AXIS Device Manager Extend

ユーザーマニュアル

目次

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デバイスを検出、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

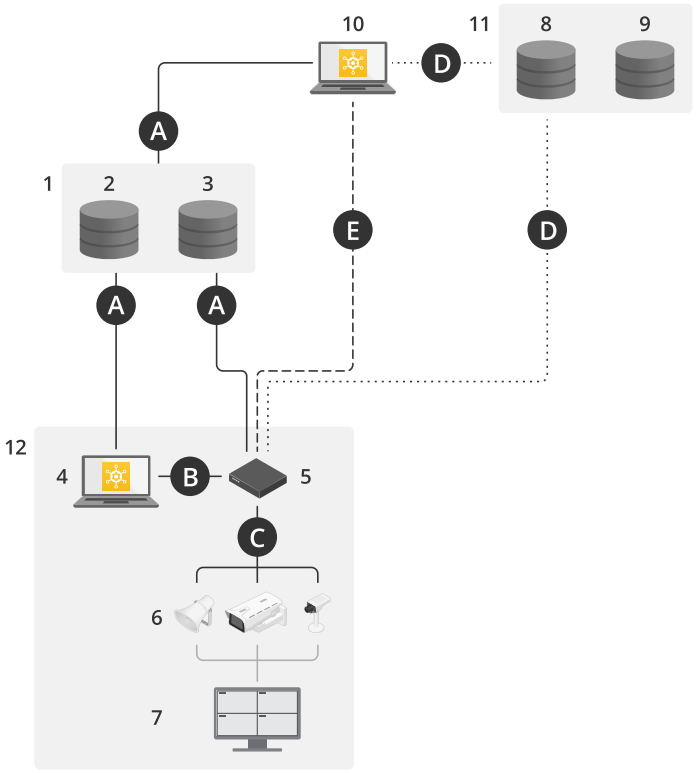
AXIS Device Manager Extendのエッジホストコンポーネントは、常に利用可能なオンプレミスの管理サービスで、カメラなどのローカル装置のメンテナンスを担当します。AXIS Device Manager Extendはエッジホスト、Axisリモート管理サービスへのリンクとして機能し、同じAPI機能が、Axisサービスプラットフォームを介したサイトのリモート管理をサポートします。

組織について

組織は、Axisシステムインストールの仮想表現であり、クラウドサービスの中心に位置しています。組織は、アクセスを規制し、最大限のセキュリティを確保する階層構造で、会社内のすべての装置とユーザーアカウントをホストします。同時に組織により、大企業だけでなく中小企業でもユーザーと装置の柔軟な管理が可能になります。

- 新しい組織を作成すると、その組織の所有者になります。組織はシステムをAxisクラウドサービスのユーザーに接続します。
- ユーザーを組織に招待できます。を参照してください。
- ユーザーにさまざまな役割を割り当てることができます。
- 組織にはデフォルトのフォルダーが含まれており、そこからニーズに合った組織構造の構築を開始できます。組織はフォルダーやサブフォルダーに構造化できます。通常、フォルダーは組織内のシステムの物理的なサイトまたは位置を表します。
- 組織内のシステムのライセンスを管理します。
- 組織を作成するには、My Axisアカウントが必要です。

ソリューションの概要

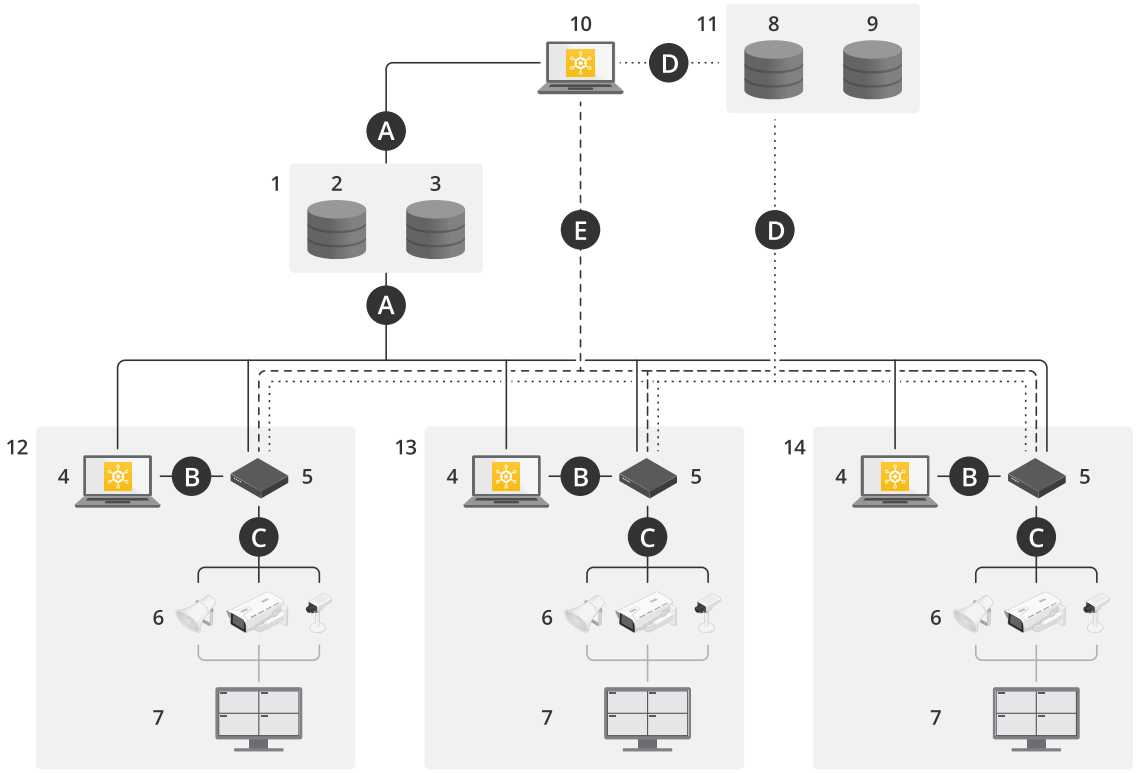


AXIS Device Manager Extend (ローカルおよびリモートアクセスを使用)

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 *デバイス*
7 *VMS*
8 *TURN*
9 *シグナリング*
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*

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	サイトのプロビジョニングに必要。プロビジョニング後は任意。

C	データ転送 (エッジホストとデバイス間) ユニキャスト検出 Multicast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	Peer to Peer (P2P)	49152-65535	DTLS (UDPおよびTCP)	

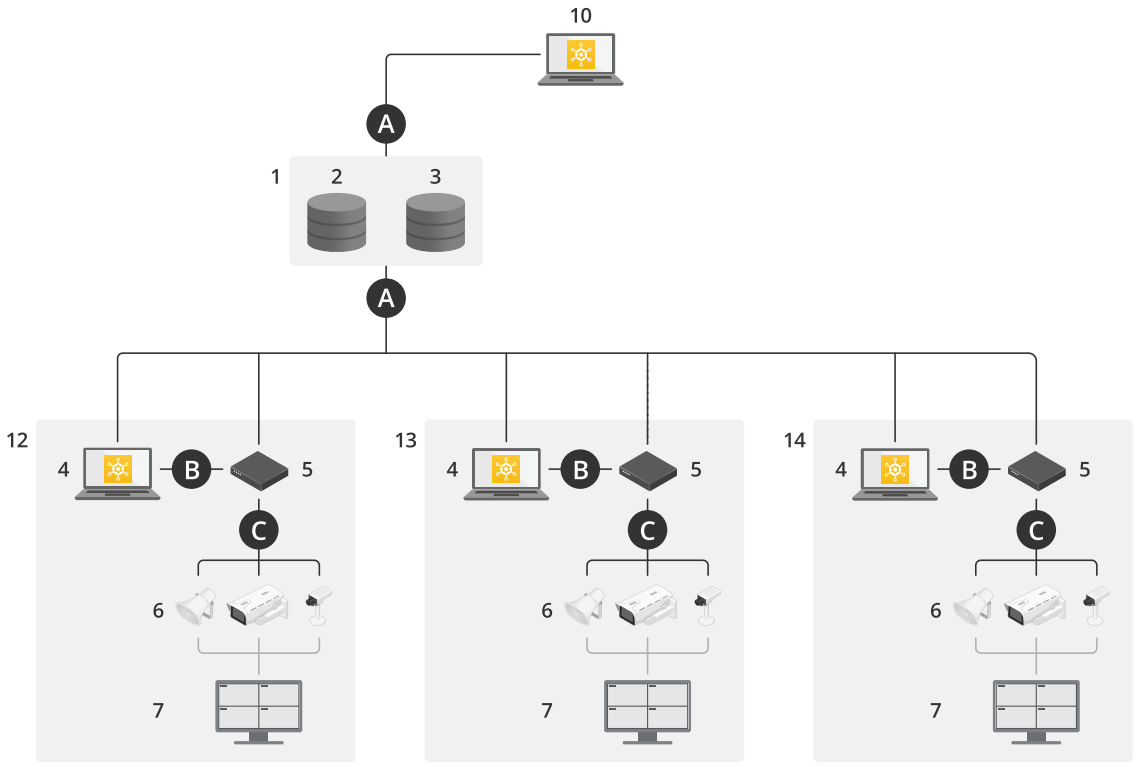


AXIS Device Manager Extend (ローカルおよびリモートアクセス、マルチサイト設定を使用)

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 *デバイス*
7 *VMS*
8 *TURN*
9 *シグナリング*
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	サイトのプロビジョニングに必要。プロビジョニング後は任意。
C	データ転送 (エッジホストとデバイス間) ユニキャスト検出 Multicast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	Peer to Peer (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 デバイス
7 VMS
8 TURN
9 シグナリング
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	サイトのプロビジョニングに必要。プロビジョニング後は任意。

C	データ転送 (エッジホストとデバイス間) ユニキャスト検出 Multicast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	Peer to Peer (P2P)	49152-65535	DTLS (UDPおよびTCP)	

- 追加要件として、Google DNS: 8.8.8.8 / 8.8.4.4またはCloudflare DNS: 1.1.1.1などのパブリックDNSが必要です。
- 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。

要件

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。

最小システム推奨:

- 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、クライアントやエッジホストは、オンラインモードでのみ自動的に更新されます。

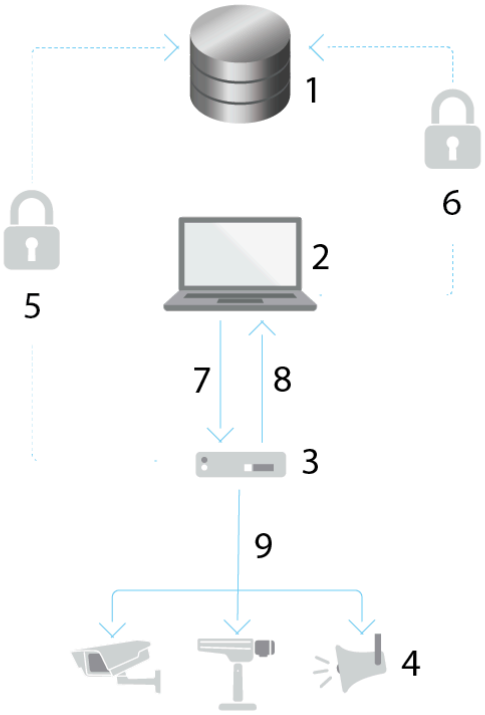
日付と時刻の同期について

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。



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 *デバイス*
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。

使用に当たって

My Axisアカウントを登録する

1. *axis.com/my-axis/login*で**My Axis**アカウントを登録します。
2. 多要素認証 (MFA) 方法として**認証アプリ (TOTP)** または**Eメール**のいずれか1つを選択し、画面に表示される指示に従います。MFAは、ユーザーの本人確認のためのさらなるレイヤーを追加するセキュリティシステムです。

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の製品ページにアクセスし、Axisデバイス管理クライアント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。
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。

組織の作成

装置をシステムに追加するには、組織のメンバーである必要があります。これは、1つ以上の施設で装置を安全に管理、保護するためです。組織のメンバーではない場合は、セットアップアシスタントがポップアップ表示され、プロセスを案内します。

組織を作成する:

1. My Axisアカウントでサインインします。
2. セットアップアシスタントの指示に従います。

追加の組織を作成する:

- 組織名のドロップダウンメニューに移動します。
- **[+ Create new organization (+新しい組織の作成)]** を選択します
- セットアップアシスタントの指示に従います。

エッジホストをインストールする

axis.comの製品ページにアクセスし、エッジホスト (Axis Device Management Server) をダウンロードします。。

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。エッジホストは、可能な限りデバイス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。
2. このサーバー上でインストーラーを実行します。

エッジホストの申し立て

Axisのデバイス管理クライアントからデバイスへの安全な接続を作成するには、まず組織に対してエッジホストの申し立てを行う必要があります。

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

デバイスの管理

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. 追加するデバイスを選択するか、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デバイスを選択します。
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アドレスからデバイスを追加

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. 追加するデバイスを選択するか、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デバイスを選択します。
9. **Add devices (デバイスを追加)** 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. 追加するデバイスを選択するか、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デバイスを選択します。
9. **Add devices (デバイスを追加)** 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

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. **[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。

デバイスにログインします。

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. アクセスするデバイスを選択するか、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デバイスを選択します。
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。

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。

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をサポートするためには、企業ネットワークの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る場合があります。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 and P2P) 5349, 49152 - 65535 DTLS (UDP and 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. [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. My Systemsパネルに移動します。
3. [ORGANIZATION (組織)] > [Users (ユーザー)] に移動します。
4. [Invite users (ユーザーの招待)] をクリックします。
5. 設定アシスタントの画面に表示される手順に従います。
   - **オペレーター**または**閲覧者**を選択した場合、そのユーザーがアクセスできるフォルダーを選択します。**管理者**ロールは、組織内のすべてのフォルダーにアクセスできることに注意してください。

注

ユーザーは、My Systems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。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。招待は、承認が保留されている間でも取り消すことができます。

ユーザーロールについて

ユーザーロールは、ユーザーが組織内のシステムでアクセスできる範囲を定義します。使用できる機能は、ユーザーロールにより異なります。

管理者

管理者はシステム全体にアクセスできます。制御権には、ユーザーや装置、ライセンス、ビデオ、その他のコンテンツの管理権限が含まれます。

また、AXIS Camera Station Proを使用して装置をオンボードすることもできます。管理者は、My Systems内でAXIS Camera Station Pro Server Monitoringを管理できます。

オペレーター

オペレーターは、ライブビデオフィードの監視と装置の制御を実行でき、再生のために録画にアクセスできます。組織のユーザーと各ロールの概要を閲覧できます。またオペレーターは、My Systems内でAXIS Camera Station Pro Server Monitoringを管理できます。

ビューワー

閲覧者はライブビデオフィードを監視できますが、装置を制御する権限、および録画へアクセスする権限はありません。組織のユーザーと各ロールの概要を閲覧できます。

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. My Systemsパネルに移動します。
3. [ORGANIZATION (組織)] から [Users (ユーザー)] に移動します。
4. 昇格させるユーザーをクリックし、[Roles and access (役割とアクセス)] をクリックします。
5. 設定アシスタントの画面に表示される手順に従います。

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. My Systemsパネルに移動します。
3. [ORGANIZATION (組織)] から [Users (ユーザー)] に移動します。
4. 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の...を表示します。
5. ...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。

複数のユーザーの削除

1. 削除するユーザーを選択します。
2. アクションメニューのゴミ箱をクリックします。
3. **[削除]** をクリックします。

AXIS OSの管理

Axisのデバイス管理クライアントを使用すると、各組織内の複数のデバイスのオペレーティングシステムを管理できます。

組織内のすべての装置で使用可能なAXIS OS更新のリストをモデル別に表示するには、[Home (ホーム)] > [AXIS OS inventory (AXIS OSインベントリ)] に移動します。特定のエッジホストで利用可能なAXIS OSアップデートのリストは、エッジホストを選択して [AXIS OS inventory (AXIS OSインベントリ)] に移動します。

モデルに基づくAXIS OSバージョンの管理

組織全体でAXIS OSをモデル別に管理する:

1. [Home > AXIS OS versions (ホーム > AXIS OSバージョン)] に移動します
2. 推奨のAXIS OSバージョンのリンクをクリックします。AXIS OSアップグレードオプションが開きます。
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AXIS OSバージョンがあらかじめ選択されます。
4. [Upgrade (アップグレード)] をクリックします。

エッジホスト上のAXIS OSを管理します。

エッジホストに追加された装置の一部またはすべてのAXIS OSを管理する:

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 [AXIS OS] 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. AXIS OSバージョンを変更する場合は、推奨されたバージョンをクリックして、装置ごとに利用可能なバージョンを確認してください。最新のAXIS OSバージョンがあらかじめ選択されます。
8. [アップグレード] をクリックします。

現在進行中および完了したAXIS OSアップグレードの表示

特定のエッジホストに接続された装置の進行中のソフトウェアアップグレードを表示する:

1. [Edge hosts (エッジホスト)] をクリックします。
2. アクセスするエッジホストをクリックします。
3. [Log (ログ)] に移動します

進行中のソフトウェアアップグレードを確認する:

4. [Log (ログ)] > [Ongoing tasks (進行中のタスク)] に移動します

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。

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. [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。

ライセンスを管理

製品のライセンス

製品のライセンスを取得するには、*[My Systems]> [Licenses (ライセンス)]* に移動します。Axisの製品とサービスのライセンスの詳細については、*My Systems*ユーザーマニュアルを参照してください。

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のデバイス管理クライアントには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。

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。

このエッジホストは、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。

注

ポート設定の詳細については、AXIS Device Manager Extendのホワイトペーパーを参照してください：*一般的なシステム設定*。

T10153497_ja

2025-10 (M22.2)