AXIS TP3604-E Cellular Back Box

Benutzerhandbuch

Inhalt

Installation 3
Funktionsweise 4
- Das Gerät im Netzwerk ermitteln 4
  - Unterstützte Browser 4
- Weboberfläche des Geräts öffnen 4
- Erstellen Sie ein Administratorenkonto 4
- Sichere Kennwörter 4
- Stellen Sie sicher, dass die Gerätesoftware nicht manipuliert wurde 5

Ihr Gerät konfigurieren 6
- SIM-Verwaltung 6
- APN konfigurieren 6
- Signalstärke und IP-Adresse überprüfen 6
- Verbindung testen 6
- Management-Ports überprüfen 6
- Weiterleitung an die Kamera aktivieren 7
- IP-Zugehörigkeit der Kamera konfigurieren 7
  - Lokaler Modus 8
  - Passthrough-Modus 8
- Einrichten von Regeln für Ereignisse 9
  - Lösen Sie eine Aktion aus 9
  - Benachrichtigung bei Öffnen des Gehäuses auslösen 9

Weboberfläche 10
Technische Daten 11
- Produktübersicht 11
- LED-Anzeigen 11
- Tasten 12
  - Steuertaste 12
- Anschlüsse 12
  - PoE-Anschluss (PoE-Eingang) 12
  - Netzwerk-Anschluss (PoE-Ausgang) 12
  - Stromanschluss 12

Gerät reinigen 13
Fehlerbehebung 14
- Zurücksetzen auf die Werkseinstellungen 14
- Optionen für AXIS OS 14
- Aktuelle AXIS OS-Version überprüfen 14
- AXIS OS aktualisieren 15
- Technische Probleme und mögliche Lösungen 15
- Support 17

Cybersicherheit 18
- Schwachstellen-Management 18
- Sicherheitsbenachrichtigungen 18
- Sicherer Produktlebenszyklus 18

Installation



Das Video zeigt die Installation der AXIS TP3604-E Cellular Back Box am Beispiel einer AXIS P32 Dome Camera und einer AXIS P14 Bullet Camera.

Anweisungen für alle Installationsszenarien sowie Sicherheitshinweise finden Sie in der Installationsanleitung.

Funktionsweise

Das Gerät im Netzwerk ermitteln

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

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. Konfigurieren und installieren Sie das Gerät.

Ihr Gerät konfigurieren

Zur Konfiguration Ihres Geräts müssen Sie die folgenden Schritte ausführen:

1. *SIM-Verwaltung, on page 6*
2. Falls Ihr Netzwerk einen eindeutigen Zugangspunktnamen (Access Point Name, APN) benötigt, *APN konfigurieren, on page 6*
3. *Signalstärke und IP-Adresse überprüfen, on page 6*
4. *Verbindung testen, on page 6*
5. *Management-Ports überprüfen, on page 6*
6. *Weiterleitung an die Kamera aktivieren, on page 7*

SIM-Verwaltung

Die SIM-Verwaltung ist obligatorisch, wenn die SIM-PIN aktiviert ist. Wenn die SIM-PIN deaktiviert ist, können Sie diesen Schritt überspringen.

1. Setzen Sie die SIM-Karte ein. Gehen Sie zu **Modem > SIM management (SIM-Verwaltung) > SIM status (SIM-Status)** und überprüfen Sie, ob das Modem und die SIM-Karte erkannt wurden.
2. Wenn die SIM-PIN-Sperre aktiviert ist, gehen Sie zu **Modem > SIM management (SIM-Verwaltung) > SIM-PIN > Unlock (Entsperren)**, um die Sperre mit der richtigen PIN zu deaktivieren.

APN konfigurieren

Hinweis

Diesen Schritt müssen Sie nur dann ausführen, wenn Ihr Netzwerk einen eindeutigen APN (Access Point Name - Name des Zugangspunktes) benötigt.

Um einen eindeutigen APN zu konfigurieren, gehen Sie zu **Modem > Cellular network (Mobilfunknetz) > APN**.

Signalstärke und IP-Adresse überprüfen

Hinweis

Für diesen Schritt ist der Zugriff auf das Mobilfunknetz erforderlich.

1. Überprüfen Sie die Signalstärke unter **System > Modem > Cellular network (Mobilfunknetz) > Radio parameters (Funkparameter) > Signal strength index (Signalstärkemesswert)**. Drei bis vier Balken weisen auf eine gute Signalqualität hin.
2. Überprüfen Sie unter **System > Modem > Cellular network (Mobilfunknetz) > User equipment IP address (Endgeräte-IP-Adresse)**, ob eine Mobilfunk-IP-Adresse zugewiesen wurde.

Verbindung testen

Hinweis

Für diesen Schritt ist der Zugriff auf das Mobilfunknetz erforderlich.

1. Gehen Sie zu **System > Modem > Cellular network (Mobilfunknetz) > Test cellular connection (Mobilfunkverbindung testen)**. Geben Sie einen Host-Namen oder eine IP-Adresse ein.
2. Vergewissern Sie sich, dass eine Verbindung hergestellt werden kann.

Management-Ports überprüfen

Bevor Sie einen Routing-Modus endgültig aktivieren, überprüfen Sie die Management-Ports der Back Box.

1. Gehen Sie zu **Cellular routing (Mobilfunk-Routing) > Back box management ports (Management-Ports der Back Box)**.
2. Passen Sie bei Bedarf die Ports an, falls die Standardwerte vom Netzwerk nicht unterstützt werden.

Weiterleitung an die Kamera aktivieren

Der letzte Schritt besteht darin, die Weiterleitung an die Kamera zu aktivieren.

1. Gehen Sie zu **Cellular routing (Mobilfunk-Routing) > Main mode (Hauptmodus)** und klicken Sie auf **Enable forwarding to connected device (Weiterleitung an verbundenes Gerät aktivieren)**.

Sobald die Weiterleitung aktiviert ist, werden die normalen Serviceports an die Kamera weitergeleitet und die Verwaltung der Back Box ist weiterhin über die reservierten Management-Ports verfügbar.

2. Überprüfen Sie den Zugriff auf die Kamera: Geben Sie in einem Webbrowser die Mobilfunk-IP-Adresse gefolgt von der Portnummer 80 ein: `http://<cellular-ip-address>:80`.
3. Überprüfen Sie den Zugriff auf die Back Box: Geben Sie in einem Webbrowser die Mobilfunk-IP-Adresse gefolgt von der Portnummer 11080 (Standard-Management-Port der Back Box bei HTTP) ein: `http://<cellular-ip-address>:11080`.

IP-Zugehörigkeit der Kamera konfigurieren

Hinweis

Dieser Schritt ist optional und nur dann erforderlich, wenn Sie die Standard-Subnetzkonfiguration ändern oder die Subnetzkonfiguration anpassen müssen.

Ein Mobilfunknetz vergibt nur eine IP-Adresse, die dann an die ID der SIM-Karte gebunden ist. Eine normale Installation besteht aus einer Back Box und einer daran angeschlossenen Kamera. Der DHCP-Modus legt fest, welche IP-Adresse der Kamera zugewiesen wird. Das ist der Hauptgrund für die Wahl des DHCP-Modus.

Standardmäßig (im lokalen Modus) verbleibt die Mobilfunk-IP-Adresse bei der Back Box und der Kamera wird eine private IP-Adresse aus dem lokalen Netzwerk der Back Box zugewiesen. Die Kamera ist weiterhin uneingeschränkt über das Mobilfunknetz erreichbar. Diese Konfiguration reicht für die meisten Einsatzszenarien bereits aus und isoliert die Kamera sicher in einem privaten Netzwerk.

Der Unterschied wird sichtbar, wenn ein Tool die IP-Adresse aus der Perspektive der Kamera betrachtet. Wenn ein VMS die von der Kamera gemeldete IP-Adresse ausliest oder wenn die Kamera so konfiguriert ist, dass sie ihre IP-Adresse in einem Video-Overlay einblendet, handelt es sich bei dieser IP-Adresse um die private LAN-IP-Adresse der Kamera und nicht um die öffentliche Mobilfunk-IP-Adresse, über die der Zugriff von außen erfolgt. Die beiden IP-Adressen stimmen nicht überein, da die Mobilfunk-IP-Adresse der in der Backbox hinterlegten SIM-Karten-ID zugeordnet ist und nicht der Kamera.

Der Passthrough-Modus löst dieses Problem, indem er die eine IP-Adresse, die das Mobilfunknetz der Back Box zuweist, an die Kamera weitergibt. Wenn der Passthrough-Modus aktiviert ist, verfügt die Kamera über genau dieselbe vom Mobilfunknetz zugewiesene IP-Adresse, sodass die von der Kamera gemeldete Adresse (auch im Video-Overlay) mit der Adresse übereinstimmt, über die sie von außen erreichbar ist. Da die Kamera nun über die Mobilfunk-IP-Adresse verfügt, ändert sich dadurch auch, wie die Kamera andere Endgeräte im Mobilfunknetz erreichen kann.

Im weiteren Verlauf dieses Abschnitts werden die einzelnen Modi ausführlich beschrieben.

Sie können die an die Back Box angeschlossene Kamera an den Standardports (`80/443/554/22`) über die Mobilfunk-IP-Adresse und die Back Box weiterhin über die reservierten Management-Ports (z. B.`11080/11443/11554/11022`) erreichen.

Der Unterschied zwischen dem lokalen und dem Passthrough-Modus besteht in Folgendem:

Lokaler Modus

- Der Kamera wird ein privates lokales Subnetz zugewiesen.
- Die interne IP-Adresse der Kamera unterscheidet sich von der über das Mobilfunknetz erreichbaren IP-Adresse.
- Wenn Sie sich nicht sicher sind, wählen Sie den Modus mit lokalem DHCP.

Passthrough-Modus

- Der Kamera wird die Mobilfunk-IP-Adresse zugewiesen.

Lokaler Modus

Lokalen Modus aktivieren

1. Wählen Sie unter **Cellular routing (Mobilfunk-Routing) > Advanced DHCP configuration (Erweiterte DHCP-Konfiguration) > DHCP server mode (DHCP-Server-Modus)** die Option **Local (Lokal)** aus.
2. Überprüfen Sie unter **Cellular routing (Mobilfunk-Routing) > Advanced DHCP configuration (Erweiterte DHCP-Konfiguration) > Local private network configuration (Konfiguration des lokalen privaten Netzwerks)**, dass die lokale IP-Adresse der Kamera nicht in Konflikt zu einer anderen erreichbaren IP-Adresse im Netzwerk steht.
3. Ändern Sie bei Bedarf die IP-Adresse unter **Cellular routing (Mobilfunk-Routing) > Advanced DHCP configuration (Erweiterte DHCP-Konfiguration) > Local private network configuration (Konfiguration des lokalen privaten Netzwerks)**. Verwenden Sie für **Starting IP address (Anfangs-IP-Adresse)** und **Ending IP address (End-IP-Adresse)** denselben Wert.
4. Klicken Sie auf **Save (Speichern)**.

Passthrough-Modus

Wenn Endgeräte (also Kameras) nicht direkt miteinander kommunizieren und der Datenverkehr immer von einem anderen VMS-LAN zu den Endgeräten fließt, gibt es keinen Pfad zwischen den Endgeräten, der IP-Shadowing erlaubt. In diesem Fall ist der Passthrough-Modus gegen IP-Shadowing geschützt.

Allgemein betrachtet wird im Passthrough-Modus das Mobilfunknetz in Richtung der Kamera erweitert. Das ist nützlich, wenn die Kamera direkt unter der über Mobilfunk erreichbaren IP-Adresse erscheinen soll.

Ernstzunehmende Bedrohung: IP-Shadowing im Passthrough-Modus

Dieser Sicherheitshinweis gilt für Konfigurationen mit nur einer Kamera. Selbst bei nur einer Kamera werden im Passthrough-Modus dennoch zwei IP-Adressen im LAN-seitigen Subnetz benötigt:

- Eine IP-Adresse für die Kamera.
- Eine IP-Adresse für den Ethernet-seitigen DHCP-Server der Back Box.

Szenario 1: Minimales Subnetz für jedes Endgerät `(/30)`

Bei diesem Modell verfügt jedes Endgerät über ein kleines, eigenständiges Subnetz.

- Ein `(/30)` stellt zwei nutzbare Host-IP-Adressen bereit.
- Eine IP-Adresse wird von der Kamera genutzt.

Die verbleibende IP-Adresse verwendet der DHCP-Server der Back Box intern.

Empfehlung für Szenario 1:

- Halten Sie die einzelnen Subnetze der Endgeräte getrennt.
- Stellen Sie sicher, dass jedes Endgerätesubnetz eindeutig ist. Die Subnetze dürfen sich nicht bei mehreren Endgeräten überschneiden.

Szenario 2: Größeres gemeinsam genutztes Subnetz mit mehreren Endgeräten

Einige Konfigurationen nutzen ein größeres Subnetz, das sich mehrere Endgeräte teilen. Die Gefahr des IP-Shadowing besteht, wenn eine Kamera versucht, ein anderes Endgerät zu erreichen, die dieselbe IP-Adresse wie der DHCP-Server der Back Box verwendet. In diesem Fall wird der Datenverkehr möglicherweise an die lokale Adresse auf der Back-Box-Seite anstelle des beabsichtigten entfernten Endgeräts weitergeleitet.

Empfehlung für Szenario 2:

- Überprüfen Sie die IP-Adresse des Back-Box-DHCP-Servers in den Passthrough-Einstellungen.
- Stellen Sie sicher, dass diese IP-Adresse keinem anderen Endgerät zugewiesen ist.
- Stellen Sie sicher, dass diese IP-Adresse im Netzwerkdienstportal keiner SIM-Karte zugewiesen ist.

Passthrough-Modus aktivieren

Hinweis

Der Zugriff auf ein Mobilfunknetz ist erforderlich.

1. Wählen Sie unter **Cellular routing (Mobilfunk-Routing) > Advanced DHCP configuration (Erweiterte DHCP-Konfiguration) > DHCP server mode (DHCP-Server-Modus)** die Option **Passthrough** aus.
2. Überprüfen Sie unter **Cellular routing (Mobilfunk-Routing) > Advanced DHCP configuration (Erweiterte DHCP-Konfiguration) > Local private network configuration (Konfiguration des lokalen privaten Netzwerks) > Server IP and prefix length (Server-IP und Präfixlänge)**, dass die automatisch ausgewählte Server-IP und die Subnetzpräfixlänge nicht mit anderen erreichbaren IP-Adressen in Konflikt stehen.
3. Klicken Sie auf **Save (Speichern)**.

Einrichten von Regeln für Ereignisse

Weitere Informationen finden Sie unter *Erste Schritte mit Regeln für Ereignisse*.

Lösen Sie eine Aktion aus

1. Gehen Sie zu **System** > **Events (Ereignisse)** und klicken Sie auf **+ Add a rule (+Regel hinzufügen)**. Die Regel legt fest, wann das Gerät bestimmte Aktionen durchführt. Regeln können als geplant, wiederkehrend oder manuell ausgelöst eingerichtet werden.
2. Unter **Name** einen Dateinamen eingeben.
3. Wählen Sie die **Bedingung**, die erfüllt sein muss, damit die Aktion ausgelöst wird. Wenn für die Regel mehrere Bedingungen definiert werden, müssen zum Auslösen der Aktion alle Bedingungen erfüllt sein.
4. Wählen Sie, welche **Aktion** bei erfüllten Bedingungen durchgeführt werden soll.

Benachrichtigung bei Öffnen des Gehäuses auslösen

In diesem Beispiel wird erklärt, wie Sie eine E-Mail-Benachrichtigung einrichten, die bei Öffnen des Gehäuses versendet wird.

Einen E-Mail-Empfänger hinzufügen:

1. Rufen Sie **System (System) > Events (Ereignisse) > Recipients (Empfänger)** auf und klicken Sie auf **Empfänger hinzufügen**.
2. Geben Sie den Namen des Empfängers ein.
3. Wählen Sie **Email (E-Mail)** als Benachrichtigungsart aus.
4. Geben Sie die E-Mail-Adresse des Empfängers ein.
5. Geben Sie die E-Mail-Adresse ein, an die die Kamera die Benachrichtigungen senden soll.
6. Geben Sie die Anmeldedaten für das sendende E-Mail-Konto sowie den SMTP-Hostnamen und die Portnummer an.
7. Um Ihr E-Mail Setup zu testen, klicken Sie auf **Test**.
8. Klicken Sie auf **Save (Speichern)**.

Eine Regel erstellen:

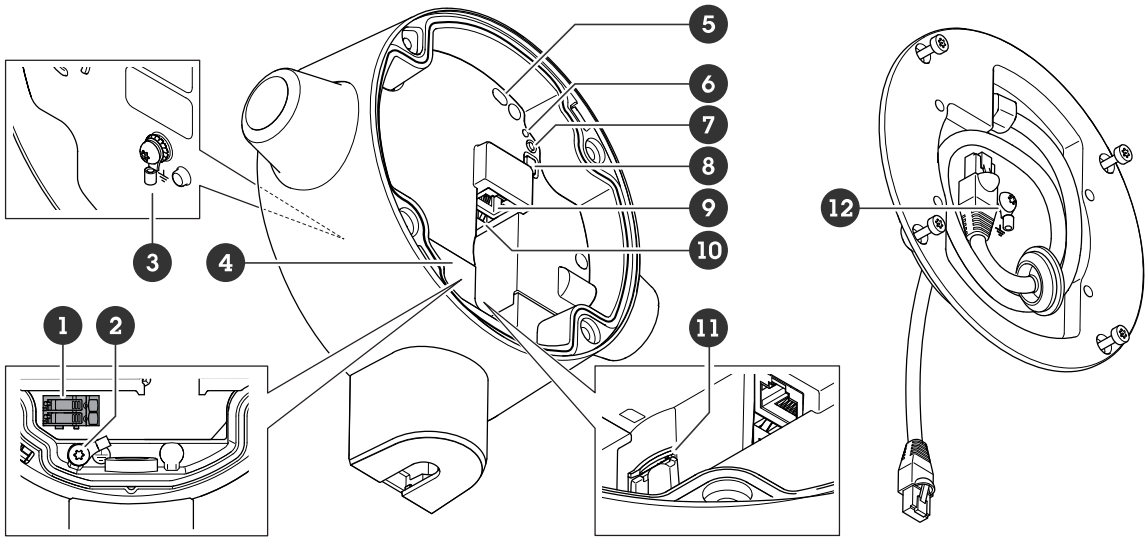
9. Gehen Sie zu **System > Ereignisse > Regeln** und klicken Sie auf **Regel hinzufügen**.
10. Geben Sie einen Namen für die Regel ein.
11. Wählen Sie aus der Liste der Bedingungen **Gehäuse wird geöffnet**.
12. Wählen Sie in der Aktionsliste **Benachrichtigung an E-Mail senden**.
13. Wählen Sie einen Empfänger aus der Liste aus.
14. Geben Sie eine Betreffzeile und eine Nachricht für die E-Mail ein.
15. Klicken Sie auf **Save (Speichern)**.

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*.

Technische Daten

Produktübersicht



1 *Wechselstromanschluss*
2 *Schutzerdung*
3 *Erdungsschraube*
4 *Schutzabdeckung (AC)*
5 *Melder zu geöffnetem Gehäuse*
6 *Reset-Taste*
7 *Status-LED*
8 *Steuertaste*
9 *PoE-Ausgang (Daten)*
10 *PoE-Eingang*
11 *SIM-Speicherkarteneinschub*
12 *Erdungsschraube (Kamera)*

LED-Anzeigen

Status-LED im Einrichtungsmodus

Status-LED	Anzeige
Aus	IR zur Erkennung eines geöffneten Gehäuses ist abgedeckt.
Grün	Normaler Betrieb; die Ethernet-Schnittstelle ist bereit.
Gelb	Leuchtet beim Start konstant. Blinkt während Gerätesoftwareaktualisierung und Wiederherstellung der Werkseinstellungen.
Gelb/rot	Keine Ethernet-Verbindung; Modem wird bei Systemstart konfiguriert.
Rot	Fehler bei der Aktualisierung der Gerätesoftware.

Status-LED im verbundenen Modus

Status-LED	Anzeige
Aus	IR zur Erkennung eines geöffneten Gehäuses ist abgedeckt.
Grün	Das Modem ist mit dem Netzwerk verbunden.
Gelb	Leuchtet beim Start konstant. Blinkt während Gerätesoftwareaktualisierung und Wiederherstellung der Werkseinstellungen.

Gelb/rot	Modem wird bei Systemstart konfiguriert.
Rot	Fehler bei der Aktualisierung der Gerätesoftware.

Tasten

Steuertaste

Die Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 14*.
- Herstellen einer Verbindung mithilfe eines O3C-Diensts mit nur einem Klick über das Internet. Um eine Verbindung herzustellen, drücken Sie die Taste, lassen Sie sie los und warten Sie, bis die Status LED dreimal grün blinkt.

Anschlüsse

PoE-Anschluss (PoE-Eingang)

RJ45-Ethernet-Anschluss mit Power over Ethernet (PoE) IEEE 802.3af/802.3at/802.3bt, Typ 3 Klasse 5.

Hinweis

Dieser Anschluss dient ausschließlich als Stromversorgungseingang; es ist keine Netzwerkverbindung verfügbar.

Hinweis

- Für einen PoE-Ausgang gemäß IEEE 802.3at Typ 2 Klasse 4 ist ein AC-Eingang erforderlich.
- Für einen PoE-Ausgang gemäß IEEE 802.3af Typ 1 Klasse 3 ist IEEE 802.3at Typ 2 Klasse 4 oder höher erforderlich.
- Bei einem PoE-Eingang gemäß IEEE 802.3af Typ 1, Klasse 3 ist das Gerät zwar funktionsfähig, kann aber keinen Stromausgang bereitstellen.

Hinweis

Die maximale Länge des Ethernet-Kabels beträgt 20 m.

Netzwerk-Anschluss (PoE-Ausgang)

Ethernet-Anschluss RJ-45

Hinweis

- Für einen PoE-Ausgang gemäß IEEE 802.3at Typ 2 Klasse 4 ist ein AC-Eingang erforderlich.
- Für einen PoE-Ausgang gemäß IEEE 802.3af Typ 1 Klasse 3 ist IEEE 802.3at Typ 2 Klasse 4 oder höher erforderlich.
- Bei einem PoE-Eingang gemäß IEEE 802.3af Typ 1, Klasse 3 ist das Gerät zwar funktionsfähig, kann aber keinen Stromausgang bereitstellen.

Hinweis

Die maximale Länge des Ethernet-Kabels beträgt 20 m.

Stromanschluss

Anschlussblock zum Anschluss an AC-Stromversorgung.

Hinweis

Für einen PoE-Ausgang gemäß IEEE 802.3at Typ 2 Klasse 4 ist ein AC-Eingang erforderlich.

Gerät reinigen

Sie können Ihr Gerät mit lauwarmem Wasser und milder, nicht scheuernder Seife reinigen.

HINWEIS

- Aggressive Chemikalien können das Gerät beschädigen. Verwenden Sie zur Reinigung Ihres Geräts keine chemischen Substanzen wie Fensterreiniger oder Aceton.
- Vermeiden Sie die Reinigung bei direktem Sonnenlicht oder bei erhöhten Temperaturen, da dies zu Flecken führen kann.

1. Verwenden Sie eine Druckluft-Dose zum Entfernen von Staub und Schmutz von dem Gerät.
2. Reinigen Sie das Gerät ggf. mit einem weichen, mit lauwarmem Wasser und lauwarmer, nicht scheuernder Seife angefeuchteten Mikrofasertuch.
3. Um eventuelle Reinigungsmittelrückstände zu entfernen, wischen Sie das Gerät mit einem weichen, mit lauwarmem Wasser angefeuchteten Mikrofasertuch ab.
4. Trocknen Sie das Gerät mit einem sauberen, nicht scheuernden Tuch ab, um Flecken zu vermeiden.

Weitere Informationen zur Reinigung von Axis Geräten finden Sie im Whitepaper *Chemische Beständigkeit gegenüber gängigen Reinigungsmitteln*.

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 etwa 15–30 Sekunden gedrückt, bis die Status-LED gelb blinkt.
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. Verwenden Sie Installations- und Verwaltungstools, um IP-Adressen zuzuweisen, das Kennwort festzulegen und auf das Gerät zuzugreifen.
   Die Softwaretools für die Installation und Verwaltung stehen auf den Supportseiten unter *axis.com/support* zur Verfügung.

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*.

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.

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 14*.

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, besuchen Sie den Bereich „Fehlerbehebung“ auf *axis.com/support*.

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.

T10233346_de

2026-10 (M2.2)

© 2026 Axis Communications AB