AXIS Device Manager

ユーザーマニュアル

目次

AXIS Device Managerについて 3
ソリューションの概要 4
要件 5
使用に当たって 6
ソフトウェアのインストール 6
サーバーとの接続 6
複数のサーバーへの接続 6
初期設定 7
デバイスの管理 8
デバイスの追加 8
製品を削除する 8
デバイスの置換 8
デバイスの復元 8
設定 10
復元ポイントの作成 10
自動復元ポイントの作成 10
複数の認証情報の管理 10
証明書のインストール 11
証明書について 11
CA証明書の作成 11
HTTPSの有効化 12
802.1Xの有効化 12
SIPアカウントの管理 13
デバイスソフトウェアの管理 14
AXIS OSアップグレード 14
トラブルシューティング 15
サポートに問い合わせる 15
報告手順 15

AXIS Device Managerについて

AXIS Device Managerは、Axis製品のインストールおよび管理ソフトウェアアプリケーションです。このソフトウェアでは、デバイスのネットワーク検出、IPアドレスの割り当て、パスワードの設定、接続状態の表示、ファームウェアのアップグレード、証明書、および複数のデバイスの構成の管理を自動的に行うことができます。

AXIS Device Managerは、以下から構成されています。

- AXIS Device Manager Service Control - Axis製品とのすべての通信を処理するサーバー。
- AXIS Device Manager Client - インターネットまたはコーポレートネットワークからのリモート管理を有効にするフロントエンドユーザーインターフェース。

複数のクライアントを同じサーバーに接続できます。クライアントは複数のサーバーに同時に接続できます。

AXIS Device Managerは、システム強化とセキュリティ向上にも大変役立ちます。詳細については、*AXIS Device Managerセキュリティガイド*を参照してください。

ソリューションの概要

要件

互換性のあるオペレーティングシステム:

要件: 64-bitオペレーティングシステム Microsoft .NET version 4.8

対応OS: Windows 10 Pro、Windows 11 Pro、Windows Server 2016、Windows Server 2019、Windows Server 2022

推奨:最新のOSサービスパック。

最小システム推奨:

- 最小(デバイス500台以下): Intel core i5または同等、4GB RAM、ネットワークインフラストラクチャー全体で100メガビット/秒
- 推奨(デバイス500～2000台): Intel core i7または同等、8GB RAM、ネットワークインフラストラクチャー全体で1000メガビット/秒
- 1サーバーあたりデバイス2000台以上は推奨されません。
- Axisデバイスで最新のAXIS OSが実行されていることを確認してください。

注

弊社では常に最新リリースの2つ前のバージョンをサポートしています。サポートされている特定のバージョンは、最新のリリースノートを確認してください。

対応デバイス:

AXIS OSバージョン4.40以上のAXIS製品(特定の製品モデルおよびファームウェアによって、サポートされる正確な機能は異なります)。

言語:

UI + ヘルプファイル:英語、フランス語、ドイツ語、イタリア語

UIのみ:アラビア語、チェコ語、中国語(簡体字)、中国語(繁体字)、オランダ語、フィンランド語、日本語、韓国語、ペルシャ語、ポーランド語、ポルトガル語(ブラジル)、ロシア語、スペイン語、スウェーデン語、タイ語、トルコ語、ベトナム語

使用に当たって

ソフトウェアのインストール

AXIS Device Manager 5をインストールするには、インストールするコンピューターの完全な管理者権限を持っていることを確認し、次の操作を行います。

1. *axis.com の製品ページに移動し、AXIS Device Managerデスクトップアプリをダウンロードします。*
2. インストーラーを実行し、画面の手順に従います。

注

インストールされていない場合は、Microsoft .NET 4.8 frameworkがインストールされます(インストールファイルに含まれています)。これには数分かかることがあります。Microsoft .NET 4.8 frameworkは、AXIS Device Managerをインストールする前にWindows Updateでインストールすることもできます。

サーバーとの接続

AXIS Device Managerを初めて起動すると、サーバーへの接続が求められます。サーバーはローカルマシンでもリモートサーバーでも実行できます。

ローカルのWindowsユーザーとしてログインするには、次の手順に従います。

1. **[This computer (このコンピューター)]** を選択します。
2. **[Log on as current user (現在のユーザーとしてログオン)]** にチェックを入れて、現在の認証情報を使ってログインします。

サーバーまたはドメインの別のユーザーとしてログインするには、次の手順に従います。

- **[Other user (他のユーザー)]** を選択します。
- **[Other user (他のユーザー)]** に、そのアカウントの認証情報を入力します。
- **[Remember me (次回から入力を省略)]** にチェックを入れて、次回クライアントを実行するときにこのステップを省略します。
- [**Log on (ログオン)**] をクリックします。

注

すべてのサーバーに保存された認証情報を消去するには、ログオン画面に移動し、**[Delete saved passwords (保存されたパスワードを削除する)]** を選択します。

リモートサーバーにログインするには、次の手順に従います。

1. [**リモートサーバー**] を選択します。
2. ドロップダウンリストからサーバーを選択するか、フィールドにIPアドレスまたはDNSアドレスを入力します。
3. 認証情報の入力
4. [**Log on (ログオン)**] をクリックします。

注

このオプションは、Windowsドメインに属さないコンピューターからリモートサーバーにログインするためには使用できません。

複数のサーバーへの接続

AXIS Device Managerで複数のサーバーに接続できます。サーバーへのログインが完了すると、メインメニューからサーバーを切り替えることができます。

1. メインメニュー > [Servers (サーバー)] > [New connection (新規接続)]の順に移動します。

2. 上記の説明のように、お使いのコンピューターまたはリモートサーバーへの接続を選択します。

初期設定

使用するためには、次を行う必要があります。

- デバイスを追加し、ユーザーアカウントを作成します。を参照してください。
- システムのサイバーセキュリティ強化を実施します。を参照してください

デバイスの管理

デバイスの追加

AXIS Device Managerは、接続されているデバイスのネットワークを自動的に検索し、すべてのデバイスへのログインを試みます。検出したデバイスのリストには、デバイスアドレス(IPアドレスまたはホスト名)、シリアル番号、モデル、状態が表示されます。シリアル番号 (S/N) は、製品ラベルに記載されています。

リストからデバイスを追加するには、次の手順に従います。

1. 追加するデバイスを選択し、**[Next (次へ)]** をクリックします。
2. **[Use host name when possible (可能な場合はホスト名を使用する)]** を選択します。ホスト名を使用してデバイスを追加した場合、そのデバイスとの以後の通信にはホスト名が使用されます。ホスト名が利用できない場合は、IPアドレスが使用されます。
3. パスワードのないデバイスにパスワードを設定します。パスワードを設定すべきでない場合は、 **[Skip (スキップ)]** を選択します。
4. **[Next (次へ)]** をクリックします。

“Ready to add devices“ (デバイスを追加できます) のページに追加されるデバイスが表示されます。

5. **[Finish (完了)]** をクリックしてデバイスを追加します。

製品を削除する

リストからデバイスを削除するには、次の手順に従います。

1. **[Device management (デバイス管理)]** に移動します。
2. デバイスを選択します。
3. を右クリックし、[**Remove (削除)**] を選択します。
4. [**Yes (はい)**] をクリックします。

デバイスの置換

AXIS Device Managerでデバイスを置き換えるには、新しいデバイスを接続し、既存のデバイスの設定を再使用します。操作が完了すると、置き換えられたデバイスは削除されます。そのデバイスで利用可能な復元ポイントが少なくとも1つなければありません。を参照してください。復元ポイントは新しいデバイスに移動されません。

1. **[Device management (デバイス管理)]** に移動します。
2. ツールバーに移動し、デバイスの置換のアイコンをクリックします。
3. 置き換えるデバイスを選択し、**[OK]** をクリックします。
4. 置き換えるデバイスを選択し、**[OK]** をクリックします。
5. **[Next (次へ)]** をクリックして、最新の復元ポイントからデバイス設定を取得します。
6. **[Parameters (パラメーター)]** > **[Additional Settings (追加設定)]** の順に移動し、適用するパラメーターと設定を選択します。
7. **[Next (次へ)]** をクリックします。
8. **[Finish (完了)]** をクリックして設定を適用します。

デバイスの復元

1つまたは複数のデバイスを、以前に作成した復元ポイントに復元することが可能です。デバイスを復元するには、各デバイスに少なくとも1つの復元ポイントが必要です。デフォルトでは、選択

したサーバー上のすべてのデバイスについて、自動復元ポイントが毎晩作成され、継続的に削除されます。復元を目的として、最新の自動復元ポイントが設定された数保持されます。

デバイスを以前の復元ポイントに復元するには、次の手順に従います。

1. [Device management (デバイス管理)] ワークスペースに移動します。
2. 復元するデバイスを1つ以上選択します。
3. 右クリックし、ドロップダウンメニューから[Backup / Restore (バックアップ/復元)] > [Restore to a Previous Time (以前の時刻に復元)] を選択します。
4. 利用可能な最新の復元ポイントのリストから復元ポイントを選択し、[Next (次へ)] をクリックします。
5. 各デバイスの設定を確認し、[Finish (完了)] をクリックします。

設定

復元ポイントの作成

手動で復元ポイントを作成するには、次の手順に従います。

- [Device management (デバイス管理)] ワークスペースに移動します。
- 復元するデバイスを1つ以上選択します。
- 右クリックし、[Backup / Restore (バックアップ/復元)] > [Create Restore Points (復元ポイントの作成)] の順に選択します。
- 復元ポイントを識別する説明を入力します。
- [OK] をクリックします。

注

手動で作成した復元ポイントは自動的に削除されません。

自動復元ポイントの作成

サーバーが複数ある場合は、サーバーリストから設定するサーバーを選択します。

- [Options (オプション)] > [Restore point settings (復元ポイント設定)] の順に移動します。
- [Create restore points automatically (復元ポイントを自動的に作成する)] を選択し、復元ポイントの自動作成を有効にします。
- 保存する自動復元ポイント数を入力し、[OK] をクリックします。

複数の認証情報の管理

この機能は、AXIS Device Managerにデバイスの管理者アカウントの認証情報を提供します。

デバイス認証情報の手動入力

デバイス認証情報の手動入力を選択すると、AXIS Device Managerで選択したデバイスの認証情報が更新されます。

- 1つ以上のデバイスを選択します。
- 右クリックし、ドロップダウンメニューから [Advanced (詳細)] -> [Enter Device Credentials (デバイス認証情報の入力)] を選択します。

注

そのデバイスに使用できることが確認できない認証情報は更新されません。その操作に関連するすべてのデバイスで、同じパスワードとユーザー名を使用する必要があります。

CSVファイルを使用して異なる認証情報を使用する

CSVファイルを使用すると、各デバイスで異なるのパスワードとユーザー名を使用できます。MACアドレス、IPアドレス、またはホストアドレスは、CSVファイルの行をAxis Device Managerデータベースの対応するデバイスにマッピングするために使用されます。

CSVファイルを使用する場合、ユーザーインターフェースからCSVファイルの列の解釈を尋ねられます。

注

CSVファイルの行がどのデバイスに属するかを指定する方法。

CSVファイルの1列にはMACアドレス、IPアドレス、ホストアドレスのいずれかを含める必要があるため、CSVファイルの1列をMACアドレスとして解釈するか、IPアドレスまたはホストアドレスとして解釈するか指定します。これは、CSVファイルの行のデータがどのデバイスに属するかを指定するために必要です。また、サーバー名として解釈する列を指定することもできます。このようにすることで、Axis Device Managerサーバーは異なるものの、同じIPアドレスまたはホストアドレスを持つデバイスを対象とするCSVファイルの行を区別することができま

す。そのような区別が必要ない場合は、サーバー名として解釈する列は必要ありません。サーバーが複数のデバイスに同じIPアドレスまたはホストアドレスを使用し、それらを互いに区別するためにポートを使用している設定では、Port (ポート)として解釈するように列を指定することができます。ポートの区別が必要ない場合、通常、列をPort (ポート)として解釈する必要はありません。ポートを専用の列に割り当てる方法の1つとして、IPアドレスまたはホストアドレスと一緒にポートを記入することができます。IPアドレスまたはホストアドレスの後に列とポート番号を続けて記入します。

証明書のインストール

証明書について

AXIS Device Managerには、サーバー/クライアント証明書を管理するための設定があります。クライアント証明書は IEEE 802.1Xに使用され、サーバー証明書はHTTPSに使用されます。変更を実行するには、[Device management (デバイス管理)] で該当するデバイスを選択し、コンテキストメニューから [Enable/update (有効化/更新)] を選択します。

CA証明書の作成

CAを使用すると、サーバー/クライアント証明書がないデバイスで、HTTPSおよびIEEE 802.1Xを有効にすることができます。CAはデバイスに独自の秘密鍵を使用して証明書を作成し、署名し、インストールするようにを指示します。

認証局を作成するには、次の手順に従います。

- **[Configuration (設定)]** タブに移動します。
- **[Security (セキュリティ)]** > **[Certificates (証明書)]** の順に移動します。
- **[Certificate authority (認証局)]** で **[Generate... (生成...)]** をクリックします。
- パスフレーズを入力し、確認します。
- [OK] をクリックします。

CAが生成され、使用できます。

注

自己署名ルート証明書と、任意のパスフレーズで保護された秘密鍵。AXIS Device Managerで生成された証明書は3年間有効です。AXIS Device Managerでサーバー/クライアント証明書を自動更新する場合は、**[Remember passphrase (パスフレーズを記憶する)]** のチェックボックスにチェックを入れる必要があります。CAが設定されていない場合は、AXIS Device Managerの外部でサーバー/クライアント証明書を作成する必要があります。その場合は、証明書の自動管理の機能は使用できません。

Import (インポート) - Import (インポート)機能を使用して、公開証明書と秘密鍵で構成されている既存のCAをインポートすることができます。パスフレーズを入力する必要があります。

[Save to file (ファイルに保存)] - CAの公開証明書を .cer または .crt 形式で保存します。ファイルには秘密鍵が含まれないため、暗号化されません。

Backup (バックアップ) - ハードウェア障害が発生した場合に備えて、CAをバックアップすることが推奨されます。これを選択した場合、Axis Device Managerが使用するCAの証明書と秘密鍵の両方がバックアップされます。バックアップされたデータは、CAを生成するために使用されたパスフレーズによって保護されます。

証明書期限切れ警告 - 証明書の期限切れた場合、またはまもなく期限が切れる場合、システム通知が作成されます。通知は、AXIS Device Managerの外部でインストールされたCAを除き、接続されたデバイスにインストールされたすべての証明書に適用されます。警告はDevice management (デバイス管理)のステータス列にシステムアラームとして表示され、“View installed certificates“ (インストールされた証明書を表示)のダイアログ内とConfiguration (設定)ワークスペースにアイコンで表示されます。

証明書の有効期限が近づいている場合、その何日前にAXIS Device Managerから通知するかを指定します。デフォルトでは、AXIS Device Managerが生成したサーバー証明書とクライアント証明書

は有効期限の警告が表示される7日前に自動的に更新されます。CAの有効期限の通知を受け取るには、[Remember passphrase (パスフレーズを記憶する)] にチェックを入れる必要があります。

HTTPSの有効化

HTTPSを有効にするには、各デバイスにサーバー証明書が必要です。AXIS Device Managerは、認証局(CA)を使用してデバイスのサーバー証明書に署名してインストールすることができます。

次の手順に従って手動で行うこともできます。

1. **[Device manager (デバイスマネージャー)]** タブに移動します。
2. デバイスを右クリックし、コンテキストメニューで各デバイスの **[Install server certificates (サーバー証明書のインストール)]** を選択します。

HTTPSを有効するには、各デバイスのサーバー証明書が1件のみでなければなりません。不要な証明書はコンテキストメニューから削除できます。

3. 証明書のインストール後、コンテキストメニューからHTTPSを有効にすることができます。

注

安全な接続(HTTPS)が利用できない場合は、HTTPを使用して接続することができます。これは安全になっていないデバイスを設定できるようにするために行います。

証明書の検証を無視する

証明書の検証が行われていない場合、AXIS Device Managerはデバイスに接続しません。サーバー証明書は、AXIS Device managerで有効なCAによって署名されるか、Windows証明書ストアを通して検証される必要があります。証明書の検証を無視することを選択すると、AXIS Device Managerはデバイスから送信された証明書が信頼できるかどうかを検証しません。

AXIS Device Managerが証明書の検証を無視するようにするには、次の手順に従います。

- **[Configuration (設定)]** タブに移動します。
- **[HTTPS]** で**[Ignore certificate validation (証明書の検証を無視する)]** を有効にします。

802.1Xの有効化

IEEE 802.1Xを有効にするには、各デバイスにクライアント証明書が必要です。AXIS Device Managerは、認証局(CA)を使用してデバイスのクライアント証明書に署名してインストールすることができます。

これは手動で行うこともできます。Device management (デバイス管理)でデバイスを右クリックし、コンテキストメニューで各デバイスのクライアント証明書のインストールを選択します。IEEE 802.1Xを有効するには、各デバイスのクライアント証明書が1件のみでなければなりません。不要な証明書はコンテキストメニューから削除できます。証明書のインストール後、コンテキストメニューからIEEE 802.1Xを有効にすることができます。

また、IEEE 802.1Xプロトコルを使用するために、IEEE 802.1X認証CA証明書が必要です。

EAPOL Version (EAPOLバージョン) - 使用するEAP (Extensible Authentication Protocol)のバージョンを選択します。

EAP identity (EAP ID) - デバイスのMACアドレス、デバイスのホスト名、またはカスタムテキストのいずれかを入力します。

Custom (カスタム) - EAP IDとする任意のテキストを入力します。

IEEE 802.1X authentication CA certificate (IEEE 802.1X認証CA証明書) - クライアント証明書に加えて、IEEE 802.1X認証CA証明書をインストールする必要があります。IEEE802.1Xを有効にするには、秘密鍵ではなく公開証明書のみが必要なため、パスフレーズは必要ありません。IEEE 802.1X認証CA証明書は、IEEE 802.1Xを有効化または更新するときにインストールされます。

Import (インポート) - デバイスにインストールし、認証サーバーを検証するために使用するCA証明書を選択します。CA証明書はAXIS Device ManagerでCAによって作成される場合と外部ソースから取得される場合があります。

View (表示) - IEEE 802.1X認証プロセスで使用されるCA証明書の詳細。

Common name (コモンネーム) - Device EAP IDまたはDevice IPアドレスのいずれかを選択します。カスタムフィールドを空白のままにすると、ホスト名が選択されます。ホスト名に問題がある場合、IPアドレスがコモンネームに使用されます。

SIPアカウントの管理

デバイスソフトウェアの管理

AXIS OSアップグレード

AXIS OSの最新バージョンは以下の2通りの方法で入手できます。

- AXIS Device Managerを使用してダウンロードする(インターネットへのアクセスが必要)
- (ハードドライブやメモリースティックなどの保存された)ファイルからインポートする

注

AXIS OSが推奨するアップグレードパスに従うことをお勧めします。詳しくは、*https://help.axis.com/axis-os#upgrade-path* を参照してください。

AXIS OSの手動アップグレード

1. 最新のAXIS OSバージョンにアップグレードするデバイスを選択し、右クリックして **[Upgrade firmware (ファームウェアのアップグレード)]** を選択します。
2. アップグレード中にデバイスにアクセスできなくなることが通知されたら、**[Yes (はい)]** をクリックします。
3. ダウンロード可能なファームウェアバージョンのリストを更新するには、**[Upgrade firmware (ファームウェアのアップグレード)]** のダイアログで **[Check for Updates (アップグレードの確認)]** をクリックします。
4. ローカルのクライアントに保存されている1つ以上のAXIS OSバージョンのファイルを参照するには、**[Browse (参照)]** ボタンをクリックします。
5. アップグレードするデバイスとAXIS OSのバージョンを選択します。
6. AXIS OSアップグレード時に選択したデバイスを工場出荷時の設定にリセットするには、**[Factory default checkbox (工場出荷時の設定にリセット)] のチェックボックス**をクリックします。これは、一部のAXIS OSバージョンでダウングレードを行う際に必要です。
7. **[OK]** をクリックして、リストで選択したデバイスのアップグレードを開始します。

注

デフォルトでは、AXIS OSファームウェアアップグレードは選択したすべてのデバイスで同時に行われます。アップグレードの順序は、**[Configuration (設定)]** > **[Connected Services (接続中のサービス)]** > **[Firmware upgrade settings (ファームウェアアップグレード設定)]** で変更できます。

自動アップグレード

AXIS Device Manager 5のデフォルトではファームウェアアップグレードを確認しないように設定されていますが、AXIS OSアップグレードがサーバーまたは axis.com で利用可能かどうかを自動的に確認するように設定できます。

AXIS OSアップグレードを手動で確認するには、アクションメニューの **[Check now (今すぐ確認)]** ボタンを押します。

AXIS OSのアップグレード順序

AXIS OSアップグレードは、すべてのデバイスで同時に行うことも、1つずつ順に行うこともできます。

- すべてのデバイスを同時にアップグレードするには、アップグレード順序に **[Parallel (同時)]** を選択します。
- デバイスを1つずつ順にアップグレードするには、**[Sequential (順次)]** を選択します。このオプションの方が時間はかかりますが、デバイスが同時にオフラインになることはありません。**[Cancel all remaining upgrades if one device fails (デバイスに異常がある場合は残りのアップグレードをキャンセルする)]** の ボックスにチェックを入れて、問題が発生したら順次アップグレードを停止するように設定することもできます。

トラブルシューティング

サポートに問い合わせる

サポートに問い合わせる際は、問題のトラブルシューティングを容易にするために、まず次の手順でチケットを作成し、システムレポートファイルを添付してください。

1. メインメニューに移動します。
2. [Help (ヘルプ)] > [System Report... (システムレポート...)] の順に移動します。
3. 選択したフォルダにレポートファイルを保存します。
4. *axis.com/support* にアクセスします。
5. サポートチケットを作成します。
6. サポートチケットにファイルを添付します。

注

応答していないシステムからシステムレポートを作成する場合は、次の手順を行います。

1. `C:\ProgramData\Axis Communications\` に移動します。
2. フォルダのコンテンツを .zipファイルにアーカイブして、サポートチケットに添付します。

報告手順

このガイドを使用しても解決できない問題がある場合は、Axisオンラインヘルプデスクに問題を連絡してください。*Axisオンラインヘルプデスク*を参照してください。弊社のサポートチームが問題を理解し、解決できるようにするために、以下の情報を含める必要があります。

- 問題の再現方法または問題の発生状況に関する明確な説明。
- 問題が発生した時刻および関係するデバイス名やIPアドレス。
- AXIS Device Manager 問題が発生した直後に生成されたシステムレポート。問題を再現できたクライアントまたはサーバーからシステムレポートを生成してください。
- 問題を示すスクリーンショットまたは録画(オプション)。
- 必要に応じて、データベースファイルを含めてください。アップロードを速めるには、これらを除外してください。

問題によっては、サポートチームが必要に応じて要求する追加情報を含めてください。

注

ネットワークトレースやデータベースファイルなど、ファイルが100 MBを超える場合は、信頼できる安全なファイル共有サービスを使用してファイルを送信してください。

補足情報	
デバッグレベルのログ	より多くの情報を収集するためにデバッグレベルでのログ作成を使用する場合があります。この作業は、Axisサポートエンジニアから要求があった場合にのみ行います。手順は、*Axisオンラインヘルプデスク*で確認できます。
ネットワークトレース	サポートエンジニアから要求された場合は、システムレポートを作成する際にネットワークトレースを生成してください。問題が再現可能であれば、問題が発生したときのネットワークトレースを取得してください。これには以下が含まれます。 • カメラで取得された60秒のネットワークトレース (カメラファームウェア5.20以降でのみ適用可能) 必要に応じて、次のVAPIXコマンドを使用して、ログイン、IPアドレス、および期間 (秒) を変更してください。 `http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=60`

補足情報	
	• サーバーとカメラ間での通信を示すサーバーで取得された10～30秒のネットワークトレース。
データベースファイル	データベースを調査または手動で修復する必要がある場合。システムレポートを生成する前に、[**Include database in the report (レポートにデータベースを含める)**] を選択します。
スクリーンショット	UIに関連するライブビューの問題の場合は、スクリーンショットを使用してください。たとえば、録画のタイムラインの表示が必要な場合や説明が難しい場合です。
画面の録画	問題を言葉で説明するのが難しい場合、たとえば問題の再現に多くのUI操作が関わる場合は、画面録画を使用してください。

T10211981_ja

2025-09 (M3.2)

© 2024 – 2025 Axis Communications AB