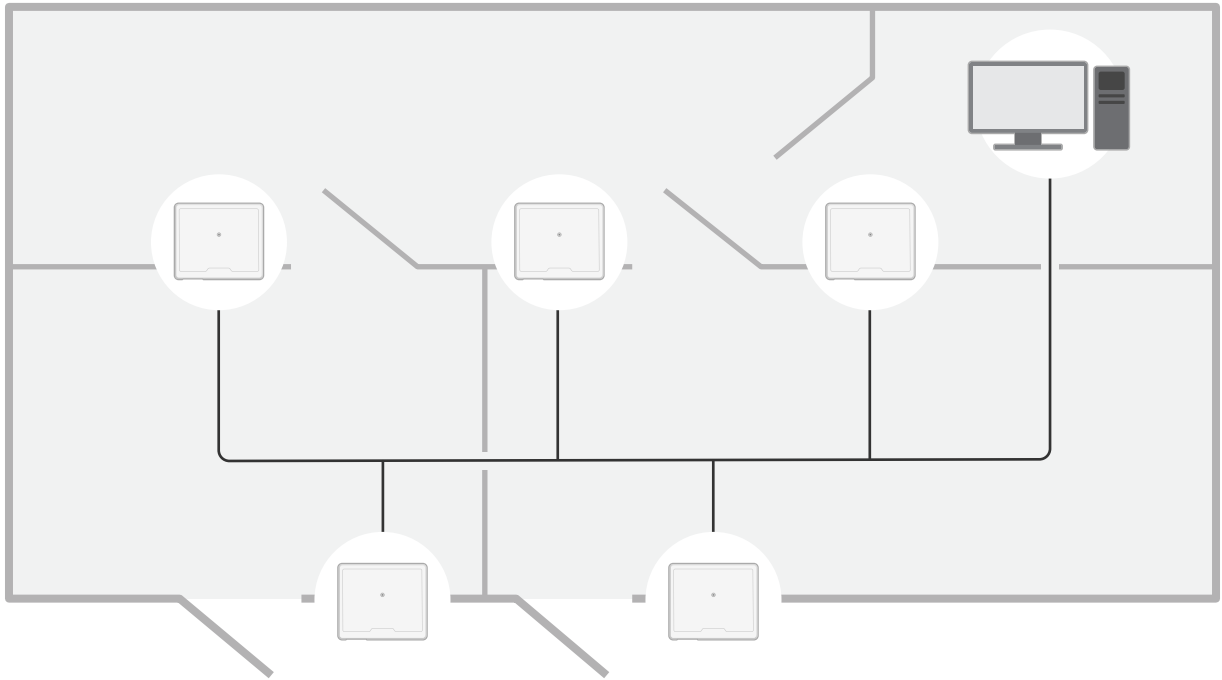


AXIS A1210 Network Door Controller
AXIS A1210-B Network Door Controller

ユーザーマニュアル

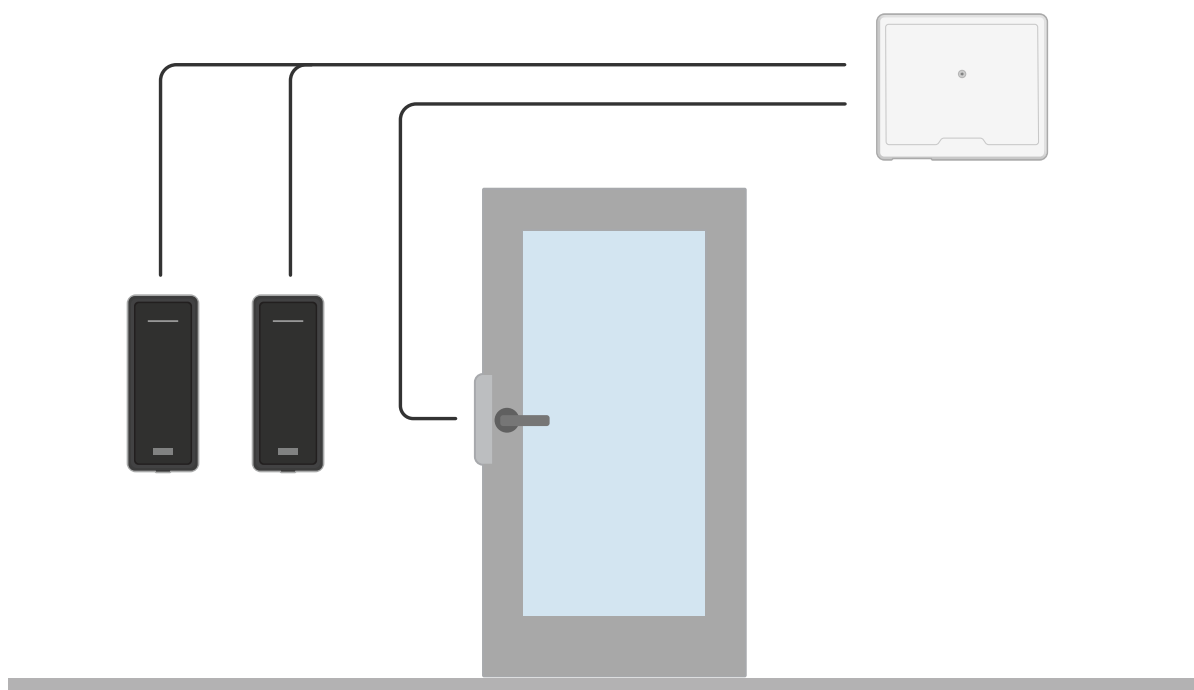
ソリューションの概要	3
はじめに	5
ネットワーク上の装置を検索する	5
装置のWebページを開きます	5
rootアカウントの新しいパスワードを設定する	5
安全なパスワード	5
ファームウェアが改ざんされていないことを確認する	6
Webページの概要	6
設置	7
装置を構成する	8
装置インターフェース	9
ステータス	9
アクセスコントロール	10
システム	10
保守	20
詳細情報	22
セキュリティ	22
仕様	23
製品の概要	23
UL 294に準拠するための要件	23
LEDインジケータ	26
ボタン	27
コネクタ	27
トラブルシューティング	33
工場出荷時の設定にリセットする	33
ファームウェアオプション	33
現在のファームウェアバージョンの確認	33
ファームウェアのアップグレード	33
技術的な問題、ヒント、解決策	34
サポートに問い合わせる	35

ソリューションの概要



ネットワークドアコントローラーは、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装置です。最大2つのリーダーに給電したり制御したりできます。

はじめに

ネットワーク上の装置を検索する

Windows®でAxis装置を探してIPアドレスの割り当てを行う方法については、AXIS IP UtilityまたはAXIS Device Managerを使用してください。いずれのアプリケーションも無料で、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装置へのアクセス方法を参照してください。*

ブラウザーサポート

以下のブラウザーで装置を使用できます。

	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、**[設定] > [Safari] > [詳細] > [Experimental Features]** に移動し、**[NSURLSession Websocket]** を無効にします。

推奨ブラウザーの詳細については、*AXIS OSポータル*にアクセスしてください。

装置のWebページを開きます

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。初めて装置にアクセスする場合は、rootパスワードを設定する必要があります。5 ページ*rootアカウントの新しいパスワードを設定する*を参照してください。

rootアカウントの新しいパスワードを設定する

デフォルトの管理者ユーザー名はrootです。rootアカウントにはデフォルトのパスワードはありません。パスワードは、装置に初めてログインしたときに設定します。

1. パスワードを入力します。安全なパスワードを設定する手順に従います。5 ページ*安全なパスワード*を参照してください。
2. パスワードを再入力して、スペルを確認します。
3. **[Add user (ユーザーの追加)]** をクリックします。

重要

rootアカウントのパスワードを忘れた場合は、33ページ*工場出荷時の設定にリセットする*にアクセスし、説明に従って操作してください。

安全なパスワード

重要

Axis装置は、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装置を保護するために、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。

装置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装置は、さまざまなタイプのインストールで使用される可能性があることから、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、次のことを強く推奨します。

- 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)。

ファーム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ファームウェア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。33ページ工場出荷時の設定にリセットする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. 装置を設定し、インストールします。

Webページの概要

このビデオでは、装置インターフェースの概要を説明します。



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/?&pid=74266§ion=webpage-overview

Axis装置のwebインターフェース

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§ion=solution-overview

装置を構成する

装置を構成する











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のソリューションを参照してください。

装置インターフェース

装置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。

-  メインメニューの表示/非表示を切り取ります。
-  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。
 -  **Change user (ユーザーの変更)**: 現在のユーザーをログアウトさせ、新しいユーザーにログインさせます。
 -  **Log out (ログアウト)**: 現在のユーザーをログアウトさせます。
-  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**: ファームウェア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。
 - Legacy device interface (従来の装置インターフェース)**: 装置インターフェースを従来の装置インターフェースに変更します。

ステータス

NTP sync (NTP同期)

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): クリックすると、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。

装置情報

ファームウェア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。

ファームウェアのアップグレード: クリックすると、[Maintenance (メンテナンス)] ページに移動し、ファームウェアのアップグレードができるようになります。

アクセスコントロール

アラーム

Device motion (デバイスの動き): ドアコントローラーの装置の動きが検知されたときに、システムでアラームをトリガーすることが、デフォルトで有効になっています。

ケーシング開放: ドアコントローラーのケーシングの開放が検知されたときに、システムでアラームをトリガーすることが、デフォルトで有効になっています。

External tamper (外部からのいたずら): これは、デフォルトでは有効になっていません。オンにすると、外部からのいたずらが検知され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、外部キャビネットが開閉されたときです。

- **Supervised input (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 Ω parallel resistor and a 4.7 K Ω serial resistor (22 k Ω の並列抵抗器と4.7 k Ω 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

Upgrade readers (リーダーのアップグレード): クリックすると、リーダーが新しいファームウェアバージョンにアップグレードされます。サポートされているリーダーは、オンラインの場合にのみアップグレードできます。

システム

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。

- **Automatic date and time (manual NTS KE servers) (日付と時刻の自動設定 (手動NTS KEサーバー)):** DHCPサーバーに接続された安全な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。
- **Automatic date and time (NTP servers using DHCP) (日付と時刻の自動設定 (DHCPを使用したNTPサーバー)):** DHCPサーバーに接続された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。
- **Automatic date and time (manual NTP servers) (日付と時刻の自動設定 (手動NTPサーバー)):** 選択した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。
- **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。夏時間と標準時間に合わせて、時刻が自動的に調整されます。

装置インターフェース

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。

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。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 address (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、静的な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。

Subnet mask (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。

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。

Hostname (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。

Hostname (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。ホスト名は、サーバーレポートとシステムログで使用されます。使用できる文字は、A~Z、a~z、0~9、-、_です。

DNS servers (DNSサーバー)

Assign DNS automatically (DNS 自動割り当て): ネットワークルータ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およびHTTPS

装置インターフェース

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。

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。暗号化された情報の交換は、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証明書の使用により制御されます。

装置で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。

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。ポート80または1024~65535の範囲の任意のポートを使用できます。管理者としてログインしている場合は、1~1023の範囲の任意のポートを入力することもできます。この範囲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。ポート443または1024~65535の範囲の任意のポートを使用できます。管理者としてログインしている場合は、1~1023の範囲の任意のポートを入力することもできます。この範囲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®: オンにすると、ネットワーク上で自動検出が可能になります。

Bonjour name (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。デフォルト名は装置名とMACアドレスです。

UPnP®: オンにすると、ネットワーク上で自動検出が可能になります。

UPnP name (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。デフォルト名は装置名とMACアドレスです。

WS-Discovery: オンにすると、ネットワーク上で自動検出が可能になります。

One-Click Cloud Connection (ワンクリッククラウド接続)

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を参照してください。

Allow O3C (O3Cを許可):

- **One-click (ワンクリック):** デフォルトの設定です。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、装置はO3Cサービスから切断されます。装置に登録すると、[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。
- **Always (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。装置が登録されると、O3Cサービスに接続したままになります。装置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 (なし):** 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。

Host (ホスト): プロキシサーバーのアドレスを入力します。

Port (ポート): アクセスに使用するポート番号を入力します。

Login (ログイン) と Password (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)

- **Basic (ベーシック):** この方法は、HTTP用の最も互換性のある認証方式です。ユーザー名とパスワードを暗号化せずにサーバーに送信するため、**Digest (ダイジェスト)** 方式よりも安全性が低くなります。
- **Digest (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。
- **Auto (オート):** このオプションを使用すると、装置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。**Digest (ダイジェスト)** 方式が**Basic (ベーシック)** 方式より優先されます。

Owner authentication key (OAK) (所有者認証キー、OAK): [Get key (キーを取得)] をクリックして、所有者認証キーを取得します。これは、装置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 (パブリック)] です。
 - **Write community (書き込みコミュニティ):** サポートされている(読み取り専用のものを除く)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。デフォルト値は [write (書き込み)] です。
 - **Activate traps (トラップの有効化):** オンにすると、トラップレポートが有効になります。装置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。装置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に変更するか、SNMPをオフにすると、トラップは自動的にオフになります。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。
 - **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):** 装置の起動時にトラップメッセージを送信します。
 - **Warm start (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。
 - **Authentication failed (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、HTTPSをアクティブにし、パスワードをHTTPSを介して送信することをお勧めします。これにより、権限のない人が暗号化されていないSNMP v1およびv2cトラップにアクセスすることも防止できます。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。
 - **Password for the account "initial" (「initial」アカウントのパスワード):** 「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をアクティブにせずパスワードを送信できますが、推奨しません。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

装置インターフェース

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、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。

Connected clients (接続されたクライアント)

装置に接続しているすべてのクライアントが一覧表示されます。



更新: クリックすると、リストを更新できます。

セキュリティ

証明書

証明書は、ネットワーク上の装置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。装置には、いくつかのCA証明書が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:

- 証明書形式: .PEM、.CER、.PFX
- 秘密鍵形式: PKCS#1、PKCS#12

重要

装置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。



リスト内の証明書をフィルターします。



証明書の追加: クリックして証明書を追加します。



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。

IEEE 802.1x

IEEE 802.1xはポートを使用したネットワークへの接続を制御するIEEEの標準規格で、有線およびワイヤレスのネットワーク装置を安全に認証します。IEEE 802.1xは、EAP (Extensible Authentication Protocol) 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といったRADIUSサーバーです。

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、装置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。

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 certificate (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、装置は、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 identity (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 version (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 を使用): IEEE 802.1xプロトコルを使用する場合に選択します。

Prevent brute-force attacks (ブルートフォース攻撃を防ぐ)

Blocking (ブロック): オンにすると、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。ページレベルと装置レベルの両方で許容される失敗の数を設定できます。

IP address filter (IPアドレスフィルター)

Use filter (フィルターを使用する): 装置へのアクセスを許可するIPアドレスを絞り込む場合に選択します。

Policy (ポリシー): 特定のIPアドレスに対してアクセスを [Allow (許可)] するか [Deny (拒否)] するかを選択します。

Addresses (アドレス): 装置へのアクセスを許可するIP番号と拒否するIP番号を入力します。CIDR形式を使用できます。

カスタム署名されたファームウェア証明書

装置インターフェース

Axisのテストファームウェアまたは他のカスタムファームウェアを装置にインストールするには、カスタム署名付きファームウェア証明書が必要です。証明書は、ファームウェアが装置の所有者とAxisの両方によって承認されたと証明します。ファームウェアは、一意のシリアル番号とチップIDで識別される特定の装置でのみ実行できます。Axisが署名を行う鍵を保有しているため、カスタム署名付きファームウェア証明書はAxisのみが作成できます。

[Install (インストール)] をクリックして、証明書をインストールします。ファーム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。

ユーザー

+ **Add user (ユーザーを追加):** クリックして、新規ユーザーを追加します。最大100人のユーザーを追加できます。

Username (ユーザー名): 一意のユーザー名を入力します。

New password (新しいパスワード): ユーザー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。

Role (役割):

- **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。管理者は他のユーザーを追加、更新、削除もできます。
- **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 (システム設定)]。
 - アプリを追加しています。
- **ビューア:** 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 user (ユーザーの更新): ユーザーのプロパティを編集します。

ユーザーの削除 (Delete user): ユーザーを削除します。rootユーザーは削除できません。

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。これは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装置を接続するために、さまざまな業界で使用されています。Axis装置のファーム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、ビデオ管理システム (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。

MQTT client (MQTTクライアント)

Connect (接続): 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。

Broker (ブローカー)

Host (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。

Port (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。

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。

Password (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): クライアントIDを入力します。クライアントがサーバーに接続すると、クライアント識別子が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。

Keep alive interval (キープアライブの間隔): キープアライブの間隔を使用すると、クライアントは長時間のTCP/IPタイムアウトを待たなくても、サーバーが使用できなくなったことを検知できます。

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。

Connect message (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。

装置インターフェース

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 publication (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

+ サブスクリプションの追加: 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: サブスクライブする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

I/O ports (I/Oポート)



装置インターフェース

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。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装置インターフェースからアクティブにすることができます。

Port (ポート)

Name (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:  の場合は開回路をクリックし、  の場合は閉回路をクリックします。

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アクティブになります。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  : オンにすると、誰かがデジタルI/O装置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

Reports (レポート)

- **View the device server report (デバイスサーバーレポートを表示):** クリックして、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):** クリックしてサーバーレポートをダウンロードします。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クリックして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。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。

+

Server(サーバー): クリックして新規サーバーを追加します。

Host (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。

- RFC 3164
- RFC 5424

Protocol (プロトコル): 使用するプロトコルとポートを選択します。

- 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)

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。

保守

Restart (再起動): 装置を再起動します。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、プリインストールしなかったアプリを再インストールし、イベントやPTZ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)
- 静的なIPアドレス
- Default router (デフォルトルーター)
- Subnet mask (サブネットマスク)
- 802.1X settings (802.1Xの設定)
- O3C settings (O3Cの設定)

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

検証済みのファーム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の装置ファーム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でホワイトペーパー「署名済みファームウェア、セキュアブート、およびプライベートキーのセキュリティ」を参照してください。

Firmware upgrade (ファームウェアのアップグレード): 新しいファームウェアバージョンにアップグレードします。新しいファームウェアには、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/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):** 新しいファームウェア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以前のファームウェア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、装置は以前のファームウェアバージョンに戻されます。

Firmware rollback (ファームウェアのロールバック): 以前にインストールされたファームウェアバージョンに戻します。

詳細情報

セキュリティ

署名付きファームウェア

署名付きファームウェアは、秘密鍵を使用してファームウェア画像に署名するソフトウェアベンダーによって実施されます。ファームウェアにこの署名が添付されている場合、装置はインストールに同意する前に、ファームウェアを検証します。装置がファームウェアの完全性が損なわれていることを検知した場合、ファームウェアのアップグレードが拒否されます。

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。署名付きファームウェアの使用に基づいているため、セキュアブートを使うと、装置は認証済みのファームウェアを使用した場合のみ起動できます。

Axis Edge Vault

Axis Edge Vaultは安全な暗号計算モジュールであり、安全に保存された証明書の暗号操作に使用できます。Edge Vaultは、改ざんから保護されたストレージを提供し、各装置がそれぞれの秘密を保護できるようにします。また、より高度なセキュリティ機能を安全に実装するための基盤を築きます。

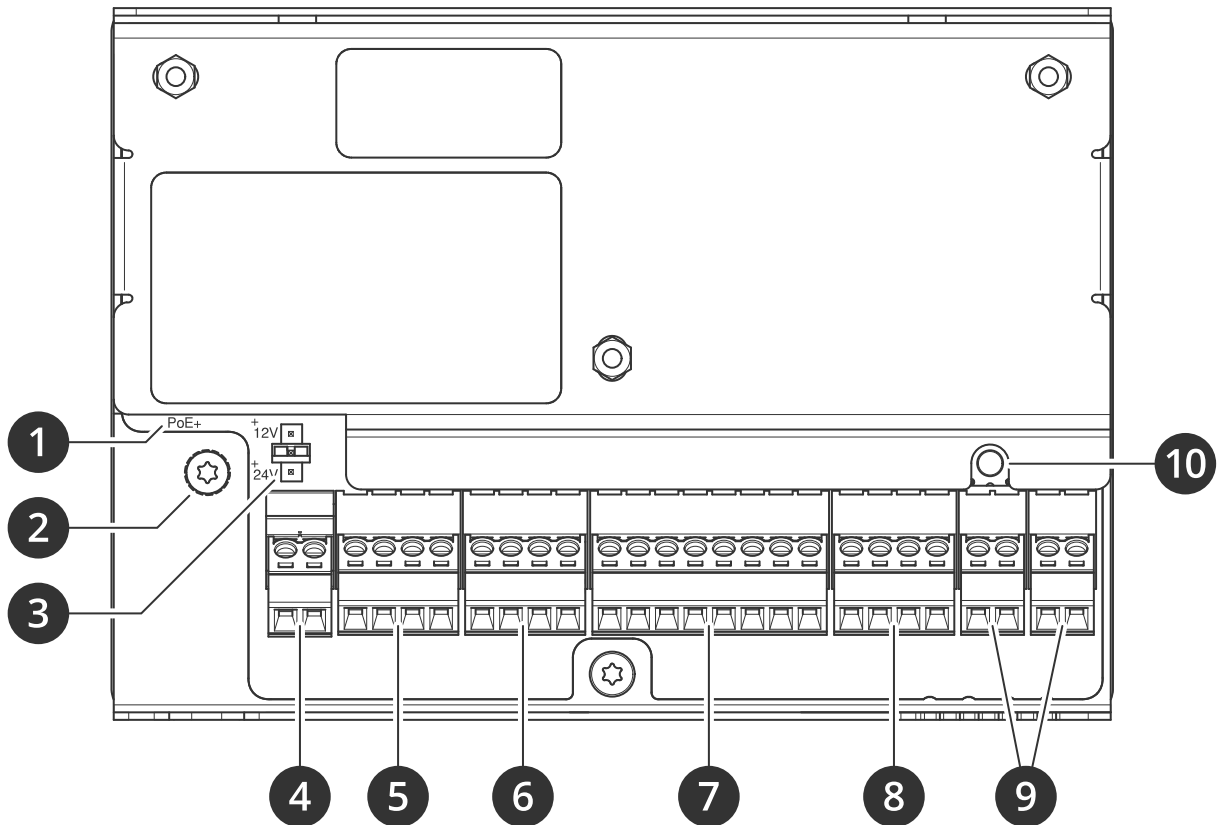
AxisデバイスID

AxisデバイスIDは、デジタルパスポートのようなもので、装置ごとに一意です。Axisルート証明書で署名された証明書として、Edge Vaultに安全かつ永続的に保存されます。AxisデバイスIDは、装置の出所を証明するように設計されており、製品のライフサイクルを通じて装置の信頼性を新たなレベルへと引き上げます。

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にアクセスし、cybersecurityを検索してください。

仕様

製品の概要



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

ULのマークが付いたテキストは、UL 294インストールでのみ有効です。

UL 294に準拠するための要件

このセクションでは、UL準拠に必要な情報と手順について説明します。UL規格に準拠した設置を行うには、本書で説明する一般的な情報および手順に加え、以下の手順に従ってください。各情報が互いに矛盾する場合、UL適合要求が常に一般的な情報や手順に取って代わります。

アクセスコントロールのパフォーマンスレベル

仕様

このセクションには、UL 294に準拠するために必要なパフォーマンスレベル情報が含まれます。

機能	レベル
破壊攻撃試験	I
セキュリティ	I
耐久性	IV
スタンバイ電源	I

サポートされるリーダー

- UL 294については、以下のリーダーとの互換性がULによって確認されています。AXIS A4020-E、AXIS A4120-E、HID Signo 20。

安全手順

- 米国電気工事規定、ANSI/NFPA 70のArticle 725.121に従って設置する必要があります。
- 本Axis製品は、工場トレーニングを受けた専門家が設置およびサービスを行う必要があります。
- 本Axis製品は、保護された敷地内(保安区域)に設置する必要があります。
- 本Axis製品は屋内に設置する必要があります。屋外での使用はULによって評価または承認されていません。
- すべての相互接続装置は、UL規格認定取得済みで、クラス2の低電圧電源制限に従っている必要があります。
- すべての電源出力はクラス2出力です。
- すべての配線方法は、ANSI/NFPA70、地域の法令および管轄する当局に従うものとします。
- UL認定アース線、14-16 AWG、黄/緑の使用を推奨します。製品のスペアパーツとして付属している非絶縁ワイヤープレッシャーリングターミナルにケーブルを圧着します。製品および使用者の安全を確保するために、適切な圧着工具と技法を使用することが重要です。
- 本Axis製品が耐用年数に達した場合は、地域の法律と規制に従って廃棄してください。本製品は、家庭用または商業用の廃棄物と一緒に廃棄しないでください。
- 本Axis製品は、スイッチで制御するレセプタクルに接続しないでください。
- バッテリー
 - 本Axis製品で使用されている3.0Vリチウムバッテリーは、UL認定コンポーネントです。(タイプ: BR2032、直径: 20 mm、メーカー: Power Glory (Omnergy)。以下のバッテリータイプも、UL認定コンポーネントです。タイプCR2032。
 - ユーザーはバッテリーを交換しないでください。バッテリーの交換が必要な場合は、訓練を受けた技術者のみが行う必要があります。
 - 使用済みバッテリーは、地域の法律や規制に従って廃棄してください。法律や規則は地域によって異なる場合があります。BR/CRリチウムバッテリーの廃棄物は、USEPAの有害廃棄物規制のリストに記載されてなく除外もされていません。リチウムバッテリーの廃棄物は、未反応または未消費のリチウムが大量に残っている場合、反応性有害廃棄物とみなされる可能性があります。使用済みリチウムバッテリーの廃棄方法については、最寄りの地方自治体の廃棄物処理担当部署にお問い合わせください。

仕様

- 動作条件

通常使用 (ULによって評価されていません)	-40° C~55° C 湿度: 20~85% RH (結露不可)
UL 294	0° C~55° C)、最大湿度85%。 いたずら検知スイッチ付きのUL規格の筐体での使用を 目的としています。

- 配線の要件
 - UL規格またはR/C AWM規格のワイヤーで、導体ゲージがAWG 22-14のものを使用する必要があります。
 - 給電装置 (PSE) またはパワーインジェクターと受電側装置 (PD) 間の接続のための最小導体ゲージは26 AWGです。
 - PoEには、最小限PoEカテゴリ5e、シールドケーブルが必要です。
 - 本製品は、米国電気工事規程の条項800、NFPA 70で規定されている屋外配線用ではありません。
- コネクター
 - 電源コネクター - ULセキュリティ用途の場合、製品は、適切な定格を有するUL 294またはUL 603認定のClass 2低電圧電源SELVおよび制限電源により給電される必要があります。
 - リレーへの外部電源 - リレーが外部電源に接続されている場合、これはUL 294認定のClass 2低電圧電源SELVおよび制限電源である必要があります。
 - ネットワークコネクター - 標準的なイーサネット配線。PoEモードB (代替A) のAXIS T8133 Midspan 30 W 1ポートから電源を供給した場合、ULによって評価済みです。
 - バッテリー入力は、リスト済みのUPSに接続するためのもので、UL 294に対するULの評価を受けていません。
 - 状態監視入力は、盗難防止向けの用途としてULによって評価されていません。
- システムに関する考慮事項
 - 監視ソフトウェアはULによって評価されてなく、補助的に使用することを目的としています。
- メンテナンス手順
 - メンテナンス手順と本Axis製品の設定方法については、ユーザーマニュアルを参照してください。
- 関連情報
 - ULによって検証されたカード形式: ISOカードMifare 1K、32ビット。
- 電源
 - **電源入力:** 10.5~28 V DC、最大36 W、10.5 Vで最大2.4 A、28 Vで最大0.9 A。
Power over Ethernet (PoE) IEEE 802.3at Type 2 Class 4、最大340 mA。バックアップ用の12 Vバッテリー。
 - **リレー:** リレーNO/NC (×2)、最大2A DC
 - **電源出力ロック:** 12/24 V DC ×2
PoE+時: 12 Vで11 W、24 Vで10 W
DC入力時: 12 Vで22.5 W、24 Vで18 W
 - **電源出力リーダー:** 12 V DC、最大6 W
 - **補助DC出力:** 12 V DC出力 ×1、最大200 mA

- 周辺機器装置 (ロック、リーダーなど) 用の合計電源容量: DC給電の場合は12 Vで2,100 mA、PoE Class 4給電の場合は12 Vで1,300 mA
- I/Oインターフェース - I/O機能
 - リーダーI/O: DC出力: 12V DC出力 (×2)、最大486 mA、設定可能な状態監視入出力 (2x2)、(デジタル入力: 0~最大30V DC、デジタル出力: 0~最大30V DC、オープンドレイン最大100 mA)
 - リーダーデータ: OSDP/RS485半二重、Wiegand
 - 補助: DC出力: 12V DC出力 (×1)、最大200 mA、設定可能な入出力 (×4)、(デジタル入力: 0~最大30V DC、デジタル出力: 0~最大30V DC、オープンドレイン最大100 mA)
 - ドア接続: ドアモニター用状態監視入力 (2x2)、REX (デジタル入力: 0~30V DC (最大))
 - 外部装置: 補助装置用の設定可能な入出力 (×2) (デジタル入力: 0~最大30V DC、デジタル出力: 0~最大30V DC、オープンドレイン最大100 mA)
- ケーブルの要件
 - コネクター用ワイヤーサイズ: CSA: AWG 28~16、CUL/UL: AWG 30~14
 - DC電源とリレー: AWG 18~16
 - イーサネットとPoE: STP CAT 5e以上
 - リーダーデータ (RS485): シールド付きツイストペア (1組)、最大1,000 mに対応
 - リーダーデータ (Wiegand): 最大150 mに対応
 - コントローラーで給電するリーダー (RS485): AWG 20-16、最大200 m (リーダーの電圧・電流入力範囲により異なる。A4020-E、A4120-Eで評価)。
 - コントローラーで給電するリーダー (Wiegand): AWG 20-16、最大150 m (リーダーの電圧・電流入力範囲により異なる)。
 - 入力としてのI/O: 最大200 mに対応

LEDインジケータ

LED	カラー	説明
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。
	無点灯	ネットワーク接続なし。
状態	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、ゆっくりと点滅。
電源	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	リレーが有効です。 ¹
	消灯	リレーが無効です。

1. 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。33ページ工場出荷時の設定にリセットするを参照してください。

コネクター

ネットワークコネクター

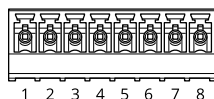
RJ45イーサネットコネクター、Power over Ethernet Plus (PoE+) 対応。

UL: Power over Ethernet (PoE) は、44~57 V DC、15.4 W / 30 Wを提供できる、UL 294認定Power over 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。

リーダーコネクター

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500 mAが、ドアコントローラーに接続されたすべてのリーダー用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	備考	仕様
DCアース (GND)	1		0 V DC
DC出力 (+12 V)	2	リーダーに電力を供給します。	12 V DC、最大500 mA
A	3	半二重	
B	4	半二重	

2台のOSDPリーダー用に設定 (マルチドロップ)

機能	ピン	備考	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	半二重	
B	4	半二重	

仕様

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。
- ・ コントローラーからリーダーに電力を供給しない場合に、以下のケーブル要件を満たす場合、リーダーデータ用の適格なケーブル長は最大1000 mです。シールド付きツイストペア (1組)、AWG 24、120 Ωインピーダンス。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	備考	仕様
DCアース (GND)	1		0 V DC
DC出力 (+12 V)	2	リーダーに電力を供給します。	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

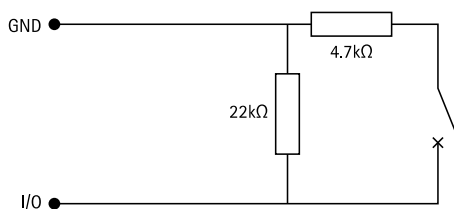
- ・ コントローラーからリーダーに電力を供給する場合、適格なケーブル長は最大150 mです。
- ・ コントローラーからリーダーに電力を供給しない場合に、以下のケーブル要件を満たす場合、リーダーデータ用の適格なケーブル長は最大150 mです。AWG 22。

状態監視入力

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。

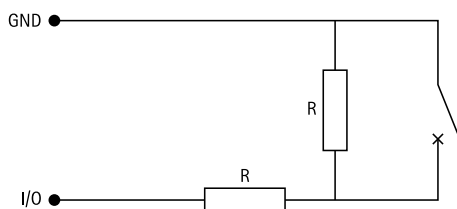
パラレルファースト接続

抵抗器の値は4.7 kΩおよび22 kΩである必要があります。



Serial first connection (シリアルファースト接続)

抵抗器の値は同じで、可能な値は1 kΩ、2.2 kΩ、4.7 kΩ、10 kΩです。



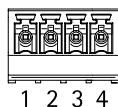
注

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 V DCに接続します。

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)。

ドアモニターのみが終端抵抗器を使用した監視をサポートします。接続が中断されると、アラームがトリガーされます。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。



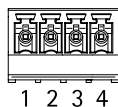
機能	ピン	備考	仕様
DCグラウンド	1, 3		0 V DC
入力	2, 4	ドアモニターとの通信用。 デジタル入力または状態監視入力 - それぞれピン1または3に接続し、動作させない場合はフロート状態 (未接続) のままにします。	0~30 V DC (最大)

重要

以下のケーブル要件を満たす場合、ケーブルの長さは最大 30 m です。AWG 24。

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	備考	仕様
DCアース (GND)	1		0 V DC

NO	2	ノーマルオープン。 リレー装置の接続用です。NOとDCアース間にフェイルセキュアロックを接続します。 ジャンパー未使用時、2つのリレーピンは他の残りの回路から直流的に絶縁されます。	最大電流 = 2 A、 最大電圧 = 30 V DC
COM	3	コモン	
NC	4	ノーマルクローズ。 リレー装置の接続用です。NCとDCグラウンド間でフェイルセーフロックを接続します。 ジャンパー未使用時、2つのリレーピンは他の残りの回路から直流的に分離されます。	

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ピン間に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	1200 mA	600 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。

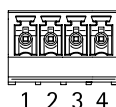
補助コネクタ

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。

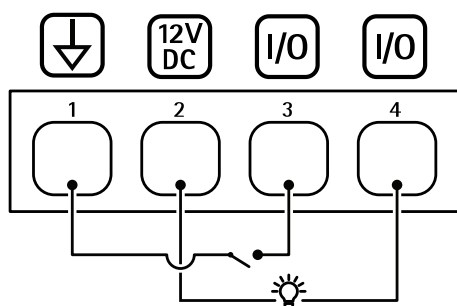
デジタル入力 - オープンサーキットとクローズサーキットの切り替えが可能な装置 (PIRセンサー、ドア/窓の接触、ガラス破損検知器など) を接続するための入力です。

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® Application Programming Interfaceまたは製品のウェブページからアクティブ化することができます。

4ピンターミナルブロック



機能	ピン	備考	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 - 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)
		デジタル出力 - アクティブ時はピン1 (DCグランド) 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、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。内部12 V DC出力 (ピン2) が使用されている場合、各I/Oは12 V DC、50 mA (最大) の外部負荷に電源を供給できます。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0~30 V DC、100 mAのDC給電を管理できます。	0~30 V DC (最大)、オープンドレイン、100 mA



- 1 DCグランド
- 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)

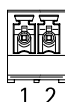
外部コネクタ

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/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。



機能	ピン	備考	仕様
DCアース	1		0 V DC
いたづら	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)

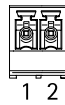


仕様

機能	ピン	備考	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100 W以下または5 A以下の安全特別低電圧 (SELV) に準拠した制限電源 (LPS) を使用してください。



機能	ピン	備考	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コントローラーへの電源供給用。 備考: 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 294またはUL 603認定電源によって供給されるDC電源。

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、以下の手順を実行します。

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。23ページ製品の概要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離します。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。これで本製品は工場出荷時の設定にリセットされました。ネットワーク上に利用可能なDHCPサーバーがない場合、デフォルトのIPアドレスは192.168.0.90になります。
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ページを使用して、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。

ファームウェアオプション

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、製品のファームウェア管理を提供します。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ファームウェア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製品のファームウェア戦略の詳細については、axis.com/support/firmwareを参照してください。

現在のファームウェアバージョンの確認

ファームウェアは、ネットワーク装置の機能を決定するソフトウェアです。問題のトラブルシューティングを行う際は、まず現在のファームウェアバージョンを確認することをお勧めします。最新のファームウェアバージョンには、特定の問題の修正が含まれていることがあります。

現在のファームウェアを確認するには、以下の手順に従います。

1. 装置インターフェース > [Status (ステータス)] に移動します。
2. [Device info (デバイス情報)] でファームウェアバージョンを確認してください。

ファームウェアのアップグレード

重要

- ・ 事前設定済みの設定とカスタム設定は、ファームウェアのアップグレード時に保存されます (その機能が新しいファームウェアで利用できる場合)。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最新のファームウェア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。ファームウェアを更新する前に、ファームウェアととも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。最新ファームウェアおよびリリースノートについては、axis.com/support/firmwareを参照してください。

注

データベースのユーザーやグループ、証明書、その他のデータのアップデートは、ファームウェア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. ファームウェアファイルをコンピューターにダウンロードします。ファームウェアファイルはaxis.com/support/firmwareから無料で入手できます。
2. 装置に管理者としてログインします。
3. [Maintenance (メンテナンス) > Firmware upgrade (ファームウェアのアップグレード)] 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。

ファームウェアのアップグレードで問題が発生する

ファームウェアのアップグレード失敗	ファームウェアのアップグレードに失敗した場合、装置は以前のファームウェアを再度読み込みます。最も一般的な理由は、間違ったファームウェアファイルがアップロードされた場合です。装置に対応したファームウェアファイル名であることを確認し、再試行してください。
-------------------	---

ファームウェアのアップグレード後に問題が発生する	ファームウェアのアップグレード後に問題が発生する場合は、[Maintenance (メンテナンス)] 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

装置が別のサブネット上にある	装置用のIPアドレスと、装置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アドレスが別の装置で使用されている	Axis装置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コマンドと装置のIPアドレスを入力します)。 <ul style="list-style-type: none">もし、「Reply from <IPアドレス>: 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装置でその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、装置を再度インストールしてください。もし、「Request timed out」が表示された場合は、Axis装置でその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、装置を再度インストールしてください。
同じサブネット上の別の装置と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装置は静的IPアドレスを使用します。つまり、デフォルトの静的IPアドレスが別の装置でも使用されていると、装置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が有効なときは、正しいプロトコル(HTTPまたはHTTPS)を使用してログインしてください。ブラウザのアドレスフィールドに、手動で「http」または「https」と入力する必要がある場合があります。 rootユーザー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。33ページ工場出荷時の設定にリセットする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を使用して装置のネットワーク上の場所を特定してください。装置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)を使用して装置を識別します。 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、 axis.com/support を参照してください。
IEEE 802.1X使用時の証明書エラー	認証を正しく行うには、Axis装置の日付と時刻を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: 30日間の試用版を無料で使用でき、中小規模のシステムに最適です。
- 手順とダウンロードについては、axis.com/vmsを参照してください。

サポートに問い合わせる

axis.com/supportでサポートに問い合わせます。

