AXIS Device Manager

ユーザーマニュアル

はじめに

サイバーセキュリティの重要性は監視とセキュリティの分野でますます大きくなっています。効果的なサイバーセキュリティを実現するには、製品やパートナーの選択からお客様とパートナーの双方が設定する要件に至るまで、あらゆるレベルでIPネットワークを適切に保護するために十分な深さのある防御を確保する必要があります。

このガイドでは、AXIS Device Managerを使用してシステムを強化し、セキュリティを高める方法について説明します。本書は主要な側面に焦点を合わせると同時に、推奨事項を示しています。

デバイスのライフサイクル管理

Axisは、デバイスのライフサイクル全体を通して強固なセキュリティ基盤を構築することの重要性を理解しています。サイバーセキュリティに対する当社のコミットメントは、当社の製品とソリューションが潜在的な脅威に対する強力な保護を提供することを保証するものです。

実装

Axisは、セキュアブートメカニズムや署名付きオペレーティングシステム、暗号化ストレージなどのセキュリティ機能を内蔵した、セキュアバイデザインのデバイスを提供しています。さらに、AXIS Device Managerが設置担当者やシステム管理者がデバイスを安全に設定・導入できるよう支援するため、最初からセキュリティで保護されたセットアップを実現することができます。

アクティブなサービス

運用段階中は、Axisは定期的にデバイスソフトウェアアップデートとセキュリティパッチを提供し、脆弱性に対する保護を提供します。さらに、AXIS Device Managerを使用すればリモート監視とメンテナンスが可能になるため、問題を迅速に解決し、ダウンタイムを最小化することができます。さらに、Axisの強化ガイドでは、具体的なセキュリティ要件を満たせるようにデバイスを設定するための推奨事項を提供しています。

運用停止

デバイスの廃棄や交換の際には、AXIS Device Managerを使用して機密データを消去し、デバイスを工場出荷時の設定に復元できるため、容易かつ安全にデバイスを運用停止することができます。デバイスには機密情報が残らず、ユーザーデータを保護し、不正アクセスを防ぐことができます。

AXIS Device Manager

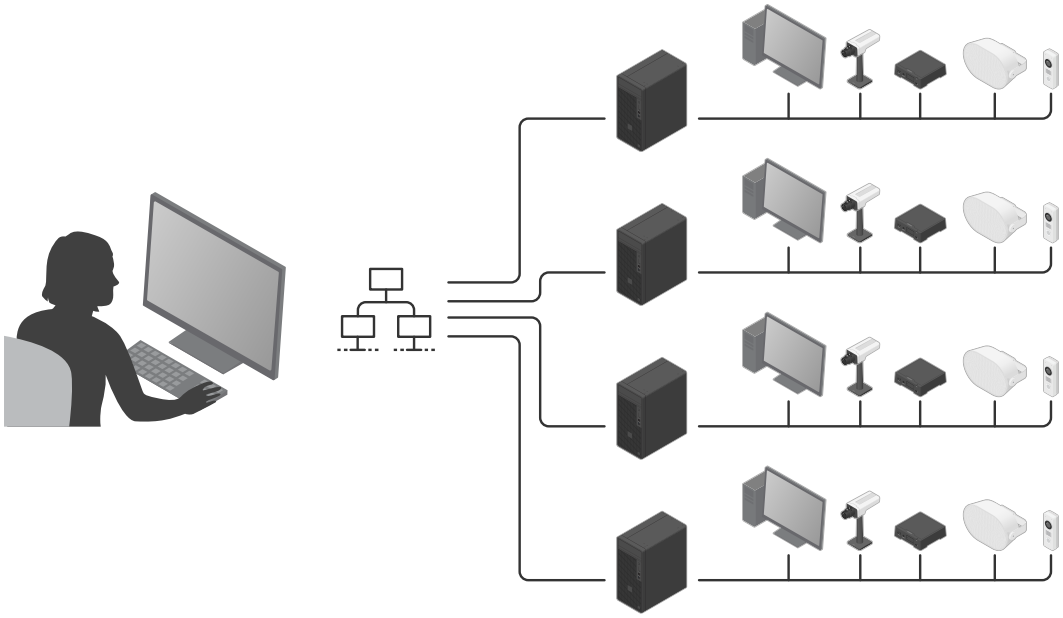
AXIS Device Managerは、設置、セキュリティ、メンテナンスといった主要なデバイス管理タスク(下図を参照) をすべて管理するための容易でコストパフォーマンスが高くサイバーセキュリティに優れた方法を提供するオンプレミスのツールです。このツールは、最大2000台程度のAxisデバイスを単一のサイトで管理する場合や、最大数千台程度のデバイスを複数のサイトに展開する場合に適しています。AXIS Device Managerを使用すると、サイバーセキュリティ制御を効率的に導入してネットワークデバイスを保護し、それらをセキュリティインフラに合わせることができます。

デバイス管理機能、AXIS Device Manager

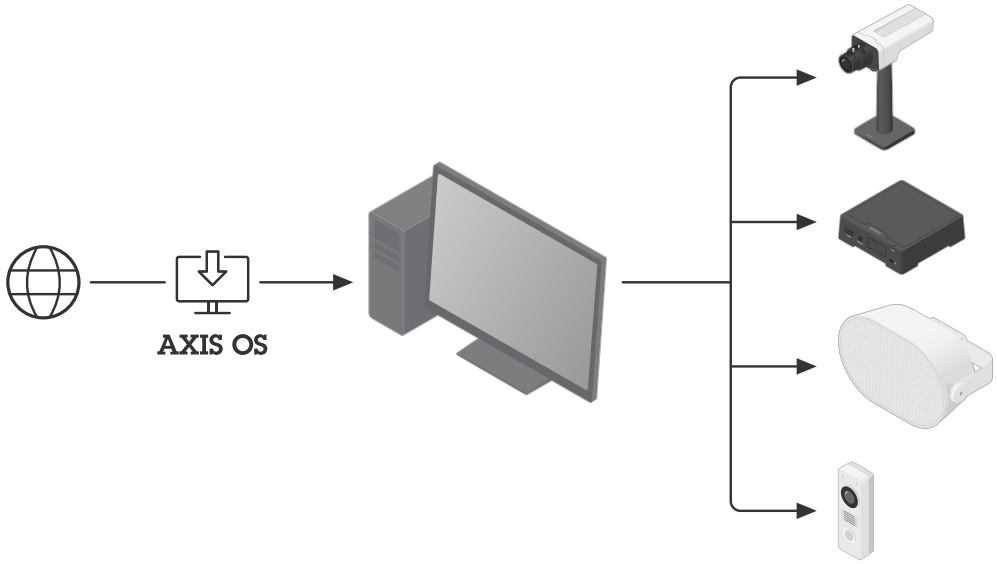
インストール	メンテナンス
IPアドレスの割り当て	装置ステータス
デバイスリストをエクスポートして資産を追跡する*	装置データの収集
ユーザー管理およびパスワード管理*	装置の設定および複数の装置への設定コピー
ACAP管理	複数のサーバー/システムへの接続
LTSまたはActive*に基づくAXIS OSのアップグレード	復元ポイント

HTTPS認証管理*	工場出荷時設定の復元
IEEE 802.1証明書を管理する*/**	デバイスの置換
装置タグ付け	認証の更新および管理*
	サイバーセキュリティの強化*

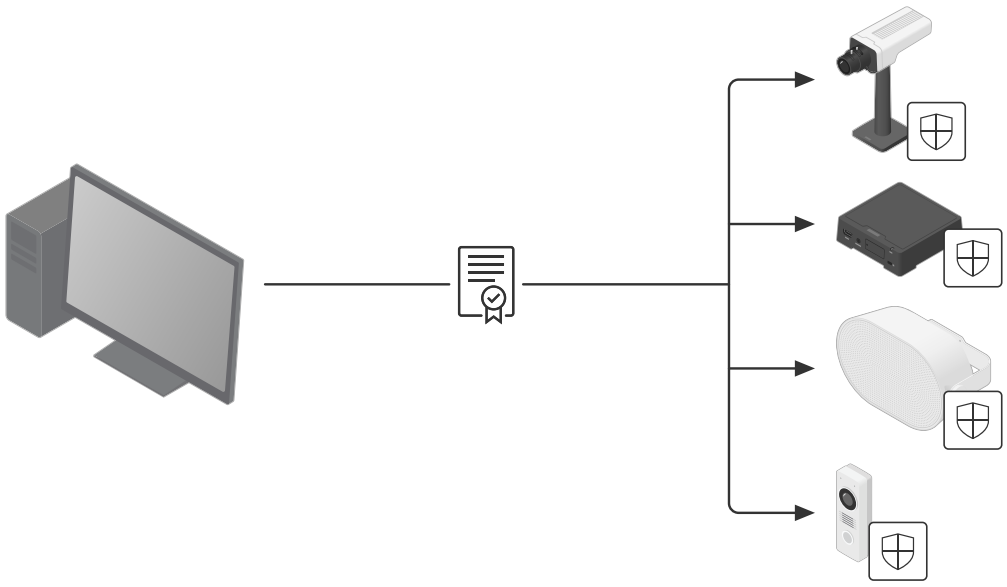
*はサイバーセキュリティ制御に関する機能を示します。
** Active Directory証明書サービスは現在サポートされていません。Linux上で動作するFreeRADIUSで検証済みです。



複数サイトの管理。



AXIS OSのアップグレード。



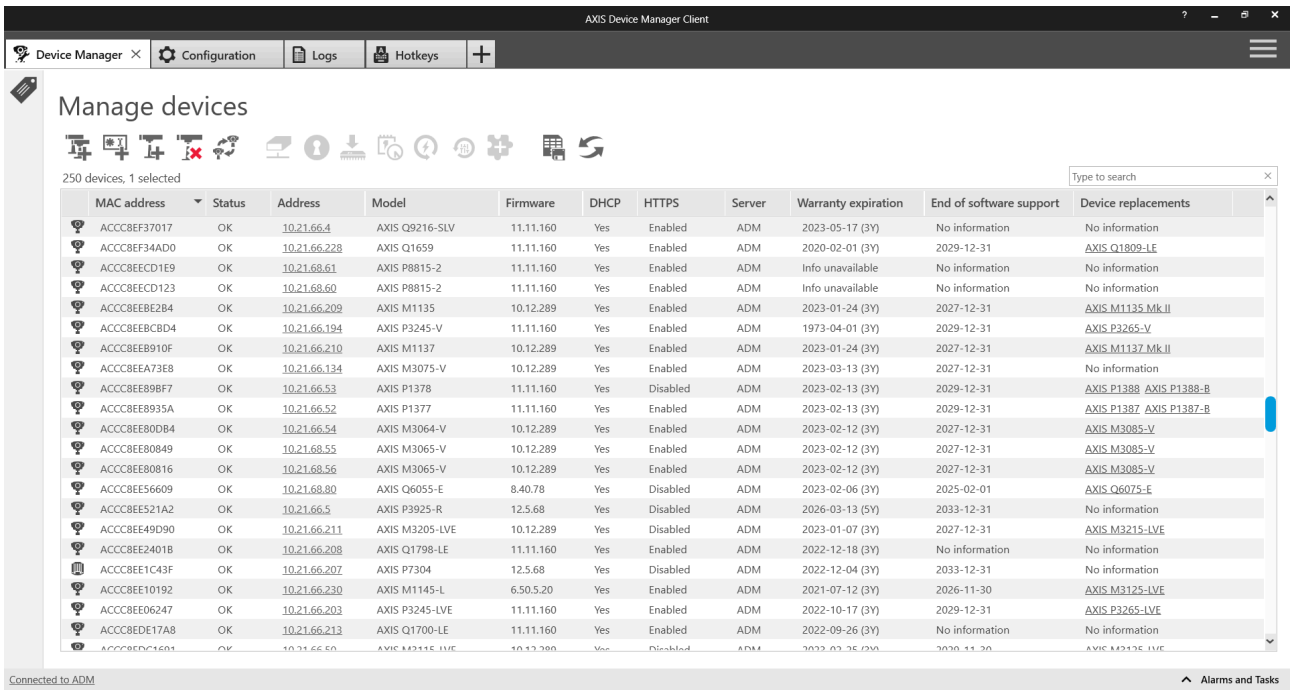
証明書の管理。

デバイスのインベントリ

エンタープライズネットワークのセキュリティ確保における基本的な側面のひとつは、ネットワーク上のデバイスのインベントリを常に完全なものにしておくことです。全体的なセキュリティポリシーの作成や確認を行う際、重要な資産だけでなく、すべてのデバイスそれぞれに関する知識と明瞭なドキュメントを保持していることが大切です。なぜなら、見落としたデバイスが攻撃者の侵入手段となる可能性があるためです。見落としたデバイスや十分に把握していないデバイスを保護することはできません。

デバイスのインベントリは、企業ネットワークのセキュリティを確保するために不可欠なステップです。AXIS Device Managerは、次のことに役立ちます。

- 監査や事故応答者と共に作業する際に、ネットワークデバイスの現在の完全なインベントリに容易にアクセスできます。
- デバイスの完全なリストを取得し、それらの総数、タイプ、モデル番号などで並べ替えることができます。
- ネットワーク上の各デバイスのステータスを確認できます。
- デバイスのソフトウェアのサポートがいつ終了するかを表示し、どの新しい製品を代替品として使用できるかを一覧表示することで、事前の計画策定に役立ちます。



MAC address	Status	Address	Model	Firmware	DHCP	HTTPS	Server	Warranty expiration	End of software support	Device replacements
ACCC8EF37017	OK	10.21.66.4	AXIS Q9216-SLV	11.11.160	Yes	Enabled	ADM	2023-05-17 (3Y)	No information	No information
ACCC8EF34AD0	OK	10.21.66.228	AXIS Q1659	11.11.160	Yes	Enabled	ADM	2020-02-01 (3Y)	2029-12-31	AXIS Q1809-LE
ACCC8EECD1E9	OK	10.21.68.61	AXIS P8815-2	11.11.160	Yes	Enabled	ADM	Info unavailable	No information	No information
ACCC8EECD123	OK	10.21.68.60	AXIS P8815-2	11.11.160	Yes	Enabled	ADM	Info unavailable	No information	No information
ACCC8EEBE2B4	OK	10.21.66.209	AXIS M1135	10.12.289	Yes	Enabled	ADM	2023-01-24 (3Y)	2027-12-31	AXIS M1135 Mk II
ACCC8EEBCBD4	OK	10.21.66.194	AXIS P3245-V	11.11.160	Yes	Enabled	ADM	1973-04-01 (3Y)	2029-12-31	AXIS P3265-V
ACCC8EEB910F	OK	10.21.66.210	AXIS M1137	10.12.289	Yes	Enabled	ADM	2023-01-24 (3Y)	2027-12-31	AXIS M1137 Mk II
ACCC8EEA73E8	OK	10.21.66.134	AXIS M3075-V	10.12.289	Yes	Enabled	ADM	2023-03-13 (3Y)	2027-12-31	No information
ACCC8EE89BF7	OK	10.21.66.53	AXIS P1378	11.11.160	Yes	Disabled	ADM	2023-02-13 (3Y)	2029-12-31	AXIS P1388 AXIS P1388-B
ACCC8EE8935A	OK	10.21.66.52	AXIS P1377	11.11.160	Yes	Enabled	ADM	2023-02-13 (3Y)	2029-12-31	AXIS P1387 AXIS P1387-B
ACCC8EE80DB4	OK	10.21.66.54	AXIS M3064-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
ACCC8EE80849	OK	10.21.68.55	AXIS M3065-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
ACCC8EE80816	OK	10.21.68.56	AXIS M3065-V	10.12.289	Yes	Enabled	ADM	2023-02-12 (3Y)	2027-12-31	AXIS M3085-V
ACCC8EE56609	OK	10.21.68.80	AXIS Q6055-E	8.40.78	Yes	Disabled	ADM	2023-02-06 (3Y)	2025-02-01	AXIS Q6075-E
ACCC8EE521A2	OK	10.21.66.5	AXIS P3925-R	12.5.68	Yes	Disabled	ADM	2026-03-13 (5Y)	2033-12-31	No information
ACCC8EE49D90	OK	10.21.66.211	AXIS M3205-LVE	10.12.289	Yes	Disabled	ADM	2023-01-07 (3Y)	2027-12-31	AXIS M3215-LVE
ACCC8EE2401B	OK	10.21.66.208	AXIS Q1798-LE	11.11.160	Yes	Enabled	ADM	2022-12-18 (3Y)	No information	No information
ACCC8EE1C43F	OK	10.21.66.207	AXIS P7304	12.5.68	Yes	Disabled	ADM	2022-12-04 (3Y)	2033-12-31	No information
ACCC8EE10192	OK	10.21.66.230	AXIS M1145-L	6.50.5.20	Yes	Enabled	ADM	2021-07-12 (3Y)	2026-11-30	AXIS M3125-LVE
ACCC8EE06247	OK	10.21.66.203	AXIS P3245-LVE	11.11.160	Yes	Enabled	ADM	2022-10-17 (3Y)	2029-12-31	AXIS P3265-LVE
ACCC8EDE17A8	OK	10.21.66.213	AXIS Q1700-LE	11.11.160	Yes	Enabled	ADM	2022-09-26 (3Y)	No information	No information

AXIS Device Managerではデバイスのインベントリが分かりやすく表示されます。

AXIS Device Managerには、Axisネットワークデバイスのリアルタイムのインベントリに自動的にアクセスする手段が備わっています。デバイスを自動的に識別し、リストを表示して並べ替えることができます。同様に重要な点として、タグを使用してお客様自身の基準に基づいてデバイスをグループ化し、並べ替えることができるため、ネットワーク上のすべてのAxisデバイスの全体像を容易に把握し、文書化することができます。

アカウントとパスワードに関するポリシー

認証と権限の制御は、ネットワークリソースの保護において重要な部分です。ポリシーを実装することは、意図しない誤用や意図的な悪用のリスクを長期的に減らすことに役立ちます。堅牢性の高いパスワードの使用を徹底することは重要なことですが、パスワードが漏洩するリスクを減らすことも重要です。デバイスのパスワードは組織内で広まることがよくあります。そうなると、デバイスに誰がアクセスできるかに対する管理ができなくなります。AXISデバイスマネージャーを使用すれば、Axisデバイスの複数のアカウントとパスワードを容易に管理することができます。

デバイス内で複数のユーザーアカウントを持つ必要がある理由：

- 異なるユーザータイプ (機械と人間) の権限レベルを制御できる。
- root (マスター) パスワードが漏洩するリスクを減らすことができる。
- あるユーザータイプの認証情報を、他に影響を与えずにリセットできる。

AXIS Device Managerにおける権限の処理

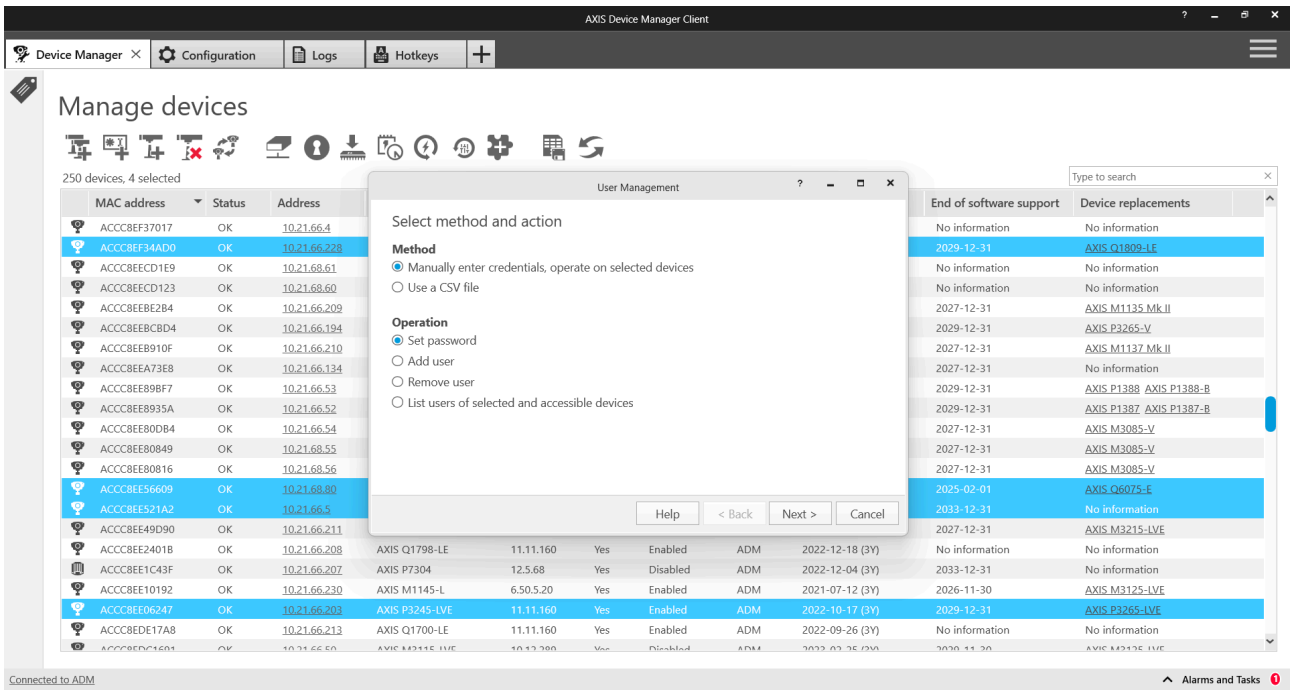
Axisデバイスは複数のアカウントをサポートしており、各アカウントには次の3種類の権限レベルのいずれかがあります。

- **Viewers (閲覧者)**:このタイプのユーザーは、ビデオとPTZ制御にアクセスできます。
- **Operators (オペレーター)**:オペレーター権限を持つユーザーは、カメラの設定とビデオストリームプロファイルを最適化できます。
- **Administrators (管理者)**:管理者は、アカウントの管理、ネットワーク設定の変更、デバイス内の複数のサービスの制御を行うことができます。

カメラにアクセスする権限ごとに独自のアカウントが必要です。例えば、「制御室担当者」という役割には特権レベル「Operators (オペレーター)」を設定するかもしれませんし、「パトロール担当者」という役割には特権レベル「Viewers (閲覧者)」しか必要でないかもしれません。

推奨ステップ

- カメラをVMSに追加する前に、AXIS Device Managerに追加しましょう。
- AXIS Device Managerで、すべてのカメラを選択し、「vms」または類似した名前の新しいユーザーアカウントを作成して強力なパスワードを設定します。各権限はVMSの要件に合わせる必要があります。それはオペレーターかもしれませんし、管理者かもしれません (メーカーにお問い合わせください)。
- 作成したアカウントとパスワードを指定して、デバイスをVMSに追加します。
- AXIS Device Managerに戻り、すべてのカメラを再び選択して、「root」アカウントのパスワードを新しい強力なパスワードにリセット (変更) します。「root」アカウントのパスワードは限られた数の個人 (AXIS Device Managerのユーザー) だけが知っている必要があります。
- だれかがメンテナンスまたはトラブルシューティングタスク用にWebブラウザ経由でデバイスにアクセスしなければならない場合に、その人にrootパスワードを**知らせてはなりません**。その代わりに、AXIS Device Managerを使用して、選択したデバイス用に管理者またはオペレーターの権限を持つ新しい (一時的な) アカウントを作成します。タスクが完了したら、AXIS Device Managerを使用してその一時アカウントを削除します。
- AXIS Device Managerでは、ローカル管理者に加えてドメインユーザーとグループがサポートされます。AXIS Device Managerサーバーをホストするマシンだけを使用してAXIS Device Managerクライアントにアクセスする場合は、ローカル管理者を使用できます。システムのメンテナンスを行うユーザーがリモートクライアントを使用する場合は、ドメインユーザーを使用することを推奨します。



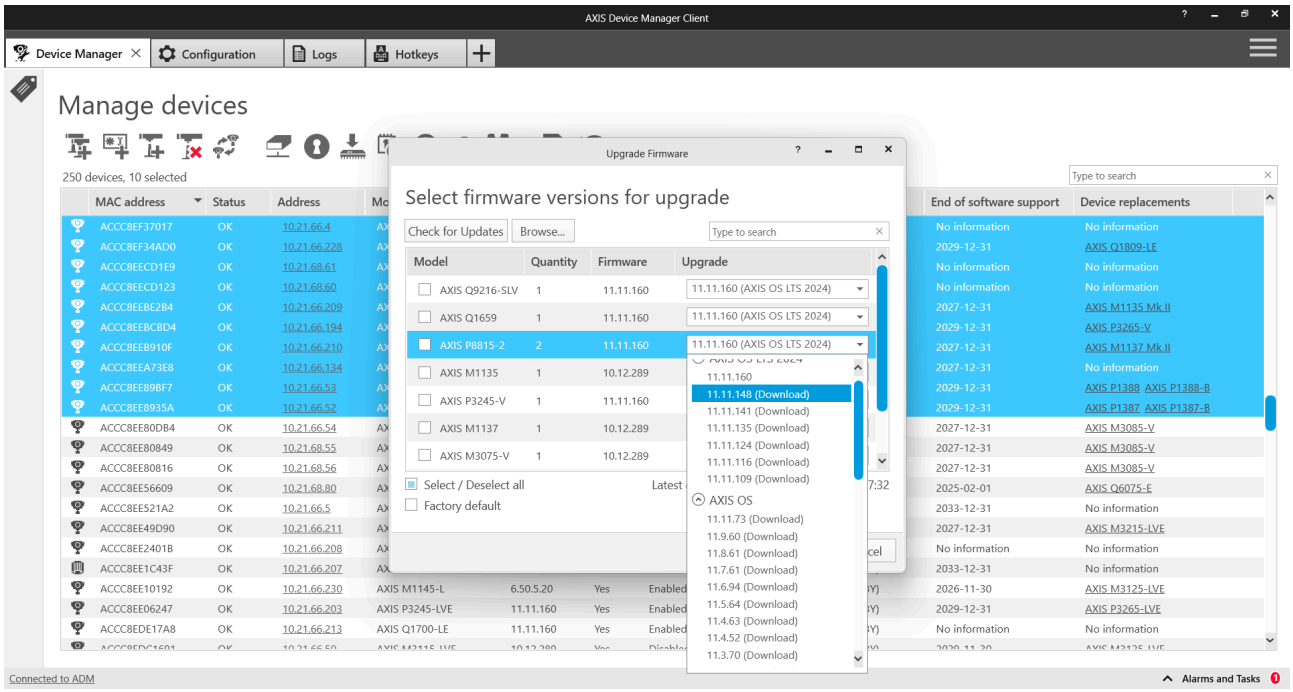
AXIS Device Managerにおけるユーザー権限とパスワードの変更。

AXIS OSのアップグレード

AXIS OSの更新バージョンには、既知の脆弱性に対するパッチが含まれています。攻撃者は既知の脆弱性を利用しようとする場合があるため、常に最新のソフトウェアを使用することは不可欠です。同様に重要な点として、AXIS OSの新バージョンを迅速に適用することで、運用能力を高め、新たなリリースアップグレードを手動で進める際のボトルネックを回避できます。AXIS Device Managerは、www.axis.com に接続し、最新のAXIS OSやサービスリリースをダウンロードします。インターネットからネットワークに直接ダウンロードすることを望まない場合は、アップグレードをUSBスティックに保存した後でAXIS Device Managerクライアントにアップロードできます。また、新しいバージョンのAXIS OSが入手可能かどうかが表示されるため、Axisデバイスへの素早い適用を実行できます。

常に最新のAXIS OSバージョンを実行する必要がある理由

- ネットワークとデバイスは、既知の脆弱性 (特に、重大な脆弱性) に対する最新のパッチによって保護されます。
- デバイスが更新されると、最新のパフォーマンス改善が適用され、また、バグや欠陥も修正されます。
- 最新の機能や機能拡張に即座にアクセスできます。



AXIS Device ManagerによるAXIS OSのアップグレードは、画面上の通知と直感的なダイアログボックスによってシンプルに行うことができます。

さらに強化する方法

適切なユーザーポリシーとパスワードポリシーを採用し、最新のAXIS OSバージョンを実行すれば、デバイスの一般的なリスクを軽減することができます。*Axis強化ガイド*では、大規模な組織や重要な組織でリスクを減らすためのその他の方法を説明しています。これには、使用されていない可能性のあるサービスを無効にしたり、攻撃や侵害の兆候を検出・監視することに役立つサービスを有効にしたりすることが含まれます。AXIS Device Managerは、これらのポリシーの一部を導入するプロセスを簡素化することができます。Axisでは、基本的な推奨設定用の設定テンプレートを提供しています。

Axis強化ガイドに従ってデバイスを強化する方法：

- *Axis強化ガイド*をお読みになり、巻末のテンプレートファイルをダウンロードします。
- 設定ファイルを編集し、該当する項目を選択します。
- AXIS Device Managerのインベントリでデバイスを選択します。
- デバイスを右クリックして、[Configure Devices (デバイスの設定) > Configure (設定)…] を選択します。
- [Configuration File (設定ファイル)] をクリックして、ダウンロードしたファイルを選択します。
- 必要に応じて設定を調整します。

認証局サービス

認証局 (CA) は、デジタル証明書をサーバー、クライアント、ユーザーに対して発行するサービスです。CAにはパブリックCAとプライベートCAがあります。通常、ComodoやSymantec (旧Verisign) などのパブリックに信頼されたCAは、パブリックWebサイトや電子メールなどのパブリックサービスに使用されます。

プライベートCA (通常はアクティブディレクトリ/証明書サービス) は、社内/プライベートネットワークサービス用の証明書を発行します。ビデオ管理システムでは、これは主にHTTPSネットワークの暗号化とIEEE 802.1xネットワークアクセスコントロールのために使用されます。AXIS Device Managerは、Axisデバイス用のCAサービスを対象としており、企業公開鍵インフラストラクチャー (PKI) の一部となり、プライベートルートCAまたはプライベート中間CAとして動作することができます。

CA署名証明書は、IEEE 802.1X (クライアント) とHTTPS (サーバー) の両方の証明書に使用されます。

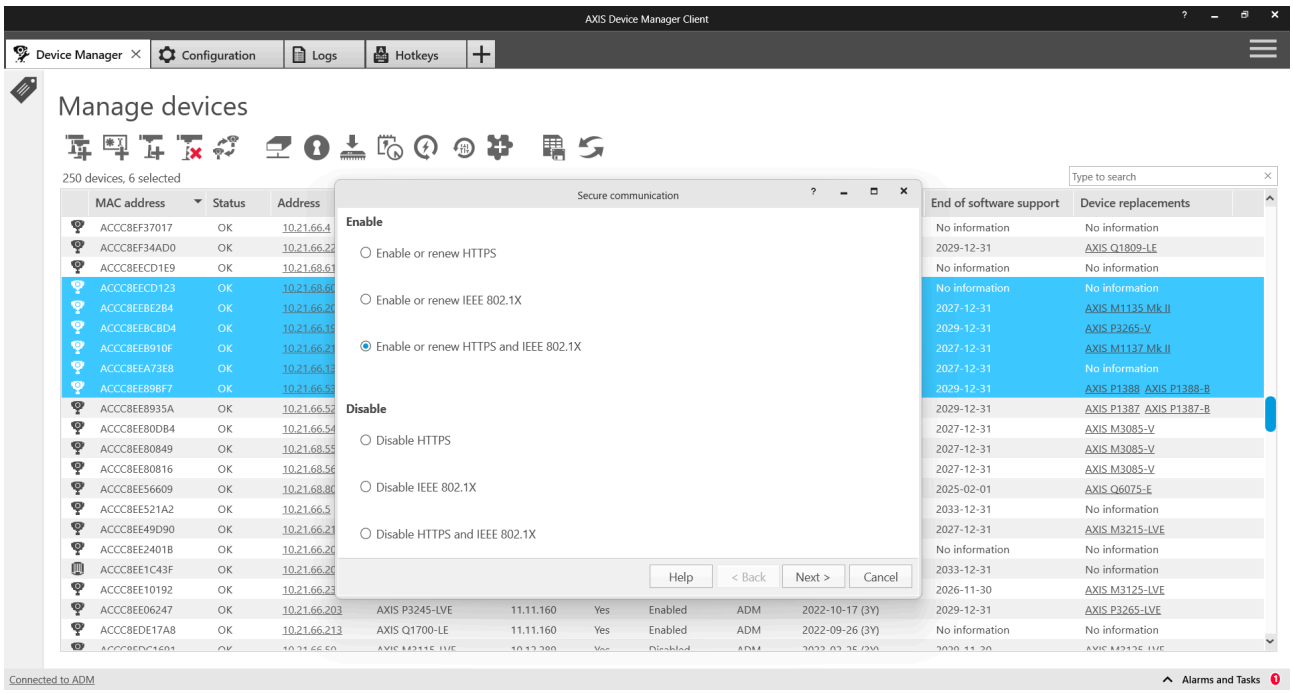
HTTPS

HTTPSは安全なバージョンのHTTPであり、クライアントとサーバーの間の通信が暗号化されます。自己署名証明書により、十分な暗号化接続が実現されます。自己署名証明書とCA署名証明書の間で、暗号化レベルに違いはありません。違いは、自己署名証明書はスプーフィング (攻撃者のコンピューターが正当なサーバーになりすまそうとすること) に対する保護を提供できないという点です。CA署名証明書は、クライアントが信頼できるデバイスにアクセスしていることを認証するための信頼ポイントを追加します。映像を暗号化するには、ビデオクライアント (VMS) でHTTPSによる映像のリクエスト (RTP over RTSP over HTTPS) がサポートされている必要があります。

IEEE 802.1X

省略して802.1Xとも呼ばれるこの規格は、許可されていないネットワークデバイスがローカルネットワークにアクセスすることを防止します。ネットワーク (およびそのリソース) へのアクセスを許可される前に、デバイスは自身を認証する必要があります。MACアドレス (MACフィルタリング) やユーザー/パスワード、クライアント証明書など、さまざまな認証方法を使用できます。使用する方法はシステムの所有者が決定します。選択する方法は脅威、リスク、コストによって異なります。

802.1Xインフラストラクチャの運用はひとつの投資であり、マネージドスイッチと追加サーバー (通常はRADIUS (Remote Authentication Dial-In User Service)) が必要です。クライアント証明書を使用するには、クライアント証明書を発行できるCA (プライベートまたはパブリック) が必要です。ほとんどの場合、このインフラストラクチャーにはメンテナンスまたは監視のための人員が必要です。



AXIS Device Managerにおける証明書の設定。

証明書ライフサイクルの管理

証明書のライフサイクル管理は、証明書の発行、インストール、検査、修正、更新に関連するすべてのプロセスやタスクを長期にわたって高いコスト効率で処理するための手段です。AXIS Device Managerを使用すると、以下が可能になるため、管理者は証明書を効率的に管理できます。

- 別のCAが利用できない場合にCA署名証明書を発行する
- IEEE 802.1X証明書の管理を容易に行う
- HTTPS証明書の管理を容易に行う
- 証明書の有効期限を監視する
- 証明書を有効期限の前に容易に更新する

プライベートルートおよび中間CAに関する推奨事項

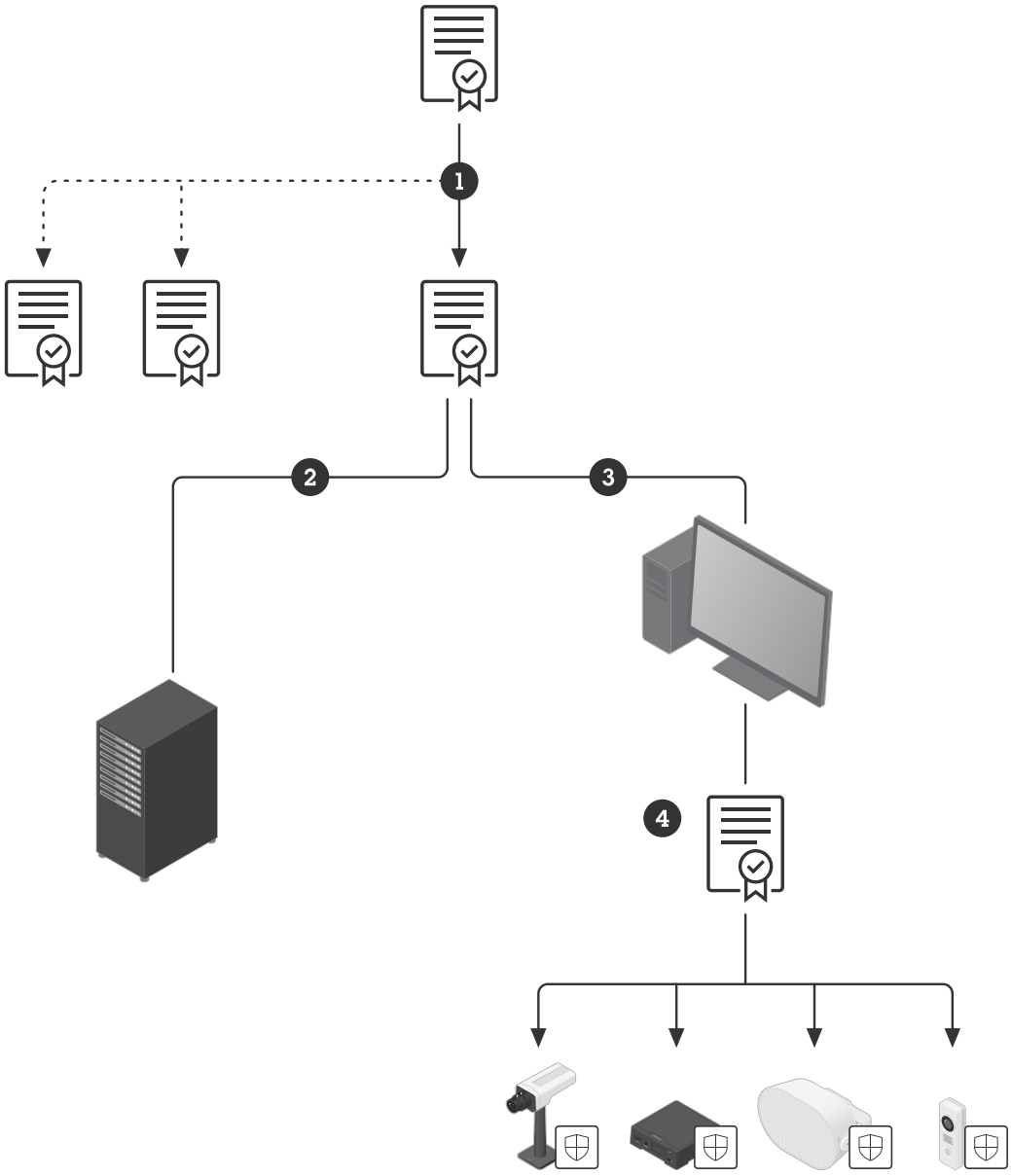
Axisデバイスを一般人向けのパブリックサーバーとして公開することは推奨されていません。これは、パブリックCAをプライベートリソース用に使用することはコスト効率が良くないためです。

HTTPSの場合、信頼されたカメラにアクセスしていることを検証する必要があるクライアントはVMSサーバーだけです。ライブ映像および録画された映像はVMSサーバーから提供されるため、オペレータークライアントがカメラに直接アクセスすることはありません。この状況では、カメラサーバー証明書を既存のエンタープライズPKIに組み込むことの価値は限定的なものとなります。

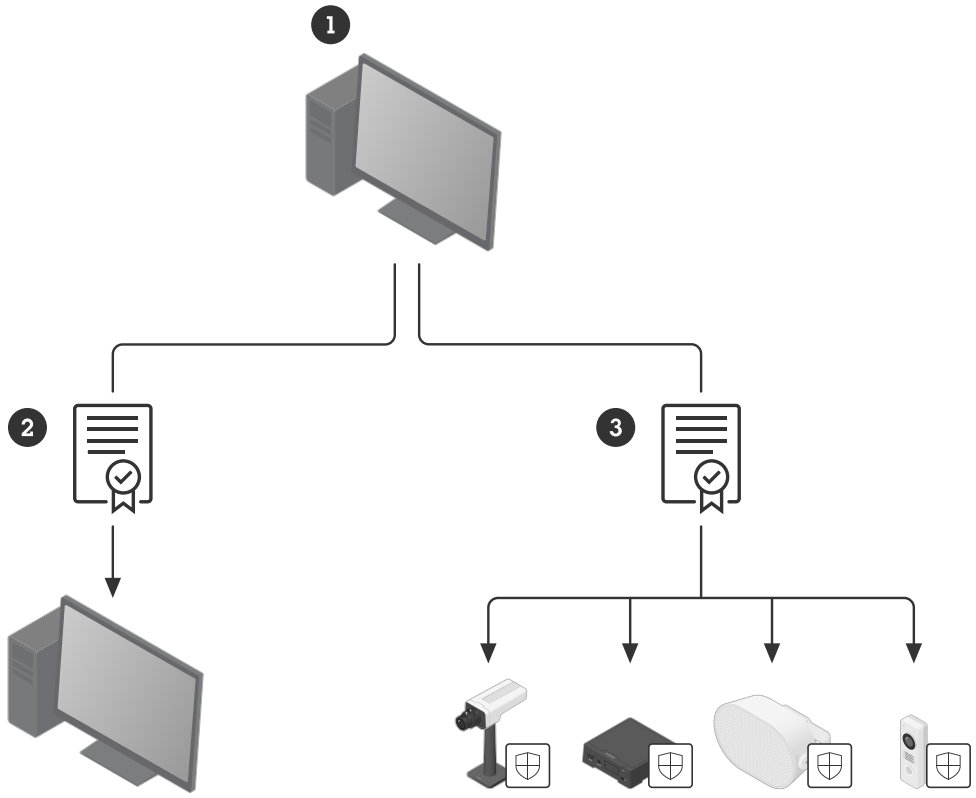
AXIS Device ManagerをプライベートCAとして使用するのは、最もコストパフォーマンスが優れたソリューションです。ルートCA証明書が生成された後、AXIS Device Manager証明書をVMSサーバーの証明書ストアにインストールしてください。他のクライアントが (メンテナンスやトラブルシューティングのために) カメラに直接アクセスする場合は、それらのクライアントにもAXIS Device ManagerルートCAをインストールしてください。

802.1Xの場合、カメラには自身をRADIUSサーバーに認証するためのクライアント証明書が必要です。エンタープライズPKI/CAの管理者に依頼して中間CA証明書を生成した後、AXIS Device Managerにインストール可能なPKCS#12 (P12) 証明書としてエクスポートしてください。

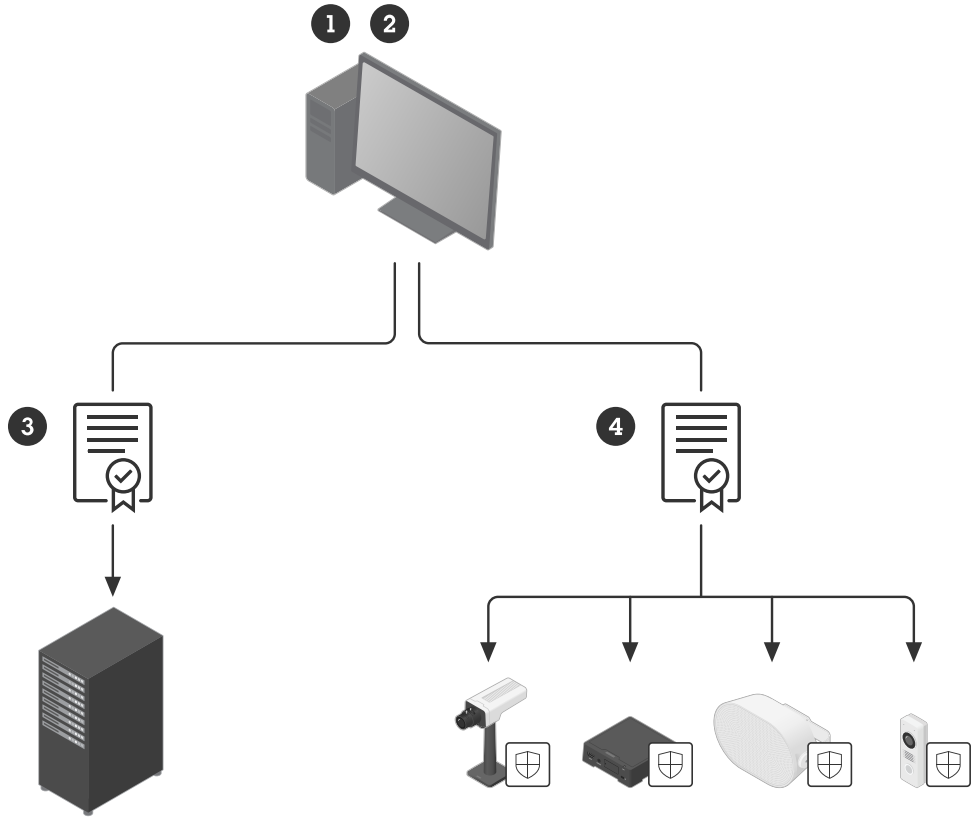
FreeRADIUSサーバーの設定サポートについては、AXIS Device Managerのテクニカルペーパーセクションをご覧ください。



HTTPS証明書を管理するには、以下が必要です。1) AXIS Device Managerで中間CAまたはルートCA証明書を生成する。2) CA証明書をVMSにエクスポートする。3) サーバー証明書をデバイスにアップロードする。



プライベートCAを使用する。IEEE 802.1Xを管理するには、以下が必要です。1) 中間CAとクライアント証明書を生成する。2) CA証明書をRADIUSサーバーにインストールする。3) AXIS Device ManagerでCA証明書をインポートする。4) CA証明書とクライアント証明書をデバイスにアップロードする。



AXIS Device ManagerをCAとして使用する。IEEE 802.1X証明書を管理するには、以下が必要です。1) AXIS Device ManagerでルートCA証明書を生成する。2) AXIS Device Managerで認証CA証明書をインポートする。3) Radiusサーバーにca証明書をインストールする。4) CA認証とクライアント証明書をデバイスにアップロードする。

まとめ

セキュリティ管理とセキュリティ制御は、効果的なサイバーセキュリティアプローチの実装における重要な部分です。そのそれぞれが、お客様のIPネットワークに対する潜在的な脅威を軽減するための明確なステータス維持を必要とする、継続的なプロセスです。AXIS Device Managerは、デバイスの管理だけでなく、ネットワークのセキュリティ向上にも役立つツールです。詳細やサポートについては、お近くのAxis代理店にお問い合わせいただくか、*www.axis.com*をご覧ください。

T10231485_ja

2025-09 (M4.2)