser und geben Sie die IP-Adresse oder den Host-Namen des Axis Geräts in die Adresszeile des Browsers ein.  
Wenn Sie die IP-Adresse nicht gehen, ermitteln Sie das Gerät im Netzwerk mithilfe von AXIS IP Utility oder AXIS Device.
2. Geben Sie den Benutzernamen und das Kennwort ein. Wenn Sie zum ersten Mal auf das Gerät zugreifen, müssen Sie ein Administratorkonto erstellen. Siehe *Erstellen Sie ein Administratorkonto auf Seite 6*.

#### Erstellen Sie ein Administratorkonto

Beim ersten Anmelden an Ihrem Gerät muss ein Administratorkonto erstellt werden.

1. Einen Benutzernamen eingeben.
2. Geben Sie ein Kennwort ein. Siehe *Sichere Kennwörter auf Seite 6*.
3. Geben Sie das Kennwort erneut ein.
4. Klicken Sie auf **Add user (Benutzer hinzufügen)**.

#### Wichtig

Das Gerät verfügt über kein Standardkonto. Wenn Sie das Kennwort für Ihr Administratorkonto verloren haben, müssen Sie das Gerät zurücksetzen. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 31*.

### Sichere Kennwörter

#### Wichtig

Das voreingestellte Kennwort wird vom Axis Gerät unverschlüsselt über das Netz gesendet. Um das Gerät zu schützen, nach dem ersten Anmelden eine sichere und verschlüsselte HTTPS-Verbindung einrichten und dann das Kennwort ändern.

Das Gerätekennwort ist der Hauptschutz für Ihre Daten und Dienste. Produkte von Axis geben keine Kennwortrichtlinien vor, da die Produkte unter den verschiedensten Bedingungen eingesetzt werden.

Doch zum Schutz Ihrer Daten empfehlen wir dringend:

- Ein Kennwort zu verwenden, das aus mindestens acht Zeichen besteht, und das bevorzugt von einem Kennwortgenerator erzeugt wurde.
- Das Kennwort geheimzuhalten.
- Das Kennwort regelmäßig und mindestens jährlich zu ändern.

### Stellen Sie sicher, dass keiner die Firmware manipuliert hat.

So stellen Sie sicher, dass das Gerät über seine ursprüngliche Firmware von Axis verfügt, bzw. übernehmen nach einem Sicherheitsangriff die volle Kontrolle über das Gerät:

1. Zurücksetzen auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 31*.  
Nach dem Zurücksetzen gewährleistet Secure Boot den Status des Geräts.
2. Konfigurieren und installieren Sie das Gerät.

### Übersicht über die Weboberfläche

In diesem Video erhalten Sie einen Überblick über die Weboberfläche des Geräts.



Rufen Sie zur Wiedergabe dieses Videos die Webversion dieses Dokuments auf.

[help.axis.com/?&pid=74266&section=web-interface-overview](http://help.axis.com/?&pid=74266&section=web-interface-overview)

*Weboberfläche des Axis Geräts*

## Ihr Gerät konfigurieren

---

### Ihr Gerät konfigurieren

Informationen zur Konfiguration Ihres Geräts finden Sie im *AXIS Camera Station Benutzerhandbuch* oder in Lösungen von Drittanbietern.















## Die Weboberfläche

Um die Weboberfläche des Geräts aufzurufen, müssen Sie die IP-Adresse des Geräts in einen Webbrowser eingeben.

### Hinweis

Die in diesem Abschnitt beschriebenen Funktionen und Einstellungen werden von Gerät zu Gerät unterschiedlich unterstützt.

Dieses Symbol  zeigt an, dass die Funktion oder Einstellung nur für einige Geräte verfügbar ist.

-  Hauptmenü anzeigen oder ausblenden.
-  Zugriff auf die Versionshinweise.
-  Auf die Hilfe zum Produkt zugreifen.
-  Die Sprache ändern.
-  Helles oder dunkles Design einstellen.
-    Das Benutzermenü enthält:
  - Informationen zum angemeldeten Benutzer.
  -  **Change account (Konto wechseln)**: Melden Sie sich vom aktuellen Konto ab und melden Sie sich bei einem neuen Konto an.
  -  **Log out (Abmelden)**: Melden Sie sich vom aktuellen Konto ab.
-  Das Kontextmenü enthält:
  - **Analytics data (Analysedaten)**: Stimmen Sie der Teilung nicht personenbezogener Browserdaten zu.
  - **Feedback**: Teilen Sie Feedback, um Ihr Benutzererlebnis zu verbessern.
  - **Rechtliches**: Lassen Sie sich Informationen zu Cookies und Lizenzen anzeigen.
  - **Info**: Lassen Sie sich Geräteinformationen anzeigen, einschließlich Firmwareversion und Seriennummer.
  - **Legacy device interface (Frühere Benutzeroberfläche)**: Wechseln Sie zur früheren Weboberfläche des Geräts.

## Status

### Zeitsynchronisierungsstatus

Zeigt Informationen zur NTP-Synchronisierung an, z. B. ob das Gerät mit einem NTP-Server synchronisiert ist und wie lange es noch bis zur nächsten Synchronisierung dauert.

**NTP settings (NTP-Einstellungen)**: Anzeigen und Aktualisieren der NTP-Einstellungen. Klicken Sie darauf, um zur Seite **Date and time (Datum und Uhrzeit)** zu wechseln, auf der Sie die NTP-Einstellungen ändern können.

### Geräteinformationen

Zeigt die Geräteinformationen an, einschließlich Firmwareversion und Seriennummer.

**Upgrade firmware (Firmwareaktualisierung):** Aktualisieren Sie die Firmware auf Ihrem Gerät. Klicken Sie darauf, um zur Wartungsseite zu gehen, auf der Sie eine Firmwareaktualisierung durchführen können.

## Zutrittskontrolle

### Alarmer

**Device motion (Gerätebewegung):** Aktivieren Sie diese Option, um einen Alarm in Ihrem System auszulösen, wenn eine Bewegung der Tür-Steuerung erkannt wird.

**Casing open (Gehäuse geöffnet):** Aktivieren Sie diese Option, um einen Alarm in Ihrem System auszulösen, wenn ein geöffnetes Gehäuse der Tür-Steuerung erkannt wird. Deaktivieren Sie diese Einstellung für Barebone-Türsteuerungen.

**External tamper (Externe Manipulation):** Aktivieren Sie diese Option, um bei erkannter externer Manipulation einen Alarm in Ihrem System auszulösen. Zum Beispiel, wenn jemand den externen Schrank öffnet oder schließt.

- **Supervised input (Überwacher Eingang):** Aktivieren Sie den Eingangsstatus des Monitors und konfigurieren Sie die Abschlusswiderstände.
  - Um die parallele erste Verbindung zu verwenden, wählen Sie **Parallele erste Verbindung mit parallelem Widerstand (22 22 K $\Omega$ ) und seriellem Widerstand (4,7 22 K $\Omega$ )**.
  - Wählen Sie für eine Serienschaltung Sie **Serienschaltung** und in der Auswahlliste **Widerstandswerte** einen Widerstandswert.

### Peripheriegeräte

**Upgrade readers (Leser aktualisieren):** Klicken Sie hier, um Leser auf eine neue Firmware-Version zu aktualisieren. Diese Funktion kann unterstützte Leser nur aktualisieren, wenn sie online sind.

## System

### Uhrzeit und Standort

#### Datum und Uhrzeit

Das Zeitformat hängt von den Spracheinstellungen des Webbrowsers ab.

#### Hinweis

Wir empfehlen Ihnen, Datum und Uhrzeit des Geräts mit einem NTP-Server zu synchronisieren.

**Synchronization (Synchronisierung):** Wählen Sie eine Option zur Synchronisierung von Datum und Uhrzeit des Geräts aus.

- **Automatic date and time (manual NTS KE servers) (Datum und Uhrzeit automatisch (manuelle NTS-KE-Server)):** Diese Option führt eine Synchronisierung mit den sicheren NTP-Schlüssel-Servern durch, die mit dem DHCP-Server verbunden sind.
  - **Manual NTS KE servers (Manuelle NTS-KE-Server):** Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.
- **Automatic date and time (NTP servers using DHCP) (Datum und Uhrzeit automatisch (NTP-Server mit DHCP)):** Synchronisieren Sie das Gerät mit den NTP-Servern, die mit dem DHCP-Server verbunden sind.
  - **Fallback NTP servers (NTP-Reserve-Server):** Geben Sie die IP-Adresse eines oder zweier Reserve-Server ein.
- **Automatic date and time (manual NTP servers) (Datum und Uhrzeit automatisch (manuelle NTP-Server)):** Führen Sie eine Synchronisierung mit NTP-Servern Ihrer Wahl durch.
  - **Manual NTP servers (Manuelle NTP-Server):** Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.

- **Benutzerdefinierte Datum und Uhrzeit:** Stellen Sie Datum und Uhrzeit manuell ein. Klicken Sie auf **Get from system (Vom System abrufen)**, um die Datums- und Uhrzeiteinstellungen einmalig von Ihrem Computer oder Mobilgerät zu abrufen.

**Time zone (Zeitzone):** Wählen Sie die zu verwendende Zeitzone aus. Die Zeit wird automatisch bei Sommer- und Standardzeit angepasst.

### Hinweis

Die Einstellungen für Datum und Uhrzeit werden vom System für alle Aufzeichnungen, Protokolle und Systemeinstellungen verwendet.

## Netzwerk

### IPv4

**Assign IPv4 automatically (IPv4 automatisch zuweisen):** Wählen Sie diese Option, damit der Netzwerkrouter dem Gerät automatisch eine IP-Adresse zuweisen kann. Für die meisten Netzwerke empfehlen wir eine automatische Zuweisung der IP-Adresse (DHCP).

**IP address (IP-Adresse):** Geben Sie für das Gerät eine eindeutige IP-Adresse ein. Statische IP-Adressen können innerhalb von isolierten Netzwerken zufällig zugewiesen werden, sofern jede Adresse eindeutig ist. Zur Vermeidung von Konflikten empfehlen wir Ihnen, sich vor dem Zuweisen einer statischen IP-Adresse an den Netzwerkadministrator zu wenden.

**Subnet mask (Subnetzmaske):** Geben Sie die Subnetzmaske ein, um festzulegen, welche Adressen sich im lokalen Netzwerk befinden. Jede Adresse außerhalb des lokalen Netzwerks wird über den Router geleitet.

**Router:** Geben Sie die IP-Adresse des Standardrouters (Gateway) ein, um Geräten zu verbinden, die in verschiedenen Netzwerken und Netzwerk-Segmenten verwendet werden.

**Fallback to static IP address if DHCP isn't available (Fallback zu statischer IP-Adresse, wenn DHCP nicht verfügbar ist):** Wählen Sie aus, ob Sie eine statische IP-Adresse hinzufügen möchten, die als Reserve verwendet werden soll, wenn DHCP nicht verfügbar ist und keine IP-Adresse automatisch zugewiesen werden kann.

### Hinweis

Wenn DHCP nicht verfügbar ist und das Gerät eine statische Fallback-Adresse verwendet, wird die statische Adresse mit einem begrenzten Bereich konfiguriert.

### IPv6

**IPv6 automatisch zuweisen:** Wählen Sie diese Option, um IPv6 einzuschalten und damit der Netzwerk-Router dem Gerät automatisch eine IP-Adresse zuweisen kann.

### Host-Name

**Assign hostname automatically (Host-Namen automatisch zuweisen):** Wählen Sie diese Option aus, damit der Netzwerkrouter dem Gerät automatisch einen Host-Namen zuweisen kann.

**Host-Name:** Geben Sie den Host-Namen manuell ein, um ihn als alternative Möglichkeit für den Zugriff auf das Gerät zu verwenden. Der Server-Bericht und das Systemprotokoll verwenden den Host-Namen. Zugelassene Zeichen sind A-Z, a-z, 0-9 und -.

### DNS servers (DNS-Server)

**Assign DNS automatically (DNS automatisch zuweisen):** Wählen Sie diese Option, damit der DHCP-Server dem Gerät automatisch Domains für die Suche und DNS-Server-Adressen zuweisen kann. Für die meisten Netzwerke empfehlen wir eine automatische Zuweisung der DNS-Server-Adresse (DHCP).

**Search domains (Suchdomains):** Wenn Sie einen Host-Namen verwenden, der nicht vollständig qualifiziert ist, klicken Sie auf **Add search domain (Suchdomain hinzufügen)** und geben Sie eine Domain ein, in der nach dem vom Gerät verwendeten Host-Namen gesucht werden soll.

**DNS servers (DNS-Server):** Klicken Sie auf **Add DNS server (DNS-Server hinzufügen)** und geben Sie die IP-Adresse des DNS-Servers ein. Dadurch werden in Ihrem Netzwerk Host-Namen in IP-Adressen übersetzt.

### HTTP und HTTPS

HTTPS ist ein Protokoll, das Verschlüsselung für Seitenanforderungen von Benutzern und für die vom Webserver zurückgegebenen Seiten bereitstellt. Der verschlüsselte Austausch von Informationen wird durch die Verwendung eines HTTPS-Zertifikats geregelt, das die Authentizität des Servers gewährleistet.

Um HTTPS auf dem Gerät verwenden zu können, muss ein HTTPS-Zertifikat installiert werden. Gehen Sie für die Erstellung und Installation von Zertifikaten zu **System > Security (System > Sicherheit)**.

**Zugriff zulassen über:** Wählen Sie aus, ob Sie einem Benutzer erlauben wollen, eine Verbindung mit dem Gerät über die Protokolle HTTP, HTTPS oder HTTP and HTTPS (HTTP und HTTPS) herzustellen.

#### Hinweis

Wenn Sie auf verschlüsselte Internetseiten über HTTPS gehen, kann es zu Beeinträchtigungen der Leistung kommen, insbesondere wenn Sie eine Seite zum ersten Mal aufrufen.

**HTTP port (HTTP-Port):** Geben Sie den zu verwendenden HTTP-Port ein. Das Gerät lässt Port 80 oder jeden Port im Bereich 1024-65535 zu. Wenn Sie als Administrator angemeldet sind, können Sie auch einen beliebigen Port im Bereich 1-1023 eingeben. Wenn Sie einen Port in diesem Bereich verwenden, erhalten Sie eine Warnung.

**HTTPS port (HTTPS-Port):** Geben Sie den zu verwendenden HTTPS-Port ein. Das Gerät lässt Port 443 oder jeden Port im Bereich 1024-65535 zu. Wenn Sie als Administrator angemeldet sind, können Sie auch einen beliebigen Port im Bereich 1-1023 eingeben. Wenn Sie einen Port in diesem Bereich verwenden, erhalten Sie eine Warnung.

**Zertifikat:** Wählen Sie ein Zertifikat, um HTTPS für das Gerät zu aktivieren.

### Protokolle zur Netzwerkerkennung

**Bonjour®:** Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.

**Bonjour-Name:** Geben Sie den im Netzwerk anzuzeigenden Namen an. Der Standardname setzt sich aus dem Namen des Geräts und seiner MAC Adresse zusammen.

**UPnP®:** Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.

**UPnP-Name:** Geben Sie den im Netzwerk anzuzeigenden Namen an. Der Standardname setzt sich aus dem Namen des Geräts und seiner MAC Adresse zusammen.

**WS-Erkennung:** Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.

### Cloud-Anbindung mit einem Mausklick

One-Click Cloud Connect (O3C) stellt in Verbindung mit einem O3C-Dienst einen einfachen und sicheren Internetzugang zu Live-Video und aufgezeichneten Videos von jedem Standort aus bereit. Weitere Informationen finden Sie unter [axis.com/end-to-end-solutions/hosted-services](http://axis.com/end-to-end-solutions/hosted-services).

### Allow O3C (O3C zulassen):

- **One-click:** Dies ist die Standardeinstellung. Halten Sie die Steuertaste am Gerät gedrückt, um über das Internet eine Verbindung mit einem O3C-Dienst herzustellen. Sie müssen das Gerät innerhalb von 24 Stunden nach dem Drücken der Steuertaste beim O3C-Dienst registrieren. Andernfalls wird sich das Gerät vom O3C-Dienst getrennt. Nach der Registrierung des Geräts ist **Always (Immer)** aktiviert und das Gerät bleibt mit dem O3C-Dienst verbunden.
- **Immer:** Das Gerät versucht ständig, über das Internet eine Verbindung mit einem O3C-Dienst herzustellen. Nach der Registrierung bleibt das Gerät mit dem O3C-Dienst verbunden. Verwenden Sie diese Option, wenn die Steuertaste am Gerät außer Reichweite ist.
- **Nein:** Deaktiviert den O3C-Dienst.

**Proxy settings (Proxy-Einstellungen):** Geben Sie falls erforderlich die Proxyeinstellungen ein, um eine Verbindung zum Proxy-Server herzustellen.

**Host:** Geben Sie die Adresse des Proxy-Servers ein.

**Port:** Geben Sie die Nummer der für den Zugriff verwendeten Ports an.

**Anmeldung und Kennwort:** Geben Sie falls erforderlich einen Benutzernamen und ein Kennwort für den Proxyserver ein.

### Authentication method (Authentifizierungsmethode):

- **Basic (Einfach):** Diese Methode ist das am besten geeignete Authentifizierungsschema für HTTP. Sie ist nicht so sicher wie die Digest-Methode, da sie den Benutzernamen und das Kennwort unverschlüsselt an den Server sendet.
- **Digest:** Diese Methode ist sicherer, da das Kennwort hier stets verschlüsselt im Netzwerk übermittelt wird.
- **Auto:** Bei dieser Option kann das Gerät die Authentifizierungsmethode automatisch je nach unterstützten Methoden auswählen. Die Methode Digest wird gegenüber der Methode Einfach bevorzugt.

**Besitzerauthentifizierungsschlüssel (OAK):** Klicken Sie auf **Schlüssel abrufen**, um den Besitzerauthentifizierungsschlüssel abzurufen. Dies ist nur dann möglich, wenn das Gerät ohne Firewall oder Proxy mit dem Internet verbunden ist.

## SNMP

Simple Network Management Protocol (SNMP) ermöglicht die Remoteverwaltung von Netzwerk-Geräten.

**SNMP:** Wählen Sie die zu verwendende SNMP-Version.

- **v1 und v2c:**
  - **Lese-Community:** Geben Sie den Namen der Community mit ausschließlich Lesezugriff auf alle unterstützten SNMP-Objekte an. Der Standardwert ist **public (öffentlich)**.
  - **Write community (Schreib-Community):** Geben Sie den Namen der Community mit Lese- oder Schreibzugriff auf alle unterstützten SNMP-Objekte (außer schreibgeschützte Objekte) an. Der Standardwert ist **schreiben**.
  - **Traps aktivieren:** Aktivieren Sie die Option, um Trap-Berichte zu erhalten. Traps werden vom Gerät bei wichtigen Ereignissen und Statusänderungen zum Versenden von Meldungen verwendet. In der Weboberfläche können Sie Traps für SNMP v1 und v2c einrichten. Traps werden automatisch deaktiviert, wenn Sie zu SNMP v3 wechseln oder SNMP deaktivieren. Wenn Sie SNMP v3 verwenden, können Sie Traps über die Verwaltungsanwendung für SNMP v3 einrichten.
  - **Trap-Adresse:** Geben Sie die IP-Adresse oder den Host-Namen des Verwaltungsservers ein.
  - **Trap-Community:** Geben Sie die Trap-Community ein, die das Gerät zum Versenden einer Trap-Meldung an das Verwaltungssystem verwenden soll.
  - **Traps:**
    - **Kaltstart:** Versendet eine Trap-Nachricht, wenn das Gerät hochgefahren wird.
    - **Warmstart:** Versendet eine Trap-Nachricht, wenn Sie eine SNMP-Einstellung ändern.
    - **Verbindungsaufbau:** Versendet eine Trap-Meldung, wenn der Status eines Links von Down zu Up wechselt.
    - **Authentifizierung fehlgeschlagen:** Versendet eine Trap-Meldung, wenn ein Authentifizierungsversuch fehlschlägt.

### Hinweis

Alle Axis Video MIB-Traps sind aktiviert, wenn Sie SNMP v1- und v2c-Traps aktivieren. Weitere Informationen dazu finden Sie unter *AXIS OS Portal > SNMP*.

- **v3:** SNMP v3 ist eine Version mit höherer Sicherheit, die Verschlüsselung und sichere Kennwörter bereitstellt. Beim Verwenden von SNMP v3 empfehlen wir Ihnen, HTTPS zu aktivieren, da Kennwörter dann über HTTPS gesendet werden.

Dadurch wird auch verhindert, dass Unbefugte auf unverschlüsselte Traps des Typs SNMP v1 und v2c zugreifen können. Wenn Sie SNMP v3 verwenden, können Sie Traps über die Verwaltungsanwendung für SNMP v3 einrichten.

- **Kennwort für das Konto "initial"**: Geben Sie das SNMP-Kennwort für das Konto mit dem Namen "initial" ein. Obwohl das Kennwort ohne Aktivierung von HTTPS gesendet werden kann, empfehlen wir es nicht. Das Kennwort für SNMP v3 kann nur einmal und vorzugsweise dann bei aktiviertem HTTPS festgelegt werden. Nach dem Einrichten des Kennworts wird das Kennwortfeld nicht mehr angezeigt. Wenn ein neues Kennwort eingerichtet werden soll, muss das Gerät auf die Werkseinstellungen zurückgesetzt werden.

### Connected clients (Verbundene Clients)

Zeigt die Anzahl der Verbindungen und der verbundenen Clients an.

**View details (Details anzeigen)**: Anzeigen und Aktualisieren der Liste der verbundenen Clients. Die Liste zeigt IP-Adresse, Protokoll, Port und PID/Process für jeden Client an.

## Sicherheit

### Zertifikate

Zertifikate werden in Netzwerken zum Authentifizieren von Geräten verwendet. Das Gerät unterstützt zwei Zertifikattypen:

- **Client-/Serverzertifikate**  
Ein Client-/Serverzertifikat identifiziert das Axis Produkt und kann selbstsigniert oder von einer Zertifizierungsstelle (Certificate Authority, CA) ausgegeben worden sein. Ein selbstsigniertes Zertifikat bietet begrenzten Schutz und kann vor Erhalt eines CA-Zertifikats verwendet werden.
- **CA-Zertifikate**  
CA-Zertifikate werden zum Authentifizieren von Peer-Zertifikaten verwendet, um zum Beispiel die Identität eines Authentifizierungsservers zu überprüfen, wenn das Gerät mit einem durch IEEE 802.1X geschützten Netzwerk verbunden ist. Auf dem Gerät sind mehrere CA-Zertifikate vorinstalliert.

Folgende Formate werden unterstützt:

- Zertifikatsformate: .PEM, .CER und .PFX
- Formate von privaten Schlüsseln: PKCS#1 und PKCS#12

#### Wichtig


Wenn Sie das Gerät auf die Werkseinstellungen zurücksetzen, werden alle Zertifikate gelöscht. Vorinstallierte CA-Zertifikate werden neu installiert.



Die Zertifikate in der Liste filtern.




**Add certificate (Zertifikat hinzufügen)**: Klicken Sie, um ein Zertifikat hinzuzufügen.

- **More (Mehr)**  : Weitere Felder anzeigen, die Sie ausfüllen oder auswählen müssen.
- **Secure keystore (Sicherer Schlüsselspeicher)**: Wählen Sie **Secure element (Sicheres Element)** oder **Trusted Platform Module 2.0** zum sicheren Speichern des privaten Schlüssels aus. Weitere Informationen zum Wählenden sicheren Schlüsselspeicher finden Sie unter [help.axis.com/en-us/axis-os#cryptographic-support](https://help.axis.com/en-us/axis-os#cryptographic-support).
- **Key type (Schlüsseltyp)**: Wählen Sie in der Dropdown-Liste zum Schutz des Zertifikats den Standard- oder einen anderen Verschlüsselungsalgorithmus aus.



Das Kontextmenü enthält:

- **Certificate information (Zertifikatsinformationen)**: Lassen Sie sich die Eigenschaften eines installierten Zertifikats anzeigen.
- **Zertifikat löschen**: Löschen Sie das Zertifikat.
- **Signierungsanforderung erstellen**: Erstellen Sie eine Anforderung zur Zertifikatsignierung, um sie an eine Registrierungsstelle zu senden und ein digitales Zertifikat zu erhalten.

**Secure keystore (Sicherer Schlüsselspeicher)**  :

- **Secure element (CC EAL6+)**: Wählen Sie diese Option aus, um sicheres Element für sicheren Schlüsselspeicher zu verwenden.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2)**: Wählen Sie diese Option aus, um TPM 2.0 für sicheren Schlüsselspeicher zu verwenden.

### IEEE 802.1x

IEEE 802.1x ist ein IEEE-Standard für portbasierte Netzwerk-Zugriffskontrolle, die eine sichere Authentifizierung für drahtgebundene und drahtlose Netzwerk-Geräte bereitstellt. IEEE 802.1x basiert auf EAP (Extensible Authentication Protocol).

Zum Zugriff auf ein mit IEEE 802.1x geschütztes Netzwerk müssen sich die Netzwerk-Geräte authentifizieren. Die Authentifizierung erfolgt durch einen Authentifizierungsserver, üblicherweise ein RADIUS-Server (zum Beispiel FreeRADIUS und Microsoft Internet Authentication Server).

#### Zertifikate

Wenn die Konfiguration ohne CA-Zertifikat erfolgt, ist die Validierung des Serverzertifikats deaktiviert und das Gerät versucht, sich selbst zu authentifizieren, unabhängig vom aktuellen Netzwerk.

Bei Verwendung eines Zertifikats bei der Implementierung von Axis authentifizieren sich das Gerät und der Authentifizierungsserver mithilfe von digitalen Zertifikaten über EAP-TLS (Extensible Authentication Protocol – Transport Layer Security).

Damit das Gerät auf ein netzwerkgeschütztes Netzwerk zugreifen darf, müssen Sie ein signiertes Clientzertifikat auf dem Gerät installieren.

**Client certificate (Clientzertifikat)**: Wählen Sie ein Clientzertifikat aus, um IEEE 802,1x zu verwenden. Der Authentifizierungsserver verwendet das Zertifikat zur Validierung der Identität des Clients.

**CA certificate (CA-Zertifikat)**: Wählen Sie CA-Zertifikate zur Validierung der Identität des Authentifizierungsservers. Wenn kein Zertifikat ausgewählt sind, versucht das Gerät, sich selbst zu authentifizieren, unabhängig vom Netzwerk, mit dem es verbunden ist.

**EAP-Identität**: Geben Sie die mit dem Clientzertifikat verknüpfte Identität des Benutzers ein.

**EAPOL-Version**: Wählen Sie die in dem Netzwerk-Switch verwendete EAPOL-Version.

**IEEE 802.1x verwenden**: Wählen Sie diese Option aus, um das IEEE 802.1x-Protokoll zu verwenden.

### Brute-Force-Angriffe verhindern

**Blocken**: Aktivieren Sie diese Option, um Brute-Force-Angriffe zu blockieren. Ein Brute-Force-Angriff versucht über Trial-and-Error, Zugangsdaten oder Verschlüsselungsschlüssel zu erraten.

**Blockierdauer**: Geben Sie ein, wie viele Sekunden ein Brute-Force-Angriff blockiert werden soll.

**Blockierbedingungen**: Geben Sie die Anzahl der pro Sekunde zulässigen Authentifizierungsfehler ein, bevor blockiert wird. Sie können die Anzahl der zulässigen Fehler sowohl auf Seiten- als auch auf Geräteebene festlegen.

### IP address filter (IP-Adressfilter)

**Use filter (Filter verwenden)**: Wählen Sie diese Option, um zu filtern, welche IP-Adressen auf das Gerät zugreifen dürfen.

**Policy (Richtlinie)**: Wählen Sie, ob Sie den Zugriff für bestimmte IP-Adressen **Allow (erlauben)** oder **Deny (verweigern)** möchten.

**Addresses (Adressen)**: Geben Sie die IP-Nummern ein, denen der Zugriff auf das Gerät erlaubt oder verweigert wird. Sie können auch das CIDR-Format verwenden.

### Spezifisch signiertes Firmwarezertifikat

Zum Installieren von Test-Firmware oder anderer benutzerdefinierter Firmware von Axis auf dem Gerät benötigen Sie ein individuell signiertes Firmwarezertifikat. Das Zertifikat prüft, ob die Firmware sowohl vom Geräteeigentümer als auch von Axis genehmigt wurde. Die Firmware kann nur auf einem bestimmten Gerät ausgeführt werden, das anhand seiner eindeutigen Seriennummer und Chip-ID identifiziert wird. Benutzersignierte Firmwarezertifikate können nur von Axis erstellt werden, da Axis den Schlüssel zum Signieren besitzt.

**Install (Installieren):** Klicken Sie, um das Zertifikat zu installieren. Sie müssen das Zertifikat installieren, bevor Sie die Firmware installieren.

### Konten

#### Accounts (Konten)



**Add account (Konto hinzufügen):** Klicken Sie, um ein neues Konto hinzuzufügen. Es können bis zu 100 Konten hinzugefügt werden.

**Account (Konto):** Geben Sie einen eindeutigen Kontonamen ein.

**New password (Neues Kennwort):** Geben Sie ein Kennwort für den Kontonamen ein. Kennwörter müssen aus 1 bis 64 Zeichen bestehen. Für das Kennwort sind nur die druckbaren Zeichen des ASCII-Codes (Code 32 bis 126), also Buchstaben, Ziffern, Satzzeichen sowie einige Sonderzeichen zulässig.

**Repeat password (Kennwort wiederholen):** Geben Sie das gleiche Kennwort erneut ein.

#### Privileges (Rechte):

- **Administrator:** Hat uneingeschränkten Zugriff auf alle Einstellungen. Administratoren können auch Konten hinzufügen, aktualisieren, bearbeiten und entfernen.
- **Operator (Bediener):** Hat Zugriff auf alle Einstellungen, außer:
  - Alle Systemeinstellungen.
  - Apps werden hinzugefügt.
- **Betrachter:** Darf keine Änderungen an den Einstellungen vornehmen.



Das Kontextmenü enthält:

**Update account (Konto aktualisieren):** Bearbeiten Sie die Eigenschaften des Kontos.

**Delete account (Konto löschen):** Das Konto löschen. Das Root-Konto kann nicht gelöscht werden.

### MQTT

MQTT (Message Queuing Telemetry Transport) ist ein Standardprotokoll für das Internet der Dinge (IoT). Es wurde für eine vereinfachte IoT-Integration entwickelt und wird in einer Vielzahl von Branchen zum Anschließen von Remote-Geräten mit kleinem Code-Footprint und minimaler Netzwerkbandbreite verwendet. Der MQTT-Client in der Axis Geräte-Firmware kann die Integration der im Gerät erzeugten Daten und Ereignisse in Systeme vereinfachen, bei denen es sich nicht um Video Management Software (VMS) handelt.

Richten Sie das Gerät als MQTT-Client ein. Die MQTT-Kommunikation basiert auf zwei Entitäten, den Clients und dem Broker. Die Clients können Nachrichten senden und empfangen. Der Broker ist für das Routing von Nachrichten zwischen den Clients zuständig.

Weitere Informationen zu MQTT finden Sie im *AXIS OS Portal*.

### ALPN



Bei ALPN handelt es sich um eine TLS/SSL-Erweiterung, mit der während der Handshake-Phase der Verbindung zwischen Client und Server ein Anwendungsprotokoll ausgewählt werden kann. Auf diese Weise können Sie die MQTT-Datenverkehr über denselben Port zulassen, der für andere Protokolle wie HTTP verwendet wird. In einigen Fällen ist möglicherweise kein dedizierter Port für die MQTT-Kommunikation vorhanden. Eine Lösung besteht in diesem Fall in der Verwendung von ALPN, um die von den Firewalls erlaubte Verwendung von MQTT als Anwendungsprotokoll auf einem Standardport zu nutzen.

### MQTT-Client

**Verbinden:** Aktivieren oder deaktivieren Sie den MQTT-Client.

**Status:** Zeigt den aktuellen Status des MQTT-Clients an.

#### Broker

**Host:** Geben Sie den Host-Namen oder die Adresse des MQTT-Servers ein.

**Protokoll:** Wählen Sie das zu verwendende Protokoll aus.

**Port:** Geben Sie die Portnummer ein.

- 1883 ist der Standardwert für MQTT über TCP
- 8883 ist der Standardwert für MQTT über SSL
- 80 ist der Standardwert für MQTT über WebSocket
- 443 ist der Standardwert für MQTT über WebSocket Secure

**ALPN protocol (ALPN-Protokoll):** Geben Sie den Namen des ALPN-Protokolls ein, den Sie vom Anbieter Ihres MQTT-Brokers erhalten haben. Dies gilt nur für MQTT über SSL und MQTT über WebSocket Secure.

**Username (Benutzername):** Geben Sie den Benutzernamen ein, den der Client für den Zugriff auf den Server verwenden soll.

**Kennwort:** Geben Sie ein Kennwort für den Benutzernamen ein.

**Client-ID:** Geben Sie eine Client-ID ein. Die Client-ID wird an den Server gesendet, wenn der Client eine Verbindung herstellt.

**Sitzung bereinigen:** Steuert das Verhalten bei Verbindung und Trennungszeit. Wenn diese Option ausgewählt ist, werden die Statusinformationen beim Verbinden und Trennen verworfen.

**Keep alive interval (Keep-Alive-Intervall):** Hiermit kann der Client erkennen, wann der Server nicht mehr verfügbar ist, ohne auf das lange TCP/IP-Timeout warten zu müssen.

**Timeout (Zeitüberschreitung):** Das Zeitintervall in Sekunden, in dem eine Verbindung hergestellt werden kann. Standardwert: 60

**Device topic prefix (Themenpräfix des Geräts):** Wird in den Standardwerten für das Thema in der Verbindungsnachricht und der LWT-Nachricht auf der Registrierkarte MQTT Client und in den Veröffentlichungsbedingungen auf der Registrierkarte MQTT-Veröffentlichung verwendet.

**Reconnect automatically (Automatisch wiederverbinden):** Gibt an, ob der Client nach einer Trennung der Verbindung die Verbindung automatisch wiederherstellen soll.

#### Nachricht zum Verbindungsaufbau

Gibt an, ob eine Nachricht gesendet werden soll, wenn eine Verbindung hergestellt wird.

**Nachricht senden:** Aktivieren Sie diese Option, damit Nachrichten versendet werden.

**Standardeinstellung verwenden:** Deaktivieren Sie diese Option, um Ihre eigene Standardnachricht eingeben zu können.

**Thema:** Geben Sie das Thema der Standardnachricht ein.

**Nutzlast:** Geben Sie den Inhalt der Standardnachricht ein.

**Beibehalten:** Wählen Sie diese Option, um den Status des Clients bei diesem Thema beizubehalten.

**QoS:** Ändern Sie die QoS-Ebene für den Paketfluss.

### Nachricht zum letzten Willen und Testament

Mit Letzter Wille und Testament (LWT) kann ein Client bei der Verbindung mit dem Broker ein Testament zusammen mit seinen Zugangsdaten bereitstellen. Wenn der Kunde die Verbindung irgendwann später auf nicht ordnungsgemäße Weise abbricht (vielleicht weil seine Stromquelle deaktiviert ist), kann er den Broker eine Nachricht an andere Kunden übermitteln lassen. Diese LWT-Nachricht hat dieselbe Form wie eine normale Nachricht und wird über die gleiche Mechanik geroutet.

**Nachricht senden:** Aktivieren Sie diese Option, damit Nachrichten versendet werden.

**Standardeinstellung verwenden:** Deaktivieren Sie diese Option, um Ihre eigene Standardnachricht eingeben zu können.

**Thema:** Geben Sie das Thema der Standardnachricht ein.

**Nutzlast:** Geben Sie den Inhalt der Standardnachricht ein.

**Beibehalten:** Wählen Sie diese Option, um den Status des Clients bei diesem Thema beizubehalten.

**QoS:** Ändern Sie die QoS-Ebene für den Paketfluss.

### MQTT publication (MQTT-Veröffentlichung)

**Use default topic prefix (Standard-Themenpräfix verwenden):** Wählen Sie diese Option aus, um das Standard-Themenpräfix zu verwenden, das im Gerätethemenpräfix auf der Registerkarte **MQTT client (MQTT-Client)** definiert ist.

**Include topic name (Themanamen einschließen):** Wählen Sie diese Option aus, um das Thema einzufügen, das die Bedingung des MQTT-Themas beschreibt.

**Include topic namespaces (Themen-Namespaces einschließen):** Wählen Sie diese Option aus, um Namespaces des ONVIF-Themas im MQTT-Thema einzuschließen.

**Include serial number (Seriennummer hinzufügen):** Wählen Sie diese Option, um die Seriennummer des Geräts in die MQTT-Nutzlast einzuschließen.

**+ Bedingung hinzufügen:** Klicken Sie darauf, um eine Bedingung hinzuzufügen.

**Retain (Beibehalten):** Definiert, welche MQTT-Meldungen als beibehalten gesendet werden.

- **None (Keine):** Alle Meldungen werden als nicht beibehalten gesendet.
- **Property (Eigenschaft):** Es werden nur statusbehaftete Meldungen als beibehalten gesendet.
- **Alle:** Es werden nur statuslose Meldungen als beibehalten gesendet.

**QoS:** Wählen Sie die gewünschte Stufe für die MQTT-Veröffentlichung.

### MQTT-Abonnements

**+ Abonnement hinzufügen:** Klicken Sie darauf, um ein neues MQTT-Abonnement hinzuzufügen.

**Abonnementfilter:** Geben Sie das MQTT-Thema ein, das Sie abonnieren möchten.

**Themenpräfix des Geräts verwenden:** Fügen Sie den Abonnementfilter als Präfix zum MQTT-Thema hinzu.

**Abonnementart:**

- **Statuslos:** Wählen Sie diese Option, um MQTT-Meldungen in statuslose Meldungen zu konvertieren.
- **Statusbehaftet:** Wählen Sie diese Option, um MQTT-Meldungen in Bedingungen zu konvertieren. Als Status wird der Nutzlast verwendet.

**QoS:** Wählen Sie die gewünschte Stufe für das MQTT-Abonnement.

## Zubehör



### E/A-Ports



Schließen Sie externe Geräte über digitale Eingänge an, die zwischen geöffnetem und geschlossenem Schaltkreis wechseln können, wie etwa PIR-Sensoren, Tür- oder Fensterkontakte und Glasbruchmelder.

Schließen Sie externe Geräte wie Relais und LEDs über digitale Ausgänge an. Sie können verbundene Geräte über die VAPIX® Application Programming Interface oder über die Weboberfläche aktivieren.

#### Port

**Name:** Bearbeiten Sie den Text, um den Port umzubenennen.


**Direction (Richtung):**  gibt an, dass es sich bei dem Port um einen Eingangsport handelt.  gibt an, dass es sich um einen Ausgangsportal handelt. Wenn der Port konfigurierbar ist, können Sie auf die Symbole klicken, um zwischen Eingang und Ausgang zu wechseln.

**Normal state (Normalzustand):** Klicken Sie auf  für einen geöffneten Schaltkreis" und auf  für einen geschlossenen Schaltkreis.

**Current state (Aktueller Status):** Zeigt den aktuellen Status der Ports an. Der Ein- oder Ausgang wird aktiviert, wenn der aktuelle Zustand vom Normalzustand abweicht. Ein Eingang am Gerät ist offen, wenn er getrennt ist oder eine Spannung von mehr als 1 V Gleichstrom anliegt.

#### Hinweis

Der Schaltkreis des Ausgangs ist während eines Neustarts offen. Nach abgeschlossenem Neustart nimmt der Schaltkreis wieder die normale Position an. Wenn die Einstellungen auf dieser Seite geändert werden, nehmen die Schaltkreise der Ausgänge wieder ihre jeweiligen normalen Positionen an, wobei es unerheblich ist, ob aktive Auslöser vorliegen.

**Supervised (Überwacht)**  : Aktivieren Sie diese Option, um Aktionen zu erkennen und auszulösen, wenn jemand die Verbindung zu digitalen E/A-Geräten manipuliert. Sie können nicht nur erkennen, ob ein Eingang geöffnet oder geschlossen ist, sondern auch, ob jemand diesen manipuliert hat (d. h. abgeschnitten oder gekürzt). Zur Überwachung der Verbindung ist im externen E/A-Kreis zusätzliche Hardware (Abschlusswiderstände) erforderlich.

## Protokolle

### Protokolle und Berichte

#### Berichte

- **View the device server report (Geräteserver-Bericht anzeigen):** Zeigt Informationen zum Produktstatus in einem Popup-Fenster bereit. Das Zugangsprotokoll wird automatisch dem Server-Bericht angefügt.
- **Download the device server report (Bericht zum Geräteserver herunterladen):** Dabei wird eine .zip-Datei mit dem vollständigen Server-Bericht als Textdatei im Format UTF-8 sowie einem Schnappschuss der aktuellen Live-Ansicht erstellt. Schließen Sie beim Kontakt mit dem Support stets die ZIP-Datei des Server-Berichts ein.
- **Download the crash report (Absturzbericht herunterladen):** So wird ein Archiv mit ausführlichen Informationen zum Produktstatus heruntergeladen. Der Absturzbericht enthält die im Server-Bericht enthaltenen Informationen sowie ausführliche Debug-Informationen. Dieser Bericht enthält möglicherweise vertrauliche Daten wie z. B. Netzwerk-Traces. Es kann einige Minuten dauern, bis der Bericht generiert wird.

#### Protokolle

- **Systemprotokoll sehen:** Klicken Sie, um Informationen zu Systemereignissen, wie z. B. Gerätestart, Warnungen und wichtige Meldungen, zu sehen.
- **View the access log (Zugangsprotokoll anzeigen):** Klicken Sie darauf, um alle fehlgeschlagenen Zugriffsversuche auf das Gerät zu sehen, bei denen z. B. ein falsches Anmeldekenntwort verwendet wurde.

### Netzwerk-Trace

#### Wichtig

Eine Datei zum Netzwerk-Trace enthält möglicherweise vertrauliche Informationen wie Zertifikate oder Kennwörter.

Ein Netzwerk-Trace hilft durch die Aufzeichnung von Aktivitäten im Netzwerk beim Beheben von Problemen.

**Trace time (Trace-Dauer):** Geben Sie die Dauer des Trace in Sekunden oder Minuten an und klicken Sie auf **Download (Herunterladen)**.

### Remote-Systemprotokoll

Syslog ist ein Standard für die Nachrichtenprotokollierung. Dadurch können die Software, die Nachrichten generiert, das System, in dem sie gespeichert sind, und die Software, die sie meldet und analysiert voneinander getrennt werden. Jede Nachricht ist mit einem Einrichtungscode versehen, der den Softwaretyp, der die Nachricht generiert, angibt, und einem Schweregrad zugewiesen.



**Server:** Klicken Sie, um einen neuen Server hinzuzufügen.

**Host:** Geben Sie den Host-Namen oder die IP-Adresse des Servers ein.

**Format:** Wählen Sie das zu verwendende syslog-Nachrichtenformat aus.

- Axis
- RFC 3164
- RFC 5424

**Protocol (Protokoll):** Wählen Sie das zu verwendende Protokoll und den zu verwendenden Port aus:

- UDP (Standardport ist 514)
- TCP (Standardport ist 601)
- TLS (Standardport ist 6514)

**Schweregrad:** Wählen Sie aus, welche Nachrichten gesendet werden sollen, wenn diese ausgelöst werden.

**CA-Zertifikat einrichten:** Sehen Sie sich die aktuellen Einstellungen an oder fügen Sie ein Zertifikat hinzu.

### Wartung

**Neustart:** Starten Sie das Gerät neu. Dies hat keine Auswirkungen auf aktuelle Einstellungen. Aktive Anwendungen werden automatisch neu gestartet.

**Wiederherstellen:** Setzen Sie die *meisten Einstellungen* auf die Werkseinstellungen zurück. Anschließend müssen Sie Gerät und Apps neu konfigurieren, nicht vorinstallierte Apps neu installieren sowie Ereignisse und PTZ-Voreinstellungen neu erstellen.

#### Wichtig

Die einzigen nach der Wiederherstellung weiterhin gespeicherten Einstellungen sind:

- Boot-Protokoll (DHCP oder statisch)
- Statische IP-Adresse
- Standardrouter
- Subnetzmaske
- Einstellungen für 802.1X
- Einstellungen für O3C

**Werkseinstellungen:** Setzen Sie *alle* Einstellungen werden auf die Werkseinstellungen zurück. Anschließend müssen Sie die IP-Adresse zurücksetzen, um auf das Gerät zugreifen zu können.

### Hinweis

Sämtliche Firmware des Axis Geräts ist digital signiert, um sicherzustellen, dass Sie nur die verifizierte Firmware auf Ihrem Gerät installieren. Diese Maßnahme erhöht das allgemeine Mindestniveau der Cybersicherheit für die Geräte von Axis. Weitere Informationen finden Sie im Whitepaper "Signierte Firmware, sicherer Start und Sicherheit von Privatschlüsseln" auf [axis.com](https://axis.com).

**Firmwareaktualisierung:** Aktualisieren Sie auf eine neue Firmwareversion. Neue Firmwareversionen können verbesserte Funktionen, Fehlerkorrekturen und vollständig neue Merkmale beinhalten. Wir empfehlen Ihnen, stets die aktuellste Version zu verwenden. Um die neueste Version herunterzuladen, gehen Sie zu [axis.com/support](https://axis.com/support).

Bei der Aktualisierung können Sie zwischen drei Optionen wählen:

- **Standardaktualisierung:** Aktualisieren Sie auf die neue Firmwareversion.
- **Werkseinstellungen:** Aktualisieren und alle Einstellungen werden auf die Werkseinstellungen zurückgesetzt. Wenn Sie diese Option wählen, können Sie nach der Aktualisierung nicht mehr zur vorherigen Firmwareversion zurückkehren.
- **Automatisches Zurücksetzen:** Aktualisieren Sie und bestätigen Sie die Aktualisierung innerhalb der festgelegten Zeit. Wenn Sie diese nicht bestätigen, wird das Gerät auf die vorherige Firmwareversion zurückgesetzt.

**Firmware zurücksetzen:** Gehen Sie auf die vorherige Firmwareversion zurück.

### Weitere Informationen

## Cybersicherheit

### Signierte Firmware

Signierte Firmware wird vom Softwarehersteller implementiert, der das Firmware-Image mit einem privaten Schlüssel signiert. Wenn eine Firmware mit dieser Signatur versehen ist, validiert ein Gerät die Firmware, bevor es die Installation der Firmware akzeptiert. Wenn das Gerät feststellt, dass die Integrität der Firmware beeinträchtigt ist, wird die Aktualisierung der Firmware abgelehnt.

### sicheres Hochfahren

Sicheres Hochfahren ist ein Bootvorgang, der aus einer ununterbrochenen Kette von kryptografisch validierter Software besteht, die im unveränderlichen Speicher (Boot-ROM) beginnt. Da sicheres Hochfahren auf der Verwendung signierter Firmware basiert, wird sichergestellt, dass ein Gerät nur mit autorisierter Firmware booten kann.

### Axis Edge Vault

Axis Edge Vault stellt eine hardwarebasierte Cybersicherheitsplattform zum Schutz des Axis Geräts bereit. Sie bietet Funktionen, die die Identität und Integrität des Geräts gewährleisten und Ihre vertraulichen Daten vor unbefugtem Zugriff schützen. Die Lösung baut auf einer soliden Grundlage von kryptografischen Computermodulen (Secure Element und TPM) und SoC-Sicherheit (TEE und Secure Boot) auf, kombiniert mit Fachwissen über die Sicherheit von Edge-Geräten.

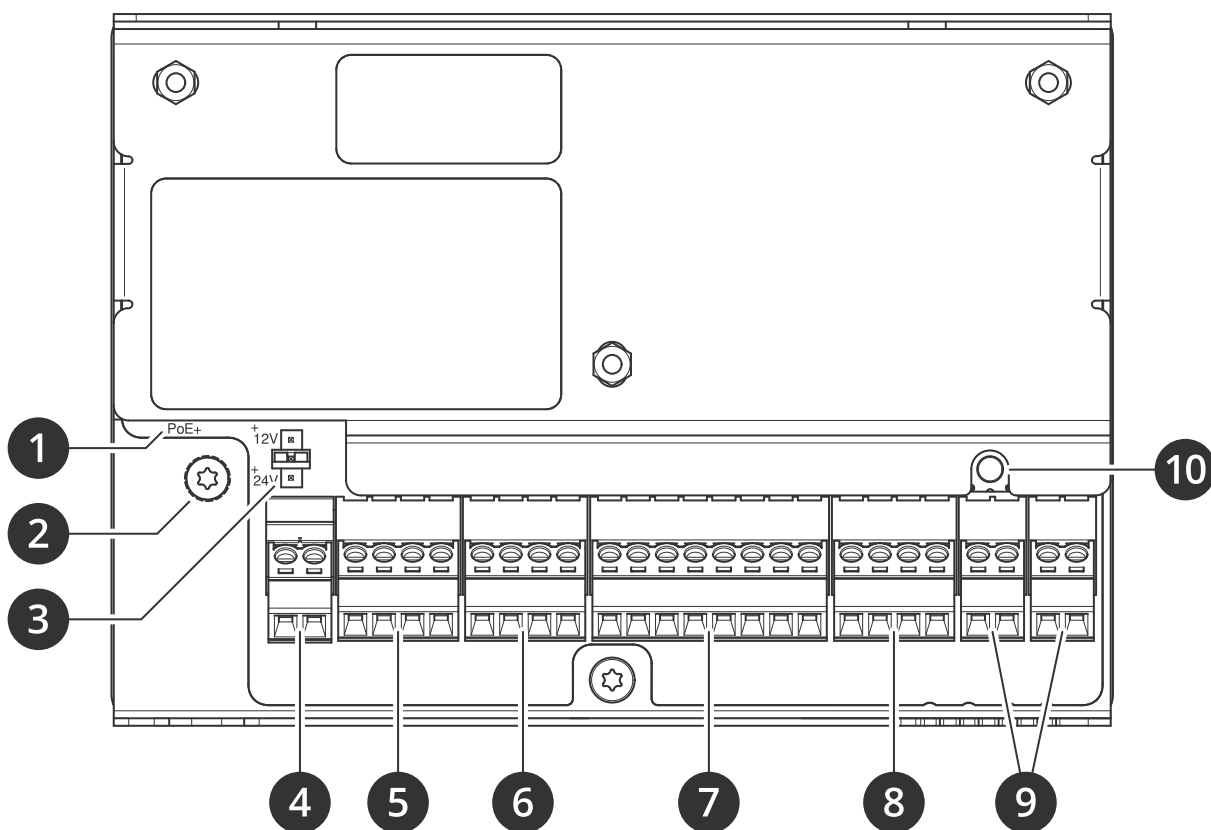
### Axis Geräte-ID

Die Möglichkeit zur Überprüfung der Identität des Geräts schafft Vertrauen in die Geräteidentität. Bei der Produktion erhalten Geräte mit Axis Edge Vault ein einzigartiges, ab Werk bereitgestelltes und IEEE 802.1AR-konformes Axis Geräte-ID-Zertifikat. Dies funktioniert wie ein Pass, der den Ursprung des Geräts belegt. Die Geräte-ID wird im sicheren Schlüsselspeicher sicher und dauerhaft als vom Root-Zertifikat von Axis signiertes Zertifikat gespeichert. Die Geräte-ID kann über die IT-Infrastruktur des Kunden für ein automatisiertes, sicheres Geräte-Onboarding und sichere Geräteidentifizierung genutzt werden.

Um mehr zu Cybersicherheitsfunktionen von Axis Edge Vault und Axis Geräten zu erfahren, gehen Sie auf [axis.com/learning/white-papers](https://axis.com/learning/white-papers) und suchen Sie nach Cybersicherheit.

## Technische Daten

### Produktübersicht



- 1 Netzwerk-Anschluss
- 2 Position Erdung
- 3 Relaisbrücke
- 4 Stromanschluss
- 5 Relaisanschluss
- 6 Tür-Verbindung
- 7 Lesegerätanschluss
- 8 Zusatzanschluss
- 9 Externe Anschlüsse
- 10 Steuertaste

### LED-Anzeigen

LED	Farbe	Bedeutung
Netzwerk	Grün	Dauerhaft bei Verbindung mit einem 100 MBit/s-Netzwerk Blinkt bei Netzwerkaktivität.
	Gelb	Leuchtet bei Verbindung mit einem 10 MBit/s-Netzwerk. Blinkt bei Netzwerkaktivität.
	Leuchtet nicht	Keine Netzwerk-Verbindung vorhanden.

Status	Grün	Leuchtet bei Normalbetrieb grün.
	Gelb	Leuchtet beim Start und beim Wiederherstellen der Einstellungen.
	Rot	Blinkt langsam bei einem Aktualisierungsfehler.
Stromversorgung	Grün	Normalbetrieb.
	Gelb	Blinkt während einer Firmware-Aktualisierung grün/orange.
Relais	Grün	Relais aktiv. <sup>1</sup>
	Leuchtet nicht	Relais nicht aktiv.

1. Aktives Relais wenn COM an NO angeschlossen.

## Tasten

### Steuertaste

Die Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 31*.

## Anschlüsse

### Netzwerk-Anschluss

RJ45-Ethernetanschluss mit Power over Ethernet Plus (PoE+).

UL: Power over Ethernet (PoE) geht nur über Ethernet IEEE 802.3af/802.3at Typ 1 Klasse 3 oder Power over Ethernet Plus (PoE+) IEEE 802.3at Typ 2 Klasse 4 mit begrenzter Leistung, der 44 bis 57 V DC, 15,4 W/30 W liefert. Power over Ethernet (PoE) wurde von UL mit AXIS T8133 Midspan 30 W 1-Port evaluiert.

### Strompriorität

Dieses Gerät kann entweder über PoE oder Gleichstromeingang mit Strom versorgt werden. Siehe *Netzwerk-Anschluss auf Seite 24* und *Stromanschluss auf Seite 29*.

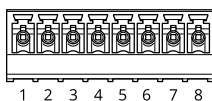
- Wenn PoE und Gleichstrom vor dem Einschalten des Geräts verbunden sind, wird PoE für die Stromversorgung verwendet.
- PoE und Gleichstrom sind beide angeschlossen und die Stromversorgung geschieht derzeit über PoE. Bei Verlust von PoE wird das Gerät für die Stromversorgung ohne Neustart mit Gleichstrom verwendet.
- PoE und Gleichstrom sind beide angeschlossen und die Stromversorgung geschieht derzeit über Gleichstrom. Bei Verlust des Gleichstroms wird das Gerät neu gestartet und verwendet PoE für die Stromversorgung.
- Wenn Gleichstrom beim Start verwendet wird und PoE nach dem Start des Geräts angeschlossen wird, wird Gleichstrom für die Stromversorgung verwendet.
- Wenn PoE beim Start verwendet wird und Gleichstrom nach dem Start des Geräts angeschlossen wird, wird PoE für die Stromversorgung verwendet.

### Lesegerätanschluss

Ein achtpoliger Anschlussblock für die Kommunikation mit dem Lesegerät (unterstützt die Protokolle RS-485 und Wiegand).

Es kann bis zu zwei OSDP-Leser (Multi-Drop) oder einen Wiegand-Leser anschließen. Eine Ausgangsleistung von 500 mA mit 12 V ist für alle an den Türcontroller angeschlossenen Lesegeräte reserviert.





Für einen OSDP-Leser konfiguriert

Funktion	Kontakt	Hinweis	Technische Daten
Erdung Gleichstrom (GND)	1		0 V Gleichstrom
Gleichstromausgang (+12 V)	2	Versorgt das Lesegerät mit Strom.	12 V Gleichstrom, max 500 mA
A	3	Halbduplex	
B	4	Halbduplex	

Für zwei OSDP-Leser konfiguriert (Mehrfach-Drop)

Funktion	Kontakt	Hinweis	Technische Daten
Erdung Gleichstrom (GND)	1		0 V Gleichstrom
Gleichstromausgang (+12 V)	2	Versorgt beide Lesegeräte mit Strom.	12 V Gleichstrom, max. 500 mA kombiniert für beide Lesegeräte
A	3	Halbduplex	
B	4	Halbduplex	

### Wichtig

- Bei Stromversorgung des Lesers über den Controller beträgt die zulässige Kabellänge maximal 200 m. Nur für Axis Lesegeräte überprüft.
- Erfolgt die Stromversorgung des Lesers nicht über den Controller, beträgt die zulässige Datenkabellänge maximal 1000 m, sofern die folgenden Kabelanforderungen erfüllt sind: 1 Twisted Pair geschirmt, AWG 24, Impedanz 120 Ohm. Nur für Axis Lesegeräte überprüft.

Für ein Wiegand-Lesegerät konfiguriert

Funktion	Kontakt	Hinweis	Technische Daten
Erdung Gleichstrom (GND)	1		0 V Gleichstrom
Gleichstromausgang (+12 V)	2	Versorgt das Lesegerät mit Strom.	12 V Gleichstrom, max 500 mA
D0	3		
D1	4		
LED 1	5	Rote LED	
LED 2	6	Grüne LED	

SABOTAGE	7	Digitaleingang – zum Aktivieren an Kontakt 1 anschließen; zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom
SUMMER	8	Digitaler Ausgang – Bei Verwendung mit einer induktiven Last, wie etwa einem Relais, muss zum Schutz vor Spannungssprüngen eine Diode parallel zur Last geschaltet werden.	0 bis max. 30 V Gleichstrom, Open Drain, 100 mA

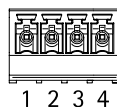
### Wichtig

- Bei Stromversorgung des Lesers über den Controller beträgt die zulässige Kabellänge maximal 150 m.
- Erfolgt die Stromversorgung des Lesers nicht über den Controller, beträgt die zulässige Datenkabellänge maximal 150 m, sofern die folgenden Kabelanforderungen erfüllt sind: AWG 22.

### Tür-Verbindung

Ein vierpoliger Anschlussblock für Türüberwachungsgeräte (Digitaleingang).

Türmonitor unterstützt das Überwachen mit Abschlusswiderständen. Bei Unterbrechen der Verbindung wird ein Alarm ausgelöst. Um überwachte Eingänge zu verwenden, Abschlusswiderstände anbringen. Das Anschlusschaltendiagramm für überwachte Eingänge beachten. Siehe Seite 29.



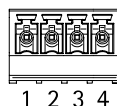
Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1, 3		0 V Gleichstrom
Eingang	2, 4	Zum Kommunizieren mit der Türüberwachung. Digitaleingang oder überwachter Eingang – zum Aktivieren mit Kontakt 1 oder 3 verbinden. Zum Türanlage nicht anschließen.	0 bis max. 30 V Gleichstrom

### Wichtig

Das Kabel darf bis zu 200 m lang sein, wenn es folgende Anforderung erfüllt: AWG 24.

### Relaisanschluss

Ein vierpoliger Anschlussblock für Relais Typ C, der zum Beispiel ein Schloss oder eine Schnittstelle zu einem Tor steuert.



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom (GND)	1		0 V Gleichstrom

NEIN	2	Schliesser-Kontakt. Zum Anschließen von Relaisgeräten. Ein ausfallsicheres Schloss an NO und Erdung Gleichstrom anschließen. Sofern die Brücken nicht verwendet werden, sind die beiden Relaiskontakte galvanisch von der übrigen Schaltung getrennt.	Max. Stromstärke = 2 A Max. Spannung = 30 V Gleichstrom
COM	3	Gemeinsam	
NC	4	Öffner-Kontakt. Zum Anschließen von Relaisgeräten. Ein ausfallsicheres Schloss an NC und Erdung Gleichstrom anschließen. Sofern die Brücken nicht verwendet werden, sind die beiden Relaiskontakte galvanisch von der übrigen Schaltung getrennt.	

### Relaisstrombrücke

Die Relaisstrombrücke überbrückt 12 V Gleichstrom oder 24 V Gleichstrom und den Relaiskontakt COM.

Mit ihr kann ein Schloss an die Kontakte GND und NO oder GND und NC geschaltet werden.

Stromquelle	Maximale Leistung bei 12 V Gleichstrom	Maximale Leistung bei 24 V Gleichstrom
Gleichstrom IN	1.600 mA	800 mA
PoE	900 mA	450 mA

### HINWEIS

Wir empfehlen Ihnen, nichtpolare Schösser mit einer externen Schutzdiode auszustatten.

### Zusatzanschluss

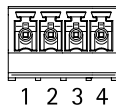
Über den Zusatzanschluss werden externe Geräte für Funktionen wie Manipulationsalarm, Bewegungserkennung, Ereignisauslösung, Alarmbenachrichtigung und andere angeschlossen. Abgesehen vom Bezugspunkt 0 V Gleichstrom und Strom (Gleichstromausgang) verfügt der Zusatzanschluss über eine Schnittstelle zum:

**Digitaleingang** – Zum Anschließen von Geräten, die zwischen geöffnetem und geschlossenem Schaltkreis wechseln können wie etwa PIR-Sensoren, Tür- und Fensterkontakte sowie Glasbruchmelder.

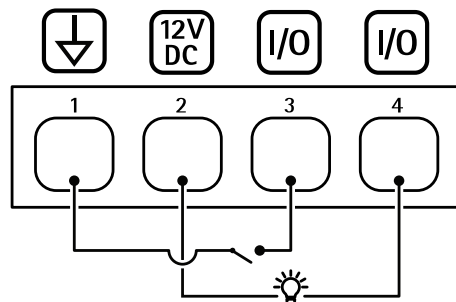
**Überwachter Eingang** – Ermöglicht das Erfassen von Manipulation an einem digitalen Eingang.

**Digitalausgang** – Zum Anschluss externer Geräte wie Relais und LEDs. Die angeschlossenen Geräte können über das VAPIX® Application Programming Interface oder über die Produktwebsite aktiviert werden.

4-poliger Anschlussblock



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstromausgang	2	Darf für die Stromversorgung von Zusatzgeräten verwendet werden. Hinweis: Dieser Kontakt darf nur für den Stromausgang verwendet werden.	Max. 12 V DC Maximale Last = 50 mA insgesamt
Konfigurierbar (Ein- oder Ausgang)	3-4	Digitaler Eingang oder überwachter Eingang – Zum Aktivieren an Kontakt 1 anschließen, zum Deaktivieren nicht anschließen. Um überwachten Eingang zu nutzen, Abschlusswiderstände anschließen. Informationen zum Anschließen der Widerstände bietet der Schaltplan.	0 bis max. 30 V Gleichstrom
		Digitaler Ausgang – Interne Verbindung mit Kontakt 1 (Erdschluss Gleichstrom), wenn aktiviert; unverbunden, wenn deaktiviert. Bei Verwendung mit einer induktiven Last wie etwa einem Relais muss zum Schutz vor Spannungssprüngen eine Diode parallel zur Last geschaltet werden. Jeder E/A kann eine 12-V-Gleichstrom-, 50 mA (max.) externe Last antreiben, wenn ein interner 12-V-Gleichstromausgang (Pin 2) verwendet wird. Bei Verwendung von Open Drain-Verbindungen in Kombination mit einem externen Netzteil kann der E/A die Gleichstromversorgung von 0 bis 30 V Gleichstrom, 100 mA, verwalten.	0 bis max. 30 V Gleichstrom, Open Drain, 100 mA

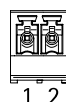


- 1 Erdung Gleichstrom
- 2 Gleichstromausgang 12 V
- 3 E/A als Eingang konfiguriert
- 4 E/A als Ausgang konfiguriert

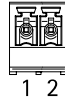
## Externer Anschluss

Zwei zweipolige Anschlussblöcke für externe Geräte wie Glasbruchmelder oder Feuermelder.

UL: Der Anschluss wurde nicht für die Verwendung als Einbruch- oder Feueralarm von UL bewertet.



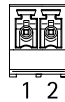
Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
SABOTAGE	2	Digitaleingang – zum Aktivieren an Kontakt 1 anschließen; zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
ALARM	2	Digitaleingang – zum Aktivieren an Kontakt 1 anschließen; zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom

## Stromanschluss

2-poliger Anschlussblock für die Gleichstromversorgung. Verwenden Sie eine mit den Anforderungen für Schutzkleinspannung (SELV) kompatible Stromquelle mit begrenzter Leistung (LPS) mit einer Nennausgangsleistung von  $\leq 100$  W oder einem dauerhaft auf  $\leq 5$  A begrenzten Nennausgangsstrom.



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom (GND)	1		0 V Gleichstrom
DC-Eingang	2	Stromversorgung der Steuerung bei Nichtverwendung von Power over Ethernet. Hinweis: Dieser Kontakt kann nur für den Stromeingang verwendet werden.	12 V Gleichstrom, max 36 W

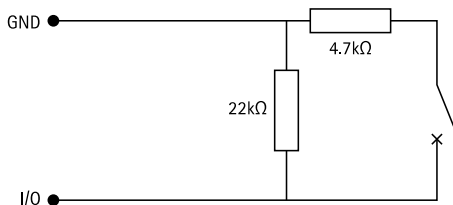
UL: Die Gleichstromleistung muss je nach Anwendung über ein UL 603-gelistetes Netzteil mit entsprechenden Nennleistungen bereitgestellt werden.

## Überwachte Eingänge

Um überwachte Eingänge zu verwenden, die Abschlusswiderstände wie im Schaltbild unten dargestellt anschließen.

### Paralleler Anschluss hat Vorrang

Die Widerstandswerte müssen 4,7 k $\Omega$  und 22 k $\Omega$  betragen.

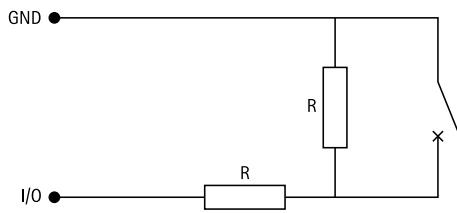


### Serienschaltung

Die Widerstandswerte müssen identisch sein und die möglichen Werte sind 1 k $\Omega$ , 2,2 k $\Omega$ , 4,7 k $\Omega$  und 10 k $\Omega$ .

## Technische Daten

---



### Hinweis

Es wird empfohlen, verdrehte und geschirmte Kabel zu verwenden. Die Abschirmung an 0 V Gleichstrom anschließen.

### Fehlerbehebung

#### Zurücksetzen auf die Werkseinstellungen

##### Wichtig

Das Zurücksetzen auf die Werkseinstellungen sollte mit Vorsicht erfolgen. Beim Zurücksetzen auf die Werkseinstellungen werden alle Einstellungen einschließlich der IP-Adresse zurückgesetzt.

So wird das Produkt auf die werksseitigen Standardeinstellungen zurückgesetzt:

1. Trennen Sie das Produkt von der Stromversorgung.
2. Halten Sie die Steuertaste gedrückt und stellen Sie die Stromversorgung wieder her. Siehe *Produktübersicht auf Seite 23*.
3. Halten Sie die Steuertaste 25 Sekunden gedrückt, bis die Status-LED zum zweiten Mal gelb leuchtet.
4. Lassen Sie die Steuertaste los. Der Vorgang ist abgeschlossen, wenn die Status-LED grün leuchtet. Das Produkt wurde auf die Werkseinstellungen zurückgesetzt. Wenn im Netzwerk kein DHCP-Server verfügbar ist, lautet die Standard-IP-Adresse 192.168.0.90.
5. Mithilfe der Softwaretools für das Installieren und Verwalten, IP-Adressen zuweisen, das Kennwort festlegen und auf das Produkt zugreifen.

Die Parameter können auch über die Weboberfläche des Geräts auf die Werkseinstellungen zurückgesetzt werden. Gehen Sie zu **Wartung > Werkseinstellungen** und klicken Sie auf **Standardeinstellungen**.

#### Firmware-Optionen

Axis bietet eine Produkt-Firmware-Verwaltung entweder gemäß des aktiven Tracks oder gemäß Tracks für Langzeitunterstützung (LTS). Beim aktiven Track erhalten Sie einen kontinuierlichen Zugriff auf alle aktuellen Funktionen des Produkts. Die LTS-Tracks bieten eine feste Plattform, die regelmäßig Veröffentlichungen mit Schwerpunkt auf Bugfixes und Sicherheitsaktualisierungen bereitstellt.

Es wird empfohlen, die Firmware vom aktiven Track zu verwenden, wenn Sie auf die neuesten Funktionen zugreifen möchten oder Axis End-to-End-Systemangebote nutzen. Die LTS-Tracks werden empfohlen, wenn Sie Integrationen von Drittanbietern verwenden, die nicht kontinuierlich auf den neuesten aktiven Track überprüft werden. Mit LTS kann die Cybersicherheit der Produkte gewährleistet werden, ohne dass signifikante Funktionsänderungen neu eingeführt oder vorhandene Integrationen beeinträchtigt werden. Ausführliche Informationen zur Vorgehensweise von Axis in Bezug auf Produktfirmware finden Sie unter [axis.com/support/Firmware](https://axis.com/support/Firmware).

#### Aktuelle Firmware überprüfen

Firmware ist die Software, mit der die Funktionalität von Netzwerk-Geräten festgelegt wird. Wir empfehlen Ihnen, vor jeder Problembeseitigung zunächst die aktuelle Firmwareversion zu überprüfen. Die aktuelle Firmwareversion enthält möglicherweise eine Verbesserung, mit der das Problem behoben werden kann.

So überprüfen Sie die aktuelle Firmware:

1. Gehen Sie zur Weboberfläche des Geräts > **Status**.
2. Die Firmwareversion finden Sie unter **Geräteinformationen**.

#### Firmware aktualisieren

##### Wichtig

- Vorkonfigurierte und angepasste Einstellungen werden beim Aktualisieren der Firmware gespeichert (sofern die Funktionen als Teil der neuen Firmware verfügbar sind). Es besteht diesbezüglich jedoch keine Garantie seitens Axis Communications AB.
- Stellen Sie sicher, dass das Gerät während der Aktualisierung an die Stromversorgung angeschlossen ist.

### Hinweis

Beim Aktualisieren mit der aktuellen Firmware im aktiven Track werden auf das Gerät die neuesten verfügbaren Funktionen versorgt. Lesen Sie vor der Aktualisierung der Firmware stets die entsprechenden Aktualisierungsanweisungen und Versionshinweise dazu. Die aktuelle Version der Firmware und die Versionshinweise finden Sie auf [axis.com/support/firmware](http://axis.com/support/firmware).

### Hinweis

Im Zuge einer Firmwareaktualisierung wird die Datenbank mit den Daten der Benutzer, Gruppen, Anmeldedetails und anderen Informationen aktualisiert. Der erste Start danach kann deshalb einige Minuten dauern. Die erforderliche Zeit hängt von der Datenmenge ab.

1. Die Firmware können Sie auf [axis.com/support/firmware](http://axis.com/support/firmware) kostenlos auf Ihren Computer herunterladen.
2. Melden Sie sich auf dem Gerät als Administrator an.
3. Navigieren Sie zu **Maintenance > Firmware upgrade (Wartung > Firmwareaktualisierung)** und klicken Sie auf **Upgrade (Aktualisieren)**.

Nach der Aktualisierung wird das Produkt automatisch neu gestartet.

4. Leeren Sie nach dem Neustart des Geräts den Cache des Browsers.

## Technische Fragen, Hinweise und Lösungen

Falls Sie hier nicht das Gesuchte finden, bitte den Bereich „Fehlerbehebung“ unter [axis.com/support](http://axis.com/support) aufrufen.

### Probleme beim Aktualisieren der Firmware

---

Aktualisierung der Firmware fehlgeschlagen	Nach fehlgeschlagener Aktualisierung der Firmware lädt das Gerät erneut die Vorversion. Die häufigste Fehlerursache ist, wenn eine falsche Firmwaredatei hochgeladen wurde. Überprüfen, ob der Name der Firmwaredatei dem Gerät entspricht und erneut versuchen.
Probleme nach dem Aktualisieren von Firmware	Bei nach dem Aktualisieren von Firmware auftretenden Problemen die Installation über die <b>Wartungsseite</b> auf die Vorversion zurückrollen.

### Probleme beim Einstellen der IP-Adresse

---

Das Gerät befindet sich in einem anderen Subnetz	Wenn sich die IP-Adresse des Geräts und die IP-Adresse des zum Zugriff auf das Gerät verwendeten Computers in unterschiedlichen Subnetzen befinden, kann die IP-Adresse nicht eingestellt werden. Wenden Sie sich an Ihren Netzwerkadministrator, um eine IP-Adresse zu erhalten.
Die IP-Adresse wird von einem anderen Gerät verwendet	Trennen Sie das Axis Gerät vom Netzwerk. Führen Sie einen Ping-Befehl aus (geben Sie in einem Befehls-/DOS-Fenster <code>ping</code> und die IP-Adresse des Geräts ein): <ul style="list-style-type: none"><li>• Wenn Folgendes angezeigt wird: <code>Reply from (Antwort von)&lt;IP address&gt;: bytes=32; time=10...</code> dies bedeutet, dass die IP-Adresse möglicherweise bereits von einem anderen Gerät im Netzwerk verwendet wird. Bitten Sie den Netzwerkadministrator um eine neue IP-Adresse, und installieren Sie das Gerät erneut.</li><li>• Wenn Folgendes angezeigt wird: <code>Request timed out</code> bedeutet, dass die IP-Adresse mit dem Axis Gerät verwendet werden kann. Prüfen Sie alle Kabel und installieren Sie das Gerät erneut.</li></ul>
Möglicher IP-Adressenkonflikt mit einem anderen Gerät im selben Subnetz.	Die statische IP-Adresse des Axis Geräts wird verwendet, bevor der DHCP-Server eine dynamische Adresse festlegt. Verwendet also ein anderes Gerät standardmäßig dieselbe statische IP-Adresse, treten beim Zugreifen auf das Gerät möglicherweise Probleme auf.



### Vom Browser aus ist kein Zugriff auf das Gerät möglich

---

Anmeldung nicht möglich	<p>Wenn HTTPS aktiviert ist, stellen Sie sicher, dass beim Anmelden das korrekte Protokoll (HTTP oder HTTPS) verwendet wird. Möglicherweise müssen Sie manuell <code>http</code> oder <code>https</code> in die Adressleiste des Browsers eingeben.</p> <p>Wenn das Kennwort für das Haupt-Konto vergessen wurde, muss das Gerät auf die werksseitigen Standardeinstellungen zurückgesetzt werden. Siehe <i>Zurücksetzen auf die Werkseinstellungen auf Seite 31</i>.</p>
Die IP-Adresse wurde von DHCP geändert	<p>Von einem DHCP-Server zugeteilte IP-Adressen sind dynamisch und können sich ändern. Wenn die IP-Adresse geändert wurde, das Gerät mit AXIS IP Utility oder AXIS Camera Management im Netzwerk zu ermitteln. Ermitteln Sie das Gerät anhand seiner Modellnummer, Seriennummer oder anhand des DNS-Namens (sofern der Name konfiguriert wurde).</p> <p>Bei Bedarf kann eine statische IP-Adresse manuell zugewiesen werden. Anweisungen dazu finden Sie auf <a href="http://axis.com/support">axis.com/support</a>.</p>
Zertifikatfehler beim Verwenden von IEEE 802.1X	<p>Damit die Authentifizierung ordnungsgemäß funktioniert, müssen die Datums- und Uhrzeiteinstellungen des Axis Geräts mit einem NTP-Server synchronisiert werden. Gehen Sie auf <i>Einstellungen &gt; System &gt; Datum und Uhrzeit</i>.</p>

### Auf das Gerät kann lokal, nicht jedoch extern zugegriffen werden

---

Für den externen Zugriff auf das Gerät wird die Verwendung einer der folgenden Anwendungen für Windows® empfohlen:

- AXIS Companion: Kostenlos, ideal für kleine Systeme mit grundlegenden Überwachungsanforderungen.
- AXIS Camera Station Video Management Software: Kostenlose 30-Tage-Testversion, ideal für kleine bis mittelgroße Systeme.

Auf [axis.com/vms](http://axis.com/vms) finden Sie Anweisungen und die Download-Datei.

### Verbindung über Port 8883 mit MQTT über SSL kann nicht hergestellt werden

---

Die Firewall blockiert den Datenverkehr über Port 8883, da er als ungesichert eingestuft wird.	<p>In einigen Fällen stellt der Server/Broker möglicherweise keinen bestimmten Port für die MQTT-Kommunikation bereit. Möglicherweise kann MQTT über einen Port verwendet werden, der normalerweise für HTTP/HTTPS-Datenverkehr verwendet wird.</p> <ul style="list-style-type: none"><li>• Wenn der Server/Broker WebSocket/WebSocket Secure (WS/WSS) unterstützt (in der Regel auf Port 443, verwenden Sie stattdessen dieses Protokoll. Prüfen Sie mit dem Betreiber des Servers/Brokers, ob WS/WSS unterstützt wird und welcher Port und welcher Basispfad verwendet werden soll.</li><li>• Wenn der Server/Broker ALPN unterstützt, kann darüber verhandelt werden, ob MQTT über einen offenen Port (wie z. B. 443) verwendet werden soll. Prüfen Sie mit dem Betreiber Ihres Servers/Brokers, ob ALPN unterstützt wird und welches Protokoll und welcher Port verwendet werden soll.</li></ul>
--	--

## Support

Supportinformationen erhalten Sie unter [axis.com/support](http://axis.com/support).

