AXIS Device Manager

Benutzerhandbuch

Inhalt

Über den AXIS Device Manager

Der AXIS Device Manager ist eine Installations- und Verwaltungssoftware 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.

Lösungsübersicht

Voraussetzungen

Kompatible Betriebssysteme:

Erforderlich: 64-Bit-Betriebssystem Microsoft .NET Version 4.8

Unterstützte Betriebssysteme: Windows 10 Pro, Windows 11 Pro, Windows Server 2016, Windows Server 2019, Windows Server 2022

Empfehlungen: Neueste OS Service Packs.

Mindestsystemempfehlungen:

- Minimum (bis zu 500 Geräte): Intel Core i5 oder gleichwertig, 4 GB RAM, 100 Mbit/s über die Netzwerkinfrastruktur
- Empfohlen (zwischen 500 und 2.000 Geräte): Intel Core i7 oder gleichwertig, 8 GB RAM, 1000 Mbit/s über die Netzwerkinfrastruktur
- Mehr als 2.000 Geräte pro Server werden nicht empfohlen.
- Stellen Sie sicher, dass auf den Geräten von Axis das neueste AXIS Betriebssystem läuft.

Hinweis

Wir unterstützen immer die beiden Vorgängerversionen der neuesten Version. Prüfen Sie die neuesten Versionshinweise um festzustellen, welche Versionen unterstützt werden.

Unterstützte Geräte:

AXIS Produkte mit AXIS OS Version 4.40 oder höher. (Bitte beachten Sie, dass die genaue unterstützte Funktionalität je nach Produktmodell und Firmware variiert)

Sprachen:

UI + Hilfedateien: Englisch, Französisch, Deutsch, Italienisch

Nur UI: Arabisch, Tschechisch, Chinesisch (vereinfacht), Chinesisch (traditionell), Niederländisch, Finnisch, Japanisch, Koreanisch, Persisch, Polnisch, Portugiesisch (Brasilien), Russisch, Spanisch, Schwedisch, Türkisch und Vietnamesisch.

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 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.

Erste Konfiguration

Zunächst müssen Sie Folgendes tun:

- Geräte hinzufügen und Benutzerkonten erstellen, siehe:
- Ihr System für die Cybersicherheit härten. Siehe

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 . 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.

Konfiguration

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 Statusspalte 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 Ablaufen 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 (Gerätemanager)** 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-Konten verwalten

Verwaltung der Gerätesoftware

AXIS OS Aktualisierungen

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.

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 AXIS OS**.
2. Im Dialogfeld **Upgrade firmware (Firmware verbessern)**: Um die Liste der zum Herunterladen bereitgestellten Firmware-Versionen zu aktualisieren, die Schaltfläche **Check for Updates (Nach Aktualisierungen suchen)** anklicken.
3. Die Schaltfläche **Browse (Durchsuchen)** anklicken, um nach einer oder mehreren auf dem lokalen Client gespeicherten Versionsdateien von AXIS OS zu suchen.
4. 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.
5. Die Geräte und die AXIS-OS-Versionen wählen und **OK** anklicken, um die aus der Liste gewählten Geräte zu verbessern.

Hinweis

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

Automatische Aktualisierungen

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

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

Reihenfolge der AXIS OS-Verbesserung

AXIS OS-Aktualisierungen 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 Verbesserungen
- 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

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*.
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. Gehen Sie zu `C:\ProgramData\Axis Communications`
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. Verzichten 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	
Debug-Level-Protokollierung	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 *Axis Online-Helpdesk*.
Netzwerk-Trace	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: • 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:

Weitere Informationen	
	`http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=60` • Ein Netzwerk-Trace von 10 bis 30 Sekunden auf dem Server, das die Kommunikation zwischen Server und Kamera dokumentiert.
Datenbankdateien	Für Fälle, die von uns eine Untersuchung oder manuelle Reparatur der Datenbank erfordern. Wählen Sie **Include database in the report (Dem Bericht die Datenbankdatei hinzufügen)** aus, bevor Sie den Systembericht erstellen.
Schnappschüsse	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.
Bildschirmaufzeichnungen	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

2025-03 (M1.9)