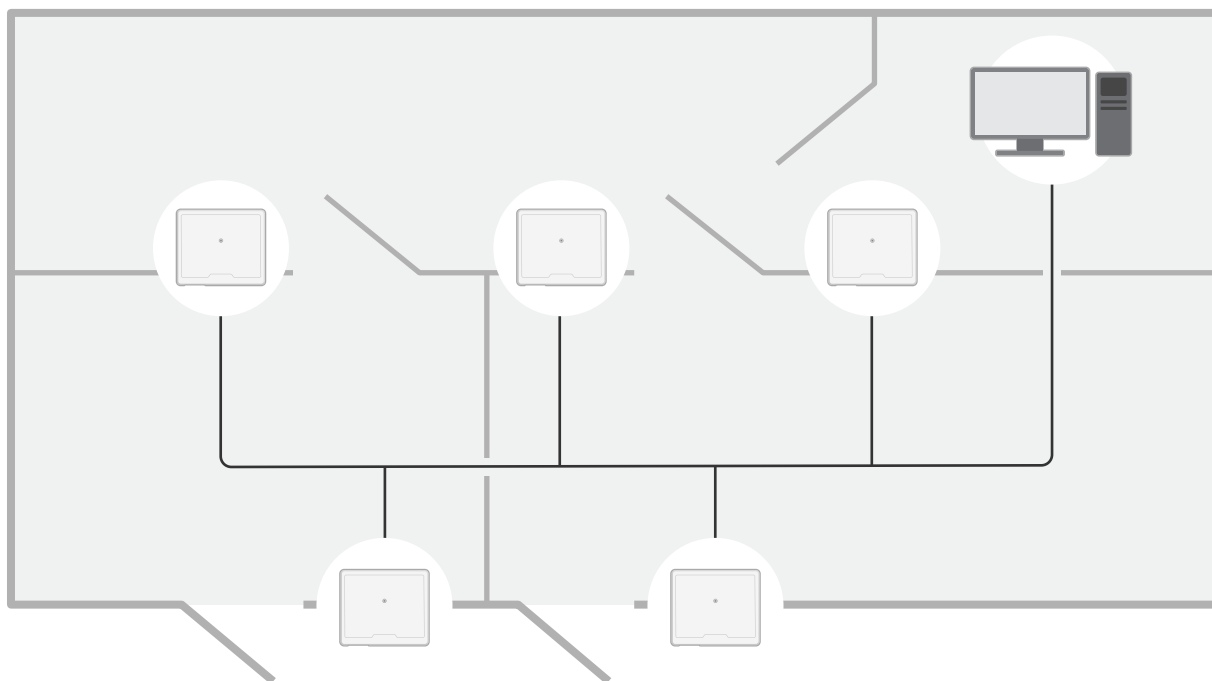


**AXIS A1210 Network Door Controller**  
**AXIS A1210-B Network Door Controller**

**ユーザーマニュアル**

ソリューションの概要 .....	3
設置 .....	5
開始する .....	6
ネットワーク上のデバイスを検索する .....	6
装置のwebインターフェースを開く .....	6
管理者アカウントを作成する .....	6
安全なパスワード .....	7
装置のソフトウェアが改ざんされていないことを確認する .....	7
webインターフェースの概要 .....	7
デバイスを構成する .....	8
webインターフェース .....	9
ステータス .....	9
デバイス .....	10
周辺機器 .....	10
アプリ .....	10
システム .....	11
メンテナンス .....	22
詳細情報 .....	23
サイバーセキュリティ .....	23
仕様 .....	24
製品概要 .....	24
LEDインジケータ .....	24
ボタン .....	25
コネクタ .....	25
トラブルシューティング .....	32
工場出荷時の設定にリセットする .....	32
AXIS OSのオプション .....	32
AXIS OSの現在のバージョンを確認する .....	32
AXIS OSをアップグレードする .....	32
技術的な問題、ヒント、解決策 .....	33
サポートに問い合わせる .....	35

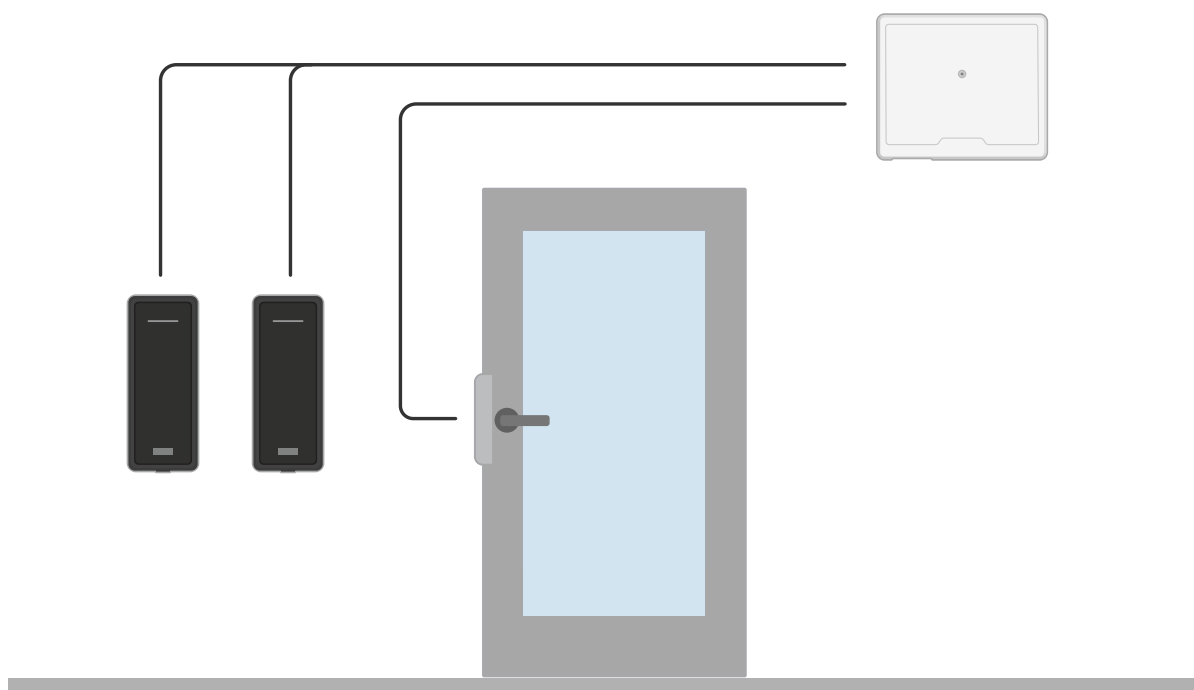
### ソリューションの概要



ネットワークコントローラーは、既存のIPネットワークに容易に接続して給電することができ、特殊な配線は必要ありません。

## ソリューションの概要

---



各ネットワークドアコントローラーは、ドアの近くに容易に取り付けることができるインテリジェントデバイスです。最大2つのリーダーに給電したり制御したりできます。

### 設置



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=74266&section=solution-overview](http://help.axis.com/?&piald=74266&section=solution-overview)*

### 開始する

#### ネットワーク上のデバイスを検索する

Windows®で検索したAxisデバイスにIPアドレスの割り当てを行うには、AXIS IP UtilityまたはAXIS Device Managerを使用します。いずれのアプリケーションも無料で、[axis.com/support](http://axis.com/support)からダウンロードできます。

IPアドレスの検索や割り当てを行う方法の詳細については、[IPアドレスの割り当てとデバイスへのアクセス方法を参照してください](#)。

#### ブラウザサポート

以下のブラウザでデバイスを使用できます。

	Chrome™	Firefox®	Edge™	Safari®
Windows®	推奨	推奨	✓	
macOS®	推奨	推奨	✓	✓
Linux®	推奨	推奨	✓	
その他のオペレーティングシステム	✓	✓	✓	✓*

\* iOS 15またはiPadOS 15でAXIS OS Webインターフェースを使用するには、[\[Settings \(設定\)\] > \[Safari\] > \[Advanced \(詳細設定\)\] > \[Experimental Features \(実験的機能\)\]](#)の順に移動して、[\[NSURLSession Websocket\]](#)を無効にします。

推奨ブラウザの詳細については、[AXIS OSポータル](#)にアクセスしてください。

#### 装置のwebインターフェースを開く

1. ブラウザーを開き、Axis装置のIPアドレスまたはホスト名を入力します。

本製品のIPアドレスが不明な場合は、AXIS IP UtilityまたはAXIS Device Managerを使用して、ネットワーク上で装置を見つけます。

2. ユーザー名とパスワードを入力します。装置に初めてアクセスする場合は、管理者アカウントを作成する必要があります。を参照してください。

装置のwebインターフェースにあるすべてのコントロールとオプションの説明については、[を参照してください](#)。

#### 管理者アカウントを作成する

装置に初めてログインするときには、管理者アカウントを作成する必要があります。

1. ユーザー名を入力してください。
2. パスワードを入力します。を参照してください。
3. パスワードを再入力します。
4. 使用許諾契約書に同意します。
5. [\[Add account \(アカウントを追加\)\]](#) をクリックします。

## 開始する

---

### 重要

装置にはデフォルトのアカウントはありません。管理者アカウントのパスワードを紛失した場合は、装置をリセットする必要があります。を参照してください。

## 安全なパスワード

### 重要

Axisデバイスは、最初に設定されたパスワードをネットワーク上で平文で送信します。最初のログイン後にデバイスを保護するために、安全で暗号化されたHTTPS接続を設定してからパスワードを変更してください。

デバイスのパスワードは主にデータおよびサービスを保護します。Axisデバイスは、さまざまなタイプのインストールで使用できるようにするためパスワードポリシーを強制しません。

データを保護するために、次のことが強く推奨されています。

- 8文字以上のパスワードを使用する (できればパスワード生成プログラムで作成する)。
- パスワードを公開しない。
- 一定の期間ごとにパスワードを変更する (少なくとも年に1回)。

## 装置のソフトウェアが改ざんされていないことを確認する

装置に元のAXIS OSが搭載されていることを確認するか、またはセキュリティ攻撃が行われた後に装置を完全に制御するには、以下の手順に従います。

1. 工場出荷時の設定にリセットします。を参照してください。  
リセットを行うと、セキュアブートによって装置の状態が保証されます。
2. デバイスを設定し、インストールします。

## webインターフェースの概要

このビデオでは、装置のwebインターフェースの概要について説明します。



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=74266&section=web-interface-overview](http://help.axis.com/?&piald=74266&section=web-interface-overview)

Axis装置のwebインターフェース

## デバイスを構成する

---

### デバイスを構成する


装置の設定方法については、*AXIS Camera Station*ユーザーマニュアルまたはサードパーティ製のソリューションを参照してください。











## webインターフェース




装置のwebインターフェースにアクセスするには、Webブラウザで装置のIPアドレスを入力します。


### 注

このセクションで説明する機能と設定のサポートは、装置によって異なります。このアイコン  は、機能または設定が一部の装置でのみ使用できることを示しています。

 メインメニューの表示/非表示を切り取ります。  リリースノートにアクセスします。  製品のヘルプにアクセスします。  言語を変更します。  ライトテーマまたはダークテーマを設定します。 

  ユーザーメニューは以下を含みます。

-  ログインしているユーザーに関する情報。
-  **アカウントの変更**：現在のアカウントからログアウトし、新しいアカウントにログインします。
-  **ログアウト**：現在のアカウントからログアウトします。

 コンテキストメニューは以下を含みます。

- **Analytics data (分析データ)**:個人以外のブラウザデータの共有に同意します。
- **フィードバック**:フィードバックを共有して、ユーザーエクスペリエンスの向上に役立てます。
- **法的情報**:Cookieおよびライセンスについての情報を表示します。
- **詳細情報**:AXIS OSのバージョンやシリアル番号などの装置情報を表示します。
- **Legacy device interface (従来の装置インターフェース)**:装置のwebインターフェースを従来のバージョンに変更します。

## ステータス

### デバイス情報

AXIS OSのバージョンとシリアル番号を含む装置情報を表示します。

**AXIS OSのアップグレード**：装置のソフトウェアをアップグレードします。アップグレードができる [Maintenance (メンテナンス)] ページに移動します。

### 時刻同期ステータス

装置がNTPサーバーと同期しているかどうかや、次の同期までの残り時間など、NTP同期情報を表示します。

**NTP settings (NTP設定)**:NTP設定を表示および更新します。NTPの設定を変更できる [Date and time (日付と時刻)] のページに移動します。

### セキュリティ

アクティブな装置へのアクセスのタイプ、使用されている暗号化プロトコル、未署名のアプリが許可されているかが表示されます。設定に関する推奨事項はAXIS OS強化ガイドに基づいています。

**強化ガイド**:Axis装置でのサイバーセキュリティとベストプラクティスをさらに学習できる *AXIS OS強化ガイド*へのリンクです。

### 接続されたクライアント


接続数と接続されているクライアントの数を表示します。


**View details (詳細を表示)**:接続されているクライアントのリストを表示および更新します。リストには、各接続のIPアドレス、プロトコル、ポート、状態、PID/プロセスが表示されます。


## デバイス

### アラーム

**Device motion (装置の動き)**:オンに設定すると、装置の動きを検知したときにシステム内でアラームがトリ

ガーされます。**ケーシング開放**  :オンに設定すると、ドアコントローラーケーシングの開放を検知したときにシステム内でアラームがトリガーされます。ベアボードコントローラーでこの設定をオフにしま

す。**外部からのいたずら**  :オンにすると、外部からのいたずらを検知したときにシステムでアラームがトリガーされます。たとえば、誰かが外部キャビネットを開閉した場合などです。

- ・ **状態監視入力**  :入力の状態を監視するときにオンにし、終端抵抗器を設定します。
  - 並列優先接続を使用するには、[Parallel first connection with a 22 K $\Omega$  parallel resistor and a 4.7 K $\Omega$  serial resistor (22 k $\Omega$ の並列抵抗器と4.7 k $\Omega$ の直列抵抗器による並列優先接続)]を選択します。
  - 直列優先接続を使用するには、[Serial first connection (直列優先接続)]を選択し、[Resistor values (抵抗器の値)] ドロップダウンリストから抵抗器の値を選択します。

## 周辺機器



### リーダー


**+** **リーダーの追加**:クリックして新規リーダーを追加します。**名前**:リーダーの名前を入力します。**リーダー**:ドロップダウンリストからリーダーを選択します。**IPアドレス**:リーダーのIPアドレスを手動で入力します。**Username (ユーザー名)**:ユーザー名を入力します。**パスワード**:パスワードを入力します。**サーバー証明書の検証の無視**:これをオンにすると、検証が無視されます。

### リーダーのアップグレード

**Upgrade readers (リーダーのアップグレード)**:クリックすると、リーダーをAXIS OSの新しいバージョンにアップグレードします。この機能では、サポート対象のリーダーがオンラインの場合にのみアップグレードします。

## アプリ

**+** **アプリの追加**:新しいアプリをインストールします。さらに**アプリを探す**:インストールする他のアプリを見つける。Axisアプリの概要ページに移動します。**署名されていないアプリを許可**  :署名なしアプリのインストールを許可するには、オンにします。**root権限のあるアプリを許可**  :オンにし

て、root権限を持つアプリに装置へのフルアクセスを許可します。  **AXIS OSおよびACAPアプリのセキュリティ更新プログラム**を表示します。

## 注

複数のアプリを同時に実行すると、装置のパフォーマンスが影響を受ける可能性があります。

アプリ名の横にあるスイッチを使用して、アプリを起動または停止します。**開く**:アプリの設定にアクセスする。利用可能な設定は、アプリケーションによって異なります。一部のアプリケーションでは設定が設けられて

いません。● コンテキストメニューに、以下のオプションが1つ以上含まれていることがあります。

- **Open-source license (オープンソースライセンス)**:アプリで使用されているオープンソースライセンスに関する情報が表示されます。
- **App log (アプリのログ)**:アプリイベントのログが表示されます。このログは、サポートにご連絡いただく際に役立ちます。
- **キーによるライセンスのアクティブ化**:アプリにライセンスが必要な場合は、ライセンスを有効にする必要があります。装置がインターネットにアクセスできない場合は、このオプションを使用します。ライセンスキーがない場合は、[axis.com/products/analytics](https://axis.com/products/analytics)に移動してください。ライセンスキーを生成するには、ライセンスコードとAxis製品のシリアル番号が必要です。
- **ライセンスの自動アクティブ化**:アプリにライセンスが必要な場合は、ライセンスを有効にする必要があります。装置がインターネットにアクセスできる場合は、このオプションを使用します。ライセンスをアクティブ化するには、ライセンスコードが必要です。
- **Deactivate the license (ライセンスの非アクティブ化)**:試用ライセンスから正規ライセンスに変更する場合など、別のライセンスと交換するために現在のライセンスを無効にします。ライセンスを非アクティブ化すると、ライセンスはデバイスから削除されます。
- **Settings (設定)**:パラメーターを設定します。
- **削除**:デバイスからアプリを完全に削除します。ライセンスを最初に非アクティブ化しない場合、ライセンスはアクティブのままです。

## システム

### 時刻と位置

#### 日付と時刻

時刻の形式は、Webブラウザの言語設定によって異なります。

## 注

装置の日付と時刻をNTPサーバーと同期することをお勧めします。

**Synchronization (同期)**:装置の日付と時刻を同期するオプションを選択します。

- **自動日時 (手動NTS KEサーバー)**: DHCPサーバーに接続されている安全なNTPキー確立サーバーと同期します。
  - **Manual NTS KE servers (手動NTS KEサーバー)**:1台または2台のNTPサーバーのIPアドレスを入力します。2台のNTPサーバーを使用すると、両方からの入力に基づいて装置が同期し、時刻を調整します。
  - **Max NTP poll time (最長NTPポーリング時間)**:装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最長待機時間を選択します。
  - **Min NTP poll time (最短NTPポーリング時間)**:装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最短待機時間を選択します。
- **自動日時設定 (DHCPを使用したNTPサーバー)**: DHCPサーバーに接続されているNTPサーバーと同期します。
  - **Fallback NTP servers (フォールバックNTPサーバー)**:1台または2台のフォールバックサーバーのIPアドレスを入力します。
  - **Max NTP poll time (最長NTPポーリング時間)**:装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最長待機時間を選択します。
  - **Min NTP poll time (最短NTPポーリング時間)**:装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最短待機時間を選択します。
- **自動日時設定 (手動NTPサーバー)**: 任意のNTPサーバーと同期します。
  - **Manual NTP servers (手動NTPサーバー)**:1台または2台のNTPサーバーのIPアドレスを入力します。2台のNTPサーバーを使用すると、両方からの入力に基づいて装置が同期し、時刻を調整します。

- **Max NTP poll time (最長NTPポーリング時間)**:装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最長待機時間を選択します。
  - **Min NTP poll time (最短NTPポーリング時間)**:装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最短待機時間を選択します。
  - **Custom date and time (日付と時刻のカスタム設定)**:日付と時刻を手動で設定する[Get from system (システムから取得)]をクリックして、コンピューターまたはモバイル装置から日付と時刻の設定を1回取得します。
- タイムゾーン:使用するタイムゾーンを選択します。時刻が夏時間と標準時間に合わせて自動的に調整されます。
- **DHCP**:DHCPサーバーのタイムゾーンを採用します。このオプションを選択する前に、装置がDHCPサーバーに接続されている必要があります。
  - **手動**:ドロップダウンリストからタイムゾーンを選択します。

### 注

システムは、すべての録画、ログ、およびシステム設定で日付と時刻の設定を使用します。

## デバイスの位置

デバイスの位置を入力します。ビデオ管理システムはこの情報を使用して、地図上にデバイスを配置できます。

- **Latitude (緯度)**:赤道の北側がプラスの値です。
- **Longitude (経度)**:本初子午線の東側がプラスの値です。
- **向き**:デバイスが向いているコンパス方位を入力します。0が真北となります。
- **ラベル**:分かりやすいデバイス名を入力します。
- **Save (保存)**:クリックして、装置の位置を保存します。

## ネットワーク

### IPv4

**Assign IPv4 automatically (IPv4自動割り当て)**:ネットワークルーターが自動的にデバイスにIPアドレスを割り当てる場合に選択します。ほとんどのネットワークでは、自動IP (DHCP) をお勧めします。**IPアドレス**:装置の固有のIPアドレスを入力します。孤立したネットワークの内部であれば、アドレスの重複がないことを条件に、静的なIPアドレスを自由に割り当てることができます。アドレスの重複を避けるため、固定IPアドレスを割り当てる前に、ネットワーク管理者に連絡することを推奨します。**サブネットマスク**:サブネットマスクを入力して、ローカルエリアネットワーク内部のアドレスを定義します。ローカルエリアネットワークの外部のアドレスは、ルーターを経由します。**Router (ルーター)**:さまざまなネットワークやネットワークセグメントに接続された装置を接続するために使用するデフォルトルーター (ゲートウェイ) のIPアドレスを入力します。**Fallback to static IP address if DHCP isn't available (DHCPが利用できない場合は固定IPアドレスにフォールバックする)**:DHCPが利用できず、IPアドレスを自動的に割り当てることができない場合に、フォールバックとして使用する固定IPアドレスを追加するときを選択します。

### 注

DHCPが使用できず、装置が静的アドレスのフォールバックを使用する場合、静的アドレスは限定された範囲で設定されます。

### IPv6

**Assign IPv6 automatically (IPv6自動割り当て)**:IPv6をオンにし、ネットワークルーターに自動的に装置にIPアドレスを割り当てさせる場合に選択します。

## ホスト名

**Assign hostname automatically (ホスト名自動割り当て):** ネットワークルーターに自動的に装置にホスト名を割り当てさせる場合に選択します。**ホスト名:** 装置にアクセスする別の方法として使用するホスト名を手動で入力します。サーバーレポートとシステムログはホスト名を使用します。使用できる文字は、A～Z、a～z、0～9、-、\_です。

### DNSサーバー

**Assign DNS automatically (DNS自動割り当て):** DHCPサーバーに自動的に装置に検索ドメインとDNSサーバーアドレスを割り当てさせる場合に選択します。ほとんどのネットワークでは、自動DNS (DHCP) をお勧めします。**Search domains (検索ドメイン):** 完全修飾でないホスト名を使用する場合は、**[Add search domain (検索ドメインの追加)]** をクリックし、装置が使用するホスト名を検索するドメインを入力します。**DNS servers (DNSサーバー):** **[Add DNS server (DNSサーバーを追加)]** をクリックして、DNSサーバーのIPアドレスを入力します。このサーバーは、ホスト名からローカルネットワーク上のIPアドレスへの変換を行います。

### HTTPとHTTPS

HTTPSは、ユーザーからのページ要求とWebサーバーから返されたページの暗号化を提供するプロトコルです。サーバーの真正性(サーバーが本物であること)を保証するHTTPS証明書が使用されます。

デバイスでHTTPSを使用するには、HTTPS証明書をインストールする必要があります。**[System (システム) > Security (セキュリティ)]** に移動し、証明書の作成とインストールを行います。

**Allow access through (次によってアクセスを許可):** ユーザーが **[HTTP]**、**[HTTPS]**、または **[HTTP and HTTPS (HTTPおよびHTTPS)]** プロトコルを介して装置に接続することを許可するかどうかを選択します。

#### 注

暗号化されたWebページをHTTPS経由で表示する場合、特に初めてページを要求するときに、パフォーマンスが低下することがあります。

**HTTP port (HTTPポート):** 使用するHTTPポートを入力します。このデバイスでは、ポート80または1024-65535の範囲内の任意のポートが許可されます。管理者としてログインしている場合は、1～1023の範囲内の任意のポートを入力することもできます。この範囲内のポートを使用すると、警告が表示されます。**HTTPS port (HTTPSポート):** 使用するHTTPSポートを入力します。このデバイスでは、ポート443または1024～65535の範囲内の任意のポートが許可されます。管理者としてログインしている場合は、1～1023の範囲内の任意のポートを入力することもできます。この範囲内のポートを使用すると、警告が表示されます。**Certificate (証明書):** 装置のHTTPSを有効にする証明書を選択します。

### ネットワーク検出プロトコル

**Bonjour®:** オンにしてネットワーク上で自動検出を可能にします。**Bonjour名:** ネットワークで表示されるフレンドリ名を入力します。デフォルト名はデバイス名とMACアドレスです。**UPnP®:** オンにしてネットワーク上で自動検出を可能にします。**UPnP名:** ネットワークで表示されるフレンドリ名を入力します。デフォルト名はデバイス名とMACアドレスです。**WS-Discovery:** オンにしてネットワーク上で自動検出を可能にします。**LLDP & CDP:** オンにしてネットワーク上で自動検出を可能にします。LLDPとCDPをオフにすると、PoE電力ネゴシエーションに影響する可能性があります。PoE電力ネゴシエーションに関する問題を解決するには、PoEスイッチをハードウェアPoE電力ネゴシエーションのみに設定してください。

### ワンクリックによるクラウド接続

One-Click cloud connection (O3C) とO3Cサービスを共に使用すると、インターネットを介して、ライブビデオや録画ビデオにどこからでも簡単かつ安全にアクセスできます。詳細については、[axis.com/end-to-end-solutions/hosted-services](https://axis.com/end-to-end-solutions/hosted-services)を参照してください。



### Allow O3C (O3Cを許可):

- ・ **ワンクリック**:これがデフォルト設定です。インターネットを介してO3Cサービスに接続するには、装置のコントロールボタンを押し続けます。コントロールボタンを押してから24時間以内に装置をO3Cサービスに登録する必要があります。登録しない場合、デバイスはO3Cサービスから切断されます。装置を登録すると、**[Always (常時)]**が有効になり、装置はO3Cサービスに接続されたままになります。
- ・ **[常時]**:装置は、インターネットを介してO3Cサービスへの接続を継続的に試行します。装置を登録すると、装置はO3Cサービスに接続したままになります。デバイスのコントロールボタンに手が届かない場合は、このオプションを使用します。
- ・ **No**: O3Cサービスを無効にします。

**Proxy settings (プロキシ設定)**: 必要な場合は、プロキシサーバーに接続するためのプロキシ設定を入力します。**[ホスト]**:プロキシサーバーのアドレスを入力します。**ポート**:アクセスに使用するポート番号を入力します。**[ログイン]**と**[パスワード]**:必要な場合は、プロキシサーバーのユーザー名とパスワードを入力します。

### Authentication method (認証方式):

- ・ **[ベーシック]**:HTTPの認証方式としては、この方式が最も互換性があります。ユーザー名とパスワードが暗号化されずにサーバーに送信されるため、安全性は**ダイジェスト**方式よりも低くなります。
- ・ **[ダイジェスト]**:この認証方式は、常に暗号化されたパスワードをネットワークに送信するため、高いセキュリティレベルが得られます。
- ・ **[オート]**:このオプションを使用すると、デバイスはサポートされている方法に応じて認証方法を選択できます。**ダイジェスト**方式が**ベーシック**方式より優先されます。

**Owner authentication key (OAK)**: **[Get key (キーを取得)]** をクリックして、オーナー認証キーを取得します。これは、デバイスがファイアウォールやプロキシを介さずにインターネットに接続されている場合にのみ可能です。

## SNMP

SNMP (Simple Network Management Protocol) を使用すると、離れた場所からネットワーク装置を管理できます。

**SNMP**: 使用するSNMPのバージョンを選択します。

- ・ **v1 and v2c (v1およびv2c)**:
  - **Read community (読み取りコミュニティ)**:サポートされているSNMPオブジェクトすべてに読み取り専用のアクセスを行えるコミュニティ名を入力します。デフォルト値は**public**です。
  - **Write community (書き込みコミュニティ)**:サポートされている(読み取り専用のもを除く)SNMPオブジェクトすべてに読み取りアクセス、書き込みアクセスの両方を行えるコミュニティ名を入力します。デフォルト設定値は**write**です。
  - **Activate traps (トラップの有効化)**:オンに設定すると、トラップレポートが有効になります。デバイスはトラップを使用して、重要なイベントまたはステータス変更のメッセージを管理システムに送信します。Webインターフェースでは、SNMP v1およびv2cのトラップを設定できます。SNMP v3に変更すると、またはSNMPをオフにすると、トラップが自動的にオフになります。SNMP v3を使用している場合は、SNMP v3管理アプリケーションからトラップを設定できます。
  - **Trap address (トラップアドレス)**:管理サーバーのIPアドレスまたはホスト名を入力します。
  - **Trap community (トラップコミュニティ)**:装置がトラップメッセージを管理システムに送信するときに使用するコミュニティを入力します。
  - **Traps (トラップ)**:
    - **Cold start (コールドスタート)**:デバイスの起動時にトラップメッセージを送信します。
    - **ウォームスタート**:SNMP設定が変更されたときに、トラップメッセージを送信します。
    - **Link up (リンクアップ)**:リンクの状態が切断から接続に変わったときにトラップメッセージを送信します。
  - **認証失敗**:認証に失敗したときにトラップメッセージを送信します。

### 注

SNMP v1およびv2cトラップをオンにすると、すべてのAXIS Video MIBトラップが有効になります。詳細については、[AXIS OSポータル > SNMP](#)を参照してください。

- ・ **v3**: SNMP v3は、暗号化と安全なパスワードを使用するより安全性の高いバージョンです。SNMP v3を使用するには、パスワードがHTTPS経由で送信されるため、HTTPSを有効にすることをお勧めします。これにより、暗号化されていないSNMP v1およびv2cトラップへの不正アクセスを防ぐこともできます。SNMP v3を使用する際は、SNMP v3管理アプリケーションでトラップを設定できます。

- アカウント「initial」のパスワード：「initial」という名前のアカウントのSNMPパスワードを入力します。HTTPSを有効化しなくてもパスワードを送信することができますが、これは推奨されません。SNMP v3のパスワードは1回しか設定できません。HTTPSが有効な場合にのみ設定することをお勧めします。パスワードの設定後は、パスワードフィールドが表示されなくなります。パスワードを設定し直すには、デバイスを工場出荷時の設定にリセットする必要があります。

## セキュリティ

### 証明書

証明書は、ネットワーク上のデバイスの認証に使用されます。この装置は、次の2種類の証明書をサポートしています。

- **Client/server Certificates (クライアント/サーバー証明書)**  
クライアント/サーバー証明書は装置のIDを認証します。自己署名証明書と認証局 (CA) 発行の証明書のどちらでも使用できます。自己署名証明書による保護は限られていますが、認証局発行の証明書を取得するまで利用できます。
- **CA証明書**  
CA証明書はピア証明書の認証に使用されます。たとえば、装置をIEEE 802.1Xで保護されたネットワークに接続するときに、認証サーバーのIDを検証するために使用されます。デバイスには、CA証明書がいくつかプリインストールされています。

以下の形式がサポートされています：


- 証明書の形式：.PEM、.CER、.PFX
- 秘密鍵の形式：PKCS#1、PKCS#12

#### 重要

デバイスを工場出荷時の設定にリセットすると、すべての証明書が削除されます。プリインストールされたCA証明書は、再インストールされます。

## +


証明書の追加：クリックして証明書を追加します。

- その他  : 入力または選択するフィールドをさらに表示します。
- セキュアキーストア:[Secure element (セキュアエレメント)] または [Trusted Platform Module 2.0] を使用して秘密鍵を安全に保存する場合に選択します。どのセキュアキーストアを選択するかの詳細については、[help.axis.com/en-us/axis-os#cryptographic-support](http://help.axis.com/en-us/axis-os#cryptographic-support)にアクセスしてください。
- Key type (キーのタイプ): ドロップダウンリストから、証明書の保護に使用する暗号化アルゴリズムとしてデフォルトかその他のいずれかを選択します。

## ⋮

コンテキストメニューは以下を含みます。

- Certificate information (証明書情報): インストールされている証明書のプロパティを表示します。
- Delete certificate (証明書の削除): 証明書の削除。
- Create certificate signing request (証明書の署名要求を作成する): デジタルID証明書を申請するために登録機関に送信する証明書署名要求を作成します。

セキュアキーストア  :

- Secure element (CC EAL6+) : セキュアキーストアにセキュアエレメントを使用するか選択します。
- Trusted Platform Module 2.0 (CC EAL4+、FIPS 140-2 Level 2) : セキュアキーストアにTPM 2.0を使用することを選択します。

Network access control and encryption (ネットワークのアクセスコントロールと暗号化)

**IEEE 802.1x** IEEE 802.1xは、有線およびワイヤレスネットワーク装置の安全な認証を提供するポートベースのネットワーク入場制御のためのIEEE標準です。IEEE 802.1xは、EAP (拡張文字認証プロトコル)に基づいています。IEEE 802.1xで保護されているネットワークにアクセスするネットワーク装置は、自己の証明を行う必要があります。認証は認証サーバーによって行われます。認証サーバーは通常、FreeRADIUSやMicrosoft Internet Authentication ServerなどのRADIUSサーバーです。**IEEE 802.1AE MACsec** IEEE 802.1AE MACsecは、メディアアクセスコントロール (MAC) セキュリティのためのIEEE標準であり、メディアアクセス独立プロトコルのためのコネクションレスデータ機密性と整合性を定義しています。**証明書CA**証明書なしで設定されている場合、サーバー証明書の検証は無効になり、デバイスは接続先のネットワークに関係なく自己の認証を試みます。証明書を使用する場合、Axisの実装では、装置と認証サーバーは、EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) を使用してデジタル証明書で自己を認証します。装置が証明書で保護されたネットワークにアクセスできるようにするには、署名されたクライアント証明書を装置にインストールする必要があります。**Authentication method (認証方式)**: 認証に使用するEAPタイプを選択します。**Client certificate (クライアント証明書)**: IEEE 802.1xを使用するクライアント証明書を選択します。認証サーバーは、この証明書を使用してクライアントの身元を確認します。**CA certificates (CA証明書)**: 認証サーバーの身元を確認するためのCA証明書を選択します。証明書が選択されていない場合、デバイスは、接続されているネットワークに関係なく自己を認証しようとします。**EAP識別情報**: クライアント証明書に関連付けられているユーザーIDを入力します。**EAPOLのバージョン**: ネットワークスイッチで使用されるEAPOLのバージョンを選択します。**Use IEEE 802.1x**: IEEE 802.1xプロトコルの使用を選択します。これらの設定は、認証方法として**IEEE 802.1x PEAP-MSCHAPv2**を使用する場合にのみ使用できます。

- ・ **パスワード**: ユーザーIDのパスワードを入力します。
- ・ **Peap version (Peapのバージョン)**: ネットワークスイッチで使用するPeapのバージョンを選択します。
- ・ **ラベル**: クライアントEAP暗号化を使用する場合は1を選択し、クライアントPEAP暗号化を使用する場合は2を選択します。Peapバージョン1を使用する際にネットワークスイッチが使用するラベルを選択します。

これらの設定を使用できるのは、認証方法として**IEEE 802.1ae MACsec (静的CAK/事前共有キー)**を使用する場合のみです。

- ・ **Key agreement connectivity association key name (キー合意接続アソシエーションキー名)**: 接続アソシエーション名 (CKN) を入力します。2~64文字 (2で割り切れる文字数) の16進文字である必要があります。CKNは、接続アソシエーションで手動で設定する必要があり、最初にMACsecを有効にするには、リンクの両端で一致している必要があります。
- ・ **Key agreement connectivity association key (キー合意接続アソシエーションキー)**: 接続アソシエーションキー (CAK) を入力します。32文字または64文字の16進数である必要があります。CAKは、接続アソシエーションで手動で設定する必要があり、最初にMACsecを有効にするには、リンクの両端で一致している必要があります。

### ブルートフォース攻撃を防ぐ

**Blocking (ブロック)**: オンに設定すると、ブルートフォース攻撃がブロックされます。ブルートフォース攻撃では、試行錯誤を繰り返す総当たり攻撃でログイン情報や暗号化キーを推測します。**Blocking period (ブロック期間)**: ブルートフォース攻撃をブロックする秒を入力します。**Blocking conditions (ブロックの条件)**: ブロックが開始されるまでに1秒間に許容される認証失敗の回数を入力します。ページレベルとデバイスレベルの両方で許容される失敗の数を設定できます。

### ファイアウォール

**Activate (アクティブ化)**: ファイアウォールをオンにします。

**Default Policy (デフォルトポリシー)**: ファイアウォールのデフォルト状態を選択します。

- ・ **Allow (許可)**: 装置へのすべての接続を許可します。このオプションはデフォルトで設定されています。
- ・ **Deny (拒否)**: 装置へのすべての接続を拒否します。

デフォルトポリシーに例外を設定するために、特定のアドレス、プロトコル、ポートから装置への接続を許可または拒否するルールを作成できます。

- ・ **アドレス**: アクセスを許可または拒否するアドレスをIPv4/IPv6またはCIDR形式で入力します。
- ・ **Protocol (プロトコル)**: アクセスを許可または拒否するプロトコルを選択します。
- ・ **ポート**: アクセスを許可または拒否するポート番号を入力します。1~65535のポート番号を追加できます。
- ・ **Policy (ポリシー)**: ルールのポリシーを選択します。





: クリックして、別のルールを作成します。


**Add rules: (ルールの追加):** クリックして、定義したルールを追加します。

- **Time in seconds: (時間 (秒)):** ルールのテストに制限時間を設定します。デフォルトの制限時間は**300**秒に設定されています。ルールをすぐに有効にするには、**0**秒に設定します。
- **Confirm rules (ルールを確認):** ルールとその制限時間を確認します。1秒を超える制限時間を設定した場合、ルールはこの時間内に有効になります。時間を**0**に設定すると、ルールがすぐに有効化されます。

**Pending rules (保留中のルール):** まだ確認していない最新のテスト済みルールの概要です。



時間制限のあるルールは、表示されたタイマーが切れるか、確認されるまで、[**Active rules (アクティブなルール)**]に表示されます。確認されない場合、タイマーが切れると、それらのルールは [**Pending rules (保留中のルール)**]に表示され、ファイアウォールは以前の設定に戻ります。それらのルールを確認すると、現在アクティブなルールが置き換えられます。


**Confirm rules (ルールを確認):** クリックして、保留中のルールをアクティブにします。 **Active rules (アクティブなルール):** 装置で現在実行中のルールの概要です。  : クリックして、アクティブなルールを削除します。



: クリックして、保留中のルールとアクティブなルールの両方をすべて削除します。

### カスタム署名付きAXIS OS証明書

Axisのテストソフトウェアまたはその他のカスタムソフトウェアを装置にインストールするには、カスタム署名付きAXIS OS証明書が必要です。証明書は、ソフトウェアが装置の所有者とAxisの両方によって承認されたことを証明します。このソフトウェアは、固有のシリアル番号とチップIDによって識別される特定の装置でのみ実行できます。Axisのみがカスタム署名付きAXIS OS証明書を作成できます (Axisが署名するためのキーを保持しているため)。 **Install (インストール):** クリックして、証明書をインストールします。ソフトウェアをインストール

する前に、証明書をインストールする必要があります。  コンテキストメニューは以下を含みます。

- **Delete certificate (証明書の削除):** 証明書の削除。

### アカウント

#### アカウント



**アカウントの追加:** クリックして、新しいアカウントを追加します。最大100個のアカウントを追加できます。 **Account (アカウント):** 固有のアカウント名を入力します。 **New password (新しいパスワード):** アカウントのパスワードを入力します。パスワードの長は1~64文字である必要があります。印刷可能なASCII文字 (コード32~126)のみを使用できます。これには、英数字、句読点、および一部の記号が含まれます。 **Repeat password (パスワードの再入力):** 同じパスワードを再び入力します。 **Privileges (権限):**

- **Administrator (管理者):** すべての設定へ全面的なアクセス権をもっています。管理者は他のアカウントを追加、更新、削除することもできます。
- **Operator (オペレーター):** 次の操作を除く、すべての設定へのアクセス権があります。
  - すべての [System settings (システムの設定)]。
- **Viewer (閲覧者):** 設定を変更するアクセス権を持っていません。



コンテキストメニューは以下を含みます。 **Update account (アカウントの更新):** アカウントのプロパティを編集します。 **Delete account (アカウントの削除):** アカウントを削除します。rootアカウントは削除できません。

#### SSHアカウント

**+** SSHアカウントの追加：クリックして、新しいSSHアカウントを追加します。

- ・ **Restrict root access (rootアクセスを制限する)**:オンにすると、rootアクセスを必要とする機能が制限されます。
- ・ **SSHの有効化**：SSHサービスを使用する場合は、オンにします。

**Account (アカウント)**:固有のアカウント名を入力します。**New password (新しいパスワード)**:アカウントのパスワードを入力します。パスワードの長は1~64文字である必要があります。印刷可能なASCII文字(コード32~126)のみを使用できます。これには、英数字、句読点、および一部の記号が含まれます。**Repeat password (パスワードの再入力)**:同じパスワードを再び入力します。コメント:コメントを入力します(オプション)。

⋮ コンテキストメニューは以下を含みます。**Update SSH account (SSHアカウントの更新)**:アカウントのプロパティを編集します。**Delete SSH account (SSHアカウントの削除)**:アカウントを削除します。rootアカウントは削除できません。

### Virtual host (仮想ホスト)

**+** 仮想ホストの追加：クリックして、新しい仮想ホストを追加します。**Enabled (有効)**:この仮想ホストを使用するには、選択します。**Server name (サーバー名)**:サーバーの名前を入力します。数字0~9、文字A~Z、ハイフン(-)のみを使用します。**ポート**:サーバーが接続されているポートを入力します。**タイプ**:使用する認証のタイプを選択します。**[Basic (ベーシック)]**、**[Digest (ダイジェスト)]**、**[Open ID]**から選択します。

⋮ コンテキストメニューは以下を含みます。

- ・ **Update (更新)**:仮想ホストを更新します。
- ・ **削除**:仮想ホストを削除します。

**Disabled (無効)**:サーバーが無効になっています。

### OpenID 設定

#### 重要

OpenIDを使用してサインインできない場合は、OpenIDを設定したときに使用したダイジェストまたはベーシック認証情報を使用してサインインします。

**Client ID**：OpenIDユーザー名を入力します。**Outgoing Proxy (発信プロキシ)**:OpenID接続でプロキシサーバーを使用する場合は、プロキシアドレスを入力します。**Admin claim (管理者請求)**:管理者権限の値を入力します。**プロバイダーURL**：APIエンドポイント認証用のWebリンクを入力します。形式はhttps://[URLを挿入]/well-known/openid-configurationとしてください。**Operator claim (オペレーター請求)**:オペレーター権限の値を入力します。**Require claim (必須請求)**:トークンに含めるデータを入力します。**Viewer claim (閲覧者請求)**:閲覧者権限の値を入力します。**Remote user (リモートユーザー)**:リモートユーザーを識別する値を入力します。これは、装置のwebインターフェースに現在のユーザーを表示するのに役立ちます。**Scopes (スコープ)**:トークンの一部となるオプションのスコープです。**Client secret (クライアントシークレット)**:OpenIDのパスワードを入力します。**Save (保存)**:クリックして、OpenIDの値を保存します。**OpenIDの有効化**：現在の接続を閉じ、プロバイダーURLからの装置認証を許可する場合は、オンにします。

### MQTT

MQTT (Message Queuing Telemetry Transport) はモノのインターネット (IoT) で使われる標準の通信プロトコルです。IoTの統合を簡素化するために設計されており、小さなコードフットプリントと最小限のネットワーク帯域幅でリモートデバイスを接続するために、さまざまな業界で使用されています。Axis装置のソフトウェアに搭載されているMQTTクライアントは、装置で生成されたデータやイベントを、ビデオ管理ソフトウェア (VMS) ではないシステムに統合することを容易にします。装置をMQTTクライアントとして設定します。MQTT通信は、クライアントとブローカーという2つのエンティティに基づいています。クライアントは、メッセージの送受信を行うことができます。ブローカーは、クライアント間でメッセージをルーティングする役割を担います。MQTTの詳細については、[AXIS OSポータル](#)を参照してください。

### ALPN

ALPNは、クライアントとサーバー間の接続のハンドシェイクフェーズ中にアプリケーションプロトコルを選択できるようにするTLS/SSL拡張機能です。これは、HTTPなどの他のプロトコルに使用されるのと同じポートでMQTTトラフィックを有効にするために使用されます。場合によっては、MQTT通信に専用のポートが開いていないこともあります。このような場合の解決策は、ALPNを使用して、ファイアウォールによって許可される標準ポートで、アプリケーションプロトコルとしてMQTTを使用するようネゴシエーションすることです。

### MQTT クライアント

**Connect (接続する):**MQTTクライアントのオン/オフを切り替えます。**Status (ステータス):**MQTTクライアントの現在のステータスを表示します。**ブローカー[ホスト]:**MQTTサーバーのホスト名またはIPアドレスを入力します。**Protocol (プロトコル):**使用するプロトコルを選択します。**ポート:**ポート番号を入力します。

- 1883はMQTTオーバTCPのデフォルト値です。
- 8883はMQTTオーバSSLのデフォルト値です。
- 80はMQTTオーバWebSocketのデフォルト値です。
- 443はMQTTオーバWebSocket Secureのデフォルト値です。

**ALPN protocol (ALPN プロトコル):**ご使用のMQTTブローカープロバイダーが提供するALPNプロトコル名を入力します。これは、MQTTオーバSSLとMQTTオーバWebSocket Secureを使用する場合にのみ適用されます。**Username (ユーザー名):**クライアントがサーバーにアクセスするために使用するユーザー名を入力します。**パスワード:**ユーザー名のパスワードを入力します。**Client ID:**クライアントIDを入力します。クライアント識別子は、クライアントがサーバーに接続する際にサーバーに送信されます。**Clean session (クリーンセッション):**接続時と切断時の動作を制御します。選択した場合、接続時と切断時にステータス情報が破棄されます。**HTTP proxy (HTTP プロキシ):**最大長が255バイトのURL。HTTPプロキシを使用しない場合、このフィールドは空白のまま構いません。**HTTPS proxy (HTTPS プロキシ):**最大長が255バイトのURL。HTTPSプロキシを使用しない場合、このフィールドは空白のまま構いません。**Keep alive interval (キープアライブの間隔):**長時間のTCP/IPタイムアウトを待たずに、サーバーを使用できなくなったことをクライアントに検知させます。**Timeout (タイムアウト):**接続を終了する時間の間隔(秒)です。デフォルト値：60**装置トピックの接頭辞:**MQTTクライアントタブの接続メッセージやLWTメッセージ、MQTT公開タブの公開条件におけるトピックのデフォルト値で使用されます。**Reconnect automatically (自動再接続):**切断された場合に、クライアントを自動的に再接続するかどうかを指定します。**接続メッセージ**接続が確立されたときにメッセージを送信するかどうかを指定します。**Send message (メッセージの送信):**オンにすると、メッセージを送信します。**Use default (デフォルトを使用):**オフに設定すると、独自のデフォルトメッセージを入力できます。**Topic (トピック):**デフォルトのメッセージのトピックを入力します。**Payload (ペイロード):**デフォルトのメッセージの内容を入力します。**Retain (保持する):**クライアントの状態をこのTopic (トピック)に保存する場合に選択します。**QoS:**パケットフローのQoS layerを変更します。**最終意思およびテストメントメッセージ**最終意思テストメント(LWT)を使用すると、クライアントはブローカーへの接続時、認証情報と共にテストメントを提供します。後ほどいずれかの時点でクライアントが予期せず切断された場合(電源の停止など)、ブローカーから他のクライアントにメッセージを送信できます。このLWTメッセージは通常のメッセージと同じ形式で、同一のメカニズムを経由してルーティングされます。**Send message (メッセージの送信):**オンにすると、メッセージを送信します。**Use default (デフォルトを使用):**オフに設定すると、独自のデフォルトメッセージを入力できます。**Topic (トピック):**デフォルトのメッセージのトピックを入力します。**Payload (ペイロード):**デフォルトのメッセージの内容を入力します。**Retain (保持する):**クライアントの状態をこのTopic (トピック)に保存する場合に選択します。**QoS:**パケットフローのQoS layerを変更します。

### MQTT公開

**Use default topic prefix (デフォルトのトピックプレフィックスを使用):**選択すると、[MQTT client (MQTTクライアント)] タブの装置のトピックプレフィックスで定義されたデフォルトのトピックプレフィックスが使用されます。**Include topic name (トピック名を含める):**選択すると、条件を説明するトピックがMQTTトピックに含まれます。**Include topic namespaces (トピックの名前空間を含める):**選択すると、ONVIFトピックの名前空間がMQTTトピックに含まれます。**シリアル番号を含める:**選択すると、装置のシリアル番号が、

MQTTペイロードに含まれます。 **+** **条件の追加:** クリックして条件を追加します。**Retain (保持する):**保持して送信するMQTTメッセージを定義します。

- **None (なし):**すべてのメッセージを、保持されないものとして送信します。
- **Property (プロパティ):**ステートフルメッセージのみを保持として送信します。
- **All (すべて):**ステートフルメッセージとステートレスメッセージの両方を保持として送信します。

**QoS:** MQTT公開に適切なレベルを選択します。

### MQTTサブスクリプション

**+** **購読の追加:** クリックして、新しいMQTTサブスクリプションを追加します。**サブスクリプションフィルター:**購読するMQTTトピックを入力します。**装置のトピックプレフィックスを使用:**サブスクリプションフィルターを、MQTTトピックのプレフィックスとして追加します。**サブスクリプションの種類:**

- **ステートレス:**選択すると、エラーメッセージがステートレスメッセージに変換されます。
- **ステートフル:**選択すると、エラーメッセージが条件に変換されます。ペイロードが状態として使用されます。



**QoS:** MQTTサブスクリプションに適切なレベルを選択します。



### アクセサリー

#### I/Oポート

デジタル入力を使用すると、開回路と閉回路の切り替えが可能な外部装置 (PIRセンサー、ドアまたは窓の接触、ガラス破損検知器など) を接続できます。


デジタル出力を使用して、リレーやLEDなどの外部装置を接続します。VAPIX®アプリケーションプログラミングインターフェースまたはWebインターフェースを通じて、接続した装置を起動できます。

**ポート名前:**テキストを編集して、ポートの名前を変更します。**Direction (方向):**  は、ポートが入力ポートであることを示します。  は、出力ポートであることを示します。ポートが設定可能な場合は、アイコン

をクリックして入力と出力を切り替えることができます。**標準の状態:**開回路には  を、閉回路には  をクリックします。**現在の状態:**ポートの現在のステータスを表示します。入力または出力は、現在の状態が通常の状態とは異なる場合に有効化されます。装置の接続が切断されているか、DC 1Vを超える電圧がかかっている場合に、装置の入力は開回路になります。

**注**

再起動中、出力回路は開かれます。再起動が完了すると、回路は正常位置に戻ります。このページの設定を変更した場合、有効なトリガーに関係なく出力回路は正常位置に戻ります。

**状態監視**  : オンに設定すると、誰かがデジタルI/Oデバイスへの接続を改ざんした場合に、そのアクションを検出してトリガーできます。入力が開いているか閉じているかを検知するだけでなく、誰かが改ざんした場合 (つまり、切断または短絡) も検知することができます。接続を監視するには、外部I/Oループ内に追加のハードウェア (終端抵抗器) が必要です。

### ログ

#### レポートとログ

### レポート

- **View the device server report (デバイスサーバーレポートを表示):**製品ステータスに関する情報をポップアップウィンドウに表示します。アクセスログは自動的にサーバーレポートに含まれます。
- **Download the device server report (デバイスサーバーレポートをダウンロード):**これによって、UTF-8形式で作成された完全なサーバーレポートのテキストファイルと、現在のライブビュー画像のスナップショットを収めた.zipファイルが生成されます。サポートに連絡する際には、必ずサーバーレポート.zipファイルを含めてください。
- **Download the crash report (クラッシュレポートをダウンロード):**サーバーの状態に関する詳細情報が付随したアーカイブをダウンロードします。クラッシュレポートには、サーバーレポートに記載されている情報と詳細なバグ情報が含まれます。レポートには、ネットワークトレースなどの機密情報が含まれている場合があります。レポートの生成には数分かかることがあります。

### ログ

- **View the system log (システムログを表示):**装置の起動、警告、重要なメッセージなど、システムイベントに関する情報をクリックして表示します。
- **View the access log (アクセスログを表示):**誤ったログインパスワードの使用など、本装置への失敗したアクセスをすべてクリックして表示します。

## ネットワークトレース

### 重要

ネットワークトレースファイルには、証明書やパスワードなどの機密情報が含まれている場合があります。

ネットワークトレースファイルはネットワーク上のアクティビティを録画するので、トラブルシューティングに役立ちます。Trace time (追跡時間):秒または分でトレースの期間を選択し、[ダウンロード]をクリックします。

## リモートシステムログ

syslogはメッセージログ作成の標準です。これによって、メッセージを生成するソフトウェア、メッセージを保存するシステム、およびそれらを報告して分析するソフトウェアを分離することができます。各メッセージには、メッセージを生成したソフトウェアの種類を示す設備コードがラベル付けされ、重大度レベルが割り当てられます。

### +

**サーバー:**クリックして新規サーバーを追加します。[ホスト]:サーバーのホスト名またはIPアドレスを入力します。**Format (形式):**使用するsyslogメッセージの形式を選択します。

- Axis
- RFC 3164
- RFC 5424

**Protocol (プロトコル):**使用するプロトコルを選択します。

- UDP (デフォルトポートは514)
- TCP (デフォルトポートは601)
- TLS (デフォルトポートは6514)

**ポート:**別のポートを使用する場合は、ポート番号を編集します。**重大度:**トリガー時に送信するメッセージを選択します。**CA証明書設定:**現在の設定を参照するか、証明書を追加します。



### メンテナンス

**Restart (再起動):** デバイスを再起動します。再起動しても、現在の設定には影響がありません。実行中のアプリケーションは自動的に再起動されます。**Restore (リストア):** ほとんどの設定が工場出荷時の値に戻ります。その後、装置とアプリを再設定し、ブライnstallしなかったアプリを再インストールし、イベントやプリセットを再作成する必要があります。

**重要**

復元後に保存される設定は以下の場合のみです。

- ブートプロトコル (DHCPまたは静的)
- 静的IPアドレス
- デフォルトのルータ
- サブネットマスク
- 802.1Xの設定
- O3C settings (O3Cの設定)
- DNSサーバーIPアドレス

**Factory default (工場出荷時設定):** すべての設定を工場出荷時の値に戻します。その後、装置にアクセス可能なIPアドレスをリセットする必要があります。

**注**

検証済みのソフトウェアのみを装置にインストールするために、すべてのAxisの装置のソフトウェアにデジタル署名が付け加えられます。これによって、Axis装置の全体的なサイバーセキュリティの最低ラインがさらに上がります。詳細については、[axis.com](http://axis.com)でホワイトペーパー「Axis Edge Vault」を参照してください。

**AXIS OS upgrade (AXIS OSのアップグレード):** AXIS OSの新しいバージョンにアップグレードします。新しいリリースには、機能の改善やバグの修正、まったく新しい機能が含まれています。常にAXIS OSの最新のリリースを使用することをお勧めします。最新のリリースをダウンロードするには、[axis.com/support/](http://axis.com/support/)に移動します。アップグレード時には、以下の3つのオプションから選択できます。

- **Standard upgrade (標準アップグレード):** AXIS OSの新しいバージョンにアップグレードします。
- **Factory default (工場出荷時設定):** アップグレードすると、すべての設定が工場出荷時の値に戻ります。このオプションを選択すると、アップグレード後にAXIS OSを以前のバージョンに戻すことはできません。
- **Autorollback (オートロールバック):** 設定した時間内にアップグレードを行い、アップグレードを確認します。確認しない場合、装置はAXIS OSの以前のバージョンに戻されます。

**AXIS OS rollback (AXIS OSのロールバック):** AXIS OSの以前にインストールしたバージョンに戻します。

### 詳細情報

## サイバーセキュリティ

サイバーセキュリティに関する製品固有の情報については、[axis.com](https://axis.com)の製品データシートを参照してください。

AXIS OSのサイバーセキュリティに関する詳細情報については、*AXIS OS 強化ガイド*を参照してください。

## 署名付きOS

署名付きOSは、ソフトウェアベンダーがAXIS OSイメージを秘密鍵で署名することで実装されます。オペレーティングシステムに署名が付けられると、装置はインストール前にソフトウェアを検証ようになります。装置でソフトウェアの整合性が損なわれていることが検出された場合、AXIS OSのアップグレードは拒否されます。

## セキュアブート

セキュアブートは、暗号化検証されたソフトウェアの連続したチェーンで構成される起動プロセスで、不変メモリ(ブートROM)から始まります。署名付きOSの使用に基づいているため、セキュアブートを使うと、装置は認証済みのソフトウェアを使用した場合のみ起動できます。

## Axis Edge Vault

ハードウェアベースのサイバーセキュリティプラットフォーム「Axis Edge Vault」により、Axisデバイスを保護することができます。装置のIDと整合性を保証し、不正アクセスから機密情報を保護する機能を提供します。これは、エッジデバイスセキュリティに関する専門知識を駆使して、暗号コンピューティングモジュール(セキュアエレメントやTPM)とSoCセキュリティ(TEEやセキュアブート)に基づき構築された強力な基盤により成り立っています。

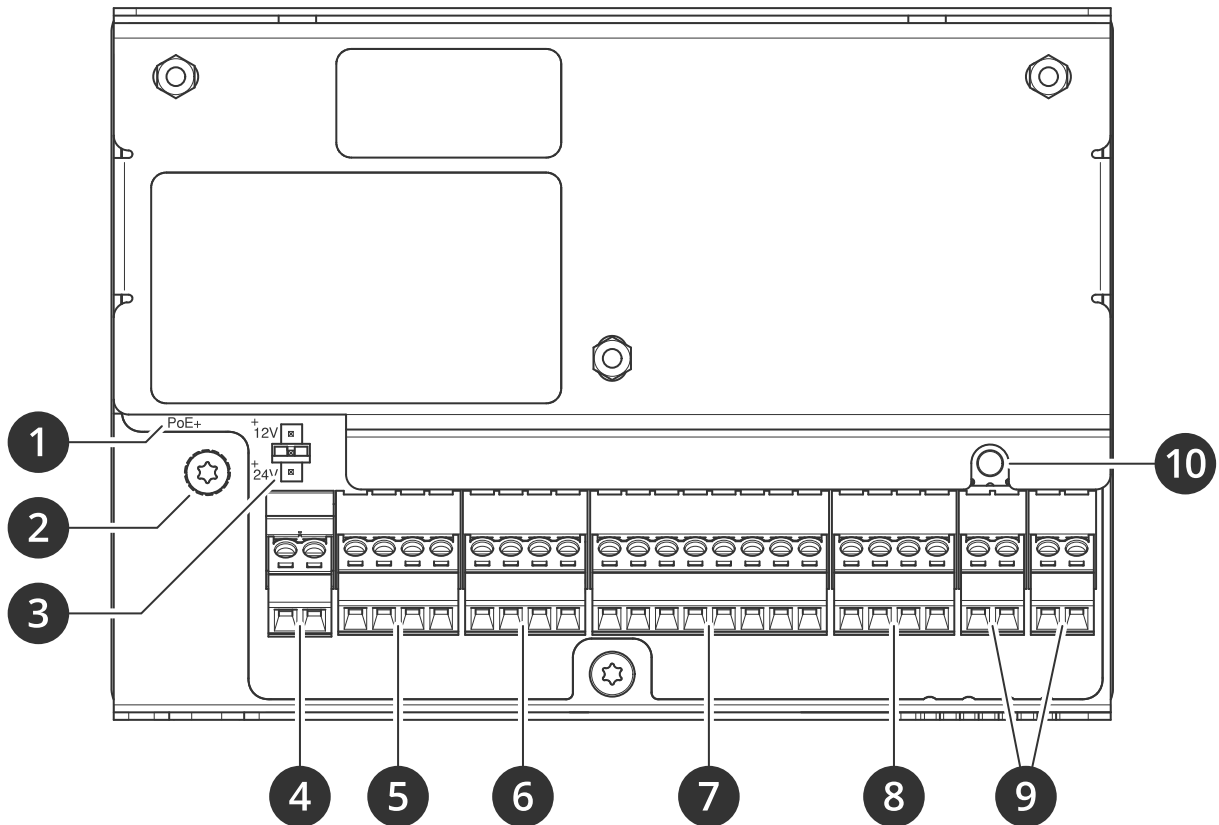
## AxisデバイスID

デバイスIDの信頼性を確立するには、デバイスの出所を確認できることが鍵となります。Axis Edge Vaultを搭載したデバイスには、生産工程で、工場でのプロビジョニングされ、国際規格(IEEE 802.1AR)に準拠した一意のAxisデバイスID証明書が割り当てられます。これがデバイスの出所を証明するパスポートのような役割を果たします。デバイスIDは、Axisルート証明書により署名された証明要素として、セキュリティで保護されたキーストアに安全かつ永続的に格納されます。お客様のITインフラストラクチャーでデバイスIDを活用し、装置のセキュアな自動化オンボーディングや、装置のセキュアな識別に役立てることができます。

Axis装置のサイバーセキュリティ機能の詳細については、[axis.com/learning/white-papers/](https://axis.com/learning/white-papers/)にアクセスし、サイバーセキュリティを検索してください。

仕様

製品概要



- 1 ネットワーク コネクター
- 2 アース位置
- 3 リレージャンパー
- 4 電源コネクター
- 5 リレーコネクタ
- 6 ドアコネクタ
- 7 リーダーコネクター
- 8 補助コネクタ
- 9 外部コネクタ
- 10 コントロールボタン

LEDインジケータ

LED	カラー	説明
ステータス	緑	正常動作であれば緑色に点灯します。
	オレンジ	起動時、設定の復元時に点灯します。
	赤	アップグレードに失敗した場合に、ゆっくり点滅します。



ネットワーク	緑	100 Mbit/sネットワークに接続している場合、点灯します。ネットワークパケットを送受信した場合、点滅します。
	オレンジ	10 Mbit/sネットワークに接続している場合、点灯します。ネットワークパケットを送受信した場合、点滅します。
	消灯	ネットワーク接続なし。
電力	緑	正常動作。
	オレンジ	ファームウェアアップグレード中は緑とオレンジで交互に点滅します。
リレー	緑	リレーアクティブ。 <sup>1</sup>
	消灯	リレーが無効です。

1. リレーが有効です。COMがNOに接続すると、リレーが有効になります。

## ボタン

### コントロールボタン

コントロールボタンは、以下の用途で使用します。

- 製品を工場出荷時の設定にリセットする。を参照してください。

## コネクタ

### ネットワークコネクタ

Power over Ethernet Plus (PoE+) 対応RJ45イーサネットコネクタ

UL : Power over Ethernet (PoE) は、44~57 V DC、15.4 W/30 Wを提供できるEthernet IEEE 802.3af/802.3at Type 1 Class 3、またはPower over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4有限電源インジェクタによって供給される必要があります。Power over Ethernet (PoE) は、AXIS T8133 Midspan 30 W 1-portが搭載されたULによって評価されています。

### 電源の優先順位

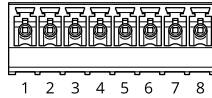
本装置は、PoEまたはDC入力から電源を供給できます。およびを参照してください。

- 装置に電源が供給されていない状態でPoEとDCの両方を接続すると、PoEが電源供給に使用されます。
- PoEとDCの両方が接続されており、現在はPoEが電源を供給しています。PoEが失われた場合、本装置は再起動せずにDCを使用して電源を供給します。
- PoEとDCの両方が接続されており、現在はDCが電源を供給しています。DCが失われた場合、本装置は再起動し、PoEを使用して電源を供給します。
- 起動時にDCが使用されている場合、装置の起動後にPoEが接続されても、電源供給にDCが使用されます。
- 起動時にPoEが使用されている場合、装置の起動後にDCが接続されても、電源供給にPoEが使用されます。

### リーダーコネクタ

リーダーとの通信用のOSDPおよびWiegandの両プロトコルに対応する8ピンターミナルブロック1台。

最大2台のOSDPリーダー (マルチドロップ) または1台のWiegandリーダーを接続できます。12 V DCでの500 mAは、ドアコントローラーに接続されたすべてのリーダーのために予約されています。



## 1台のOSDPリーダー用に設定

機能	ピン	注	仕様
DCアース (GND)	1		0 V DC
DC出力 (+12 V)	2	リーダーに電源を供給します。	12 V DC、最大500 mA
A	3	ハーフデュプレックス	
B	4	ハーフデュプレックス	

## 2台のOSDPリーダー用に設定 (マルチドロップ)

機能	ピン	注	仕様
DCアース (GND)	1		0 V DC
DC出力 (+12 V)	2	両方のリーダーに電力を供給します。	両方のリーダーに合わせて12 V DC、最大500 mA
A	3	ハーフデュプレックス	
B	4	ハーフデュプレックス	

### 重要

- ・ コントローラーからリーダーに電力を供給する場合、適格なケーブル長は最大200 mです。Axisリーダーについてのみ検証済み。
- ・ コントローラー経由でリーダーが給電されていない状況下では、シールド付きツイストペア1本、AWG 24、120オームインピーダンスというケーブル要件が満たされている場合、リーダーデータの適格なケーブル長は最大1000 m (3280.8フィート) となります。Axisリーダーについてのみ検証済み。

## 1台のWiegandリーダー用に設定済み

機能	ピン	注	仕様
DCアース (GND)	1		0 V DC
DC出力 (+12 V)	2	リーダーに電源を供給します。	12 V DC、最大500 mA
D0	3		
D1	4		
LED 1	5	赤LED	
LED 2	6	緑LED	

いたずら	7	デジタル入力 - 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。	0~30 V DC (最大)
ブザー	8	デジタル出力 - リレーなど、誘導負荷とともに使用する場合は、過渡電圧から保護するために、ダイオードを負荷と並列に接続します。	0~30 V DC (最大)、オープンドレイン、100 mA

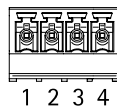
### 重要

- ・ コントローラーからリーダーに電力を供給する場合、適格なケーブル長は最大150 mです。
- ・ コントローラー経由でリーダーが給電されていない状況下では、AWG 22というケーブル要件が満たされている場合、リーダーデータの適格なケーブル長は最大150 m (500フィート) となります。

### ドアコネクタ

ドア監視装置用4ピンターミナルブロック1台 (デジタル入力)。

ドアモニターは終端抵抗器を使用した監視に対応しています。接続が中断されると、アラームがトリガーされます。状態監視入力を使用するには、終端抵抗器を設置します。状態監視入力の接続図を使用します。を参照してください。



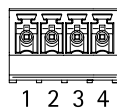
機能	ピン	メモ	仕様
DCアース	1, 3		0 V DC
入力	2, 4	ドアモニターとの通信対象。デジタル入力/状態監視入力 - 有効にするにはピン1または3にそれぞれ接続し、無効にする場合はフロート状態 (未接続) のままにします。	0~30 V DC (最大)

### 重要

AWG 24のケーブル要件を満たす場合、ケーブルの長さは最大200 m (656フィート) です。

### リレーコネクタ

ロックやゲートへのインターフェースなどの制御に使用できるフォームCリレー用の1台の4ピンターミナルブロックです。



機能	ピン	メモ	仕様
DCアース (GND)	1		0 V DC
NO	2	Normally Open。 リレー装置の接続用。NOとDCアースの間にフェイルセキアロックを接続します。 ジャンパーが使用されていない場合、2つのリレーピンは回路の残りの部分から電気的に分離されています。	最大電流 = 2 A 最大電圧 = 30 V DC
COM	3	コモン	
NC	4	Normally Closed。 リレー装置の接続用。NCとDCアースの間にフェイルセーフロックを接続します。 ジャンパーが使用されていない場合、2つのリレーピンは回路の残りの部分から電気的に分離されています。	

### リレー電源ジャンパー

リレー電源ジャンパーが取り付けられている場合、12 V DCまたは24 V DCをリレーCOMにピンに接続します。これはGNDピンとNOピン間、もしくはGNDピンとNCピン間のロックに接続するために使用できます。

電源	12 V DCでの最大電力	24 V DCでの最大電力
DC入力	1 600 mA	800 mA
PoE	900 mA	450 mA

### 注意

ロックに極性がない場合は、外部フライバックダイオードを追加することをお勧めします。

### 補助コネクタ

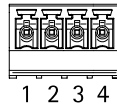
補助コネクタに外部装置を接続し、動体検知、イベントトリガー、アラーム通知などと組み合わせて使用することができます。補助コネクタは、0 V DC基準点と電力 (DC出力) に加えて、以下へのインターフェースを提供します。

**デジタル入力** - 開回路と閉回路の切り替えが可能な装置 (PIRセンサー、ドア/窓の接触、ガラス破損検知器など) を接続するための入力です。

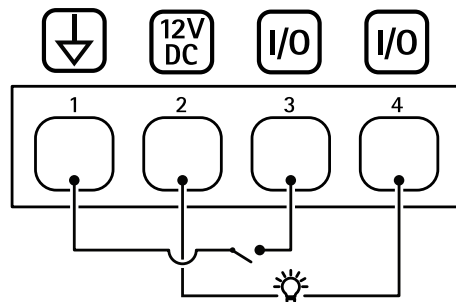
**状態監視入力** - デジタル入力のいたづらを検知する機能が有効になります。

**デジタル出力** - リレーやLEDなどの外部装置を接続します。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースまたは製品のWebページから起動できます。

4ピンターミナルブロック



機能	ピン	メモ	仕様
DCアース	1		0 V DC
DC出力	2	補助装置の電源供給に使用できます。 注:このピンは、電源出力としてのみ使用できます。	12 V DC 最大負荷 = 合計50 mA
設定可能 (入力または出力)	3-4	デジタル入力/状態監視入力 - 有効にするにはピン1に接続し、無効にする場合はフロート状態 (未接続) のままにします。状態監視を使用するには、終端抵抗器を設置します。抵抗器を接続する方法については、接続図を参照してください。	0~30 V DC (最大)
		デジタル出力 - アクティブ時はピン1 (DCアース) に内部で接続し、非アクティブ時はフロート状態 (未接続) になります。リレーなどの誘導負荷と共に使用する場合は、電圧過渡から保護するために、負荷と並列にダイオードを接続してください。I/Oは、内部12 V DC出力 (PIN 2) が使用されている場合、12 V DC、50 mA (複合最大) の外部負荷を駆動することができます。オープンドレイン接続を外部電源と組み合わせて使用する場合、I/Oはそれぞれ0~30 V DCで100 mAのDC電源供給に対応できます。	0~30 V DC (最大)、オープンドレイン、100 mA



- 1 DCアース
- 2 DC出力 12V
- 3 I/O (入力として設定)
- 4 I/O (出力として設定)

### 外部コネクタ

ガラスの破壊検知や火災検知などの外部装置で使用する2台の2ピンターミナルブロックです。

UL：このコネクタは、盗難または火災警報用途向けとしてはULによって評価されていません。



## 仕様

機能	ピン	メモ	仕様
DCアース	1		0 V DC
いたずら	2	デジタル入力 - 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。	0~30 V DC (最大)



機能	ピン	メモ	仕様
DCアース	1		0 V DC
アラーム	2	デジタル入力 - 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。	0~30 V DC (最大)

### 電源コネクタ

DC電源入力用2ピンターミナルブロック。定格出力が $\leq 100$  W以下または $\leq 5$  A以下の安全特別低電圧 (SELV) に準拠した有限電源 (LPS) を使用してください。



機能	ピン	メモ	仕様
DCアース (GND)	1		0 V DC
DC入力	2	Power over Ethernetを使用しないときの装置への電源供給用。 注:このピンは、電源入力としてのみ使用できません。	12 V DC、最大36 W

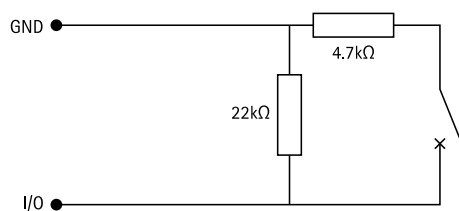
UL : アプリケーションに応じて適切な定格で、UL 603の認定を受けた電源によって供給されるDC電源。

### 監視入力

状態監視入力を使用するには、下図に従って終端抵抗器を設置します。

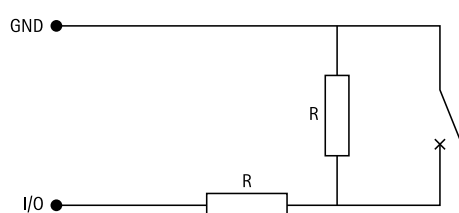
#### パラレルファースト接続

抵抗器の値は 4.7 k $\Omega$  及び 22 k $\Omega$  である必要があります。



## 最初の直列接続

抵抗器の値は同じで、可能な値は $1\text{k}\Omega$ 、 $2.2\text{k}\Omega$ 、 $4.7\text{k}\Omega$ 、 $10\text{k}\Omega$ です。



## 注

シールド付きツイストケーブルを使用することをお勧めします。シールドを $0\text{VDC}$ に接続します。

### トラブルシューティング

#### 工場出荷時の設定にリセットする

##### 重要

工場出荷時の設定へのリセットは慎重に行ってください。工場出荷時の設定へのリセットを行うと、IPアドレスを含むすべての設定が工場出荷時の値にリセットされます。

本製品を工場出荷時の設定にリセットするには、以下の手順に従います。

1. 本製品の電源を切ります。
2. コントロールボタンを押した状態で電源を再接続します。を参照してください。
3. ステータスLEDが再びオレンジ色に変わるまで、コントロールボタンを押し続けます (25秒間)。
4. コントロールボタンを放します。プロセスが完了すると、ステータスLEDが緑色に変わります。ネットワーク上にDHCPサーバーがない場合、装置IPアドレスは以下のいずれかにデフォルト設定されます。
  - **AXIS OS 12.0以降の装置**：リンクローカルアドレスサブネット (169.254.0.0/16) から取得
  - **AXIS OS 11.11以前の装置**：192.168.0.90/24
5. インストールおよび管理ソフトウェアツールを使用して、IPアドレスの割り当て、パスワードの設定、製品へのアクセスを行います。

装置のwebインターフェースを使用して、各種パラメーターを工場出荷時の設定に戻すこともできます。**[Maintenance (メンテナンス) > Factory default (工場出荷時の設定)]**に移動し、**[Default (デフォルト)]**をクリックします。

#### AXIS OSのオプション

Axisは、アクティブトラックまたは長期サポート (LTS) トラックのどちらかに従って、装置のソフトウェアの管理を提供します。アクティブトラックでは、最新の製品機能すべてに常時アクセスできますが、LTSトラックの場合、バグフィックスやセキュリティ更新に重点を置いた定期的リリースが提供される固定プラットフォームを使用します。

最新の機能にアクセスする場合や、Axisのエンドツーエンドシステム製品を使用する場合は、アクティブトラックのAXIS OSを使用することをお勧めします。最新のアクティブトラックに対して継続的な検証が行われないサードパーティの統合を使用する場合は、LTSトラックをお勧めします。LTSにより、大きな機能的な変更や既存の統合に影響を与えることなく、サイバーセキュリティを維持することができます。Axis装置のソフトウェア戦略の詳細については、[axis.com/support/device-software/](https://axis.com/support/device-software/)にアクセスしてください。

#### AXIS OSの現在のバージョンを確認する

装置の機能はAXIS OSによって決まります。問題のトラブルシューティングを行う際は、まずAXIS OSの現在のバージョンを確認することをお勧めします。最新バージョンには、特定の問題の修正が含まれていることがあります。

AXIS OSの現在のバージョンを確認するには:

1. 装置のwebインターフェース > **[Status (ステータス)]** に移動します。
2. **[Device info (デバイス情報)]** で、AXIS OSのバージョンを確認します。



### AXIS OSをアップグレードする

#### 重要

- ・ 事前設定済みの設定とカスタム設定は、装置のソフトウェアのアップグレード時に保存されます(その機能が新しいAXIS OSで利用できる場合)。ただし、この動作をAxis Communications ABが保証しているわけではありません。
- ・ アップグレードプロセス中は、装置を電源に接続したままにしてください。

#### 注

アクティブトラックのAXIS OSの最新バージョンで装置をアップグレードすると、製品に最新機能が追加されます。アップグレードする前に、AXIS OSと共に提供されるアップグレード手順とリリースノートを必ずお読みください。AXIS OSの最新バージョンとリリースノートについては、[axis.com/support/device-software/](https://axis.com/support/device-software/)にアクセスしてください。

#### 注

データベースのユーザーやグループ、認証情報、その他のデータの更新は、AXIS OSのアップグレード後に行われるため、最初の起動が完了するまで数分かかることがあります。必要な時間はデータの量によって異なります。

1. AXIS OSのファイルをコンピューターにダウンロードします。これらのファイルは[axis.com/support/device-software/](https://axis.com/support/device-software/)から無料で入手できます。
2. デバイスに管理者としてログインします。
3. **[Maintenance (メンテナンス)] > [AXIS OS upgrade (AXIS OSのアップグレード)]**に移動し、**[Upgrade (アップグレード)]**をクリックします。

アップグレードが完了すると、製品は自動的に再起動します。

4. 製品の再起動後、Webブラウザのキャッシュをクリアします。

### 技術的な問題、ヒント、解決策

このページで解決策が見つからない場合は、[axis.com/support/](https://axis.com/support/)のトラブルシューティングセクションに記載されている方法を試してみてください。

#### AXIS OSのアップグレード時の問題

---

AXIS OSのアップグレードに失敗する	アップグレードに失敗した場合、装置は前のバージョンを再度読み込みます。最も一般的な理由は、AXIS OSの間違ったファイルがアップロードされた場合です。装置に対応したAXIS OSのファイル名であることを確認し、再試行してください。
AXIS OSのアップグレード後の問題	アップグレード後に問題が発生する場合は、 <b>[Maintenance (メンテナンス)]</b> ページから、以前にインストールされたバージョンにロールバックします。

#### IPアドレスの設定で問題が発生する

---

デバイスが別のサブネット上にある	デバイス用のIPアドレスと、デバイスへのアクセスに使用するコンピューターのIPアドレスが異なるサブネットにある場合は、IPアドレスを設定することはできません。ネットワーク管理者に連絡して、適切なIPアドレスを取得してください。
------------------	---

## トラブルシューティング

---

IPアドレスが別のデバイスで使用されている	デバイスをネットワークから切断します。pingコマンドを実行します (コマンドウィンドウまたはDOSウィンドウで、pingコマンドとデバイスのIPアドレスを入力します)。 <ul style="list-style-type: none"><li>もし、「Reply from &lt;IP address&gt;: bytes=32; time=10...」という応答を受取った場合は、ネットワーク上の別のデバイスでそのIPアドレスがすでに使われている可能性があります。ネットワーク管理者から新しいIPアドレスを取得し、デバイスを再度インストールしてください。</li><li>もし、「Request timed out」が表示された場合は、AxisデバイスでそのIPアドレスを使用できます。この場合は、すべてのケーブル配線をチェックし、デバイスを再度インストールしてください。</li></ul>
同じサブネット上の別のデバイスとIPアドレスが競合している可能性がある	DHCPサーバーによって動的アドレスが設定される前は、Axisデバイスは静的IPアドレスを使用します。つまり、デフォルトの静的IPアドレスが別のデバイスでも使用されていると、デバイスへのアクセスに問題が発生する可能性があります。

### ブラウザーから装置にアクセスできない

---

ログインできない	HTTPSが有効になっているときは、ログインを試みるときに正しいプロトコル (HTTP または HTTPS) を使用していることを確認してください。場合によっては、ブラウザーのアドレスフィールドに手動でhttpまたはhttpsを入力する必要があります。rootアカウントのパスワードを忘れた場合は、装置を工場出荷時の設定にリセットする必要があります。を参照してください。
DHCPによってIPアドレスが変更された	DHCPサーバーから取得したIPアドレスは動的なアドレスであり、変更されることがあります。IPアドレスが変更された場合は、AXIS IP UtilityまたはAXIS Device Managerを使用してデバイスのネットワーク上の場所を特定してください。デバイスのモデルまたはシリアル番号、あるいはDNS名 (設定されている場合) を使用してデバイスを識別します。必要に応じて、静的IPアドレスを手動で割り当てることができます。手順については、 <a href="http://axis.com/support">axis.com/support</a> にアクセスしてください。
IEEE 802.1X使用時の証明書エラー	認証を正しく行うには、Axisデバイスの日付と時刻をNTPサーバーと同期させなければなりません。[System (システム) > Date and time (日付と時刻)] に移動します。

### 装置にローカルにアクセスできるが、外部からアクセスできない

---

装置に外部からアクセスする場合は、以下のいずれかのWindows®向けアプリケーションを使用することをお勧めします。

- AXIS Companion：無料で使用でき、最小限の監視が必要な小規模システムに最適です。
- AXIS Camera Station 5：小規模から中規模のシステムに最適です。30日間の試用版を無料で使用できます。
- AXIS Camera Station Pro：小規模から中規模のシステムに最適です。90日間の試用版を無料で使用できます。

手順とダウンロードについては、[axis.com/vms](http://axis.com/vms)にアクセスしてください。

### MQTTオーバSSLを使用してポート8883経由で接続できない

---

ファイアウォールによって、ポート8883が安全ではないと判断されたため、ポート8883を使用するトラフィックがブロックされています。	場合によっては、サーバー/ブローカーによってMQTT通信用に特定のポートが提供されていない可能性があります。この場合でも、HTTP/HTTPSトラフィックに通常使用されるポート経由でMQTTを使用できる可能性があります。 <ul style="list-style-type: none"><li>• サーバー/ブローカーが、通常はポート443経由で、WebSocket/WebSocket Secure (WS/WSS) をサポートしている場合は、代わりにこのプロトコルを使用してください。サーバー/ブローカープロバイダーに問い合わせ、WS/WSSがサポートされているかどうか、どのポートと基本パスを使用するかを確認してください。</li><li>• サーバー/ブローカーがALPNをサポートしている場合、ポート443などのオープンポート経由でMQTTをネゴシエーションできます。ALPNがサポートされているかどうか、どのALPNプロトコルとポートを使用するかについては、サーバー/ブローカープロバイダーに確認してください。</li></ul>
--	---

### サポートに問い合わせる

さらにサポートが必要な場合は、[axis.com/support/](https://axis.com/support/)にアクセスしてください。

