

# AXIS Device Manager

## Inhalt

Über den AXIS Device Manager .....	3
Funktionsweise .....	4
Software installieren .....	4
Mit einem Server verbinden.....	4
Verbindungen mit mehreren Servern einrichten .....	4
Den Server konfigurieren.....	5
Erste Konfiguration .....	5
Geräte verwalten .....	6
Geräte hinzufügen.....	6
Geräte entfernen.....	6
Geräte ersetzen.....	6
Geräte wiederherstellen .....	6
Apps installieren .....	7
Konfiguration .....	8
Verwaltung der Wiederherstellungspunkte .....	8
Wiederherstellungspunkt erstellen.....	8
Wiederherstellungspunkte automatisch erstellen .....	8
Mehrere Zugangsdaten verwalten .....	8
Zertifikate installieren .....	9
Informationen zu Zertifikaten .....	9
Erstellen Sie eine Zertifizierungsstelle (CA) .....	9
HTTPS aktivieren.....	10
802.1X aktivieren .....	10
SIP-Einstellungen konfigurieren.....	11
SIP-Konten verwalten.....	12
SIP-Konten hinzufügen .....	12
SIP-Konten entfernen .....	14
Metadaten auf Geräten aktivieren.....	14
Verwaltung der Gerätesoftware.....	15
AXIS OS-Upgrades.....	15
Fehlerbehebung.....	16
Software-Bestellliste .....	16
Support.....	16
Eskalationsverfahren .....	16

### Über den AXIS Device Manager

Der AXIS Device Manager ist eine Installations- und Verwaltungssoftwareanwendung für Axis Produkte. Die Software kann das Netzwerk automatisch nach Geräten durchsuchen, IP-Adressen zuweisen, Kennwörter vergeben, den Verbindungsstatus anzeigen, die Aktualisierung von Firmware und Zertifikate verwalten sowie mehrere Geräte konfigurieren.

Der AXIS Device Manager besteht aus:

- AXIS Device Manager Service Control – der Server, der die gesamte Kommunikation mit Axis Produkten abwickelt
- AXIS Device Manager Client – die Benutzeroberfläche, die die Fernverwaltung über das Internet oder das Unternehmensnetzwerk aktiviert

Verschiedene Clients können mit demselben Server verbunden werden. Ein Client kann mit mehreren Servern gleichzeitig verbunden sein.

AXIS Device Manager ist auch sehr nützlich, um Ihr System zu stärken und die Sicherheit zu erhöhen. Weitere Informationen finden Sie in der Übersicht *AXIS Device Manager Security Guide*.

## Funktionsweise

### Software installieren

Um AXIS Device Manager 5 zu installieren, vergewissern Sie sich, dass Sie auf dem Computer, auf dem Sie die Installation durchführen, über volle Administratorrechte verfügen, und gehen Sie dann wie folgt vor:

1. *Rufen Sie die Produktseite auf [axis.com](http://axis.com) auf und laden Sie die Desktop-Anwendung AXIS Device Manager herunter*
2. Führen Sie das Installationsprogramm aus und folgen Sie den Anweisungen auf dem Bildschirm.

#### Hinweis

Falls nicht bereits installiert, wird das Microsoft .NET 4.8 Framework installiert (in der Installationsdatei enthalten). Dies wird ein paar Minuten dauern. Das Microsoft .NET 4.8 Framework kann auch über Windows Update vor der Installation von AXIS Device Manager installiert werden.

### Mit einem Server verbinden

Wenn Sie AXIS Device Manager zum ersten Mal starten, werden Sie aufgefordert, eine Verbindung zu einem Server herzustellen. Der Server kann auf dem lokalen Rechner oder einem entfernten Server betrieben werden.

So melden Sie sich als lokaler Windows-Benutzer an:

1. Wählen Sie **This computer (Dieser Computer)**.
2. Prüfen Sie **Log on as current user (Als aktueller Benutzer anmelden)**, um sich mit Ihren aktuellen Zugangsdaten anzumelden.

Um sich als ein anderer Benutzer auf dem Server oder in der Domain anzumelden:

- Wählen Sie **Other user (Anderer Benutzer)**.
- Unter **Other user (Anderer Benutzer)** geben Sie die Zugangsdaten für dieses Konto ein.
- Aktivieren Sie **Remember me (An mich erinnern)**, um diesen Schritt bei der nächsten Ausführung des Clients zu überspringen.
- **Log on (Anmelden)** anklicken.

#### Hinweis

Um die gespeicherten Zugangsdaten für alle Server zu löschen, rufen Sie den Anmeldebildschirm auf und wählen **Delete saved passwords (Gespeicherte Passwörter löschen)**.

Um sich bei einem entfernten Server anzumelden:

1. **Remote-Server** wählen.
2. Einen Server aus der Dropdown-Liste wählen oder die IP-Adresse oder DNS-Adresse in das Feld eingeben.
3. Geben Sie Ihre Zugangsdaten ein
4. **Log on (Anmelden)** anklicken.

#### Hinweis

Diese Option kann nicht verwendet werden, um sich von einem Computer außerhalb einer Windows-Domain an einem Remote-Server anzumelden.

### Verbindungen mit mehreren Servern einrichten

Sie können mit dem AXIS Device Manager eine Verbindung zu mehreren Servern herstellen. Wenn Sie sich erfolgreich bei einem Server angemeldet haben, können Sie im Hauptmenü zwischen den Servern wechseln.

1. Hauptmenü > Servers > New connection (Server > neue Verbindung) aufrufen
2. Wählen Sie, wie oben beschrieben, entweder eine Verbindung zu Ihrem Computer oder zu einem Remote-Server.

### Den Server konfigurieren

Nach dem Installieren des Servers von AXIS Device Manager auf dem Computer kann der Server über die Dienststeuerung gestartet und gestoppt werden und es können die Server-Einstellungen geändert werden.

So konfigurieren Sie den Server:

1. Doppelklicken Sie auf das Symbol, um **AXIS Device Manager Service Control** zu öffnen
2. Markieren Sie das Kontrollkästchen **Modify settings (Einstellungen ändern)**
3. Geben Sie dem Server einen Namen. Der Server-Name identifiziert den Server. Er wird im Client des AXIS Device Manager angezeigt, wenn der Client mit mehr als einem Server verbunden ist. Der Standardname ist der Name des Computers, auf dem die Installation der Software durchgeführt wurde.
4. Geben Sie den HTTP-Port ein. Der Standard-HTTP-Port ist 55762.
5. Geben Sie den TCP-Port ein. Der Standard-TCP-Port ist 55764.

#### Hinweis

Die Serverportnummer muss zwischen 1024 und 65533 liegen. Die TCP-Portnummer wird immer aus der Serverportnummer + 2 gebildet. Wenn z. B. die Serverportnummer 55765 beträgt, dann ist die TCP-Portnummer 55767.

#### Hinweis

Für größere Installationen empfehlen wir **AXIS Device Manager Service Administration**. Diese Konsolenanwendung kann per Befehlseingabe oder mit einem Batch-Script verwendet werden, um unter anderem den Dienst zu starten und zu stoppen sowie die Datenbank zu sichern. Die Konsolenanwendung `AdmAdminConsole.exe` befindet sich im Installationsverzeichnis des Servers.

### Erste Konfiguration

Zunächst müssen Sie Folgendes tun:

- Geräte hinzufügen und Benutzerkonten erstellen, siehe: *Geräte hinzufügen, on page 6*
- Ihr System für die Cybersicherheit härten. Siehe *Zertifikate installieren, on page 9*

## Geräte verwalten

### Geräte hinzufügen

AXIS Device Manager durchsucht das Netzwerk automatisch nach verbundenen Geräten und versucht, sich bei allen Geräten anzumelden. Die Liste der gefundenen Geräte zeigt die Geräteadresse (IP-Adresse oder Host-Name), Seriennummer, Modell und Status. Die Seriennummer (S/N) finden Sie auf dem Produktaufkleber.

So fügen Sie Geräte aus der Liste hinzu:

1. Wählen Sie die hinzuzufügenden Geräte aus und klicken Sie auf **Next (Weiter)**.
2. Wählen Sie **Use host name when possible (Nach Möglichkeit Host-Namen verwenden)**. Wenn Sie ein Gerät unter Verwendung des Host-Namens hinzufügen, wird bei allen weiteren Verbindungen mit dem Gerät der Host-Name verwendet. Wenn kein Hostname verfügbar ist, wird die IP-Adresse verwendet.
3. Einstellung des Kennworts für Geräte ohne Kennwort. **Skip (Überspringen)** wählen, wenn kein Kennwort eingestellt werden soll.
4. Klicken Sie auf **Next (Weiter)**.

Die Seite „Bereit für das Hinzufügen von Geräten“ zeigt die hinzuzufügenden Geräte.

5. **Finish (Fertigstellen)** anklicken, um die Geräte hinzuzufügen.

### Geräte entfernen

Zum Entfernen von Geräten aus der Liste:

1. Wechseln Sie zu **Device management (Geräteverwaltung)**.
2. Wählen Sie die Geräte aus.
3. Rechtsklicken und **Remove (Entfernen)** auswählen.
4. **Yes (Ja)** anklicken

### Geräte ersetzen

Zum Ersetzen eines Geräts im AXIS Device Manager ein neues Gerät anschließen und die Konfiguration des alten Gerätes weiterverwenden. Das ersetzte Gerät wird gelöscht, wenn der Vorgang erfolgreich verläuft. Für dieses Gerät mindestens ein Wiederherstellungspunkt verfügbar sein, siehe dazu *Wiederherstellungspunkt erstellen, on page 8*. Wiederherstellungspunkte werden nicht auf das neue Gerät übertragen.

1. Wechseln Sie zu **Device management (Geräteverwaltung)**.
2. Rufen Sie die Symbolleiste auf und klicken Sie das Symbol zum Ersetzen des Geräts an.
3. Das Ersatzgerät wählen und **OK** anklicken.
4. Das zu ersetzende Gerät wählen und durch ersteres ersetzen; **OK** anklicken.
5. **Next (Weiter)** anklicken, um eine Gerätekonfiguration von dem letzten Wiederherstellungspunkt abzurufen.
6. Rufen Sie **Parameters (Parameter) > Additional Settings (Zusätzliche Einstellungen)** auf und wählen Sie die Parameter und Einstellungen aus, die Sie anwenden möchten.
7. Klicken Sie auf **Next (Weiter)**.
8. Zum Übernehmen dieser Einstellungen **Fertigstellen** anklicken.

### Geräte wiederherstellen

Es ist möglich, eines oder mehrere Geräte auf zuvor erstellte Wiederherstellungspunkte zurückzusetzen. Für jedes Gerät muss mindestens ein Wiederherstellungspunkt vorhanden sein, um es zurückzusetzen. Automatische Wiederherstellungspunkte werden standardmäßig jede Nacht für alle Geräte auf dem ausgewählten Server erstellt und kontinuierlich entfernt. Zum Zweck der Wiederherstellung wird eine Anzahl der neuesten automatischen Wiederherstellungspunkte aufbewahrt.

Geräte wiederherstellen auf einen früheren Wiederherstellungspunkt:

1. Den Arbeitsbereich **Device management (Geräteverwaltung)** aufrufen.
2. Wählen Sie einen oder mehrere wiederherzustellende Geräte aus.
3. Klicken Sie mit der rechten Maustaste und wählen Sie **Backup / Restore (Backup / Wiederherstellung) > Restore to a Previous Time (Wiederherstellung auf einen früheren Zeitpunkt)** aus der Dropdown-Liste.
4. Aus der Liste der neuesten verfügbaren Wiederherstellungspunkte einen Wiederherstellungspunkt wählen und **Weiter** anklicken.
5. Die Einstellung für jedes Gerät prüfen und **Fertigstellen** anklicken.

### Apps installieren

Eine App ist eine Software, die auf Axis-Geräte hochgeladen und dort installiert werden kann. Apps lassen sich auf Geräten installieren, die die AXIS Camera Application Platform unterstützen. Sie erweitern den Funktionsumfang des Geräts, z. B. Erfassungs-, Erkennungs-, Tracking- und Zählfunktionen. Apps müssen zunächst von *axis.com* oder von der Website des App-Anbieters heruntergeladen werden. Einige Anwendungen erfordern außerdem eine bestimmte AXIS OS-Version oder ein bestimmtes Gerätemodell. Falls die App eine Lizenz erfordert, kann die Lizenzschlüsseldatei gleichzeitig mit der App oder später mit Hilfe der Einrichtungsseiten des Geräts installiert werden. Sollte sich eine App nicht installieren lassen, prüfen Sie unter *axis.com*, ob das Gerätemodell und die AXIS OS-Version die AXIS Camera Application Platform unterstützen.

Eine App installieren:

1. Gehen Sie auf *axis.com* und laden Sie die App herunter.
2. Gehen Sie zu **Browse to Application (Zur Anwendung navigieren)**.
3. Klicken Sie auf **Browse (Durchsuchen)** und gehen Sie zu Ihrem Download-Ordner.
4. Wählen Sie die App aus und klicken Sie auf **Next (Weiter)**.

Wenn für den Start der App eine Lizenz erforderlich ist, muss die Lizenzdatei bereits heruntergeladen worden sein. Ist dies nicht der Fall, klicken Sie auf **No (Nein)** und fahren Sie mit Schritt 8 fort:

5. Wählen Sie **Yes (Ja)** und klicken Sie auf **Next (Weiter)**.
6. Klicken Sie auf **Browse (Durchsuchen)** und wählen Sie die Lizenzdatei aus.
7. Klicken Sie auf **Next (Weiter)**.
8. Wählen Sie die gewünschte Installationsart aus:
  - **Rückstufung der Anwendung** installiert eine Vorversion der Anwendungen
  - **Anwendung überschreiben** installiert die Anwendungen erneut.

#### Hinweis

Das Rückstufen oder das Überschreiben setzt auf den Geräten die Anwendungseinstellungen zurück.

#### Bereit für die Installation

Die Geräte, auf denen die App installiert wird, werden aufgelistet. Wenn die Apps bereits auf einigen Geräten installiert sind, wird die vorhandene App überschrieben. Durch das Überschreiben werden alle App-Einstellungen gelöscht.

9. Klicken Sie auf **Finish (Fertig)**.

## Konfiguration

### Verwaltung der Wiederherstellungspunkte

Ein Wiederherstellungspunkt ist eine gespeicherte Gerätekonfiguration, die zur Sicherung und Wiederherstellung von Geräteeinstellungen verwendet werden kann. Automatische Wiederherstellungspunkte werden für alle neu konfigurierten Geräte auf einem Server jede Nacht erstellt. Wurden auf einem Gerät seit dem letzten Wiederherstellungspunkt keine Einstellungen verändert, wird auch kein Wiederherstellungspunkt erstellt. Für eine maximale Speicherkapazität werden die ältesten Wiederherstellungspunkte automatisch gelöscht. Zum Zweck der Wiederherstellung wird eine Anzahl der neuesten automatischen Wiederherstellungspunkte aufbewahrt.

#### Wiederherstellungspunkt erstellen

Zum Erstellen eines manuellen Wiederherstellungspunkts:

- Den Arbeitsbereich **Device management (Geräteverwaltung)** aufrufen.
- Wählen Sie einen oder mehrere wiederherzustellende Geräte aus.
- Rechtsklicken und **Sichern/Wiederherstellen > Wiederherstellungspunkte erstellen** wählen.
- Geben Sie eine Beschreibung ein, die den Wiederherstellungspunkt identifiziert.
- Klicken Sie auf **OK**.

#### Hinweis

Manuell erstellte Wiederherstellungspunkte werden nicht automatisch entfernt.

#### Wiederherstellungspunkte automatisch erstellen

Wählen Sie bei mehr als einem Server den zu konfigurierenden Server aus der Serverliste aus.

- **Options (Optionen) > Restore point settings (Einstellungen für Wiederherstellungspunkte)** wählen.
- Wählen Sie **Wiederherstellungspunkte automatisch erstellen**, um das automatische Erstellen von Wiederherstellungspunkten zu aktivieren.
- Die Anzahl der zu speichernden automatischen Wiederherstellungspunkte eingeben und **OK** anklicken.

#### Mehrere Zugangsdaten verwalten

Mit dieser Funktion erhält AXIS Device Manager Zugangsdaten für ein Administratorkonto für die Geräte.

##### Zugangsdaten für das Gerät manuell eingeben

Wenn Sie sich entscheiden, die Zugangsdaten für das Gerät manuell einzugeben, werden die Zugangsdaten in AXIS Device Manager für die ausgewählten Geräte aktualisiert.

- Wählen Sie ein oder mehrere Geräte aus.
- Klicken Sie mit der rechten Maustaste darauf und wählen Sie **Advanced (Erweitert) -> Enter Device Credentials (Zugangsdaten für das Gerät eingeben)** aus der Dropdown-Liste.

#### Hinweis

Zugangsdaten, bei denen nicht überprüft werden kann, ob sie für das Gerät funktionieren, werden nicht aktualisiert. Für alle Geräte, die an einem solchen Betrieb teilnehmen, müssen das gleiche Kennwort und der gleiche Benutzername verwendet werden.

##### Verwendung einer CSV-Datei für verschiedene Zugangsdaten

Bei Verwendung einer CSV-Datei können Sie für jedes Gerät ein eigenes Kennwort und einen eigenen Benutzernamen verwenden. Die MAC-Adresse, IP-Adresse oder Host-Adresse wird verwendet, um die Zeilen der CSV-Datei den entsprechenden Geräten in der Axis Device Manager-Datenbank zuzuordnen.

Wenn Sie eine CSV-Datei verwenden, werden Sie von der Benutzeroberfläche aufgefordert anzugeben, wie die Spalten der CSV-Datei zu interpretieren sind.

### Hinweis

So geben Sie an, zu welchem Gerät eine Zeile in der CSV-Datei gehört.

Eine Spalte in der CSV-Datei muss entweder MAC-Adressen, IP-Adressen oder Host-Adressen enthalten. Geben Sie also eine Spalte in der CSV-Datei an, die entweder als MAC-Adresse oder als IP- oder Host-Adresse interpretiert werden soll. Dies wird benötigt um anzugeben, zu welchem Gerät die Daten in einer Zeile in der CSV-Datei gehören. Zusätzlich kann eine Spalte angegeben werden, die als Servername interpretiert werden soll. Auf diese Weise können Zeilen in der CSV-Datei, die auf Geräte bei verschiedenen Axis Device Manager-Servern abzielen, aber dieselbe IP-Adresse oder Host-Adresse haben, unterschieden werden. Wenn eine solche Unterscheidung nicht getroffen werden muss, ist eine Spalte überflüssig, die als Servername zu interpretieren ist. In einem Setup, in dem ein Server dieselbe IP-Adresse oder Host-Adresse für mehrere Geräte verwendet, aber Ports benutzt, um sie voneinander zu unterscheiden, kann eine Spalte angegeben werden, die als Port interpretiert wird. Wenn keine Unterscheidung nach Port erforderlich ist, gibt es normalerweise keinen Grund, eine Spalte als Port zu interpretieren. Eine Möglichkeit, den Port in einer eigenen Spalte anzugeben, besteht darin, den Port zusammen mit der IP-Adresse oder der Host-Adresse anzugeben. Nach der IP-Adresse oder der Host-Adresse folgen ein Doppelpunkt und die Port-Nummer.

## Zertifikate installieren

### Informationen zu Zertifikaten

Der AXIS Device Manager liefert die Einstellungen zum Verwalten der Zertifikate von Server und Client. Client-Zertifikate werden für IEEE 802.1X und Server-Zertifikate für HTTPS verwendet. Um Änderungen vorzunehmen, wählen Sie die geeigneten Geräte in der Geräteverwaltung aus und wählen dann im Kontextmenü Enable/update (Aktivieren/Aktualisieren).

### Erstellen Sie eine Zertifizierungsstelle (CA)

Zertifizierungsstellen ermöglichen das Aktivieren von HTTPS IEEE 802.1X auf Geräten ohne installierte Server/Client-Zertifikate. Die CA weist Geräte an, Zertifikate mit ihren eigenen Privatschlüsseln zu erstellen, zu signieren und zu installieren

So erstellen Sie eine Zertifizierungsstelle:

- Gehen Sie auf die Registerkarte **Configuration (Konfiguration)**.
- Rufen Sie **Security (Sicherheit) > Certificates (Zertifikate)** auf
- Klicken Sie unter **Certificate authority (Zertifizierungsstelle) Generate... (Generieren...)** an
- Geben Sie eine Passphrase ein und bestätigen Sie sie.
- Klicken Sie auf **OK**.

Die CA wird nun erstellt und ist einsatzbereit.

### Hinweis

Ihr eigensigniertes root-Zertifikat und Ihr privater Schlüssel, der durch eine von Ihnen gewählte Passphrase geschützt ist. Ein von AXIS Device Manager erstelltes Zertifikat hat eine Gültigkeit von 3 Jahren. Wenn Sie möchten, dass AXIS Device Manager Server-/Client-Zertifikate automatisch erneuert, müssen Sie das Kontrollkästchen **Remember passphrase (Passphrase erinnern)** aktivieren. Wenn keine CA eingerichtet ist, müssen die Server/Client-Zertifikate außerhalb des AXIS Device Manager erstellt werden. Damit gehen allerdings die Vorteile der automatischen Zertifikatsverwaltung verloren.

**Importieren** – Mit diesem Funktionsmerkmal lässt sich eine vorliegende, aus einem öffentlichen Zertifikat und einem Privatschlüssel bestehende, CA importieren. Es muss eine Kennphrase angegeben werden.

**Als Datei Speichern** – Das öffentliche Zertifikat der CA im Dateiformat .cer oder .crt speichern. Diese Datei enthält keinen Privatschlüssel. Sie wird deshalb auch nicht verschlüsselt.

**Sicherungskopie** – Es wird empfohlen, eine Sicherungskopie zu erstellen, um vor den Folgen von Hardwareversagen geschützt zu sein. Mit dieser Option wird eine Sicherungskopie sowohl des Zertifikats als auch des Privatschlüssels der vom Axis Device Manager verwendeten CA erstellt. Die Sicherungsdateien werden durch die zum Erstellen der CA verwendete Kennphrase geschützt.

**Zertifikatablaufwarnung** Wenn ein Zertifikat demnächst abläuft oder abgelaufen ist, wird eine Systembenachrichtigung erzeugt. Diese erfolgt für alle auf verbundenen Geräten installierte Zertifikate. Ausgenommen davon sind außerhalb des AXIS Device Manager installierte CAs. Die Warnung wird in der Spalte der Geräteverwaltung als Systemalarm, im Dialogfenster *Installierte Zertifikate* ansehen als Symbol und auch im Arbeitsbereich *Konfiguration* angezeigt.

Geben Sie an, wie der AXIS Device Manager Sie über das Ablauf von Zertifikaten informieren soll. Standardmäßig werden vom AXIS Device Manager erstellte Server- und Client-Zertifikate automatisch sieben Tage vor der eingestellten Warnmeldung erneuert. Um Benachrichtigungen zum Ablauf von CAs zu erhalten, das Wahlfeld *Kennphrase merken* markieren.

### HTTPS aktivieren

Um HTTPS zu aktivieren, muss auf jedem Gerät ein Server-Zertifikat vorhanden sein. AXIS Device Manager kann eine Zertifizierungsstelle (CA) verwenden, um Server-Zertifikate für Geräte zu signieren und zu installieren.

Sie können dies auch manuell tun:

1. Rufen Sie die Registerkarte **Device manager (Gerätmanager)** auf.
2. Klicken Sie mit der rechten Maustaste die Geräte an und wählen Sie im Kontextmenü **Install server certificates (Serverzertifikate installieren)** für jedes Gerät.

Vor der Aktivierung von HTTPS darf auf jedem Gerät nur ein Serverzertifikat vorhanden sein. Überzählige Zertifikate können über das Kontextmenü gelöscht werden.

3. Nach dem Installieren der Zertifikate lässt sich HTTPS über das Kontextmenü aktivieren.

#### Hinweis

Falls keine sichere Verbindung (HTTPS) verfügbar ist, kann eine Verbindung über HTTP eingerichtet werden. Auf diese Weise können noch nicht gesicherte Geräte konfiguriert werden.

### Zertifikatsvalidierung ignorieren

AXIS Device Manager baut keine Verbindung zu Geräten ohne validiertes Zertifikat auf. Das Server-Zertifikat muss von der im Axis Device Manager aktiven CA signiert werden oder über den Windows Certification Store geprüft werden. Wenn die Option *Zertifikatsprüfung übergehen* gewählt wird, prüft der AXIS Device Manager nicht, ob das vom Gerät gesendete Zertifikat vertrauenswürdig ist.

Damit AXIS Device Manager die Zertifikatsvalidierung ignoriert.

- Gehen Sie auf die Registerkarte **Configuration (Konfiguration)**.
- Unter **HTTPS**, aktivieren Sie **Ignore certificate validation (Zertifikatsvalidierung ignorieren)**.

### 802.1X aktivieren

Um IEEE 802.1X zu aktivieren, muss auf jedem Gerät ein Client-Zertifikat vorhanden sein. AXIS Device Manager kann eine Zertifizierungsstelle (CA) verwenden, um Client-Zertifikate für Geräte zu signieren und zu installieren.

Dies kann auch manuell in der Geräteverwaltung durchgeführt werden. Dazu die Geräte rechtsklicken und im Kontextmenü für die gewählten Geräte die Option *Server-Zertifikate installieren* wählen. Vor der Aktivierung von IEEE 802.1X darf auf jedem Gerät nur ein Client-Zertifikat vorhanden sein. Überzählige Zertifikate können über das Kontextmenü gelöscht werden. Nach dem Installieren der Zertifikate lässt sich IEEE 802.1X über das Kontextmenü aktivieren.

Um das Protokoll IEEE 802.1X nutzen zu können, ist ebenfalls ein Authentifizierungszertifikat für IEEE 802.1X von einer Zertifizierungsstelle erforderlich.

**EAPOL-Version** – Die bevorzugte Version des Extensible Authentication Protocol (EAP) wählen.

**EAP-Identität** – Entweder die MAC-Adresse, den Hostnamen oder eine benutzerdefinierte Bezeichnung für das Gerät eingeben.

**Benutzerdefiniert** – Als EAP-Identität eine benutzerdefinierte Bezeichnung eingeben.

CA-Zertifikat für die Authentifizierung von IEEE 802.1X – Zusätzlich zum Clientzertifikat muss ein CA-Zertifikat für die Authentifizierung von IEEE 802.1X installiert werden. Zum Aktivieren von IEEE 802.1X ist nur das öffentliche Zertifikat erforderlich und kein Privatschlüssel. Eine Kennphrase ist also nicht erforderlich. Das Authentifizierungszertifikat für IEEE 802.1X wird beim Aktivieren oder Aktualisieren von IEEE 802.1X installiert.

**Importieren** – Das CA-Zertifikat wählen, das auf den Geräten zum Prüfen des Authentifizierungsservers installiert werden soll. Das CA-Zertifikat kann entweder von der auf dem AXIS Device Manager installierten CA oder von einer externen Instanz erstellt werden.

**Ansehen** – Die Angaben zum beim Authentifizierungsverfahren für IEEE 802.1X verwendeten CA-Zertifikat ansehen.

**Geläufiger Name** – Die EAP-Identität oder die IP-Adresse des Gerätes wählen. Wenn kein benutzerdefinierter Name angegeben wird, wird der Hostname verwendet. Wenn der Hostname problematisch ist, wird die IP-Adresse als geläufiger Name verwendet.

### SIP-Einstellungen konfigurieren

Verwenden Sie den Setup-Assistenten, um die SIP- und Port-Einstellungen auf ausgewählten Geräten zu konfigurieren. Mit dem Setup-Assistent können Sie den bereits im Gerät vorhandenen Wert beibehalten oder einen Wert eingeben, der auf alle ausgewählten Geräte angewendet wird. Sie können auch Werte aus einer CSV-Datei laden, um gerätespezifische Werte auf ausgewählte Geräte anzuwenden.

Verwenden Sie in der CSV-Datei eine Zeile für jedes Gerät und eine Spalte für jeden Parameter zur Einstellung. Mit dem Setup-Assistent können Sie festlegen, welche Werte abgerufen werden sollen.

So verwenden Sie eine CSV-Datei für Gerät-spezifische Einstellungen für mehrere Geräte:

1. Den Arbeitsbereich **Device management (Geräteverwaltung)** aufrufen.
2. Wählen Sie das Gerät aus, die Sie konfigurieren möchten.
3. Klicken Sie mit der rechten Maustaste und wählen Sie **Configure devices (Geräte konfigurieren) > Advanced (Erweitert) > SIP configuration (SIP-Konfiguration) > Settings (Einstellungen)**.
4. Wenn Sie eine CSV-Datei verwenden möchten, überprüfen Sie, ob Sie die Verwendung einer CSV-Datei zulassen. Andernfalls fahren Sie mit 5 fort.
  - 4.1. Klicken Sie auf **Browse (Navigieren)** und wählen Sie die CSV-Datei aus, die Sie verwenden möchten.
  - 4.2. Klicken Sie auf **Next (Weiter)**.
  - 4.3. Wählen Sie in der Drop-Down-Liste aus, wie die Spalten der CSV-Datei benannt werden sollen.
  - 4.4. Wählen Sie entweder die MAC-Adresse, die IPv4-Adresse oder die Host-Adresse für eine Spalte in der CSV-Datei aus und ordnen Sie diese den Geräten in den Zeilen zu.
5. Klicken Sie auf **Next (Weiter)**.
6. Wählen Sie eine der folgenden SIP- und Port-Einstellungen aus:
  - **Enable SIP (SIP aktivieren)** – Aktiviert SIP auf den ausgewählten Geräten.
  - **Allow incoming SIP calls (Eingehende SIP-Anrufe zulassen)** – Erlaubt eingehende SIP-Anrufe auf Ihren Geräten.
  - **SIP port (SIP-Port)** – Zuweisen einer Portnummer, die für SIP-Anrufe verwendet wird.
  - **TLS port (TLS-Port)** – Zuweisen einer Portnummer, die für die TLS-Verschlüsselung verwendet wird.
  - **RTP start port (RTP-Startport)** – Zuweisen einer RTP-Portnummer für den Audio-Datenaustausch.
7. Klicken Sie auf **Next (Weiter)**.
8. Wählen Sie eine der folgenden Audio- und Anruf-Einstellungen aus:
  - **Audio direction (Audio-Richtung)** – Wählen Sie zwischen **Send only (Nur senden)**, **Receive only (Nur empfangen)** und **Send and receive (Senden und empfangen)**.

- **DTMF payload type (DTMF-Nutzlasttyp)** – Wählen Sie den DTMF-Nutzlasttyp für die Übertragung von DTMF-Ziffern, -Tönen und -Signalen.
  - **Calling timeout (Zeitüberschreitung für Anrufe)** – Wählen Sie die Anzahl der Sekunden, die gewartet werden soll, bis ein Anruf als Zeitüberschreitung gilt.
  - **Incoming call timeout (Zeitüberschreitung eingehender Anruf)** – Wählen Sie die Anzahl der Sekunden, die gewartet werden soll, bis ein eingehender Anruf als Zeitüberschreitung gilt.
  - **End calls after (Anrufe nach einer bestimmten Zeit beenden)** – Wählen Sie die Anzahl der Sekunden, die gewartet werden soll, bis ein eingehender Anruf automatisch beendet wird. Sie können auch eine unbegrenzte Anrufdauer zulassen.
9. Klicken Sie auf **Next (Weiter)**.
  10. Wählen Sie einen der folgenden NAT-Traversal-Parameter aus:
    - **ICE Enable (ICE aktivieren)** – Aktiviert Interactive Connectivity Establishment (ICE) auf den ausgewählten Geräten.
    - **TURN Enable (TURN aktivieren)** – Aktiviert Traversal Using Relays around Network Address Translation (TURN).
    - **TURN server address (TURN-Serveradresse)** – Geben Sie die Adresse des TURN-Servers ein.
    - **TURN username (TURN-Benutzername)** – Geben Sie den TURN-Benutzernamen ein.
    - **TURN password (TURN-Kennwort)** – Geben Sie das TURN-Kennwort ein.
    - **STUN Enable (STUN aktivieren)** – Aktiviert Session Traversal Utilities for Network Address Translation (STUN)
    - **STUN server address (STUN-Serveradresse)** – Geben Sie die Adresse des STUN-Servers ein.
  11. Klicken Sie auf **Next (Weiter)**.
  12. Überprüfen Sie die Konfiguration der aufgeführten Geräte.
  13. Wenn alles in Ordnung ist, klicken Sie auf **Finish (Fertig)**.

## SIP-Konten verwalten

Im Axis Device Manager können Sie Ihre SIP-Einstellungen konfigurieren und SIP-Konten hinzufügen oder entfernen.

### SIP-Konten hinzufügen

Um SIP-Konten hinzuzufügen, müssen Sie diese in einer CSV-Datei angeben. Sie können eine Vorlage im Setup-Assistenten erstellen.

Eine neue Vorlage erstellen:

1. Den Arbeitsbereich **Device management (Geräteverwaltung)** aufrufen.
2. Wählen Sie das Gerät aus, die Sie konfigurieren möchten.
3. Klicken Sie mit der rechten Maustaste und wählen Sie **Configure devices (Geräte konfigurieren) > Advanced (Erweitert) > SIP configuration (SIP-Konfiguration) > Add SIP accounts (SIP-Konten hinzufügen)**.
4. Klicken Sie auf **Generate template (Vorlage erstellen)**
5. Wählen Sie einen Speicherort für die CSV-Datei.
6. Fügen Sie die Konten zur Datei hinzu. Verwenden Sie eine Zeile für jedes Konto, das Sie einem Gerät hinzufügen möchten. Sie können einem Gerät mehrere Konten hinzufügen.

Die CSV-Datei hat das folgende Layout:

Spaltenname	Beschreibung	Obligatorisch/Optional	Hinweise
deviceIdentifier	MAC-Adresse, IP-Adresse oder Host-Adresse	obligatorisch	Diese Spalte gibt an, zu welchem Gerät das Konto hinzugefügt werden soll. Es kann sich dabei entweder um eine MAC-Adresse, eine IPv4-Adresse oder eine Host-Adresse handeln.
aktiv	Boolesche Variable	obligatorisch	
makeDefault	Boolesche Variable	obligatorisch	
answerAutomatically	Boolesche Variable	obligatorisch	
name	string	obligatorisch	
userId	string	obligatorisch	
Domain	string	optional	Falls diese Spalte in der CSV-Datei fehlt, werden alle Konten als Peer-to-Peer in der Einstellung festgelegt. Falls diese Spalte vorhanden ist, wird das Konto als Peer-to-Peer in der Einstellung festgelegt, wenn die Zelle leer ist, und als Registriert, wenn sie etwas enthält.
Kennwort	string	obligatorisch	
authenticationId	string	obligatorisch	
callerId	string	obligatorisch	
registrar	string	optional	
transportMode	udp or tcp	obligatorisch	In MVP1 wird TLS nicht unterstützt.

So fügen Sie die Konten zu den ausgewählten Geräten hinzu:

- Den Arbeitsbereich **Device management (Geräteverwaltung)** aufrufen.
- Wählen Sie das Gerät aus, die Sie konfigurieren möchten.
- Klicken Sie mit der rechten Maustaste und wählen Sie **Configure devices (Geräte konfigurieren) > Advanced (Erweitert) > SIP configuration (SIP-Konfiguration) > Add SIP accounts (SIP-Konten hinzufügen)**.
- Auf **Browse (Durchsuchen)** klicken.
- Wählen Sie die CSV-Datei aus, zu der Sie die Konten hinzugefügt haben.
- Klicken Sie auf **Weiter**.
- Überprüfen Sie die Konfiguration der aufgeführten Geräte.
- Wenn alles in Ordnung ist, klicken Sie auf **Finish (Fertig)**.

## SIP-Konten entfernen

So entfernen Sie alle SIP-Konten außer dem Standard-Konto auf ausgewählten Geräten:

1. Den Arbeitsbereich **Device management (Geräteverwaltung)** aufrufen.
2. Wählen Sie das Gerät aus, die Sie konfigurieren möchten.
3. Klicken Sie mit der rechten Maustaste und wählen Sie **Configure devices (Geräte konfigurieren) > Advanced (Erweitert) > SIP configuration (SIP-Konfiguration) > Remove accounts (Konten entfernen)**.
4. Aktivieren Sie im Setup-Assistent die Option **Remove all accounts except the default account on the selected devices (Alle Konten außer dem Standardkonto auf den ausgewählten Geräten entfernen)**.
5. Klicken Sie auf **Finish (Fertig)**.

## Metadaten auf Geräten aktivieren

In diesem Schutzzielbeispiel werden wir Metadaten auf mehreren Geräten aktivieren. Bevor Sie diese Aufgabe ausführen, empfehlen wir Ihnen, sie zunächst auf einem Gerät auszuprobieren, um Probleme mit mehreren Geräten zu vermeiden. So aktivieren Sie Metadaten auf einem oder mehreren Geräten:

1. Den Arbeitsbereich **Device management (Geräteverwaltung)** aufrufen.
2. Wählen Sie die Geräte aus, für die Sie Metadaten aktivieren möchten.
3. Klicken Sie mit der rechten Maustaste und wählen Sie **Configure devices (Geräte konfigurieren) > Advanced (Erweitert) > Set configuration (Konfiguration festlegen)**.
4. Klicken Sie auf **OK**
5. Wählen Sie **Set NTP servers (NTP-Server einrichten)** im Drop-Down-Menü.
6. Stellen Sie in der Drop-Down-Liste **Uri** sicher, dass die Methode **Post** lautet.
7. Fügen Sie im Adressfeld Folgendes hinzu: **axis-cgi/analyticsmetadataconfig.cgi**
8. Fügen Sie den folgenden Code in **Content (Inhalt)** ein:

```
{ "apiVersion": "1.0", "context": "my context", "method": "setEnabledProducers", "params": {
  "producers": [ { "name": "objectanalytics", "videochannels": [ { "channel": 1, "enabled": true }
] ] ] }
```

9. Prüfen Sie, ob **Content-Type (Inhaltstyp)** **application/json** lautet.
10. Klicken Sie auf **Senden**.

### Hinweis

Bitte beachten Sie, dass AXIS Device Manager keine Antwort zurückgibt, wenn Sie die oben beschriebene Methode verwenden. Überprüfen Sie immer das Fenster **Tasks (Aufgaben)** auf Fehler. Sie können auch eine spezielle Software wie POSTMAN verwenden, um die API mit verbesserter Funktionalität zu testen. Einige VMS können Einschränkungen haben, die nur einen einzigen Produzenten gleichzeitig zulassen, sodass Sie möglicherweise die zusätzlichen Produzenten über die oben erwähnte API deaktivieren müssen.

## Verwaltung der Gerätesoftware

### AXIS OS-Upgrades

Neue AXIS OS-Versionen können auf zwei Arten bezogen werden:

- Herunterladen mithilfe von AXIS Device Manager (Internetzugang erforderlich)
- oder aus einer Datei (bspw. auf der Festplatte oder einem USB-Stick) importieren.

#### Hinweis

Es wird geraten, dem für AXIS OS empfohlenen Upgrade-Pfad zu folgen. Mehr dazu lesen Sie hier: <https://help.axis.com/axis-os#upgrade-path>

#### Manuelle Verbesserung von AXIS OS

1. Wählen Sie die Geräte aus, die Sie mit einer neuen AXIS OS-Version verbessern möchten, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Upgrade Firmware (Firmware aktualisieren)**.
2. Wenn Sie darüber informiert werden, dass die Geräte während des Upgrades nicht mehr zugänglich sind, klicken Sie auf **Yes (Ja)**.
3. So aktualisieren Sie die Liste der zum Herunterladen verfügbaren Firmware-Versionen. Klicken Sie im Dialog **Upgrade Firmware (Firmware aktualisieren)** auf **Check for Updates (Nach Updates suchen)**.
4. Die Schaltfläche **Browse (Durchsuchen)** anklicken, um nach einer oder mehreren auf dem lokalen Client gespeicherten Versionsdateien von AXIS OS zu suchen.
5. Wählen Sie die Geräte und die AXIS OS-Versionen aus, die Sie aktualisieren möchten.
6. Um die Werkseinstellungen der ausgewählten Geräte während der Verbesserung von AXIS OS wiederherzustellen, klicken Sie das Kontrollkästchen **Factory default (Werkseinstellungen)** an. Dies ist bei einigen AXIS OS-Versionen eine Voraussetzung für ein Downgrade.
7. Klicken Sie auf **OK**, um das Upgrade der ausgewählten Geräte in der Liste zu starten.

#### Hinweis

AXIS OS-Upgrades werden voreingestellt bei allen gewählten Geräten gleichzeitig durchgeführt. Die Reihenfolge des Upgrade kann unter **Configuration > Connected Services > Firmware upgrade settings (Konfiguration – Verbundene Dienste – Einstellungen für die Firmware-Verbesserung)** geändert werden.

#### Automatische Upgrades

In der Standardeinstellung von AXIS Device Manager 5 wird nicht nach Firmware-Upgrades gesucht, aber es kann eingerichtet werden, dass automatisch geprüft wird, ob AXIS OS-Upgrades auf dem Server oder auf axis.com verfügbar sind.

Um manuell nach AXIS OS-Upgrades zu suchen, klicken Sie im Menü Aktion die Schaltfläche **Check now (Jetzt prüfen)** an.

#### Reihenfolge der AXIS OS-Verbesserung

AXIS OS-Upgrades können für alle Geräte gleichzeitig oder für ein Gerät nach dem anderen durchgeführt werden.

- Um alle Geräte auf einmal zu aktualisieren, wählen Sie **Parallel** als Reihenfolge der Upgrades.
- Um die Geräte nacheinander zu verbessern, wählen Sie **Sequential (nacheinander)**. Diese Option dauert länger, jedoch sind nicht alle Geräte gleichzeitig offline. Bei der sequenziellen Verbesserung können Sie darüber hinaus den Vorgang stoppen, falls ein Problem mit der Kontrolle von auftritt. **Alle verbleibenden Verbesserungen abbrechen**, wenn bei einem Gerät Fehler auftreten .

## Fehlerbehebung

### Software-Bestellliste

So erhalten Sie die Software-Bestellliste (SBOM):

1. Rufen Sie die *Produkt-Support-Seite für den AXIS Device Manager* auf [axis.com](http://axis.com) auf.
2. Klicken Sie auf **SOFTWARE BILL OF MATERIALS (Software-Bestellliste)**.

Mehr über SBOM lesen Sie auf dem *AXIS OS Portal* unter [axis.com](http://axis.com).

### Support

Wenn Sie sich an den Support wenden, erstellen Sie zunächst ein Ticket und fügen eine Systemberichtsdatei bei, um die Fehlersuche für Ihr spezielles Problem zu erleichtern:

1. Gehen Sie zum Hauptmenü.
2. Navigieren Sie zu **Help (Hilfe) > System Report... (Systembericht...)**.
3. Speichern Sie die Berichtsdatei in einem gewählten Ordner.
4. Gehen Sie zu [axis.com/support](http://axis.com/support).
5. Erstellen Sie ein Support Ticket.
6. Hängen Sie Ihrem Support Ticket die Datei an.

#### Hinweis

So erstellen Sie einen Systembericht über ein nicht reagierendes System:

1. Zu `C:\ProgramData\Axis Communications\` wechseln
2. Archivieren Sie den Inhalt des Ordners in einer .zip-Datei und hängen Sie diese an das Support Ticket an.

### Eskalationsverfahren

Wenden Sie sich bei Problemen, die mit dieser Anleitung nicht behoben werden können, an den *Axis Online Helpdesk*. Damit unser Support-Team Ihr Problem nachvollziehen und lösen kann, werden folgende Angaben benötigt:

- Eine klare Beschreibung, unter welchen Umständen das Problem auftritt und wie es reproduziert werden kann.
- Uhrzeit sowie Name oder IP-Adresse des betroffenen Geräts, bei dem das Problem auftritt.
- AXIS Device Manager Systembericht, der direkt nach dem Auftreten des Problems erstellt wurde. Der Systembericht muss durch den Client oder Server erstellt worden sein, auf dem das Problem aufgetreten ist.
- Optionale Bildschirmfotos oder Aufzeichnungen, die das Problem zeigen.
- Fügen Sie bei Bedarf die Datenbankdateien bei. Verzichteten Sie auf diese Dateien, um das Hochladen zu beschleunigen.

Bei einigen Problemen sind zusätzliche Informationen erforderlich, die das Support-Team bei Bedarf anfordert.

#### Hinweis

Übermitteln Sie Dateien ab einer Größe von 100 MB, z. B. Netzwerk-Trace- oder Datenbankdateien, über einen sicheren, vertrauenswürdigen File-Sharing-Dienst.

Weitere Informationen	
<b>Debug-Level-Protokollierung</b>	Um weitere Informationen zu erhalten, ist gelegentlich eine Untersuchung auf Fehlerprotokollebene erforderlich. Dies geschieht nur auf Anweisung eines Axis Support-Mitarbeiters. Eine entsprechende Anleitung finden Sie im <i>Axis Online-Helpdesk</i> .
<b>Netzwerk-Trace</b>	Falls auf Anweisung des Supporttechnikers erforderlich, erzeugen Sie beim Erstellen des Systemberichts Netzwerk-Traces. Falls das Problem reproduzierbar ist, erzeugen Sie die Netzwerk-Traces während dem Auftreten des Problems. Dazu zählen: <ul style="list-style-type: none"> <li>• Ein Netzwerk-Trace von 60 Sekunden auf der Kamera (nur anwendbar auf Kameras mit Firmware ab Version 5.20). Verwenden Sie den folgenden VAPIX-Befehl, um bei Bedarf die Anmeldung, die IP-Adresse und die Dauer (in Sekunden) zu ändern: <code>http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&amp;duration=60</code></li> <li>• Ein Netzwerk-Trace von 10 bis 30 Sekunden auf dem Server, das die Kommunikation zwischen Server und Kamera dokumentiert.</li> </ul>
<b>Datenbankdateien</b>	Für Fälle, die von uns eine Untersuchung oder manuelle Reparatur der Datenbank erfordern. Wählen Sie <b>Include database in the report (Dem Bericht die Datenbankdatei hinzufügen)</b> aus, bevor Sie den Systembericht erstellen.
<b>Schnappschüsse</b>	Verwenden Sie Screenshots, wenn es sich um ein Problem mit der Live-Ansicht handelt, das mit der Benutzeroberfläche zu tun hat. Dies ist beispielsweise hilfreich, wenn es sich um die Anzeige einer Zeitleiste für Aufzeichnungen handelt oder wenn sich etwas schwer beschreiben lässt.
<b>Bildschirmaufzeichnungen</b>	Verwenden Sie Bildschirmaufzeichnungen, wenn sich das Problem nur schwer mit Worten beschreiben lässt. Ein Beispiel hierfür ist, wenn zum Reproduzieren des Problems viele Interaktionen mit der Benutzeroberfläche erforderlich sind.

T10211981\_de

2026-04 (M6.2)

© 2024 – 2026 Axis Communications AB