

## **AXIS Device Manager Extend**

**ユーザーマニュアル**

# AXIS Device Manager Extend

## 目次

---

バージョン情報 .....	3
ソリューションの概要 .....	4
前提条件 .....	7
はじめに .....	9
My Axisアカウントを登録する .....	9
クライアントをインストールしてアカウントをアクティブにする .....	9
エッジホストの設置 .....	10
エッジホストの申し立て .....	10
装置の管理 .....	11
検出された装置をエッジホストに追加する .....	11
製品を削除する .....	12
装置にログインします。 .....	12
設定 .....	14
リモートアクセスのアクティブ化 .....	14
サイトを削除する .....	14
ユーザーを組織に追加する .....	14
ユーザー権限の昇格 .....	14
ユーザーの削除 .....	15
ファームウェアの管理 .....	16
装置モデルに基づくファームウェアの管理 .....	16
エッジホストで装置のファームウェアを管理します。 .....	16
進行中および完了したファームウェアアップグレードを表示する .....	16
ポリシー .....	18
セキュリティポリシーの作成と適用 .....	18
アプリポリシーの作成と適用 .....	18
ポリシーの編集 .....	19
ポリシーの削除 .....	19
トラブルシューティング .....	20
ファイアウォールの設定方法 .....	20

# AXIS Device Manager Extend

## バージョン情報

---

### バージョン情報

AXIS Device Manager Extendソリューションは、システム管理者が組織のネットワーク上でAxis装置を検出、設定、操作するためのインターフェースを提供します。

#### デスクトップAXIS Device Manager Extend アプリ

デスクトップアプリは、必要に応じて使用できるソフトウェアユーティリティプログラムです。また、システムを管理するための常に利用可能なユーザーインターフェースです。専用のマシンで、ローカルにインストールされたエッジホストと一緒に実行することも、エッジホストとは別に、リモートで接続されたラップトップで実行することもできます。クライアントはユーザーにシステムの全体的なステータスと、すぐに利用可能な管理アクションを表示します。

#### エッジホスト

AXIS Device Manager Extendのエッジホストコンポーネントは、常に利用可能なオンプレミスの管理サービスで、カメラなどのローカル装置のメンテナンスを担当します。AXIS Device Manager Extendはエッジホスト、Axisリモート管理サービスへのリンクとして機能し、同じAPI機能が、Axisサービスプラットフォームを介したサイトのリモート管理をサポートします。

# AXIS Device Manager Extend

## ソリューションの概要

### ソリューションの概要

AXIS Device Manager Extend (ローカルおよびリモートアクセスを使用)

- 1 Axis
- 2 IAM (My Axis)
- 3 組織データ
- 4 ローカルクライアント
- 5 エッジホスト
- 6 装置
- 7 VMS
- 8 TURN
- 9 信号伝達
- 10 リモートクライアント
- 11 リモートアクセスWebRTCサーバー
- 12 サイト1

Con- nection (接続)	URLとIP	ポート	プロトコル	コメント
A	prod.adm.connect.axis.com (52.224.128.152または40.127.155.231)	443	HTTPS	必須
B	HTTP検出 (クライアントからエッジホ ストへ) データ転送 (クライアントとエッジホ ストの間) マルチキャスト検出 (クライアントか らエッジホストへ) マルチキャスト検出 (エッジホストか らクライアントへ)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	サイトをプロビジョニ ングする必要があります。 プロビジョニング 後はオプションです。
C	データ転送 (エッジホストと装置の間) ユニキャスト検出 マルチキャスト検出 HTTP検出	80 / カスタ ムポート、 443 1900 1900, 5353 80,443	HTTP、HTTPS SSDP、Bonjour	必須
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS、DTLS (UDPおよびTCP)	WebRTC規格に準拠 オプション (デフォル トではオフに設定)
E	ピアツーピア (P2P)	49152-6553 5	DTLS (UDPおよび TCP)	

AXIS Device Manager Extend (ローカルおよびリモートアクセス、マルチサイト設定を使用)

- 1 Axis
- 2 IAM (My Axis)
- 3 組織データ
- 4 ローカルクライアント
- 5 エッジホスト
- 6 装置
- 7 VMS

# AXIS Device Manager Extend

## ソリューションの概要

- 8 TURN
- 9 信号伝達
- 10 リモートクライアント
- 11 リモートアクセスWebRTCサーバー
- 12 サイト1
- 13 サイト2
- 14 サイト3

接続	URLとIP	ポート	プロトコル	コメント
A	prod.adm.connect.axis.com (52.224.128.152または40.127.155.231)	443	HTTPS	必須
B	HTTP検出(クライアントからエッジホストへ) データ転送(クライアントとエッジホストの間) マルチキャスト検出(クライアントからエッジホストへ) マルチキャスト検出(エッジホストからクライアントへ)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	サイトをプロビジョニングする必要があります。プロビジョニング後はオプションです。
C	データ転送(エッジホストと装置の間) ユニキャスト検出 マルチキャスト検出 HTTP検出	80 / カスタムポート、 443 1900 1900, 5353 80,443	HTTP、HTTPS SSDP、Bonjour	必須
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS、DTLS (UDPおよびTCP)	WebRTC規格に準拠オプション(デフォルトではオフに設定)
E	ピアツーピア (P2P)	49152-65535	DTLS (UDPおよびTCP)	

AXIS Device Manager Extend (ローカルおよびリモートアクセス、VPN接続を使用)

- 1 Axis
- 2 IAM (My Axis)
- 3 組織データ
- 4 ローカルクライアント
- 5 エッジホスト
- 6 装置
- 7 VMS
- 8 TURN
- 9 信号伝達
- 10 リモートクライアント
- 11 リモートアクセスWebRTCサーバー
- 12 サイト1
- 13 サイト2
- 14 サイト3

接続	URLとIP	ポート	プロトコル	コメント
A	prod.adm.connect.axis.com (52.224.128.152または40.127.155.231)	443	HTTPS	必須

# AXIS Device Manager Extend

## ソリューションの概要

B	HTTP検出 (クライアントからエッジホストへ) データ転送 (クライアントとエッジホストの間) マルチキャスト検出 (クライアントからエッジホストへ) マルチキャスト検出 (エッジホストからクライアントへ)	37080 37443 6801 6801	HTTP HTTPS UDP UDP	サイトをプロビジョニングする必要があります。プロビジョニング後はオプションです。
C	データ転送 (エッジホストと装置の間) ユニキャスト検出 マルチキャスト検出 HTTP検出	80 / カスタムポート、 443 1900 1900, 5353 80,443	HTTP、HTTPS SSDP、Bonjour	必須
D	signaling.prod.webrtc.connect.axis.com *.turn.prod.webrtc.connect.axis.com	443 443, 5349	HTTPS HTTPS、DTLS (UDPおよびTCP)	WebRTC規格に準拠オプション (デフォルトではオフに設定)
E	ピアツーピア (P2P)	49152-65535	DTLS (UDPおよびTCP)	

- 追加の要件は、Google DNSなどのパブリックDNSです。8.8.8.8/8.8.4.4またはCloudflare DNS: 1.1.1.1
- AXIS Device Manager Extendシステムの全機能をサポートするには、AとCの両方の接続が必要です。
- アプリケーションは現在開発中です。そのため、ファイアウォールの設定でAXIS Device Manager Extendデスクトップアプリおよび任意のエッジホストに対して送信ネットワーク接続を許可してください。

# AXIS Device Manager Extend

## 前提条件

---

### 前提条件

#### 互換性のあるオペレーティングシステム:

- Windows 10 ProおよびEnterprise
- Windows 11 ProおよびEnterprise
- Windows Server 2016、2019、および2022 (x64ベースのシステム)
- システム管理者権限は、インストールと設定の変更に必要です。

#### 推奨される最小システム:

- CPU: Intel Core i5
- RAM: 4 GB
- ネットワーク: 100 Mbps

#### インターネット接続。

##### 注

AXIS Device Manager Extendアプリケーションは、インストールで使用されるMy Axisアカウントで作成され、関連付けられた組織に属すると識別される証明書でインターネット接続がプロビジョニングされる必要があります。ただし、保証情報やマルチサイトサポートなどの特定の機能を利用するには、インターネット接続が必要です。また、クライアントやサイトコントローラーは、オンラインモードでのみ自動的に更新されます。

#### 日付と時刻の同期について

##### 注

すべてのシステムコンポーネントが同期されている必要があります。そうでない場合は、エッジホストとクライアントまたはバックエンド間の証明書認証が失敗する可能性があります。すべてのホストマシンを共通のネットワークタイムサーバーに同期して、潜在的な問題を避けることをお勧めします。

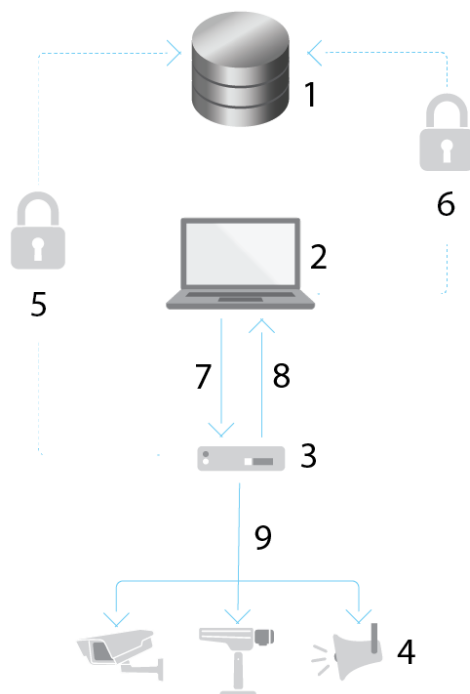
#### ネットワークポートを開く:

AXIS Device Manager Extendデスクトップアプリからエッジホストへの安全な接続、エッジホスト検出、Axisリモートサービス。

# AXIS Device Manager Extend

## 前提条件

---



- 1 Axisサービスプラットフォーム
- 2 AXIS Device Manager Extendデスクトップアプリ
- 3 エッジホスト
- 4 装置
- 5 HTTPS (ポート443)
- 6 HTTPS (ポート443)
- 7 HTTPS (ポート37443)、UDPマルチキャスト検出 (ポート6801)、HTTP検出 (ポート37080)
- 8 UDPマルチキャスト検出 (ポート6801)
- 9 HTTPSおよびHTTP (ポート443および80)、マルチキャスト検出 —SSDP (ポート1900) — Bonjour (ポート5353)、ユニキャスト検出 (ポート1900)、HTTP検出 (ポート80および443)

### 送信ネットワークアクセス

アプリケーションは現在開発中です。そのため、ファイアウォールの設定でAXIS Device Manager Extendデスクトップアプリおよび任意のエッジホストに対して送信ネットワーク接続を許可してください。



# AXIS Device Manager Extend

## はじめに

---

### はじめに



このビデオを見るには、このドキュメントのWebバージョンにアクセスしてください。

[help.axis.com/?&piald=63389&section=get-started](https://help.axis.com/?&piald=63389&section=get-started)


ソフトウェアのインストール、組織の作成、装置の追加

## My Axisアカウントを登録する

[axis.com/my-axis/login](https://axis.com/my-axis/login)でMy Axisアカウントを登録します。

多要素認証 (MFA) をアクティブにすることで、My Axisアカウントの安全性を高くすることができます。MFAは、ユーザーの身元を確認するために別の確認レイヤーを追加するセキュリティシステムです。

MFAをアクティブにする

1. My Axisの認証情報を使用してログインします。
2.  に移動し、[Account settings (アカウント設定)] を選択します。
3. [Security settings (セキュリティ設定)] をクリックします。
4. 2段階認証をオンにします。

ログインページにリダイレクトされます。

5. My Axisの認証情報を使用してログインします。

MFAがアクティブになりました。

以下の方法でMFAがアクティブな場合にログインします。

1. My Axisアカウントにログインします。

メールが送信されます。

2. 電子メールを開き、[Authenticate (認証)] をクリックします。

電子メールを受信しなかった場合は、迷惑メールフォルダー内にあるかどうかを確認してください。そこに電子メールがない場合は、ITサポートにお問い合わせください。

## クライアントをインストールしてアカウントをアクティブにする

[axis.com](https://axis.com)で製品ページに移動し、AXIS Device Manager Extendデスクトップアプリインストーラーをダウンロードします。

1. アプリケーションをダウンロードした場所を特定し、クリックしてインストールします。

# AXIS Device Manager Extend

## はじめに

---

2. クライアントを選択し、[Install (インストール)] をクリックします。
3. お使いのMy Axisアカウントでサインインします。
4. アクティベーションを完了するには、電子メールアドレスを確認します。
5. 組織を作成するか既存の組織に参加します。

## エッジホストの設置

エッジホストとデスクトップクライアントが、AXIS Device Manager Extendインストーラーに含まれています。サイトコントローラーは、可能な限り装置の近くのサーバーにインストールすることをお勧めします。

1. エッジホストをインストールするサーバーを選択します。
2. サーバーでインストーラーを実行し、エッジホストのインストールのみを選択します。

## エッジホストの申し立て

AXIS Device Manager Extendデスクトップアプリから装置への安全な接続を作成するには、まずエッジホストを組織に申し立てする必要があります。

1. ステータスが [Unclaimed (未請求)] のエッジホストをクリックします。
  - 1.1 リストにエッジホストがない場合は、[Add new edge host (新規エッジホストを追加)] をクリックします。
  - 1.2 エッジホストが設置されている場所のIPアドレスを入力します
2. エッジホストの名前を入力する
3. オプションの説明を追加する (推奨)
4. [Claim edge host (エッジホストの申し立て)] をクリックします

# AXIS Device Manager Extend

## 装置の管理

---

### 装置の管理

#### 検出された装置をエッジホストに追加する

1. [Edge hosts (エッジホスト)] に移動します。
2. 装置を追加する申し立て先エッジホストをリストで選択します。
3. [Devices (装置)] > [Discovered (検出済み)] に移動します。
4. 追加する装置を選択するか、選択列の一番上にあるボックスにチェックを入れてすべての装置を選択します。
5. [Add devices to edge host (装置をエッジホストに追加)] をクリックします。

装置が [Managed (マネージド)] タブに表示され、そのステータスを [Edge host overview (エッジホストの概要)] で確認できます。

#### IPアドレスからの装置の追加

サブネット、個々のIPアドレス、またはIP範囲から自動的に検出されない装置を追加します。

#### IPアドレス範囲から装置を追加する

1. 組織が申し立てしたエッジホストに移動します。
2. [Settings > Device discovery (設定 > 装置検出)] に移動します。
3. [Add by IP (IPで追加)] をクリックします。
4. [Manual entry (手動エントリ)] を選択します。
5. IP範囲を入力します。
6. [Add IP addresses (IPアドレスを追加する)] をクリックします。
7. [Devices (装置)] > [Discovered (検出済み)] に移動します。
8. 追加する装置を選択するか、選択列の一番上にあるボックスにチェックを入れてすべての装置を選択します。
9. [Add devices (装置の追加)] をクリックします。

#### ファイルから装置を追加する

1. 組織が申し立てしたエッジホストに移動します。
2. [Settings > Device discovery (設定 > 装置検出)] に移動します。
3. [Add by IP (IPで追加)] をクリックします。
4. [Import from file (ファイルからインポート)] を選択します。
5. IPアドレスを含むカンマ区切り (.CSV) ファイルを選択します。
6. [Import (インポート)] をクリックします。
7. [Devices (装置)] > [Discovered devices (検出された装置)] に移動します。
8. 追加する装置を選択するか、選択列の一番上にあるボックスにチェックを入れてすべての装置を選択します。

# AXIS Device Manager Extend

## 装置の管理

---

9. [Add devices (装置の追加)] をクリックします。

### 注

ファイルには次の情報が必要です。  
IPアドレスの列のヘッダー。  
1つの列。  
最大25,600のIPアドレス。

## 製品を削除する



エッジホストからの装置の削除

1. [Edge host (エッジホスト)] をクリックします。
2. エッジホストを選択します。
3. [Devices (装置)] に移動します。
4. 追加する装置を選択するか、選択列の一番上にあるボックスにチェックを入れてすべての装置を選択します。
5. アクションメニューの [Remove devices from edge host (エッジホストから装置を削除)] アイコンをクリックします。
6. [Remove (削除)] をクリックします。

削除された装置は [Devices (装置)] > [Discovered (検出済み)] で見つけることができます。

## 装置にログインします。

1. [Edge hosts (エッジホスト)] をクリックします。
2. エッジホストを選択します。
3. [Devices > Managed (装置 > マネージド)] に移動します。
4. アクセスする装置を選択するか、選択列の一番上にあるボックスにチェックを入れてすべての装置を選択します。
5. [Log in (ログイン)] をクリックすると、複数の装置に自動的にログインします。
6. ユーザー名とパスワードを入力します。
7. [Log in (ログイン)] をクリックします。

# AXIS Device Manager Extend

## 装置の管理

---

注

ユーザー名とパスワードが正しい場合、[Status (ステータス)] に [Reachable (到達可能)] と表示されます。

# AXIS Device Manager Extend

## 設定

### 設定

#### リモートアクセスのアクティブ化

ファイアウォール設定でアウトバウンド接続がブロックされている場合、サイトにリモートでアクセスするにはプロキシ接続を入力する必要があります。

1. リモートアクセスをアクティブにするエッジホストを選択します。
2. [Settings > Edge hosts connections (設定 > Edge ホスト 接続)] に移動します。
3. [Allow remote access to edge host (エッジホストへのリモートアクセスを許可する)] をアクティブにします。
4. インターネットにアクセスするためにプロキシアドレスを入力する必要がある場合は、[Proxy address (プロキシアドレス)] でそのアドレスを入力します。

接続がアクティブな場合、通知が表示されます。

#### 注

他のネットワーク上のエッジホストへの接続に対応する場合は、自社のネットワークファイアウォールの「許可リスト」に次の設定を追加する必要があります。エンドポイントポートプロトコル signaling.prod.webrtc.connect.axis.com 443 HTTPS \*.turn.prod.webrtc.connect.axis.com 443 HTTPS webRTC (TurnおよびP2P) 5349、49152 - 65535 DTLS (UDPおよびTCP)

#### サイトを削除する

組織からエッジホストを削除する前に、エッジホストに *12ページ製品を削除する* を削除する必要があります。その後、この装置は [Devices > Discovered (装置 > 検出済み)] で見つけることができます。

1. [Edge hosts (エッジホスト)] をクリックします。
2. 矢印キーを使用してエッジホストを選択するか、マウスポインターでサイトにポインターを合わせます。
3. [...] をクリックし、ドロップダウンメニューから [Remove edge host (エッジホストを削除)] を選択します。
4. [I'm aware of the risks. (リスクは承知している)] にチェックを入れます。
5. [Remove (削除)] をクリックします。

#### ユーザーを組織に追加する

1. ユーザー設定を行う組織を選択します。
2. [Users (ユーザー)] に移動します。
3. [Invite to organization (組織に招待)] をクリックします。
4. 組織に招待するユーザーの電子メールアドレスを入力します。
5. [Send invite (招待を送信)] をクリックします。

#### 注

ユーザーは、AXIS Device Manager Extendへのサインイン時に使用できる招待状電子メールを受け取ります。デフォルトのユーザー権限は [Viewer (閲覧者)] です。My Axisアカウントを持ってないユーザーは、その電子メールを使用して組織にアクセスする必要があります。受け入れの保留中に、招待を取り消すことができます。

### ユーザー権限の昇格

1. ユーザー設定を行う組織を選択します。
2. [Users (ユーザー)] に移動します。
3. 昇格させるユーザーの [Role (役割)] に移動します。
4. ドロップダウンメニューをクリックして新しい役割を選択します。

#### 注

選択すると、すぐに役割が変更されます。セキュリティ上の理由から、招待は閲覧者の役割に限定されます。

### ユーザーの削除

1. ユーザー設定を行う組織を選択します。
2. [Users (ユーザー)] に移動します。
3. 削除するユーザーにマウスポインターを合わせて、新しいオプションメニューを表示します。...
4. ...をクリックし、ドロップダウンメニューから [Remove user (ユーザーの削除)] を選択します。

# AXIS Device Manager Extend

## ファームウェアの管理

---

### ファームウェアの管理

AXIS Device Manager Extendを使用すると、各組織の複数の装置のファームウェアを管理できます。

モデル別にグループ化された組織内のすべての装置で利用可能なファームウェア更新の一覧については、[Home > Firmware inventory (ホーム>ファームウェアインベントリ)]にアクセスしてください。特定のエッジホストで利用可能なファームウェア更新のリストについては、エッジホストを選択し、[Firmware inventory (ファームウェアインベントリ)]に移動します。

### 装置モデルに基づくファームウェアの管理

組織全体のファームウェアを装置モデル別に管理するには:

1. [Home (ホーム)] > [Firmware inventory (ファームウェアインベントリ)]に移動します。
2. 管理するモデルを確認します。
3. [Upgrade to (アップグレード先)] ドロップダウンメニューをクリックして、利用可能なファームウェアを確認します。最新のファームウェアがあらかじめ選択されています。
4. [Upgrade (アップグレード)] をクリックします。

### エッジホストで装置のファームウェアを管理します。

エッジホスト上の一部またはすべての装置のファームウェアを管理するには:

1. [Edge hosts (エッジホスト)] に移動します。
2. アクセスするエッジホストをクリックします。
3. [Devices (装置)] に移動します。
4. 管理するすべてまたは一部の装置を選択します。
5. アクションメニューの [Firmware (ファームウェア)] アイコンをクリックします。
6. リスト内のモデルのすべてまたは一部を確認します。
7. 選択したファームウェアを変更する場合は、推奨されたファームウェアをクリックして、装置ごとに利用可能なファームウェアを確認してください。最新のファームウェアがあらかじめ選択されています。
8. [Upgrade (アップグレード)] をクリックします。

### 進行中および完了したファームウェアアップグレードを表示する

完了したファームウェアアップグレードを確認するには:

1. [Sites (サイト)] に移動します。
2. アクセスするサイトをクリックします。
3. [Tasks (タスク)] に移動します。

進行中のファームウェアアップグレードを確認するには:

4. [Sites (サイト)] に移動します。
5. アクセスするサイトをクリックします。



# AXIS Device Manager Extend

## ファームウェアの管理

---

6. [Tasks>Ongoing tasks (タスク>進行中のタスク)] に移動します。

# AXIS Device Manager Extend

## ポリシー

---

### ポリシー

ポリシーによって装置が自動的に管理されます。サイト全体でサイバーセキュリティを維持するためにポリシーを作成します。装置にアプリを自動的にインストールして更新するようにポリシーを設定することもできます。

### セキュリティポリシーの作成と適用

この使用事例では、基本的なセキュリティポリシーを作成して、エッジホストに接続された特定の数の装置に適用します。

基本的なセキュリティポリシーを作成します。

1. [Edge hosts (エッジホスト)] に移動します。
2. アクセスするエッジホストをクリックします。
3. [Devices (装置)] に移動します。
4. [Policies (ポリシー)] の横にある+アイコンをクリックします。
5. [Basic security (基本セキュリティ)] を選択し、[Continue (続行)] をクリックします。
6. ポリシーに名前を付けます。
7. セキュリティニーズに合った設定を選択します。推奨されるセキュリティレベルについては、デフォルト設定のままにします。
  - 選択した装置のrootパスワードを変更するには、[Device root password (装置のrootパスワード)] をクリックし、新しいrootパスワードを入力します。
8. [Create (作成)] をクリックします。

ポリシーを適用します。

1. ポリシーを適用する装置を選択します。
2. アクションメニューの [Policy options (ポリシーのオプション)] アイコンをクリックします。
3. セキュリティポリシーを選択し、[Save (保存)] をクリックします。

### アプリポリシーの作成と適用

この使用事例では、アプリポリシーを作成して、エッジホストに接続された特定の数の装置に適用します。

1. [Edge hosts (エッジホスト)] に移動します。
2. アクセスするエッジホストをクリックします。
3. [Devices (装置)] に移動します。
4. [Policies (ポリシー)] の横にある+アイコンをクリックします。
5. [Apps (アプリ)] を選択し、[Continue (続行)] をクリックします。
6. ポリシーに名前を付けます。
7. 装置にインストールして更新するアプリを選択します。
8. ドロップダウンメニューから更新ウィンドウを選択します。
9. [Create (作成)] をクリックします。

# AXIS Device Manager Extend

## ポリシー

---

ポリシーを適用します。

1. ポリシーを適用する装置を選択します。
2. アクションメニューの **[Policy options (ポリシーのオプション)]** アイコンをクリックします。
3. 適用するアプリポリシーを選択します。
4. **[Save (保存)]** をクリックします。

### 注

選択したアプリは、削除されると自動的に再インストールされます。

## ポリシーの編集

既存のポリシーを編集するには:

1. **[Edge hosts (エッジホスト)]** に移動します。
2. アクセスするエッジホストをクリックします。
3. **[Devices (装置)]** に移動します。
4. 編集するポリシーの横にある [...] をクリックし、ドロップダウンメニューから **[Edit policy (ポリシーの編集)]** をクリックします。
5. ニーズに合わせてポリシー設定を編集します。
6. **[Save (保存)]** をクリックします。

## ポリシーの削除

既存のポリシーを削除するには:

- **[Edge hosts (エッジホスト)]** に移動します。
- アクセスするエッジホストをクリックします。
- **[Devices (装置)]** に移動します。
- 編集するポリシーの横にある [...] をクリックし、ドロップダウンメニューから **[Delete policy (ポリシーの削除)]** をクリックします。
- **[Delete (削除)]** をクリックします。

### 注

そのポリシーが適用されている装置は、ポリシーの設定を保持しますが、設定は永続的ではなくなります。

# AXIS Device Manager Extend

## トラブルシューティング

---

### トラブルシューティング

#### ファイアウォールの設定方法

AXIS Device Manager Extendクライアントにはaxis.comドメインとそのサブドメインへのアクセス権が必要です。

AXIS Device Manager ExtendエッジホストがAxisサービスと通信するには、次のIPアドレスとポートを組織のファイアウォールの許可リストに追加する必要があります。

- 40.127.155.231 (EU)、ポート443
- 52.224.128.152および40.127.155.231 (米国)、ポート443
- パブリックDNSサーバーIP、ポート53

または、ファイアウォール設定でprod.adm.connect.axis.comドメイン (上記のIPアドレスを指すDNS Aレコード) を使用することもできます。

AXIS Device Manager Extendエッジホストはすべての送信リクエストにprod.adm.connect.axis.comドメイン名を使用します。

この方法では、ネットワークでパブリックDNSサーバーを使用し、DNSサーバーIPアドレス (およびデフォルトのポート53) へのトラフィックを許可する必要があります。

