AXIS Device Manager Extend

Benutzerhandbuch

AXIS Device Manager Extend

Inhalt

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.

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	Anmerkung
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	Erforderlich für die Bereitstellung des Standorts. 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*
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	Anmerkung
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	Erforderlich für die Bereitstellung des Standorts. 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 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	Anmerkung
A	prod.adm.connect.axis.com (52.224.128.152 oder 40.127.155.231)	443	HTTPS	Erforderlich

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	Erforderlich für die Bereitstellung des Standorts. 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 MBit/s

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 Site Controller nur im Online-Modus automatisch.

Synchronisierte Zeit und Datum

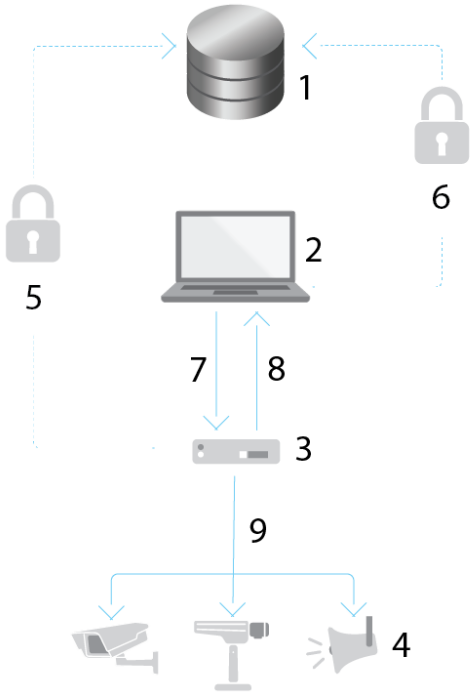
Hinweis

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.

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.

Erste Schritte

Installieren der Software, Erstellen einer Organisation und Hinzufügen von Geräten

Ein MyAxis-Konto einrichten

Ein **MyAxis**-Konto wird unter *axis.com/my-axis/login* eingerichtet.

Ihr MyAxis-Konto wird sicherer, wenn Sie die mehrstufige Authentifizierung (MFA) aktivieren. MFA ist ein Sicherheitssystem, das zur Gewährleistung der Identität des Benutzers eine weitere Überprüfungsebene hinzufügt.

Aktivieren Sie MFA:

1. Melden Sie sich mit den Zugangsdaten zu **MyAxis** an.
2. Rufen Sie auf und wählen Sie **Account settings (Kontoeinstellungen)** aus.
3. Klicken Sie auf **Security settings (Sicherheitseinstellungen)**.
4. Aktivieren Sie **2-Step verification (2-Stufen-Überprüfung)**.

Sie werden zu einer Anmeldeseite weitergeleitet.

5. Melden Sie sich mit den Zugangsdaten zu **MyAxis** an.

Die MFA ist jetzt aktiv.

Anmeldung bei aktivierter MFA:

1. Melden Sie sich bei Ihrem **MyAxis**-Konto an.

Sie erhalten eine E-Mail.

2. Öffnen Sie die E-Mail und klicken Sie auf **Authenticate (Authentifizieren)**.

Falls Sie keine E-Mail erhalten haben, überprüfen Sie, ob sie sich im Spam-Ordner befindet. Befindet sie sich dort nicht, wenden Sie sich an den IT-Support.

Den Client installieren und Ihr Konto aktivieren

Rufen Sie die Produktseite auf 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.

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 des Standortcontrollers 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 **Geräte > 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 **Geräte hinzufügen**.

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.

9. Klicken Sie auf **Geräte hinzufügen**.

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 **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 **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 **Anmelden**.

Hinweis

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

Konfiguration

Fernzugriff aktivieren

Blockiert Ihre Firewalleinstellungen 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

Zur Unterstützung der Verbindung mit Edge-Hosts in anderen Netzwerken müssen Sie der „Freigabeliste" der Firewall Ihres Unternehmensnetzwerks möglicherweise folgende Konfiguration 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 12*. Die Geräte finden Sie dann unter **Geräte > Erkannt**.

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 Auswahlmenü **Edge-Host entfernen**.
4. Markieren Sie **Ich bin mir der Risiken bewusst.**
5. Klicken Sie auf **Entfernen**.

Benutzern Ihrer Organisation hinzufügen

1. Wählen Sie die Organisation, in der Sie Benutzereinstellungen konfigurieren möchten.
2. Gehen Sie zu **Benutzer**.
3. Klicken Sie auf **Zur Organisation einladen**.
4. Geben Sie die E-Mail-Adresse des Benutzers ein, den Sie zu Ihrer Organisation einladen möchten.
5. Klicken Sie auf **Einladung senden**.

Hinweis

Der Benutzer erhält eine Einladungsmail, die er zur Anmeldung bei AXIS Device Manager Extend verwenden kann. Die Standardbenutzerrolle ist **Beobachter**. Wenn sie kein My Axis-Konto besitzen, müssen sie sich mit dieser E-Mail anmelden, um auf die Organisation zugreifen zu können. Einladungen können zurückgenommen werden, solange sie noch nicht angenommen wurden.

Benutzerrolle höherstufen

1. Wählen Sie die Organisation, in der Sie Benutzereinstellungen konfigurieren möchten.

2. Gehen Sie zu **Benutzer**.
3. Gehen Sie zu **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. Gehen Sie zu **Benutzer**.
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**.

Firmware-Verwaltung

Mit AXIS Device Manager Extend können Sie die Firmware mehrerer Geräte in jeder Organisation verwalten.

Um eine nach Modell zusammengefasste Liste mit für jedes Gerät in Ihrem Unternehmen verfügbaren Firmwareaktualisierungen zu erhalten, gehen Sie zu **Startseite > Firmwareinventar**. Um eine Liste mit an einem bestimmten Edge-Host verfügbaren Firmwareaktualisierungen zu erhalten, wählen Sie den Edge-Host und gehen Sie dann zu **Firmwareinventar**.

Gerätemodellbasierte Firmware verwalten

So verwalten Sie Firmware nach Gerätemodell für ihre gesamte Organisation:

1. Gehen Sie zu **Startseite > Firmwareinventar**
2. Markieren Sie das zu verwaltende Modell.
3. Klicken Sie in das Auswahlmenü **Aktualisieren auf**, um die verfügbaren Optionen zu sehen. Die aktuelle Firmware wird vorausgewählt.
4. Klicken Sie auf **Aktualisieren**.

Gerätefirmware auf einem Edge-Host verwalten.

So lässt sich die Firmware einiger oder aller Geräte auf einem Edge-Host verwalten:

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 Aktionsmenü auf das Symbol für die **Firmware**
6. Überprüfen Sie alle oder einige Modelle in der Liste.
7. Wenn Sie die ausgewählte Firmware ändern möchten, klicken Sie auf die Firmware, um zu sehen, welche für die einzelnen Geräte verfügbar ist. Die aktuelle Firmware wird vorausgewählt.
8. Klicken Sie auf **Aktualisieren**.

Aktuelle und abgeschlossene Firmwareaktualisierungen sehen

So lassen sich abgeschlossene Firmwareaktualisierungen sehen:

1. Gehen Sie zu **Standorte**.
2. Klicken Sie auf den Standort, auf den Sie zugreifen möchten.
3. Gehen Sie zu **Aufgaben**

So lassen sich aktuelle Firmwareaktualisierungen sehen:

4. Gehen Sie zu **Standorte**.
5. Klicken Sie auf den Standort, auf den Sie zugreifen möchten.
6. Gehen Sie zu **Aufgaben > Laufende Aufgaben**

Richtlinien

Richtlinien

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 **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.

9. Klicken Sie auf **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. Klicken Sie auf **Speichern**.

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 Auswahlmenü 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 Auswahlmenü 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.

Fehlerbehebung

So konfigurieren Sie die Firewalleinstellungen

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 Firewalleinstellungen 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.

Benutzerhandbuch
AXIS Device Manager Extend

Vers. M18.2
Datum: April 2024
Teil-Nr. T10153497