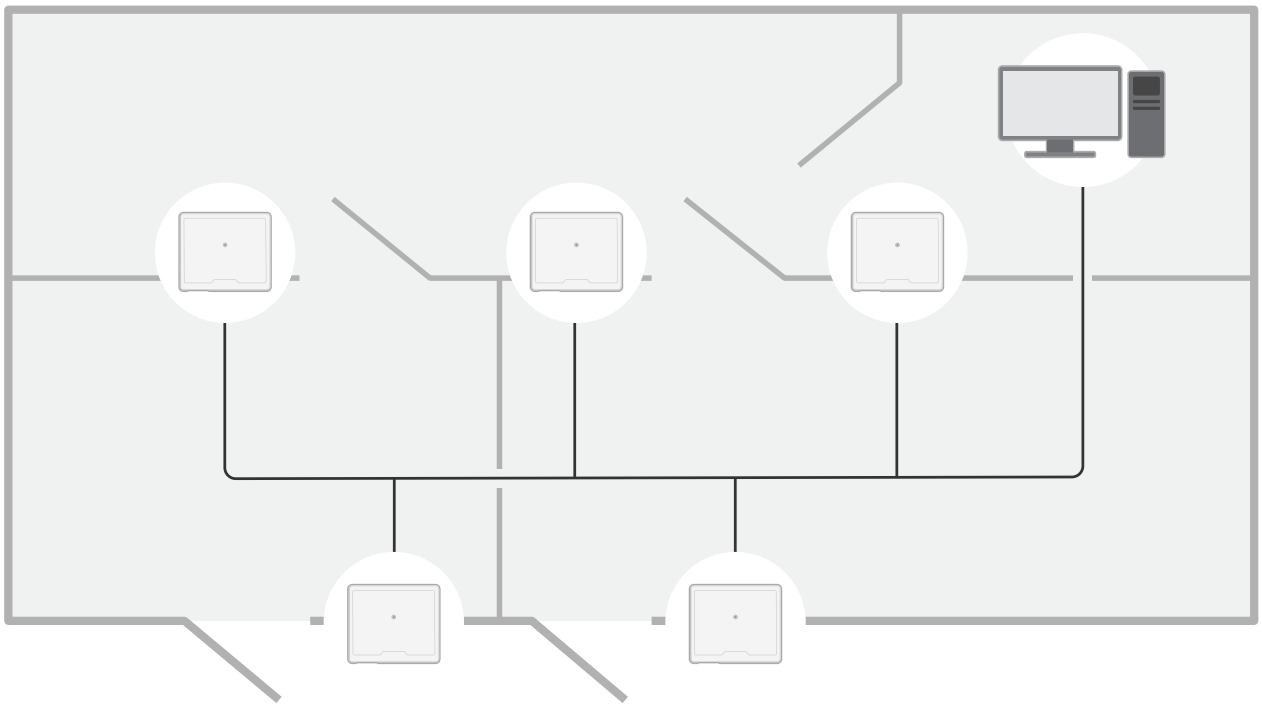
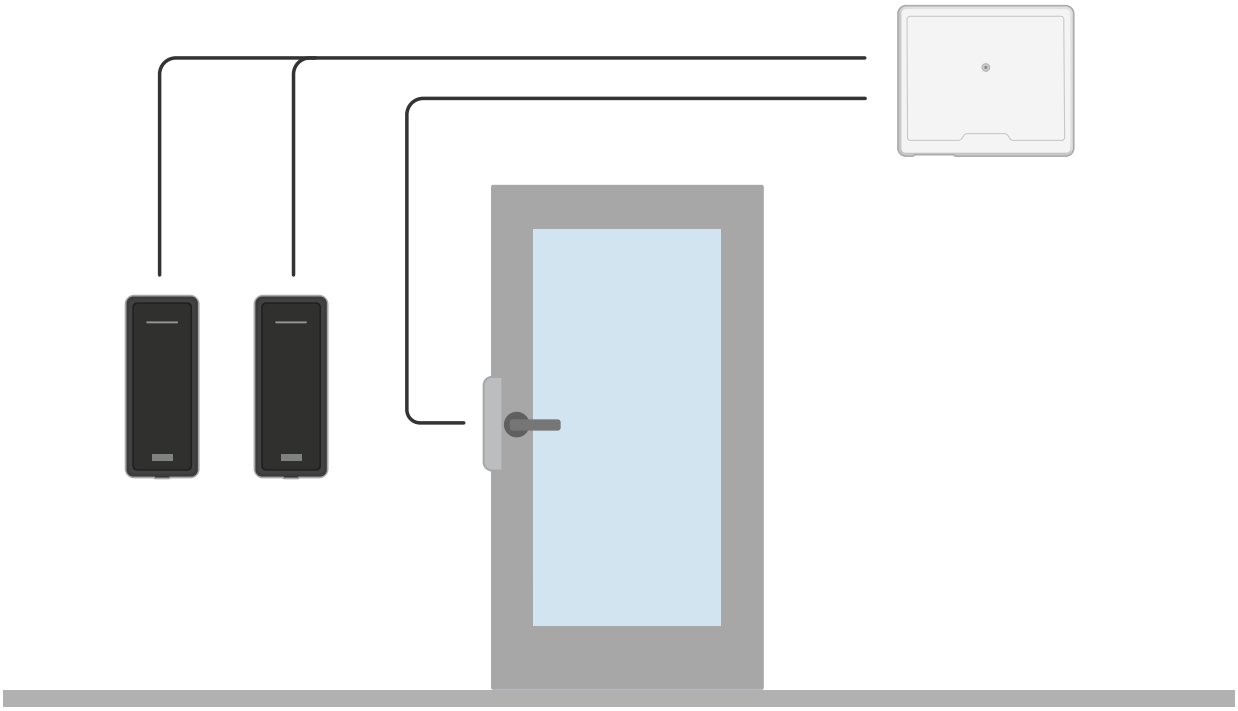
Inhalt

Lösungsübersicht 2
Installation 3
..... 3
Funktionsweise 4
Das Gerät im Netzwerk ermitteln 4
Unterstützte Browser 4
Weboberfläche des Geräts öffnen 4
Erstellen Sie ein Administratorenkonto 4
Sichere Kennwörter 5
Stellen Sie sicher, dass die Gerätesoftware nicht manipuliert wurde 5
Übersicht über die Weboberfläche 5
Ihr Gerät konfigurieren 6
Door override (Zugangsvorrang) 6
OSDP-LED-Profil 6
Kartenformat 7
Weboberfläche 9
Mehr erfahren 10
Cybersicherheit 10
Signiertes Betriebssystem 10
Sicheres Hochfahren 10
Axis Edge Vault 10
Axis Geräte-ID 10
Technische Daten 11
Produktübersicht 11
..... 11
LED-Anzeigen 11
Tasten 12
Steuertaste 12
Anschlüsse 12
Netzwerk-Steckverbinder 12
Stromprioritä 12
Lesegerätanschluss 12
Türanschluss 14
Relaisanschluss 14
Zusatzanschluss 15
Externer Anschluss 16
Stromanschluss 17
Überwachte Eingänge 17
Fehlerbehebung 19
Zurücksetzen auf die Werkseinstellungen 19
Optionen für AXIS OS 19
Aktuelle AXIS OS-Version überprüfen 19
AXIS OS aktualisieren 20
Technische Probleme und mögliche Lösungen 20
Support 22
Cybersicherheit 23
Schwachstellen-Management 23
Sicherheitsbenachrichtigungen 23
Sicherer Produktlebenszyklus 23

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 Funktion ausgestattete Geräte, die einfach in Türnähe angebracht werden können. Sie können bis zu zwei Lesegeräte mit Strom versorgen und steuern.

Installation



Funktionsweise

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

✓: Empfohlen

*: Wird mit Einschränkungen unterstützt

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 Administratorenkonto, on page 4*.

Eine Beschreibung aller Funktionen und Einstellungen in der Weboberfläche von Geräten mit AXIS OS finden Sie in der *Hilfe zur AXIS OS-Weboberfläche*.

Erstellen Sie ein Administratorenkonto

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

1. Geben Sie ein Konto ein.
2. Geben Sie ein Passwort ein. Siehe *Sichere Kennwörter, on page 5*.
3. Geben Sie das Kennwort erneut ein.
4. Stimmen Sie der Lizenzvereinbarung zu.
5. Klicken Sie auf **Konto 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, on page 19*.

Sichere Kennwörter

Wichtig

Verwenden Sie HTTPS (das standardmäßig aktiviert ist), um Ihr Kennwort oder andere sensible Einstellungen über das Netzwerk festzulegen. HTTPS ermöglicht sichere und verschlüsselte Netzwerkverbindungen und schützt so sensible Daten wie beispielsweise Kennwörter.

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.
- Ändern Sie das Kennwort regelmäßig und mindestens einmal jährlich.

Stellen Sie sicher, dass die Gerätesoftware nicht manipuliert wurde.

So stellen Sie sicher, dass das Gerät über seine ursprüngliche AXIS OS-Version verfügt, bzw. übernehmen nach einem Sicherheitsangriff die volle Kontrolle über das Gerät:

1. Zurücksetzen auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 19*. 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.



Weboberfläche des Axis Geräts

Ihr Gerät konfigurieren

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

Door override (Zugangsvorrang)

Wichtig

Diese Funktion übernimmt die direkte Steuerung der Türrelais und setzt die Relais-Konfiguration in AXIS Camera Station außer Kraft. Verwenden Sie diese Option nur, wenn Sie vom Axis Support dazu aufgefordert wurden.

1. Beenden Sie den Dienst „Secure Entry" in AXIS Camera Station.
2. Rufen Sie in der Weboberfläche der Tür-Steuerung **Advanced (Erweitert) > Door override (Tür außer Kraft setzen)** auf.
3. Lesen Sie die Informationen auf der Seite sorgfältig durch und klicken Sie anschließend auf **I understand (Ich habe verstanden)**.
4. Aktivieren Sie **Door override (Tür außer Kraft setzen)** und klicken Sie auf **Enable (Aktivieren)**.
5. Rufen Sie das Türrelais auf und klicken Sie **Lock (Verriegeln)**, **Unlock (Entriegeln)** oder **Access (Zugang)**, um die Tür zu verriegeln, zu entriegeln oder Zugang zu gewähren.
6. Rufen Sie das Relais auf, das Sie konfigurieren möchten, und klicken Sie auf **Activate (Aktivieren)** oder **Deactivate (Deaktivieren)**, um das Relais zu aktivieren oder zu deaktivieren.

OSDP-LED-Profil

Sie können die LED-Profile Ihres OSDP-Lesers anpassen, um die Lichteffekte und Töne festzulegen, die bei verschiedenen Ereignissen verwendet werden. Eine vollständige Liste der Profile finden Sie unter *LED profiles (LED-Profile)*.

Licht- und Audiopegel einstellen

1. Rufen Sie **Peripherals (Peripheriegeräte)** > **Readers (Leser)** > **OSDP LED profile (OSDP-LED-Profil)** auf.
2. Öffnen Sie das Drop-Down Menü **Light and audio levels (Licht- und Geräuschpegel)**.
3. Stellen Sie mit dem Schieber die Helligkeit des LED-Streifens, des Gegenlichts und der Lautstärke ein.
4. Klicken Sie auf **Save (Speichern)**.

Hinweis

Wenn Sie die Einstellungen für Licht und Geräuschpegel ändern, werden diese Einstellungen für alle an den Controller angeschlossenen Leser aktualisiert.

OSDP-LED-Einstellungen testen:

Über das **OSDP-LED-Testmenü** können Sie die Audio- und Beleuchtungseinstellungen für jedes Ihrer Leserprofile einsehen.

So testen Sie die Einstellungen für Ihre OSDP-LED-Profile:

1. Rufen Sie **Peripherals (Peripheriegeräte)** > **Readers (Leser)** > **OSDP LED profile (OSDP-LED-Profil)** auf.
2. Erweitern Sie das Drop-Down-Menü **OSDP LED test (OSDP-LED-Test)**.
3. Wählen Sie eine LED-Anzeige aus.
4. Wählen Sie den Leser aus, den Sie testen möchten.
5. Klicken Sie auf **Start**.
6. Klicken Sie auf **Edit feedback (Feedback bearbeiten)**, um die Licht- und Audio-Einstellungen für Ihr Profil zu ändern.
   - Wählen Sie im Drop-Down -Menü **Color (Farbe)** eine neue Farbe aus.

- Wählen Sie gegebenenfalls eine Audiofrequenz aus dem Drop-Down-Menü **Audio** aus.
- Sie können die Einstellungen des Profils auch zurücksetzen, indem Sie auf **Reset to default values (Auf Standardwerte zurücksetzen)** klicken.
- Klicken Sie auf **Save (Speichern)**.

Einstellungen des OSDP-LED-Profils ändern:

1. Rufen Sie **Peripherals (Peripheriegeräte)** > **Readers (Leser)** > **OSDP LED profile (OSDP-LED-Profil)** auf.
2. Wechseln Sie zum **OSDP LED profile (OSDP-LED-Profil)**.
3. Klicken Sie auf neben dem Profil, das Sie ändern möchten.
4. Bearbeiten Sie die entsprechenden Einstellungen:
   - Wählen Sie im Drop-Down-Menü **Behavior (Verhalten)** das gewünschte Verhalten für Ihre LEDs aus.
   - Wählen Sie die Farbe Ihrer LEDs aus dem Drop-Down-Menü **Color (Farbe)** aus.
   - Stellen Sie die **Einschalt-** und **Ausschaltdauer** für Ihre LEDs ein.
   - Stellen Sie die **Wiederholungsrate** der LED-Anzeige ein.
   - Wählen Sie im Drop-Down-Menü **Audio** die Optionen **Beep duration, on (Signalton-Dauer, ein)** und **Beep duration, off (Signalton-Dauer, aus)** aus und stellen Sie die **Wiederholungsrate** Ihrer Signalton-Reaktion ein. Stellen Sie sicher, dass **Beep duration, on (Signalton-Dauer, ein)** und **Beep duration, off (Signalton-Dauer, aus)** identisch sind.
5. Klicken Sie auf **Save (Speichern)**.

Vorhandene Einstellungen von einem anderen Controller importieren

1. Rufen Sie **Peripherals (Peripheriegeräte)** > **Readers (Leser)** > **OSDP LED profile (OSDP-LED-Profil)** auf.
2. Klicken Sie auf **Import (Importieren)**.
3. Wählen Sie die Datei aus, die Sie hochladen möchten.
4. Klicken Sie auf **Import (Importieren)**.

Aktuelle Einstellungen exportieren

1. Rufen Sie **Peripherals (Peripheriegeräte)** > **Readers (Leser)** > **OSDP LED profile (OSDP-LED-Profil)** auf.
2. Klicken Sie auf **Export (Exportieren)**.
3. Wählen Sie den Speicherort zum Speichern der JSON-Datei aus und klicken Sie auf **Save (Speichern)**.

Kartenformat

Diese Funktion ist ausschließlich für erfahrene Nutzer bestimmt. Sobald das **Kartenformat** eingeschaltet ist:

- Wenn Sie 37 Bit umfassende Zugangsdaten verwenden, werden die letzten 5 Bits entfernt.
- Wenn Sie 64-Bit-Zugangsdaten (QR-Code) verwenden, wird die erste 24-Bit-Sequenz entfernt.

Sie können entweder die Beispieldaten oder den Kartenleser verwenden, um die Zugangsdaten anzuzeigen.

1. Wechseln Sie zu **Advanced (Erweitert)** > **Card format (Kartenformat)**.
2. Lesen Sie die Warnung und klicken Sie auf **„Ich verstehe"**, um das **Kartenformat** zu aktivieren.
3. Wählen Sie im Drop-Down-Menü **Reader data visualization (Datenvisualisierung für den Leser)** Ihren Leser aus.
4. Klicken Sie auf **Get reader data (Leserdaten abrufen)** oder **Use sample data (Beispieldaten verwenden)**, um einen Ausgang für Karten zu erstellen. Dies gilt für alle Karteninhaber auf dem Gerät.

5. Schalten Sie die Option **Trim reader data (Leserdaten kürzen)** ein, um die Endbits aus den Zugangsdaten der Karte zu entfernen.
6. **Aktivieren** anklicken.

Weboberfläche

Informationen zu allen Funktionen und Einstellungen, die in der Weboberfläche von Geräten mit AXIS OS verfügbar sind, finden Sie in der *Hilfe zur AXIS OS-Weboberfläche*.

Mehr erfahren

Cybersicherheit

Produktspezifische Informationen zur Cybersicherheit finden Sie im Datenblatt des Produkts unter axis.com.

Ausführliche Informationen zur Cybersicherheit in AXIS OS finden Sie im *AXIS OS Härtungsleitfaden*.

Signiertes Betriebssystem

Signiertes OS wird vom Softwarehersteller implementiert, der das AXIS OS-Image mit einem privaten Schlüssel signiert. Wenn die Signatur an das Betriebssystem angefügt wurde, validiert das Gerät die Software vor der Installation. Wenn das Gerät feststellt, dass die Integrität der Software beeinträchtigt ist, wird die Aktualisierung von AXIS OS abgelehnt.

Sicheres Hochfahren

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

Axis Edge Vault

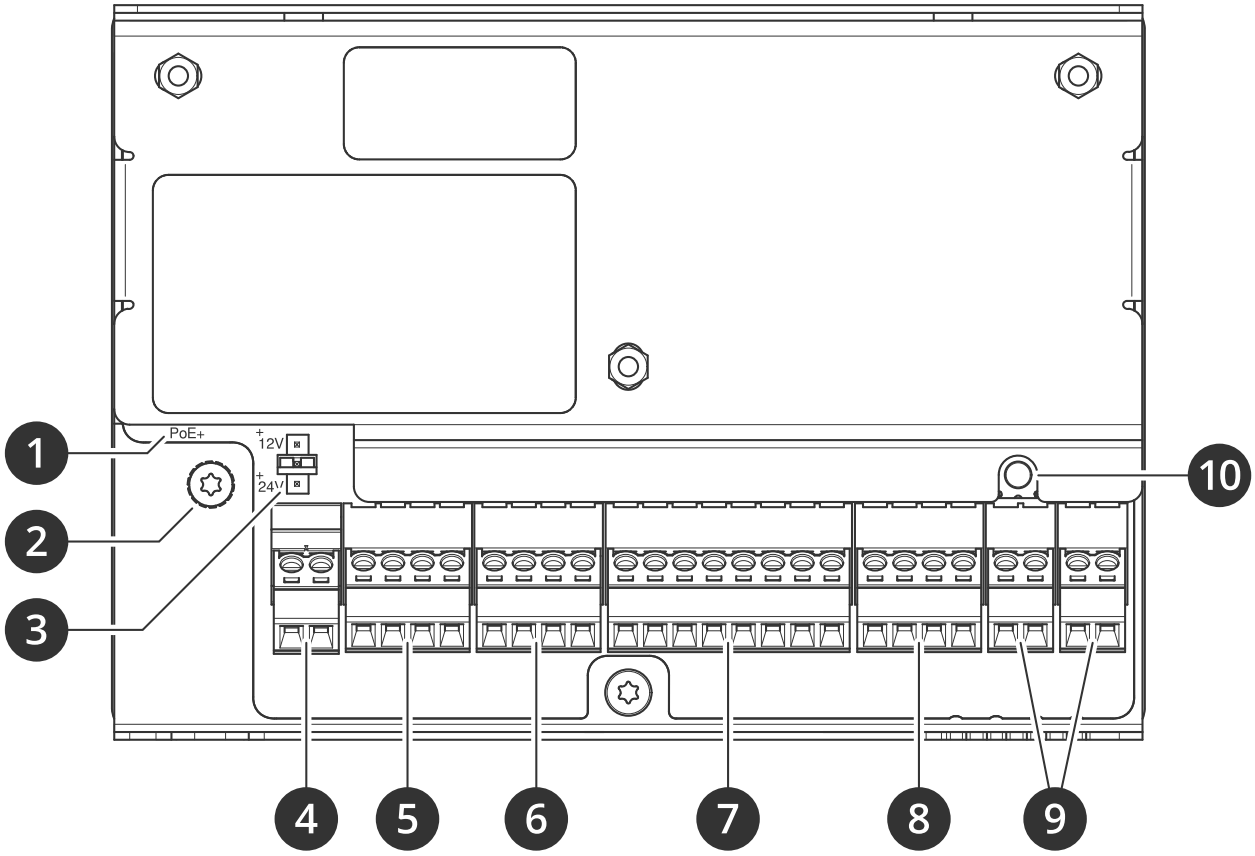
Axis Edge Vault stellt eine Hardware-basierte Cybersicherheitsplattform bereit, die das Axis Gerät schützt. Sie bietet Funktionen, die die Identität und Integrität des Geräts gewährleisten und Ihre vertraulichen Daten vor unbefugtem Zugriff schützen. Es sorgt für eine starke Grundlage kryptografischer Berechnungsmodule (Sicherheitselement und TPM) und SoC-Sicherheit (TEE und Secure Boot), die wir mit Expertise in Edge-Gerätesicherheit kombinieren.

Axis Geräte-ID

Den Ursprung eines Gerätes überprüfen zu können, ist der Schlüssel zum Vertrauen in die Geräteidentität. In der Produktion wird Geräten mit Axis Edge Vault ein eindeutiges, von der Fabrik bereitgestelltes und IEEE 802.1AR-kompatibles Zertifikat für die Axis Geräte-ID zugewiesen. Dies funktioniert wie ein Reisepass und weist den Ursprung des Gerätes nach. Die Geräte-ID wird sicher und permanent als vom Axis Root-Zertifikat signiertes Zertifikat im sicheren Schlüsselspeicher aufbewahrt. Die Geräte-ID kann über die IT-Infrastruktur des Kunden für ein automatisiertes, sicheres Geräte-Onboarding und sichere Geräteidentifizierung genutzt werden.

Technische Daten

Produktübersicht



1 *Netzwerk-Steckverbinder*
2 *Position Erdung*
3 *Relaisbrücke*
4 *Stromanschluss*
5 *Relaisanschluss*
6 *Türanschluss*
7 *Lesegerätanschluss*
8 *Zusatzanschluss*
9 *Externe Anschlüsse*
10 *Steuertaste*

LED-Anzeigen

LED	Farbe	Anzeige
Status	Grün	Leuchtet bei Normalbetrieb grün.
	Gelb	Dauerhaft beim Hochfahren und beim Wiederherstellen von Einstellungen
	Rot	Blinkt langsam bei einem Aktualisierungsfehler.
Netzwerk	Grün	Dauerhaft bei Verbindung mit einem Netzwerk mit 100 MBit/s Blinkt bei Netzwerkaktivität.
	Gelb	Dauerhaft bei Verbindung mit einem 10 MBit/s-Netzwerk. Blinkt bei Netzwerkaktivität.
	Aus	Keine Netzwerk-Verbindung

Stromversorgung	Grün	Normalbetrieb.
	Gelb	Blinkt während einer Firmware-Aktualisierung grün/orange.
Relais	Grün	Relais aktiv.[1]
	Aus	Relais nicht aktiv.

Tasten

Steuertaste

Die Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 19*.

Anschlüsse

Netzwerk-Steckverbinder

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.

Stromprioritität

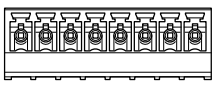
Dieses Gerät kann entweder über PoE oder Gleichstromeingang mit Strom versorgt werden. Siehe *Netzwerk-Steckverbinder, on page 12* und *Stromanschluss, on page 17*.

- 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 können bis zu zwei OSDP-Leser (Multi-Drop) oder ein Wiegand-Leser angeschlossen werden. 500 mA bei 12 V DC sind für alle an die Tür-Steuerung angeschlossenen Kartenleser reserviert.



Für einen OSDP-Leser konfiguriert

1. *Aktives Relais wenn COM an NO angeschlossen.*

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

Für zwei OSDP-Leser konfiguriert (Mehrfach-Drop)

Funktion	Pin	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	Pin	Hinweis	Technische Daten
Erdung Gleichstrom (GND)	1		0 V Gleichstrom
Gleichstromausgang (+12 V)	2	Versorgt das Netzgerät 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

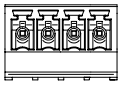
Wichtig

- 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.

Türanschluss

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 Anschlussschaltdiagramm für überwachte Eingänge beachten. Siehe *page 17*.



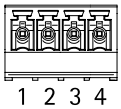
Funktion	Pin	Hinweise	Technische Daten
Erdung Gleichstrom	1, 3		0 V Gleichstrom
Eingang	2, 4	Zur Kommunikation mit dem Türmonitor. Digitaleingang oder überwachter Eingang – Zum Aktivieren an Kontakt 1 oder 3 anschließen, zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom

Wichtig

Das Kabel darf bis zu 200 m (656 ft) lang sein, wenn es folgende Anforderungen erfüllt: AWG 24.

Relaisanschluss

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



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

NEIN	2	Schließer-Kontakt. Zum Anschluss von Relaisgeräten. Schalten Sie ein ausfallsicheres Schloss zwischen NO und DC-Masse an. Bei Nichtverwendung der Steckbrücken sind die zwei Relaiskontakte galvanisch vom restlichen Schaltkreis getrennt.	Max. Strom = 2 A Max. Spannung = 30 V DC
COM	3	Gemeinsam	
NC	4	Öffner-Kontakt. Zum Anschluss von Relaisgeräten. Schalten Sie ein ausfallsicheres Schloss zwischen NC und DC-Masse an. Bei Nichtverwendung der Steckbrücken sind die zwei Relaiskontakte galvanisch vom restlichen Schaltkreis 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, nichtpolare Schlösser mit einer externen Schutzdiode auszustatten.

Zusatzanschluss

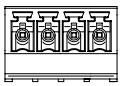
Über den Zusatzanschluss wird Zusatzausrüstung für Funktionen wie Manipulationsalarm, Bewegungserkennung, Ereignisauslösung, Alarmbenachrichtigung und andere angeschlossen. Abgesehen vom Bezugspunkt 0 V Gleichstrom und Strom (Gleichstromausgang) verfügt der Zusatzanschluss über eine Schnittstelle zum:

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

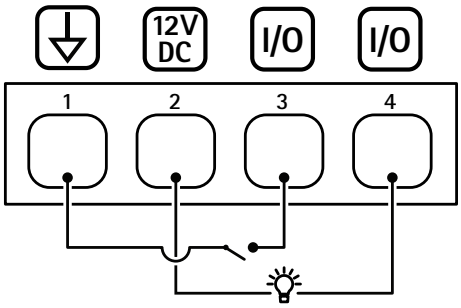
Überwachter Eingang – Ermöglicht das Erfassen von Manipulation an einem digitalen Eingang.

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	Pin	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstrom-ausgang	2	Kann für die Stromversorgung von Zusatzausrüstung verwendet werden. Hinweis: Dieser Kontakt kann nur als Stromausgang verwendet werden.	12 V Gleichstrom 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 I/O kann eine externe Last mit 12 V Gleichstrom und 50 mA (max. kombiniert) antreiben, wenn ein interner 12-V-Gleichstromausgang (Pin 2) verwendet wird. Bei der Verwendung von Open-Drain-Anschlüssen in Kombination mit einer externen Stromversorgung können die E/As eine Gleichstromversorgung von jeweils 0 bis 30 V DC, 100 mA bereitstellen.	0 bis max. 30 V Gleichstrom, Open Drain, 100 mA

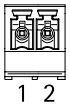


1 *Erdung Gleichstrom*
2 *Gleichstromausgang 12 V*
3 *E/A als Eingang konfiguriert*
4 *E/A als Ausgang konfiguriert*

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	Pin	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	Pin	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. Eine den Anforderungen für Schutzkleinspannung (SELV) entsprechende Stromquelle mit begrenzter Leistung (LPS) verwenden. Die Nennausgangsleistung muss dabei auf ≤100 W begrenzt sein oder der Nennausgangsstrom auf ≤5 A.



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

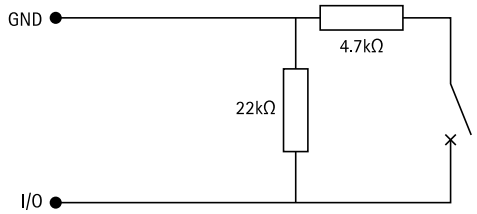
UL: Die Gleichstromleistung muss je nach Anwendung über ein UL 603-gelistetes Netzteil mit entsprechenden Nennleistungen bereitgestellt werden.

Überwachte Eingänge

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

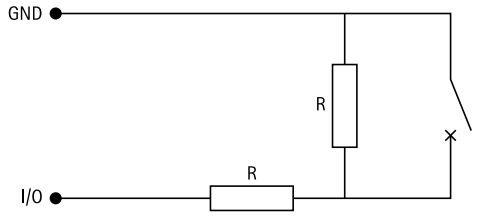
Parallele erste Verbindung

Die Widerstandswerte müssen 4,7 kΩ und 22 kΩ betragen.



Serielle erste Verbindung

Die Widerstandswerte müssen identisch sein und die möglichen Werte sind 1 kΩ, 2,2 kΩ, 4,7 kΩ und 10 kΩ.



Hinweis

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

Fehlerbehebung

Zurücksetzen auf die Werkseinstellungen

Wichtig

Das Zurücksetzen auf die Werkseinstellungen muss mit Umsicht geschehen. Beim Zurücksetzen auf die Werkseinstellungen werden alle Einstellungen einschließlich der IP-Adresse zurückgesetzt.

Um das Produkt auf die Werkseinstellungen zurückzusetzen:

1. Trennen Sie das Gerät von der Stromversorgung.
2. Halten Sie die Steuertaste gedrückt und stellen Sie die Stromversorgung wieder her. Siehe *Produktübersicht, on page 11*.
3. Halten Sie die Steuertaste 25 Sekunden gedrückt, bis die LED-Statusanzeige zum zweiten Mal gelb leuchtet.
4. Lassen Sie die Steuertaste los. Der Vorgang ist abgeschlossen, wenn die LED-Statusanzeige grün wird. Wenn im Netzwerk kein DHCP-Server verfügbar ist, wird die IP-Adresse des Geräts standardmäßig auf eine der folgenden Adressen eingestellt:
   - **Geräte mit AXIS OS 12.0 und höher:** Beziehen sich auf das Subnetz der Adressen lokaler Links (169.254.0.0/16)
   - **Geräte bis AXIS OS 11.11:** 192.168.0.90/24
5. Die Softwaretools für das Installieren und Verwalten ermöglichen das Zuweisen von IP-Adressen, Festlegen des Kennworts und Zugreifen auf das Produkt.

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

Optionen für AXIS OS

Axis bietet eine Softwareverwaltung für Geräte 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, AXIS OS 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 Gerätesoftware finden Sie unter *axis.com/support/device-software*.

Aktuelle AXIS OS-Version überprüfen

AXIS OS bestimmt die Funktionalität unserer Geräte. Wir empfehlen Ihnen, vor jeder Problembehebung zunächst die aktuelle AXIS OS-Version zu überprüfen. Die aktuelle Version enthält möglicherweise eine Verbesserung, die das Problem behebt.

So überprüfen Sie die aktuelle AXIS OS-Version:

1. Rufen Sie die Weboberfläche des Geräts > **Status** auf.
2. Die AXIS OS-Version ist unter **Device info (Geräteinformationen)** angegeben.

AXIS OS aktualisieren

Wichtig

- Bei der Aktualisierung der Gerätesoftware werden Ihre vorkonfigurierten und benutzerdefinierten Einstellungen gespeichert. Axis Communications AB kann nicht garantieren, dass die Einstellungen gespeichert werden, selbst wenn die Funktionen in der neuen AXIS OS-Version verfügbar sind.
- Ab AXIS OS 12.6 müssen Sie jede einzelne LTS-Version zwischen der aktuellen Version Ihres Geräts und der Zielversion installieren. Wenn beispielsweise die derzeit installierte Gerätesoftwareversion AXIS OS 11.2 ist, müssen Sie die LTS-Version AXIS OS 11.11 installieren, bevor Sie das Gerät auf AXIS OS 12.6 aktualisieren können. Weitere Informationen finden Sie unter *AXIS OS Lifecycle guide: Upgrade path* (AXIS OS Lebenszyklus-Leitfaden: Aktualisierungspfad).
- Stellen Sie sicher, dass das Gerät während der Aktualisierung an die Stromversorgung angeschlossen ist.

Hinweis

- Beim Aktualisieren mit der aktuellen AXIS OS-Version im aktiven Track werden auf dem Gerät die neuesten verfügbaren Funktionen bereitgestellt. Lesen Sie vor der Aktualisierung stets die entsprechenden Aktualisierungsanweisungen und Versionshinweise. Die aktuelle AXIS OS-Version und die Versionshinweise finden Sie unter *axis.com/support/device-software*.
- Da im Zuge einer AXIS OS-Aktualisierung die Datenbank mit den Daten der Benutzer und Gruppen, Zugangsdaten und anderen Informationen aktualisiert wird, kann der erste Start einige Minuten dauern. Die dafür benötigte Zeit hängt von der Datenmenge ab.

1. Die AXIS OS-Datei können Sie von *axis.com/support/device-software* kostenlos auf Ihren Computer herunterladen.
2. Melden Sie sich auf dem Gerät als Administrator an.
3. Rufen Sie **Maintenance (Wartung) > AXIS OS upgrade (AXIS OS-Aktualisierung)** auf und klicken Sie **Upgrade (Aktualisieren)** an.

Nach der Aktualisierung wird das Produkt automatisch neu gestartet.

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

Technische Probleme und mögliche Lösungen

Probleme beim Aktualisieren von AXIS OS

Aktualisierung von AXIS OS fehlgeschlagen

Nach fehlgeschlagener Aktualisierung lädt das Gerät erneut die Vorversion. Die häufigste Fehlerursache ist, wenn eine falsche AXIS OS-Datei hochgeladen wurde. Überprüfen, ob der Name der AXIS OS-Datei dem Gerät entspricht und erneut versuchen.

Probleme nach der AXIS OS-Aktualisierung

Bei nach dem Aktualisieren auftretenden Problemen die Installation über die **Wartungsseite** auf die Vorversion zurücksetzen.

Probleme beim Einrichten der IP-Adresse

IP-Adresse kann nicht eingestellt werden

- 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 unter Umständen von einem anderen Gerät verwendet. Zur Überprüfung:
  1. Trennen Sie das Axis Gerät vom Netzwerk.
  2. Geben Sie in einem Befehls-/DOS-Fenster `ping` und die IP-Adresse des Geräts ein.
  3. Erscheint daraufhin `Reply from <IP address>: bytes=32; time=10...`, heißt das, 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.
  4. `Request timed out` bedeutet, dass die IP-Adresse mit dem Axis Gerät verwendet werden kann. Prüfen Sie alle Kabel und installieren Sie das Gerät erneut.
- Es besteht unter Umständen ein Konflikt mit der IP-Adresse eines anderen Geräts 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.

Probleme beim Zugriff auf das Gerät

Anmeldung bei Gerätezugriff über einen Browser nicht möglich

Stellen Sie bei aktiviertem HTTPS sicher, dass Sie das richtige Protokoll (HTTP oder HTTPS) bei der Anmeldung verwenden. Gegebenenfalls müssen Sie manuell `http` oder `https` in das Adressfeld des Browsers eingeben.

Bei Verlust des Kennworts für das Haupt-Konto müssen Sie das Gerät auf die Werkseinstellungen zurücksetzen. Anweisungen finden Sie unter *Zurücksetzen auf die Werkseinstellungen, on page 19*.

Die IP-Adresse wurde von DHCP geändert

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. Das Gerät anhand seiner Modellnummer, Seriennummer oder anhand des DNS-Namens (sofern der Name konfiguriert wurde) ermitteln.

Bei Bedarf können Sie manuell eine statische IP-Adresse zuweisen. Anweisungen dazu finden Sie auf *axis.com/support*.

Zertifikatfehler beim Verwenden von IEEE 802.1X

Damit die Authentifizierung ordnungsgemäß funktioniert, müssen die Datums- und Uhrzeiteinstellungen des Axis Geräts mit einem NTP-Server synchronisiert werden. Gehen Sie auf **System > Date and time (System > Datum und Uhrzeit)**.

Der Browser wird nicht unterstützt.

Eine Liste der empfohlenen Browser finden Sie unter *Unterstützte Browser, on page 4*.

Externer Zugriff auf das Gerät ist nicht möglich

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

- AXIS Camera Station Edge: Kostenlos, ideal für kleine Systeme mit grundlegenden Überwachungsanforderungen.
- AXIS Camera Station Pro: Kostenlose 90-Tage-Testversion, ideal für kleine bis mittelgroße Systeme.

Auf *axis.com/vms* finden Sie Anweisungen und die Download-Datei.

Probleme mit MQTT

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

Die Firewall blockiert den Datenaustausch über Port 8883, da dieser als unsicher gilt.

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.

- 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.
- Wenn der Server/Broker ALPN unterstützt, kann die Verwendung von MQTT über einen offenen Port, z. B. 443, ausgehandelt werden. Erkundigen Sie sich bei Ihrem Server-/Brokeranbieter, ob ALPN unterstützt wird und welches ALPN-Protokoll und welchen Port Sie verwenden müssen.

Falls Sie hier nicht das Gesuchte finden, bitte den Bereich „Fehlerbehebung" unter *axis.com/support* aufrufen.

Support

Weitere Hilfe erhalten Sie hier: *axis.com/support*.

Cybersicherheit

Cybersicherheit trägt zu einem erfolgreichen Produktlebenszyklus bei, bei dem Risiken auf ein Minimum reduziert werden. Ausführliche Informationen und Dokumente zu unserer Cybersicherheitsstrategie finden Sie auf *axis.com/about-axis/cybersecurity*. Befolgen Sie die nachstehenden Richtlinien zur Cybersicherheit, um Sicherheitsbenachrichtigungen von Axis zu erhalten und Ihr Produkt für eine sichere Benutzung und Außerbetriebnahme zu konfigurieren.

Unter *Axis Trust Center* finden Sie Informationen darüber, wie Axis die Einhaltung von Sicherheitsvorschriften, Transparenz, Datenschutz und den Schutz der Privatsphäre implementiert.

Schwachstellen-Management

Axis ist eine *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)*. Um das Risiko einer Gefährdung für Sie so gering wie möglich zu halten, halten wir uns bei der Erkennung und Behebung von Sicherheitslücken in unseren Geräten, unserer Software und unseren Diensten an die Branchenstandards. Weitere Informationen zu unseren Richtlinien zur Verwaltung von Sicherheitslücken oder zur Meldung einer Schwachstelle finden Sie unter *axis.com/vulnerability-management*.

Sicherheitsbenachrichtigungen

Sicherheitsbenachrichtigungs-E-Mails von Axis können Sie auf *axis.com/security-notification-service* abonnieren. Wir informieren Sie über Schwachstellen, geben entsprechende Sicherheitshinweise und benachrichtigen Sie zu anderen sicherheitsrelevanten Themen für Ihr Axis Produkt.

Sicherer Produktlebenszyklus

Axis minimiert Risiken über die gesamte Lebensdauer unserer Produkte hinweg durch eine sichere Verwaltung des Lebenszyklus. Nutzen Sie unsere Sicherheitsrichtlinien unter *help.axis.com*, um Ihre Axis Produkte sicherer zu konfigurieren und zum Betrieb zu nutzen und um Informationen zu folgenden Themen zu erhalten:

Sichere Erstnutzung – Axis Produkte sind standardmäßig mit einem hohen Sicherheitsniveau in der Konfiguration vorkonfiguriert, um von Anfang an eine sichere Inbetriebnahme und verschlüsselte Kommunikation zu gewährleisten.

Bestimmungsgemäßer Gebrauch und häufige Fehler bei der Konfiguration – Unsere Anleitungen enthalten Informationen zur bestimmungsgemäßen Verwendung von Axis Produkten, einschließlich häufiger sicherheitsrelevanter Fehlbedienungen und Fehler bei der Konfiguration, die vermieden werden sollten.

Sicherheitslücken und Transparenz in der Lieferkette verwalten – Mit jeder Softwareversion wird auf *axis.com* eine Software-Bestellliste (SBOM) veröffentlicht, um Sicherheitslücken offenzulegen und die Transparenz in der Lieferkette zu verbessern.

Stilllegung und die sichere Löschung von Daten – Um ein Produkt am Ende seines Lebenszyklus sicher außer Betrieb zu nehmen, setzen Sie es auf die Werkseinstellungen zurück. Dadurch werden Ihre Konfigurationen, gespeicherten Daten und vertraulichen Informationen gelöscht.

T10181041_de

2026-10 (M11.6)

© 2022 – 2026 Axis Communications AB