

## **AXIS Device Manager Extend**

# AXIS Device Manager Extend

## Inhalt

---

<b>Info</b> .....	3
<b>Über Organisationen</b> .....	4
<b>Lösungsübersicht</b> .....	5
<b>Voraussetzungen</b> .....	10
<b>Funktionsweise</b> .....	12
Ein MyAxis-Konto einrichten .....	12
Den Client installieren und Ihr Konto aktivieren .....	12
Organisation erstellen .....	12
Edge-Host installieren .....	12
Edge-Host anfordern .....	13
<b>Geräte verwalten</b> .....	14
Ihrem Edge-Host ermittelte Geräte hinzufügen .....	14
Geräte entfernen .....	15
Bei Ihren Geräten anmelden .....	15
<b>Konfiguration</b> .....	16
Fernzugriff aktivieren .....	16
Einen Standort entfernen .....	16
Hinzufügen von Benutzern zu Ihrer Organisation .....	16
Informationen zu Benutzerrollen .....	17
Benutzerrolle höherstufen .....	17
Benutzer entfernen .....	17
<b>AXIS OS-Verwaltung</b> .....	18
Verwaltung der AXIS OS-Versionen je nach Modell .....	18
Verwaltung von AXIS OS auf einem Edge-Host .....	18
Laufende und abgeschlossene AXIS OS-Aktualisierungen anzeigen .....	18
<b>Bestell- und Lieferbedingungen</b> .....	19
Eine Sicherheitsrichtlinie erstellen und anwenden .....	19
Eine App-Richtlinie erstellen und anwenden .....	19
Eine Richtlinie bearbeiten .....	20
Eine Richtlinie löschen .....	20
<b>Lizenzen verwalten</b> .....	21
Ihr Produkt lizenzieren .....	21
<b>Fehlerbehebung</b> .....	22
So konfigurieren Sie die Firewall-Einstellungen .....	22

# AXIS Device Manager Extend

## Info

---

### Info

Die Lösung AXIS Device Manager Extend stellt Systemadministratoren eine Schnittstelle zum Erkennen, Konfigurieren und Betreiben von Axis Geräten in den Netzwerken ihrer Organisation bereit.

#### Die Desktop-Anwendung AXIS Device Manager Extend

Bei der Desktop-Anwendung handelt es sich um ein Software-Dienstprogramm, das On-Demand oder über die stets verfügbare Benutzeroberfläche für die Verwaltung des Systems verwendet werden kann. Es kann auf einem dedizierten Rechner zusammen mit einem lokal installierten Edge-Host oder separat vom Edge-Host auf einem entfernt angeschlossenen Laptop ausgeführt werden. Der Client zeigt dem Benutzer den Gesamtstatus des Systems und leicht verfügbare Verwaltungsmaßnahmen an.

#### Der Edge-Host

Bei der Komponente Edge-Host in AXIS Device Manager Extend handelt es sich um einen stets verfügbaren, On-Premise-Verwaltungsservice, der für die Verwaltung von lokalen Geräten, wie Kameras, zuständig ist. Der Edge-Host im AXIS Device Manager Extend fungiert auch als Verbindung zum Axis Fernverwaltungsservice, wo dieselbe API-Funktionalität die Fernverwaltung von Standorten über die Axis Service-Plattform unterstützt.

# AXIS Device Manager Extend

## Über Organisationen

---

### Über Organisationen

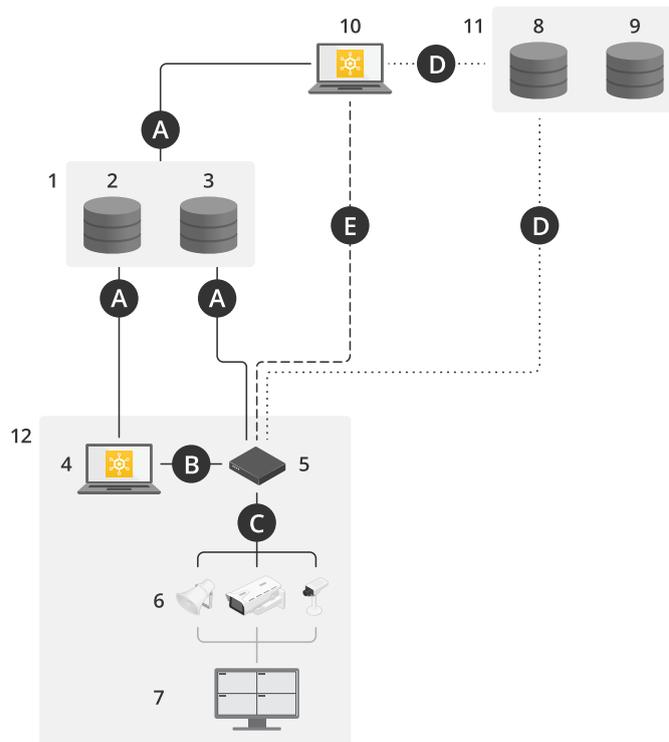
Die Organisation ist eine virtuelle Abbildung Ihrer Axis Systeminstallationen und die Zentrale Ihrer Cloud-Dienste. Eine Organisation hostet alle Geräte und Benutzerkonten eines Unternehmens in einer Hierarchie, die den Zugang regelt und maximale Sicherheit gewährleistet. Gleichzeitig ist eine flexible Benutzer- und Geräteverwaltung für kleine und große Unternehmen möglich.

- Wenn Sie eine neue Organisation erstellen, werden Sie Eigentümer. Die Organisation verbindet Ihr System mit den Benutzern des Cloud-Dienstes von Axis.
- Sie können Benutzer zur Organisation einladen. Siehe *Hinzufügen von Benutzern zu Ihrer Organisation auf Seite 16*.
- Sie können Benutzern verschiedene Rollen zuweisen.
- Die Organisation enthält einen Standardordner, in dem Sie Ihre Strukturen entsprechend Ihren Anforderungen erstellen können. Organisationen können in Form von Ordnern und Unterordnern strukturiert werden. Ein Ordner steht in der Regel für den konkreten Stand- bzw. Einsatzort eines Systems innerhalb einer Organisation.
- Verwalten Sie Ihre Lizenzen für Ihr System innerhalb Ihrer Organisation.
- Zum Erstellen einer Organisation benötigen Sie ein My Axis Konto.

# AXIS Device Manager Extend

## Lösungsübersicht

### Lösungsübersicht



AXIS Device Manager Extend mit lokalem Zugriff und Fernzugriff

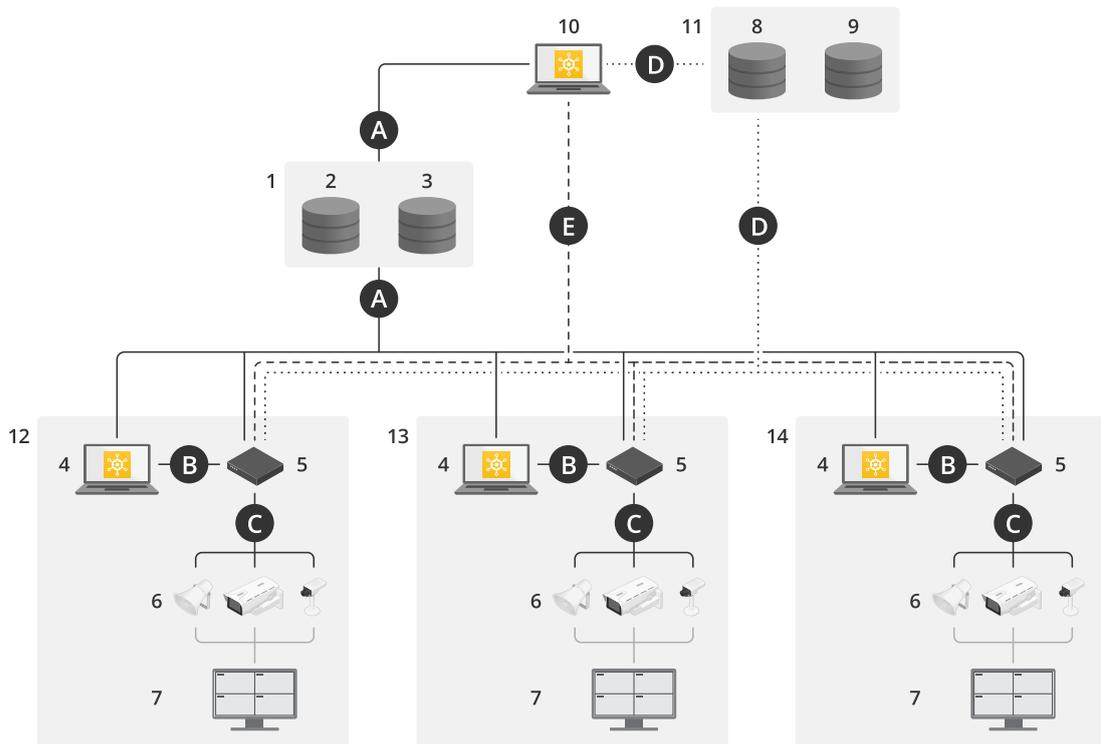
- 1 Axis
- 2 IAM (My Axis)
- 3 Organisationsdaten
- 4 Lokaler Client
- 5 Edge-Host
- 6 Geräte
- 7 VMS
- 8 TURN
- 9 Signalgebung
- 10 Remote Client
- 11 Fernzugriff auf WebRTC-Server
- 12 Standort 1

Verbindung	URL und IP	Port	Protokoll	Kommentar
A	prod.adm.connect.axis.com (52.224.128.152 oder 40.127.155.231)	443	HTTPS	Erforderlich

# AXIS Device Manager Extend

## Lösungsübersicht

B	HTTP-Erkennung (vom Client bis zum Edge-Host) Datenübertragung (vom Client bis zum Edge-Hosts) Multicast-Erkennung (vom Client bis zum Edge-Host) Multicast-Erkennung (vom Edge-Host bis zum Client)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Bereitstellung des Standorts erforderlich. Optional nach Bereitstellung.
C	Datenübertragung (zwischen Edge-Host und Geräten) Unicast-Erkennung Multicast-Erkennung HTTP-Erkennung	80 / benutzerdefinierter Port, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Erforderlich
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS (UDP und TCP)	Auf WebRTC-Standard basierend Optional und standardmäßig ausgeschaltet
E	Peer-to-Peer (P2P)	49152-65535	DTLS (UDP und TCP)	



AXIS Device Manager Extend mit einem standortübergreifenden Setup mit lokalem und Fernzugriff

- 1 Axis
- 2 IAM (My Axis)
- 3 Organisationsdaten
- 4 Lokaler Client
- 5 Edge-Host
- 6 Geräte

# AXIS Device Manager Extend

## Lösungsübersicht

---

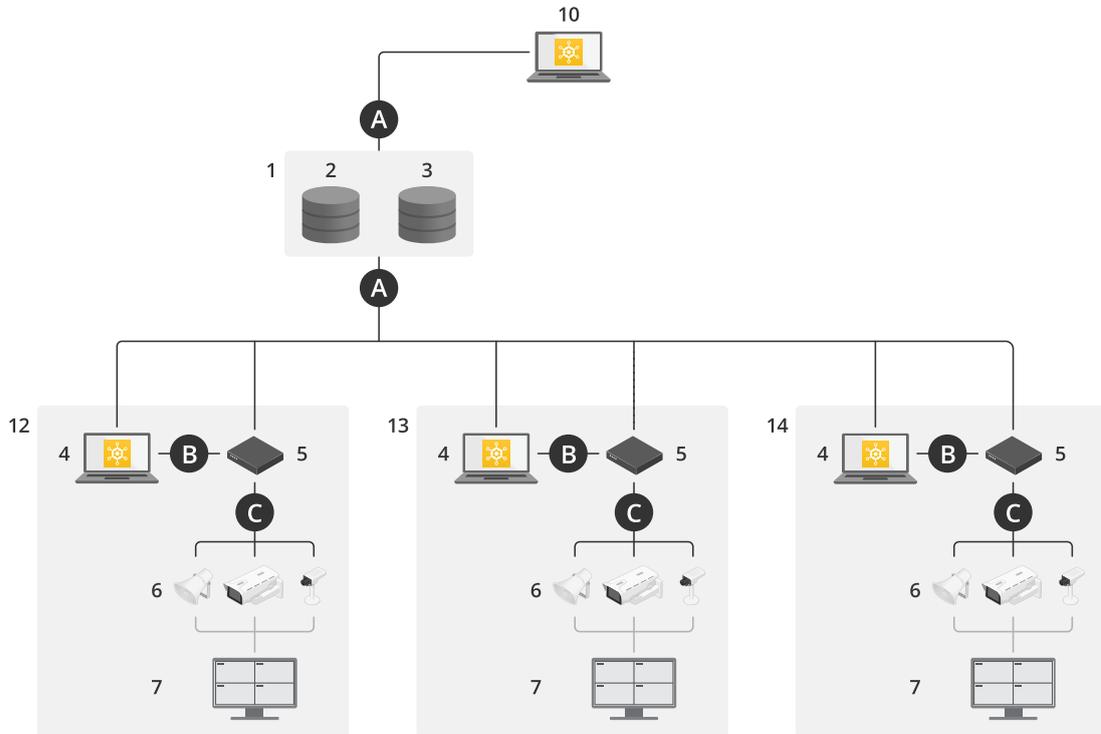
- 7 VMS
- 8 TURN
- 9 Signalgebung
- 10 Remote Client
- 11 Fernzugriff auf WebRTC-Server
- 12 Standort 1
- 13 Standort 2
- 14 Standort 3

Verbindung	URL und IP	Port	Protokoll	Kommentar
A	prod.adm.connect.axis.com (52.224.128.152 oder 40.127.155.231)	443	HTTPS	Erforderlich
B	HTTP-Erkennung (vom Client bis zum Edge-Host) Datenübertragung (vom Client bis zum Edge-Hosts) Multicast-Erkennung (vom Client bis zum Edge-Host) Multicast-Erkennung (vom Edge-Host bis zum Client)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Bereitstellung des Standorts erforderlich. Optional nach Bereitstellung.
C	Datenübertragung (zwischen Edge-Host und Geräten) Unicast-Erkennung Multicast-Erkennung HTTP-Erkennung	80 / benutzerdefinierter Port, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Erforderlich
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS (UDP und TCP)	Auf WebRTC-Standard basierend Optional und standardmäßig

# AXIS Device Manager Extend

## Lösungsübersicht

E	Peer-to-Peer (P2P)	49152-65535	DTLS (UDP und TCP)	ausgeschaltet
---	--------------------	-------------	--------------------	---------------



AXIS Device Manager Extend mit lokalem Zugriff und Fernzugriff über VPN-Verbindung

- 1 Axis
- 2 IAM (My Axis)
- 3 Organisationsdaten
- 4 Lokaler Client
- 5 Edge-Host
- 6 Geräte
- 7 VMS
- 8 TURN
- 9 Signalgebung
- 10 Remote Client
- 11 Fernzugriff auf WebRTC-Server
- 12 Standort 1
- 13 Standort 2
- 14 Standort 3

Verbindung	URL und IP	Port	Protokoll	Kommentar
A	prod.adm.connect.axis.com (52.224.128.152 oder 40.127.155.231)	443	HTTPS	Erforderlich

# AXIS Device Manager Extend

## Lösungsübersicht

---

B	HTTP-Erkennung (vom Client bis zum Edge-Host) Datenübertragung (vom Client bis zum Edge-Hosts) Multicast-Erkennung (vom Client bis zum Edge-Host) Multicast-Erkennung (vom Edge-Host bis zum Client)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	Bereitstellung des Standorts erforderlich. Optional nach Bereitstellung.
C	Datenübertragung (zwischen Edge-Host und Geräten) Unicast-Erkennung Multicast-Erkennung HTTP-Erkennung	80 / benutzerdefinierter Port, 443 1900 1900, 5353 80,443	HTTP, HTTPS SSDP, Bonjour	Erforderlich
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS, DTLS (UDP und TCP)	Auf WebRTC-Standard basierend Optional und standardmäßig ausgeschaltet
E	Peer-to-Peer (P2P)	49152-65535	DTLS (UDP und TCP)	

- Zusätzlich ist ein öffentlicher DNS erforderlich, z. B. Google DNS: 8.8.8.8 / 8.8.4.4 oder Cloudflare DNS: 1.1.1.1
- Zur Unterstützung der vollen Funktionalität des AXIS Device Manager Extend sind sowohl A- als auch C-Anschlüsse erforderlich.
- Wir entwickeln die Anwendung ständig weiter und raten Ihnen daher, der Desktop-Anwendung AXIS Device Manager Extend und jedem Edge-Host den Firewall-Zugriff auf ausgehende Netzwerk-Verbindungen zu erlauben.

# AXIS Device Manager Extend

## Voraussetzungen

---

### Voraussetzungen

#### Kompatible Betriebssysteme:

- Windows 10 Pro und Enterprise
- Windows 11 Pro und Enterprise
- Windows Server 2016, 2019 und 2022 (x64-basiertes System)
- Systemadministratorrechte für die Installation und Konfiguration erforderlich.

#### Mindestsystemempfehlungen:

- CPU: Intel Core i5
- RAM: 4 GB
- Netzwerk: 100 Mbps

#### Internetverbindungen

##### Hinweis

Für die Anwendung AXIS Device Manager Extend muss eine Internetverbindung mit Zertifikaten bereitgestellt werden, die diese als zu der Organisation gehörend ausweisen, die mit dem bei der Installation verwendeten My Axis-Konto erstellt und verknüpft wurde. Zur Nutzung bestimmter Funktionen wie Informationen zur Gewährleistung und Multisite-Support ist jedoch eine Internetverbindung erforderlich. Darüber hinaus aktualisiert der Client und/oder Edge-Host nur im Online-Modus automatisch.

#### Synchronisierte Zeit und Datum

##### Hinweis

Stellen Sie sicher, dass alle Systemkomponenten synchronisiert sind, da andernfalls die Zertifikatsauthentifizierung zwischen dem Edge-Host und dem Client oder Backend fehlschlagen könnte. Es wird empfohlen, dass zur Vermeidung von möglichen Problemen alle Host-Rechner mit einem gemeinsamen Network Time Server synchronisiert werden.

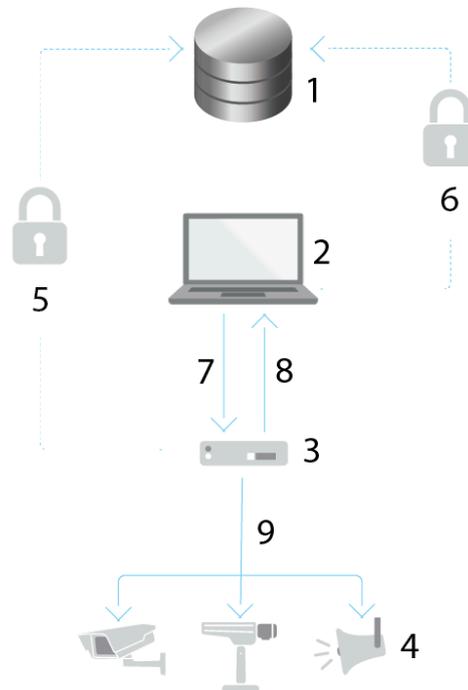
#### Offene Netzwerk-Ports:

Für sichere Verbindungen von der Anwendung AXIS Device Manager Extend Desktop zum Edge-Host, Edge Host Discovery und Axis Remote Service.

# AXIS Device Manager Extend

## Voraussetzungen

---



- 1 Axis Service-Plattform
- 2 Desktop-Anwendung AXIS Device Manager Extend
- 3 Edge-Host
- 4 Geräte
- 5 HTTPS (Port 443)
- 6 HTTPS (Port 443)
- 7 HTTPS (Port 37443), UDP Multicast-Erkennung (Port 6801), HTTP-Erkennung (Port 37080)
- 8 UDP Multicast-Erkennung (Port 6801)
- 9 HTTPS und HTTP (Port 443 und 80), Multicast-Erkennung – SSDP (Port 1900) – Bonjour (Port 5353), Unicast-Erkennung (Port 1900), HTTP-Erkennung (Port 80 und 443)

### Zugriff auf ausgehende Netzwerke

Wir entwickeln die Anwendung ständig weiter und raten Ihnen daher, der Desktop-Anwendung AXIS Device Manager Extend und jedem Edge-Host den Firewall-Zugriff auf ausgehende Netzwerk-Verbindungen zu erlauben.

# AXIS Device Manager Extend

## Funktionsweise

---

### Funktionsweise

#### Ein MyAxis-Konto einrichten

Ein My Axis-Konto wird unter [axis.com/my-axis/login](https://axis.com/my-axis/login) eingerichtet.

Um Ihr My Axis Konto noch sicherer zu machen, aktivieren Sie die Multifaktor-Authentifizierung (MFA). MFA ist ein Sicherheitssystem, das eine weitere Verifizierungsebene hinzufügt, um die Identität des Benutzers sicherzustellen.

So aktivieren Sie MFA:

1. Gehen Sie auf [axis.com/my-axis/login](https://axis.com/my-axis/login).
2. Melden Sie sich mit den Zugangsdaten zu MyAxis an.
3. Rufen Sie  auf und wählen Sie **Account settings** (Kontoeinstellungen) aus.
4. Klicken Sie auf **Security settings (Sicherheitseinstellungen)**.
5. Klicken Sie auf **Handle your 2-factor authentication (2-Faktor-Authentifizierung bearbeiten)**.
6. Geben Sie Ihre MyAxis Anmeldedaten ein.
7. Wählen Sie eine der Authentifizierungsmethoden **Authenticator App (TOTP)** oder **Email (E-Mail)** aus und befolgen Sie die Anweisungen auf dem Bildschirm.

#### Den Client installieren und Ihr Konto aktivieren

Rufen Sie die Produktseite auf [axis.com](https://axis.com) auf und laden Sie das Installationsprogramm der Desktop-Anwendung **AXIS Device Manager Extend** herunter.

1. Suchen Sie den Speicherort der Anwendung und klicken Sie darauf, um diese zu installieren.
2. Wählen Sie **Client** und klicken Sie auf **Installieren**.
3. Melden Sie sich in Ihrem My Axis-Konto an.
4. Bestätigen Sie Ihre E-Mail-Adresse, um die Aktivierung abzuschließen.
5. Erstellen Sie eine Organisation oder treten Sie einer vorhandenen Organisation bei.

#### Organisation erstellen

Um Geräte zu Ihrem System hinzufügen zu können, müssen Sie Teil einer Organisation sein. So warten und schützen Sie Ihre Geräte auf sichere Weise an einem oder mehreren Standorten. Wenn Sie noch nicht Mitglied einer Organisation sind, wird ein Setup-Assistent angezeigt, der Sie durch den Prozess führt.

Um eine Organisation zu erstellen:

1. Melden Sie sich mit Ihrem My Axis-Konto bei **AXIS Device Manager Extend** an.
2. Befolgen Sie die Anweisungen des Setup-Assistenten.

Zusätzliche Organisationen erstellen:

- Rufen Sie das Drop-Down Menü mit dem Namen Ihrer Organisation auf.
- Wählen Sie **+ Create new organization (Neue Organisation erstellen)**
- Befolgen Sie die Anweisungen des Setup-Assistenten.

# AXIS Device Manager Extend

## Funktionsweise

---

### Edge-Host installieren

Sowohl der Edge-Host als auch der Desktop-Client sind im Installationsprogramm des AXIS Device Manager Extend enthalten. Wir empfehlen die Installation von Edge-Host auf einem möglichst nah an den Geräten stehenden Server.

1. Wählen Sie einen Server, auf dem Sie den Edge-Host installieren möchten.
2. Führen Sie das Installationsprogramm auf dem Server aus und installieren Sie nur den Edge-Host.

### Edge-Host anfordern

Damit die Desktop-Anwendung AXIS Device Manager Extend eine sichere Verbindung zu Ihren Geräten herstellen kann, müssen Sie zuerst einen Edge-Host für Ihre Organisation anfordern.

1. Klicken Sie auf einen Edge Host mit dem Status **Nicht angefordert**
  - 1.1 Klicken Sie auf **Neuen Edge-Host hinzufügen**, wenn kein Edge-Host in der Liste vorhanden ist.
  - 1.2 Geben Sie die IP-Adresse des Edge-Hosts ein.
2. Geben Sie den Namen des Edge-Hosts ein
3. Fügen Sie eine optionale Beschreibung hinzu (empfohlen)
4. Klicken Sie auf **Edge-Host anfordern**

### Geräte verwalten

#### Ihrem Edge-Host ermittelte Geräte hinzufügen

1. Gehen Sie zu Edge-Hosts.
2. Wählen Sie in der Liste, der Sie Geräte hinzufügen möchten, einen angeforderten Edge-Host.
3. Gehen Sie zu Geräte > Erkannt.
4. Wählen Sie die hinzuzufügenden Geräte oder wählen Sie alle Geräte aus, indem Sie das Kontrollkästchen oben in der Auswahlspalte markieren.
5. Klicken Sie auf Dem Edge-Host Geräte hinzufügen .

Die Geräte werden jetzt auf der Registerkarte **Verwaltet** aufgeführt, und der jeweilige Satus kann in der **Edge Host-Übersicht** überprüft werden.

#### Geräte aus IP-Adressen hinzufügen

Fügen Sie Geräte hinzu, die nicht automatisch aus Subnetzen, einzelnen IP-Adressen oder einem IP-Bereich erfasst werden.

#### Geräte aus IP-Bereich hinzufügen

1. Gehen Sie zu einem Edge-Host Ihres Unternehmens.
2. Gehen Sie zu **Einstellungen > Geräteerkennung**.
3. Klicken Sie auf **Nach IP hinzufügen**
4. Wählen Sie **Manuelle Eingabe**
5. Geben Sie den IP-Adressbereich ein
6. Klicken Sie auf **IP-Adressen hinzufügen**
7. Gehen Sie zu **Devices (Geräte) > Discovered (Erkannt)**
8. Wählen Sie die hinzuzufügenden Geräte oder wählen Sie alle Geräte aus, indem Sie das Kontrollkästchen oben in der Auswahlspalte markieren.
9. Klicken Sie auf **Add devices** .

#### Geräte aus einer Datei hinzufügen

1. Gehen Sie zu einem Edge-Host Ihres Unternehmens.
2. Gehen Sie zu **Einstellungen > Geräteerkennung**.
3. Klicken Sie auf **Nach IP hinzufügen**
4. Wählen Sie **Aus Datei importieren**.
5. Wählen Sie die durch Kommata getrennte (. CSV-)Datei mit den IP-Adressen
6. Klicken Sie auf **Importieren**.
7. Gehen Sie zu **Geräte > Erkannte Geräte**
8. Wählen Sie die hinzuzufügenden Geräte oder wählen Sie alle Geräte aus, indem Sie das Kontrollkästchen oben in der Auswahlspalte markieren.

# AXIS Device Manager Extend

## Geräte verwalten

---

9. Klicken Sie auf **Add devices** .

### Hinweis

Die Datei sollte folgende Elemente beinhalten:  
Eine Kopfzeile für die Spalte mit IP-Adressen.  
Eine einzelne Spalte.  
Maximal 25.600 IP-Adressen.

## Geräte entfernen



*Geräte von einem Edge-Host entfernen*

1. Klicken Sie auf **Edge-Host**
2. Wählen Sie einen Edge-Host.
3. Gehen Sie zu **Devices (Geräte)**
4. Wählen Sie die zu entfernenden Geräte oder wählen Sie alle Geräte aus, indem Sie das Kontrollkästchen oben in der Auswahlspalte aktivieren.
5. Klicken Sie im Aktionsmenü auf das Symbol **Geräte von Edge-Host entfernen**.
6. Klicken Sie auf **Remove (Entfernen)**.

Die entfernten Geräte finden Sie dann unter **Geräte > Erkannt**.

## Bei Ihren Geräten anmelden

1. Klicken Sie auf **Edge-Hosts**
2. Wählen Sie einen Edge-Host.
3. Gehen Sie zu **Geräte > Verwaltet**.
4. Wählen Sie die Geräte aus, auf die Sie zugreifen möchten, oder wählen Sie alle Geräte aus, indem Sie das Kontrollkästchen oben in der Auswahlspalte markieren.
5. Klicken Sie auf **Anmelden**, um sich automatisch bei mehreren Geräten anzumelden.
6. Geben Sie den Benutzernamen und das Kennwort ein.
7. Klicken Sie auf **Log in (Anmelden)**

### Hinweis

Wenn der Benutzername und das Kennwort korrekt sind, wird als **StatusErreichbar** angezeigt.

### Konfiguration

#### Fernzugriff aktivieren

Blockiert Ihre Firewall-Einstellungen ausgehende Verbindungen, müssen Sie möglicherweise eine Proxyverbindung eingeben, um remote auf den Standort zugreifen zu können.

1. Wählen Sie den Edge-Host, für den Sie den Fernzugriff aktivieren möchten.
2. Gehen Sie zu **Einstellungen > Edge-Hosts-Verbindungen**.
3. Aktivieren Sie **Fernzugriff auf Edge-Host zulassen**.
4. Wenn Sie für den Internetzugang eine Proxyadresse eingeben müssen, geben Sie unter **Proxyadresse** eine Adresse ein.

Sie werden benachrichtigt, sobald die Verbindung aktiv ist.

#### Hinweis

Um die Verbindung zu Edge-Hosts in anderen Netzwerken zu unterstützen, müssen Sie möglicherweise die folgende Konfiguration zur „Berechtigungsliste“ Ihrer Unternehmensnetzwerk-Firewall hinzufügen: Endpoint Port Protocol signaling.prod.webrtc.connect.axis.com 443 HTTPS \*.turn.prod.webrtc.connect.axis.com 443 HTTPS webRTC (Turn and P2P) 5349, 49152 - 65535 DTLS (UDP und TCP)

#### Einen Standort entfernen

Bevor Sie einen Edge-Host aus Ihrem Unternehmen entfernen, müssen Sie die zum Edge-Host gehörigen *Geräte entfernen auf Seite 15*. Die Geräte finden Sie dann unter **Geräte > Erkennt**.

1. Klicken Sie auf **Edge-Hosts**.
2. Wählen Sie mithilfe der Pfeiltasten den Edge-Host oder gleiten Sie mit dem Mauszeiger darüber.
3. Klicken Sie auf ... und wählen Sie im Auswahlm Menü **Edge-Host entfernen**.
4. Markieren Sie **Ich bin mir der Risiken bewusst**.
5. Klicken Sie auf **Remove (Entfernen)**.

#### Hinzufügen von Benutzern zu Ihrer Organisation

1. Wählen Sie die Organisation, in der Sie Benutzereinstellungen konfigurieren möchten.
2. Wechseln Sie zum Bereich **My Systems**.
3. Wechseln Sie zu **Organization > Users (Organisation > Benutzer)**.
4. Klicken Sie auf **Benutzer einladen**.
5. Geben Sie die E-Mail-Adresse des Benutzers ein, den Sie zu Ihrer Organisation einladen möchten.
6. Wählen Sie die Rolle aus, die den Benutzern zugewiesen werden soll. Bitte beachten Sie, dass Sie einige Benutzer, die eine andere Rolle haben sollen, in einer separaten Einladung einladen müssen.
7. Wenn Sie **Operator** oder **Viewer** ausgewählt haben, wählen Sie aus, auf welche Ordner die Benutzer Zugriff haben sollen. Bitte beachten Sie, dass die Rollen **Admin** Zugriff auf alle Ordner in der Organisation haben.
8. Klicken Sie auf **Invite user (Benutzer einladen)**.

# AXIS Device Manager Extend

## Konfiguration

---

### Hinweis

Der Benutzer erhält eine Einladungsmail, die er zur Anmeldung bei My Systems verwenden kann. Wenn der Benutzer kein My Axis Konto besitzt, muss er sich mit dieser E-Mail registrieren, um auf die Organisation zugreifen zu können. Einladungen können zurückgenommen werden, solange sie noch nicht angenommen wurden.

## Informationen zu Benutzerrollen

Benutzerrollen legen fest, auf welche Systeme in Ihrer Organisation ein Benutzer zugreifen kann. Die verfügbaren Funktionen variieren entsprechend der Rolle des Benutzers.

### Admin

Administratoren haben Zugriff auf das gesamte System. Dies schließt die Verwaltung von Benutzern, Geräten, Lizenzen, Videos und anderen Inhalten mit ein.

Außerdem können sie mithilfe von AXIS Camera Station Pro und AXIS Installer Geräte einbinden. Administratoren können über „My Systems (Meine Systeme)“ die Überwachung der AXIS Camera Station Pro-Server verwalten.

### Bediener

Bediener können Live-Videostreams überwachen, Geräte steuern und Aufzeichnungen wiedergeben. Sie erhalten eine Übersicht über die Benutzer innerhalb der Organisation und ihre jeweiligen Rollen. Bediener können ebenfalls über „My Systems (Meine Systeme)“ die Überwachung der AXIS Camera Station Pro-Server verwalten.

### Betrachter

Betrachter können Live-Videostreams überwachen, jedoch keine Geräte steuern oder auf Aufzeichnungen zugreifen. Sie erhalten eine Übersicht über die Benutzer innerhalb der Organisation und ihre jeweiligen Rollen.

## Benutzerrolle höherstufen

1. Wählen Sie die Organisation, in der Sie Benutzereinstellungen konfigurieren möchten.
2. Rufen Sie **Users (Benutzer)** auf.
3. Gehen Sie zu der **Rolle** des Benutzers, den Sie hochstufen möchten.
4. Klicken Sie auf das Auswahlmenü, um die neue Rolle auszuwählen.

### Hinweis

Die Rolle ändert sich nach der Auswahl sofort. Aus Sicherheitsgründen sind die Einladungen auf die Beobachterrolle beschränkt.

## Benutzer entfernen

1. Wählen Sie die Organisation, in der Sie Benutzereinstellungen konfigurieren möchten.
2. Rufen Sie **Users (Benutzer)** auf.
3. Bewegen Sie den Mauszeiger über der Benutzerleiste des Benutzers, den Sie entfernen möchten, um ein neues Optionsmenü zu öffnen: ...
4. Klicken Sie auf ... und wählen Sie im Auswahlmenü **Benutzer entfernen**.

# AXIS Device Manager Extend

## AXIS OS-Verwaltung

---

### AXIS OS-Verwaltung

Mit dem AXIS Device Manager Extend können Sie das Betriebssystem mehrerer Geräte in jeder Organisation verwalten.

Um eine nach Modell zusammengefasste Liste mit für jedes Gerät in Ihrem Unternehmen verfügbaren AXIS OS-Aktualisierungen zu erhalten, gehen Sie zu **Home > AXIS OS inventory (Startseite > AXIS OS Inventar)**. Um eine Liste mit an einem bestimmten Edge-Host verfügbaren Aktualisierungen von AXIS OS zu erhalten, wählen Sie den Edge-Host und gehen Sie dann zu **AXIS OS Inventar**.

### Verwaltung der AXIS OS-Versionen je nach Modell

Zur Verwaltung von AXIS OS nach Modell in Ihrem Unternehmen:

1. Wechseln Sie zu **Home > AXIS OS versions (Startseite > AXIS OS Versionen)**
2. Klicken Sie auf den Link für die empfohlene AXIS OS-Version. Dadurch werden die Optionen zur Verbesserung von AXIS OS geöffnet.
3. Klicken Sie in das Auswahlménü **Aktualisieren** auf, um die verfügbaren Optionen zu sehen. Die neueste AXIS OS-Version wird vorausgewählt.
4. Klicken Sie auf **Aktualisieren**.

### Verwaltung von AXIS OS auf einem Edge-Host.

So verwalten Sie AXIS OS auf einigen oder allen Geräten, die einem Edge-Host hinzugefügt wurden:

1. Gehen Sie zu **Edge-Hosts**
2. Klicken Sie auf den Edge-Host, auf den Sie zugreifen möchten.
3. Gehen Sie zu **Geräte**.
4. Wählen Sie alle oder nur die Geräte aus, die Sie verwalten möchten.
5. Klicken Sie im Aktionsménü auf das Symbol **AXIS OS**
6. Überprüfen Sie alle oder einige Modelle in der Liste.
7. Wenn Sie die AXIS OS-Version ändern möchten, klicken Sie auf die Version, um zu sehen, welche für die einzelnen Geräte verfügbar ist. Die neueste AXIS OS-Version wird vorausgewählt.
8. Klicken Sie auf **Upgrade (Aktualisieren)**.

### Laufende und abgeschlossene AXIS OS-Aktualisierungen anzeigen

So können Sie sich die aktuellen Softwareaktualisierungen von Geräten anzeigen lassen, die an einen bestimmten Edge-Host angeschlossen sind:

1. Klicken Sie auf **Edge-Hosts**
2. Klicken Sie auf den Edge-Host, auf den Sie zugreifen möchten.
3. Rufen Sie **Log (Anmelden)** auf

So können Sie sich aktuelle Softwareaktualisierungen anzeigen lassen:

4. Gehen Sie zu **Log > Laufende Aufgaben**

# AXIS Device Manager Extend

## Bestell- und Lieferbedingungen

---

### Bestell- und Lieferbedingungen

Mit Richtlinien lassen sich Ihre Geräte automatisch verwalten. Erstellen Sie Richtlinien, um die Cybersicherheit Ihres Standorts zu gewährleisten. Sie können auch Richtlinien zum automatischen Installieren und Aktualisieren von Apps auf Ihren Geräten festlegen.

#### Eine Sicherheitsrichtlinie erstellen und anwenden

In diesem Beispiel erstellen wir eine Basissicherheitsrichtlinie für eine ausgewählte Anzahl von mit einem Edge-Host verbundenen Geräten und wenden sie an.

So erstellen Sie eine Basissicherheitsrichtlinie:

1. Gehen Sie zu **Edge-Hosts**
2. Klicken Sie auf den Edge-Host, auf den Sie zugreifen möchten.
3. Gehen Sie zu **Geräte**.
4. Klicken Sie auf das +-Symbol neben den **Richtlinien**
5. Wählen Sie **Basissicherheit** und klicken Sie auf **Fortfahren**
6. Geben Sie Ihrer Richtlinie einen Namen
7. Wählen Sie die Einstellungen aus, die Ihren Sicherheitsanforderungen entsprechen. Behalten Sie die Standardeinstellungen für die empfohlene Sicherheitsstufe bei.
  - Um das Root-Kennwort für die ausgewählten Geräte zu ändern, klicken Sie auf **Root-Kennwort für das Gerät** und geben Sie das neue Root-Kennwort ein.
8. Klicken Sie auf **Create (Erstellen)**.

Richtlinie übernehmen:

1. Wählen Sie die Geräte aus, für die die Richtlinie übernommen werden soll.
2. Klicken Sie im Aktionsmenü auf das Symbol **Richtlinienoptionen**.
3. Wählen Sie die Sicherheitsrichtlinien und klicken Sie auf **Speichern**.

#### Eine App-Richtlinie erstellen und anwenden

In diesem Beispiel erstellen wir eine App-Richtlinie für eine ausgewählte Anzahl von mit einem Edge-Host verbundenen Geräten und wenden sie an.

1. Gehen Sie zu **Edge-Hosts**
2. Klicken Sie auf den Edge-Host, auf den Sie zugreifen möchten.
3. Gehen Sie zu **Geräte**.
4. Klicken Sie auf das +-Symbol neben den **Richtlinien**
5. Wählen Sie **Apps** und klicken Sie auf **Weiter**
6. Geben Sie Ihrer Richtlinie einen Namen
7. Wählen Sie die Apps aus, die auf Ihren Geräten installiert und aktualisiert werden sollen.
8. Wählen Sie das Aktualisierungsfenster im Auswahlmenü aus.

# AXIS Device Manager Extend

## Bestell- und Lieferbedingungen

---

9. Klicken Sie auf **Create (Erstellen)**.

Richtlinie übernehmen:

1. Wählen Sie die Geräte aus, für die die Richtlinie übernommen werden soll.
2. Klicken Sie im Aktionsmenü auf das Symbol **Richtlinienoptionen**.
3. Wählen Sie die App-Richtlinie, die Sie übernehmen möchten.
4. **Save (Speichern)** anklicken.

### Hinweis

Die ausgewählten Apps werden automatisch neu installiert, wenn sie entfernt wurden.

## Eine Richtlinie bearbeiten

So lässt sich eine vorhandene Richtlinie bearbeiten:

1. Gehen Sie zu **Edge-Hosts**
2. Klicken Sie auf den Edge-Host, auf den Sie zugreifen möchten.
3. Gehen Sie zu **Geräte**.
4. Klicken Sie auf ... neben der Richtlinie, die Sie bearbeiten möchten, und wählen Sie **Richtlinie bearbeiten** aus dem Auswahlmü aus.
5. Bearbeiten Sie die Richtlinieneinstellungen Ihrem Bedarf entsprechend.
6. Klicken Sie auf **Speichern**.

## Eine Richtlinie löschen

So lässt sich eine vorhandene Richtlinie löschen:

- Gehen Sie zu **Edge-Hosts**
- Klicken Sie auf den Edge-Host, auf den Sie zugreifen möchten.
- Gehen Sie zu **Geräte**.
- Klicken Sie auf ... neben der Richtlinie, die Sie bearbeiten möchten, und wählen Sie **Richtlinie löschen** aus dem Auswahlmü aus.
- Klicken Sie auf **Löschen**

### Hinweis

Alle Geräte, auf denen diese Richtlinie angewendet wird, behalten die Einstellungen der Richtlinie bei. Die Einstellungen sind jedoch nicht mehr persistent.

# AXIS Device Manager Extend

## Lizenzen verwalten

---

### Lizenzen verwalten

#### Ihr Produkt lizenzieren

Um Ihr Produkt zu lizenzieren, rufen Sie *My Systems > Licenses (Lizenzen)* auf. Weitere Informationen zu den Lizenzen für Axis Produkte und Dienste finden Sie im *My Systems-Benutzerhandbuch*.

# AXIS Device Manager Extend

## Fehlerbehebung

---

### Fehlerbehebung

#### So konfigurieren Sie die Firewallinstellungen

AXIS Device Manager Extend Client erfordert Zugriff auf die axis.com-Domain und eine beliebige Subdomain.

Damit der Edge-Host von AXIS Device Manager Extend mit dem Axis Service kommunizieren kann, müssen folgende IP-Adressen und Ports von der Firewall der Organisation zur Berechtigungsliste hinzugefügt werden:

- 40.127.155.231 (EU), Port 443
- 52.224.128.152 und 40.127.155.231 (USA), Port 443
- Eine öffentliche DNS-Server-IP, Port 53

Alternativ kann in den Firewallinstellungen die Domain prod.adm.connect.axis.com (ein DNS A-Record mit Verweisen auf die oben angegebenen IP-Adressen) verwendet werden.

AXIS Device Manager Extend Edge Host verwendet für alle ausgehenden Anfragen den prod.adm.connect.axis.com-Domainnamen.

Dazu muss das Netzwerk einen öffentlichen DNS-Server verwenden und den Datenverkehr zur IP-Adresse des DNS-Servers (und dem Standardport 53) zulassen.

