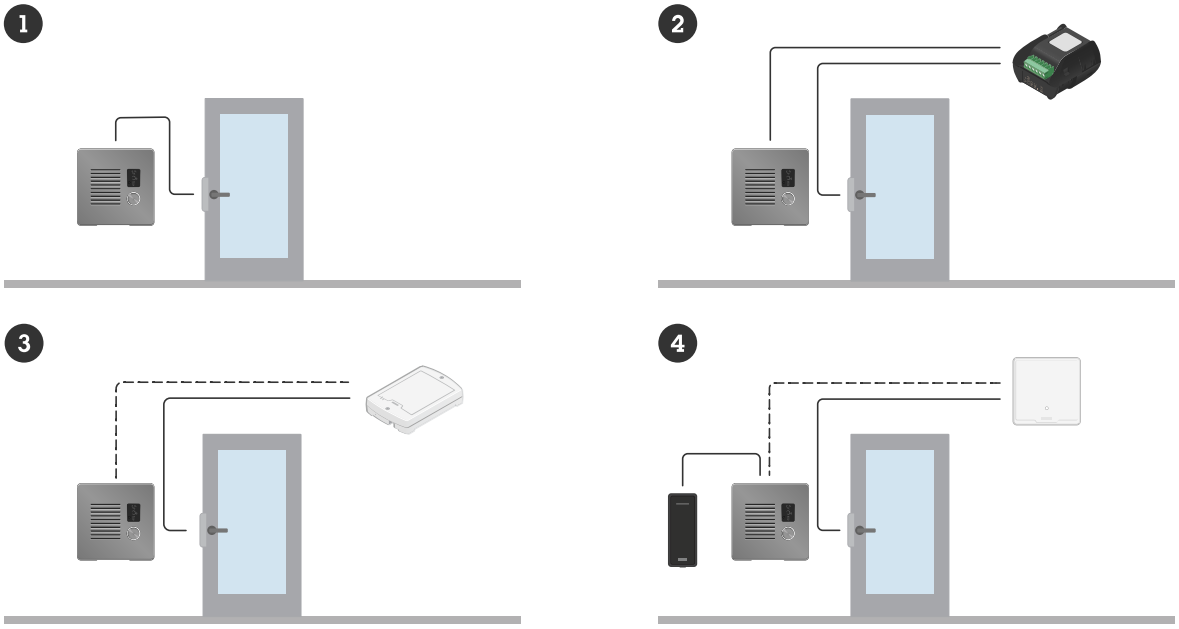
AXIS I7010-VE Network Intercoms

AXIS I7010-VE Network Intercom
AXIS I7010-VE Safety Network Intercom

ユーザーマニュアル

目次

設定の概要



1 インターコム
2 インターカムとAXIS A9801の組み合わせ
3 インターカムとAXIS A9161の組み合わせ
4 インターカム、リーダー、アクセスコントロールシステムの組み合わせ

使用に当たって

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*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。

ブラウザーサポート

以下のブラウザーでデバイスを使用できます。

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

✓: 推奨:

*: 制限付きでサポート

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。

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

ネットワーク上でパスワードやその他の機密設定を行う場合は、HTTPS (デフォルトで有効になっています) を使用してください。HTTPSを使用すると、安全で暗号化された形でネットワークに接続できるため、パスワードなどの機密データを保護できます。

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)。

デバイス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。

デバイスを構成する

このセクションでは、ハードウェアのインストールが完了した後に製品を起動して実行するために、設置者が行う必要のあるすべての重要な設定について説明しています。

ダイレクトSIP (P2P) を設定する

VoIP (Voice over IP) は、IPネットワーク上の音声通信とマルチメディア通信を可能にするテクノロジー群です。詳細については、を参照してください。

この装置では、SIPプロトコルによってVoIPが有効になっています。SIPの詳細については、を参照してください。

SIPSの設定には2つのタイプがあり、ダイレクトまたはピアツーピア (P2P) がその1つです。同じIPネットワーク内の少数のユーザーエージェント間で通信が行われ、PBXサーバーが提供する追加機能が必要ない場合は、ピアツーピアを使用します。設定する方法については、を参照してください。

1. [Communication > SIP > Settings (通信 > SIP > 設定)] に移動し、[Enable SIP (SIPの有効化)] を選択します。
2. デバイスでの着信呼び出しの受信を許可するには、[Allow incoming calls (着信呼び出しを許可)] を選択します。

注意

着信呼び出しを許可すると、デバイスはネットワークに接続されたすべてのデバイスからの呼び出しを受け付けます。公共のネットワークまたはインターネットから装置にアクセスできる場合は、着信の呼び出しを無効化することをお勧めします。

3. [Call handling (呼び出しの処理)] をクリックします。
4. [Calling timeout (呼び出しタイムアウト)] で、応答がない場合に呼び出しが終了するまでの秒数を設定します。
5. 着信呼び出しを許可している場合は、[Incoming call timeout (着信呼び出しタイムアウト)] で着信呼び出しでタイムアウトするまでの秒数を設定します。
6. [Ports (ポート)] をクリックします。
7. [SIP port (SIPポート)] の番号と [TLS port (TLSポート)] の番号を入力します。

注

- SIP port (SIPポート) - SIPセッション用。このポートを経由する信号トラフィックは暗号化されません。デフォルトポート番号は5060です。
- TLS port (TLS ポート) - TLSで保護されたSIPセッションで使用します。このポートを経由する信号トラフィックは、Transport Layer Security (TLS) を使用して暗号化されます。デフォルトポート番号は5061です。
- RTP start port (RTP開始ポート) - SIP呼び出しの最初のRTPメディアストリームで使用するポートを入力します。デフォルトの開始ポートは4000です。一部のファイアウォールでは、特定のポート番号のポートを経由するRTPトラフィックをブロックできます。ポート番号は、1024～65535の間で指定してください。

8. [NAT traversal (NATトラバーサル)] をクリックします。
9. NATトラバーサルを有効にするためのプロトコルを選択します。

注

NATトラバーサルは、デバイスがNATルーターまたはファイアウォール経由でネットワークに接続している場合に使用します。詳細については、を参照してください。

10. [保存] をクリックします。

サーバーを介してSIPを設定する (PBX)

VoIP (Voice over IP) は、IPネットワーク上の音声通信とマルチメディア通信を可能にするテクノロジー群です。詳細については、を参照してください。

この装置では、SIPプロトコルによってVoIPが有効になっています。SIPの詳細については、を参照してください。

SIPSの設定には2つのタイプがあり、PBXサーバーはそのうちの1つでです。PBXサーバーは、IPネットワークの内外で無制限の数のユーザーエージェントの間で通信を行う必要がある場合に使用します。PBXプロバイダーによっては、設定に機能が追加される場合があります。詳細については、を参照してください。

1. PBXプロバイダーから以下の情報を入手してください。
   - ユーザーID
   - ドメイン
   - パスワード
   - 認証ID
   - 呼び出し側ID
   - レジストラ
   - RTP開始ポート
2. **[Communication (通信)] > [SIP] > [Accounts (アカウント)]** に移動し、[**+ Add account (アカウントを追加)**] をクリックします。
3. アカウントの [**Name (名前)**] を入力します。
4. [**Registered (登録済み)**] を選択します。
5. Transport mode (伝送モード)を選択します。
6. PBXプロバイダーからのアカウント情報を追加します。
7. [**保存**] をクリックします。
8. ピアツーピアの場合と同じ方法でのSIPの設定については、を参照してください。PBXプロバイダーのRTP開始ポートを使用します。

近くのカメラからのビデオ ストリームをSIP通話に含める

Axisカメラがインターコムの近くにマウントされている場合は、カメラからのビデオストリームをインターコムのSIPおよびVMS通話に含めることができます。

要件

H.264および解像度1280x720、800x800、640x480のいずれかを備えたAxisカメラ。

インターコムをカメラに接続する方法：

1. [**System > Edge-to-edge > Pairing (システム > エッジツーエッジ > ペアリング)**] に移動します。
2. **Camera pairing (カメラのペアリング)**に、Axisカメラのアドレス、ユーザー名、パスワードを入力します。
3. [**接続**] をクリックします。

連絡先の作成

この例では、連絡先リストで新しい連絡先を作成する方法について説明します。開始する前に、[**Communication > SIP (通信 > SIP)**] でSIPを有効にしてください。

新しい連絡先を作成する方法:

1. [Communication > Contact list (通信 > 連絡先リスト)] に移動します。
2. [+ Add contact (連絡先を追加)] をクリックします。
3. 連絡先の姓名を入力します。
4. 連絡先のSIPアドレスを入力します。

注
SIPアドレスの詳細については、を参照してください。

5. 呼び出し元のSIPアカウントを選択します。

注
可用性オプションは、[System (システム)] > [Events (イベント)] > [Schedules (スケジュール)] で定義します。

6. 連絡先の [Availability (可用性)] を選択します。連絡先が対応できないときに呼び出しがあった場合、フォールバックがない限り、呼び出しはキャンセルされます。

注
フォールバックとは、元の連絡先が応答しない場合、または対応できない場合に転送される連絡先です。

7. [Fallback (フォールバック)] で、[None (なし)] を選択します。
8. [保存] をクリックします。

呼び出しボタンの設定

デフォルトでは、呼び出しボタンはVMS (ビデオ管理ソフトウェア) 呼び出しを行うように設定されています。この設定を維持する場合は、AxisインターカムをVMSに追加するだけです。

この例では、訪問者が呼び出しボタンを押したときに連絡先リストにある連絡先を呼び出すように、システムを設定する方法について説明します。

1. [Communication > Calls > Call button (通信 > 呼び出し > 呼び出しボタン)] に移動します。
2. [Recipients (送信先)] で、[VMS] を削除します。
3. [Recipients (送信先)] で、既存の連絡先を選択するか、新しい連絡先を作成します。

呼び出しボタンを無効にするには、[Enable call button (呼び出しボタンを有効にする)] をオフにします。

DTMFを使用して来訪時にドアのロックを解除する

訪問者がインターカムから呼び出しを行うと、応答者は自身のDual-Tone Multi-Frequency (DTMF) を使用して、ドアのロックを解除できます。ドアコントローラーにより、ドアのロック/ロック解除を行います。

この例では、次の方法について説明します。
- インターカムのDTMF信号を定義する
- 次のようにインターカムを設定します。
  - ドアコントローラーにドアのロックを解除するように要求するか、**または**
  - 内部リレーを使用してドアのロックを解除します。

すべての設定はインターカムのWebページで行います。

開始する前に
- 装置からのSIP呼び出しを許可し、SIPアカウントを作成します。「」および「」を参照してください。

インターカムのDTMF信号を定義する
1. [Communication (通信)] > [SIP] > [DTMF] に移動します。

2. [+ Add sequence (シーケンスを追加)] をクリックします。
3. [Sequence (シーケンス)] に「1」と入力します。
4. [Description (説明)] に、「Unlock door (ドアロック解除)」と入力します。
5. [Accounts (アカウント)] で、SIPアカウントを選択します。
6. [保存] をクリックします。

内部リレーを使用してドアのロックを解除するように、インターカムを設定する

7. [System > Events > Rules (システム > イベント > ルール)] に移動し、ルールを追加します。
8. [Name (名前)] フィールドに「DTMF unlock door (DTMFドアロック解除)」と入力します。
9. 条件リストの [Call (呼び出し)] で、[DTMF] を選択し、続いて [Unlock door (ドアのロック解除)] を選択します。
10. アクションのリストから [I/O] で [Toggle I/O once (I/Oを一度切り替える)] を選択します。
11. ポートのリストから、[Relay 1 (リレー1)] を選択します。
12. 継続時間 を 00:00:07 に変更します。この場合、ドアのロックが7秒間解除されます。
13. [保存] をクリックします。

認証情報保持者にドアを開くことを許可する

エントリーリストを使用すると、認証情報保持者がカードやPINを使用してドアを開くなどのアクションをトリガーできるように設定できます。この例では、カードを使用してドアを10回開くことができる認証情報所持者を追加する方法について説明します。

要件

- [Reader (リーダー)] > [Chip types (チップタイプ)] で正しいチップタイプがアクティブになっていることを確認します。

エントリーリストをオンにし、認証情報保持者を追加します。

1. [Reader (リーダー)] > [Entry list (エントリーリスト)] に移動します。
2. [Use Entry list (エントリーリストを使用)] をオンにします。
3. [+ Add credential holder (認証情報保持者を追加)] をクリックします。
4. 認証情報保持者の姓名を入力します。この名前は一意である必要があります。
5. [Card (カード)] を選択します。
6. 認証情報保持者のカードを装置でスワイプし、[Get latest (最新データを取得)] をクリックします。
7. イベント条件を [Access granted (アクセス許可)] のままにします。
8. [Valid to (有効期限)] で、[Number of times (回数)] を選択します。
9. [Number of times (回数)] に「10」と入力します。
10. [保存] をクリックします。

ルールの作成:

1. [System > Events (システム > イベント)] に移動します。
2. [Rules (ルール)] で、[+ Add a rule (ルールを追加)] をクリックします。
3. [Name (名前)] に、「Open door (ドアを開ける)」と入力します。
4. 条件のリストで、[Entry list (エントリーリスト)] > [Access granted (アクセス許可)] を選択します。
5. アクションのリストから、[I/O] > [Toggle I/O once (I/Oを1回切り替え)] を選択します。
6. ポートのリストで、[Door (ドア)] を選択します。

7. [State (状態)] で、[Active (アクティブ)] を選択します。
8. 継続時間を00:00:07に設定します。
9. [保存] をクリックします。

イベントのルールを設定する

特定のイベントが発生したときにデバイスにアクションを実行させるように、ルールを作成することができます。ルールは条件とアクションで構成されます。条件を使用して、アクションをトリガーすることができます。たとえば、デバイスは動きを検知したときに、録画を開始したり、電子メールを送信したりすることができ、デバイスが録画をしている間にオーバーレイテキストを表示することができます。

詳細については、ガイド「*イベントのルールの使用開始*」を参照してください。

アクションをトリガーする

1. [System > Events (システム > イベント)] に移動し、ルールを追加します。このルールでは、装置が特定のアクションを実行するタイミングを定義します。ルールは、スケジュールや繰り返しとして設定することも、手動でトリガーするように設定することもできます。
2. [Name (名前)] に入力します。
3. アクションをトリガーするために満たす必要がある [Condition (条件)] を選択します。ルールに複数の条件を指定した場合は、すべての条件が満たされたときにアクションがトリガーされます。
4. 条件が満たされたときにデバイスが実行する Action (アクション) を選択します。

注

アクティブなルールを変更する場合は、ルールを再度オンにして変更内容を有効にする必要があります。

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ブラウザーで装置の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ー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。

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。

Upgrade AXIS OS (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 [**Time and location (時刻と場所)**] 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。

進行中の録画

進行中の録画と指定されたストレージ容量を表示します。

録画: 進行中でフィルター処理された録画とそのソースを表示します。詳細については、を参照してください

録画を保存するストレージの空き容量を表示します。

ビデオ

インストール

キャプチャーモード:キャプチャーモードは、カメラが画像をキャプチャーする方法を定義するプリセット設定です。キャプチャーモードを変更すると、ビューエリアやプライバシーマスクなど、他の多くの設定に影響を与える場合があります。

取り付け位置:カメラのマウント方法によって、画像の向きが変わる場合があります。

Power line frequency (電源周波数):画像のちらつきを最小限に抑えるために、お使いの地域で使用されている周波数を選択してください。アメリカ地域では、通常60 Hzが使用されています。世界の他の部分では、ほとんどの場合50 Hzで使用されています。お客様の地域の電源周波数がわからない場合は、地方自治体に確認してください。

Rotate (回転):画像の向きを選択できます。

画像

表示

シーンプロファイル:監視シナリオに適したシーンプロファイルを選択します。シーンプロファイルは、カラーレベル、輝度、シャープネス、コントラスト、ローカルコントラストなどの画像設定を、特定の環境や目的に合わせて最適化します。

- **フォレンジック**：監視目的での使用に適したシーンプロファイルです。
- **屋内向け**:屋内環境での使用に適したシーンプロファイルです。
- **屋外対応**:屋外環境での使用に適したシーンプロファイルです。
- **ビビッド**:デモ目的での使用に最適なシーンプロファイルです。
- **トラフィックオーバービュー**:車両の交通監視に適したシーンプロファイルです。
- **ナンバープレート**：ナンバープレートのキャプチャーに最適。

彩度:スライダーを使用して色の強さを調整します。たとえば、グレースケール画像にすることができます。

コントラスト:スライダーを使用して、明暗の差を調整します。

輝度:スライダーを使用して光の強度を調整します。これにより、対象物が見やすくなります。輝度は画像キャプチャーの後で適用され、画像内の情報には影響しません。暗い場所でより詳細に表示するには、ゲインや露光時間を増やすのが一般的です。

Sharpness (シャープネス):スライダーを使ってエッジのコントラストを調整することで、画像内の物体をよりシャープに見せることができます。シャープネスを上げると、ビットレートが上がり、必要なストレージ容量も増加する可能性があります。

ワイドダイナミック レンジ

WDR : 画像の暗い部分と明るい部分の両方が見えるようにする場合にオンにします。

ローカルコントラスト:スライダーで画像のコントラストを調整します。値が大きいほど、暗い部分と明るい部分のコントラストが高くなります。

トーンマッピング:スライダーを使用して、画像に適用されるトーンマッピングの量を調整します。この値を0に設定すると、標準のガンマ補正のみが適用され、この値を大きくすると、画像内の最も暗い部分と最も明るい部分の可視性が高くなります。

ホワイトバランス

届いた光の色温度がカメラで検知される場合は、その色がより自然に見えるように画像を調整することができます。これで十分でない場合は、リストから適切な光源を選択できます。

ホワイトバランスの自動設定では、色のゆらぎを抑えるため、ホワイトバランスが緩やかに変更されます。光源が変わったときや、カメラの電源を初めて投入したときは、新しい光源に適合するまでに最大で30秒かかります。シーン内に色温度が異なる複数のタイプの光源がある場合は、最も支配的な光源が自動ホワイトバランスアルゴリズムの基準になります。この動作を変更するには、基準として使用する光源に合った固定ホワイトバランスの設定を選択してください。

照度環境:

- **Automatic (自動)**:光源の色を自動的に識別し、それに合わせて色を補正します。通常はこの設定をお勧めします。ほとんどの状況で使用できます。
- **自動 - 屋外**:光源の色を自動的に識別し、それに合わせて色を補正します。通常はこの設定をお勧めします。屋外のほとんどの状況で使用できます。
- **カスタム - 屋内**:蛍光灯以外の人工照明がある部屋向けの固定カラー調整。通常の色温度が約2800 Kの場合に適しています。
- **カスタム - 屋外**:色温度が約5500 Kの晴天気象条件向けの固定カラー調整。
- **Fixed - fluorescent 1 (固定 - 蛍光灯1)**:色温度が約4000 Kの蛍光灯向けの固定カラー調整。
- **Fixed - fluorescent 2 (固定 - 蛍光灯2)**:色温度が約3000 Kの蛍光灯向けの固定カラー調整。
- **固定 - 屋内**:蛍光灯以外の人工照明がある部屋向けの固定カラー調整。通常の色温度が約2800 Kの場合に適しています。
- **固定 - 屋外1**:色温度が約5500 Kの晴天気象条件向けの固定カラー調整。
- **固定 - 屋外2**:色温度が約6500 Kの曇天気象条件向けの固定カラー調整。
- **街灯 - 水銀灯**:街灯で一般的に使用される水銀灯の紫外線発光に対する固定カラー調整。
- **街灯 - ナトリウム灯**:街灯で一般的に使用されるナトリウム灯の黄色・オレンジ色を補正する固定カラー調整。
- **Hold current (現在の状態で固定)**:現在の設定を保持し、照度が変化しても補正を行いません。
- **手動**:白色の被写体を利用して、ホワイトバランスを修正します。ライブビュー画像の中で、カメラに白として解釈させる物体に円をドラッグします。[**Red balance (レッドバランス)**] と [**Blue balance (ブルーバランス)**] スライダーを使用して、ホワイトバランスを手動で調整します。

露出

露出モードを選択すると、さまざまなタイプの光源によって生じるちらつきなど、画像内で急速に変化する不規則な影響を緩和できます。自動露出モード、または電源ネットワークと同じ周波数を使用することをお勧めします。

露出モード:

- Automatic (自動):カメラが開口、ゲイン、シャッターを自動的に調整します。
- 自動開口 :カメラが開口とゲインを自動的に調整します。シャッターは固定です。
- 自動シャッター :カメラがシャッターとゲインを自動的に調整します。開口は固定です。
- 現在の状態で固定:現在の露出設定に固定します。
- ちらつき防止 :カメラが開口とゲインを自動的に調整し、次のシャッター速度のみを使用します。1/50秒 (50 Hz) と1/60秒 (60 Hz)。
- ちらつき防止 (50Hz) :カメラが開口とゲインを自動的に調整し、シャッター速度は1/50秒を使用します。
- ちらつき防止 (60Hz) :カメラが開口とゲインを自動的に調整し、シャッター速度は1/60秒を使用します。
- ちらつき低減 :これはちらつき防止と同じですが、明るいシーンでは1/100秒 (50 Hz) および1/120秒 (60 Hz) より速いシャッター速度を使用できます。
- ちらつき低減 (50 Hz) :ちらつき防止と同じですが、明るいシーンでは1/100秒より速いシャッター速度を使用できます。
- ちらつき低減 (60 Hz) :ちらつき防止と同じですが、明るいシーンでは1/120秒より速いシャッター速度を使用できます。
- 手動録画 :開口、ゲイン、シャッターは固定です。

露出エリア :露出エリアを使用すると、入口のドアの前のエリアなど、シーンの選択した部分の露出を最適化できます。

注

露出エリアは元の画像 (回転していない状態) に関連付けられているため、エリアの名前が元の画像に適用されます。つまり、たとえばビデオストリームが90°回転した場合、ストリーム内のゾーンの [Upper (上)] は [Right (右)] になり、[Left (左)」は「Lower (下)」になります。

- Automatic (自動):ほとんどの状況に適しています。
- 中央:画像の中央部の固定エリアを使用して露出が計算されます。このエリアは、ライブビュー内でサイズと位置が固定されています。
- フル :ライブビュー全体を使用して露出が計算されます。
- 上 :画像の上部にあるサイズと位置が固定されたエリアを使用して露出が計算されます。
- 下 :画像の下部にあるサイズと位置が固定されたエリアを使用して露出が計算されます。
- 左 :画像の左にあるサイズと位置が固定されたエリアを使用して露出が計算されます。

- **右**:画像の右にあるサイズと位置が固定されたエリアを使用して露出が計算されます。
- **スポット**:ライブビュー内にあるサイズと位置が固定されたエリアを使用して露出が計算されます。
- **カスタム**:ライブビュー内の一部のエリアを使用して露出が計算されます。エリアのサイズと位置を調整できます。

最大シャッター:最良の画質が得られるように、シャッター速度を選択します。シャッター速度が遅いと (露出が長いと)、動きがあるときに動きによる画像のブレが生じることがあり、シャッター速度が速すぎると画質に影響を与えることがあります。最大ゲインで最大シャッターが機能すると、画質が向上します。

最大ゲイン:適切な最大ゲインを選択します。最大ゲインを増やすと、暗い画像で細部を確認できるレベルは向上しますが、ノイズレベルも増加します。ノイズが多くなると、帯域幅とストレージの使用も多くなる可能性があります。最大ゲインを高い値に設定した場合、昼と夜で照明環境がかなり異なっていると、画像が大きく変化する可能性があります。最大シャッターで最大ゲインが機能すると、画質が向上します。

動き適応型の露出機能:これを選択して低光量下で動きによる画像のブレを減らします。

Blur-noise trade-off (ブレとノイズのトレードオフ):スライダーを使用して動きによる画像のブレとノイズの間で優先度を調整します。動く物体の細部が不鮮明になっても、帯域幅の使用とノイズが少ないことを優先する場合は、このスライダーを [**低ノイズ**] の方に移動します。帯域幅の使用とノイズが多くなっても、動く物体の細部を鮮明に保つことを優先する場合は、スライダーを [**動きによる画像のブレが少ない**] の方に移動します。

注

露出の変更は、露出時間を調整して行うこともゲインを調整しても行うこともできます。露出時間を長くすると動きによる画像のブレが増し、ゲインを大きくするとノイズが増えます。[Blur-noise trade-off (ブレとノイズのトレードオフ)] を [Low noise (低ノイズ)] 側に調整した場合、自動露出にするとゲインを上げることよりも露出時間を長くすることが優先され、トレードオフを [Low motion blur (動きによる画像のブレが少ない)] 側に調整するとその逆になります。低光量の条件下では、設定された優先度にかかわらず、最終的にはゲインと露出時間の両方が最大値に達します。

開口のロック:オンにすると、[Aperture (開口)] スライダーで設定された開口サイズが維持されます。オフにすると、開口サイズをカメラで自動的に調整できます。たとえば、点灯した状態が継続しているシーンで開口をロックすることができます。

開口:スライダーを使用して開口サイズ (レンズからどれだけ光を取り込むか) を調整します。暗い場所でより多くの光をセンサーに取り込み、より明るい画像を得るには、スライダーを [Open (開く)] 方向に移動します。開口を開くと被写界深度は減少し、カメラの近くまたは遠くにある物体はフォーカスが合っていないように見える可能性があります。画像のフォーカスを拡大するには、スライダーを [Closed (閉じる)] 方向に移動します。

露出レベル:スライダーを使用して画像の露出を調整します。

デフォグ機能:オンにすると、霧の影響を検知して自動的に霧を除去するため、より鮮明な画像が得られます。

注

コントラストが低い、光のレベルの変動が大きい、オートフォーカスがわずかにオフの場合は、[Defog (デフォッグ)] をオンにすることをお勧めします。その場合は、映像のコントラストが増大するなど、画質に影響することがあります。また、光量が多すぎる場合にも、デフォッグがオンになると画質に悪影響が出るおそれがあります。

ストリーム

概要

解像度:監視シーンに適した画像の解像度を選択します。解像度が高いと、帯域幅とストレージが増大します。

フレームレート:ネットワーク上の帯域幅の問題を避けるため、またはストレージサイズを削減するために、フレームレートを固定値に制限できます。フレームレートをゼロのままにすると、フレームレートは現在の状況で可能な最大値となります。フレームレートを高くすると、より多くの帯域幅とストレージ容量が必要になります。

Pフレーム:Pフレームは、前のフレームからの画像の変化のみを示す予測画像です。適切なPフレーム数を入力します。値が大きいほど、必要な帯域幅は小さくなります。ただし、ネットワークが輻輳している場合には、ビデオ画質が著しく劣化する可能性があります。

圧縮:スライダーを使用して画像の圧縮率を調整します。圧縮率が高いほどビットレートが低くなり、画質が低下します。圧縮率が低いと画質が向上しますが、録画時により多くの帯域幅とストレージを必要とします。

署名付きビデオ:オンにすると、署名付きビデオ機能がビデオに追加されます。署名付きビデオは、ビデオに暗号化署名を追加することでビデオをいたずらから保護します。

Zipstream

Zipstreamテクノロジーは映像監視用に最適化されたビットレート低減テクノロジーで、H.264またはH.265ストリームの平均ビットレートをリアルタイムで削減します。Axis Zipstream テクノロジーは、動く物体を含むシーンなど、画像内に関心領域が複数あるシーンに対して高いビットレートを適用します。シーンがより静的であれば、Zipstreamは低いビットレートを適用し、ストレージの使用量を削減します。詳細については、「*Axis Zipstreamによるビットレートの低減*」を参照してください。

ビットレート低減の [Strength (強度)] を選択します。
- Off (オフ):ビットレート低減はありません。
- 低:ほとんどのシーンで認識できる画質低下なし。これはデフォルトのオプションです。あらゆるタイプのシーンでビットレートの低減に使用できます。
- 中間:一部のシーンでは、動きのない部分など、関心の低い領域でノイズが少なく、ディテールレベルがやや低くなることで、目に見える効果が得られます。
- 高:一部のシーンでは、動きのない部分など、関心の低い範囲でノイズが少なく、ディテールレベルが低くなることで、目に見える効果が得られます。クラウドに接続された装置やローカルストレージを使用する装置にはこのレベルを推奨します。
- Higher (さらに高):一部のシーンでは、動きのない部分など、関心の低い範囲でノイズが少なく、ディテールレベルが低くなることで、目に見える効果が得られます。
- Extreme (極限):大部分のシーンで目に見える効果が得られます。ビットレートは、可能な限り小さなストレージに最適化されています。

Optimize for storage (ストレージ用に最適化する):オンにし、画質を維持しながらビットレートを最小限に抑えます。この最適化は、Webクライアントに表示されるストリームには適用されません。この機能は、VMSがBフレームをサポートしている場合のみ使用できます。
[Optimize for storage (ストレージ用に最適化)] をオンにすると、[Dynamic GOP (ダイナミックgroup of pictures)] もオンになります。

Dynamic FPS (ダイナミックFPS) (フレーム/秒):オンにすると、シーン内のアクティビティのレベルに応じて帯域幅が変化します。動きが多い場合、より多くの帯域幅が必要です。

下限:シーンの動きに応じて、最小フレーム/秒とストリームのデフォルトフレーム/秒の間でフレームレートを調整するための値を入力します。フレーム/秒が1以下になるような動きの少ないシーンでは、下限を設定することをお勧めします。

Dynamic GOP (ダイナミック group of pictures):オンにすると、シーン内のアクティビティのレベルに応じて、I-フレームの間隔が動的に調整されます。

上限:最大GOP長 (2つのI-フレーム間のP-フレームの最大数) を入力します。Iフレームは、他のフレームとは無関係の自己完結型の画像フレームです。

ビットレート制御

- Average (平均):より長い時間をかけてビットレートを自動的に調整し、使用可能なストレージに基づいて最適な画質を提供する場合に選択します。
  - クリックすると、利用可能なストレージ、保存時間、ビットレート制限に基づいて目標ビットレートが計算されます。
  - Target bitrate (目標ビットレート):目標とするビットレートを入力します。
  - Retention time (保存期間):録画を保存する日数を入力します。
  - ストレージ:ストリームに使用できるストレージの概算が表示されます。
  - Maximum bitrate (最大ビットレート):オンにすると、ビットレートの制限が設定されます。
  - Bitrate limit (ビットレートの制限):目標ビットレートより高いビットレートの制限を入力してください。
- Maximum (最大):オンにすると、ネットワーク帯域幅に基づいてストリームの最大瞬時ビットレートが設定されます。
  - Maximum (最大):最大ビットレートを入力します。
- Variable (可変):オンにすると、シーン内のアクティビティのレベルに基づいてビットレートが変化します。動きが多い場合、より多くの帯域幅が必要です。ほとんどの場合、このオプションをお勧めします。

向き

Mirror (ミラーリング):オンにすると画像が反転します。

音声

Include (対象):オンにすると、ビデオストリームで音声が使用されます。

ソース :使用する音声ソースを選択します。

ステレオ :オンにすると、内蔵の音声だけでなく、外部のマイクからの音声も取り込むことができます。

オーバーレイ

+:クリックするとオーバーレイが追加されます。ドロップダウンリストからオーバーレイの種類を次の中から選択します。

- **テキスト**:テキストをライブビュー画像に統合し、すべてのビュー、録画、スナップショットに表示する場合に選択します。独自のテキストを入力することもできます。また、あらかじめ設定された修飾子を含めることで、時間、日付、フレームレートなどを自動的に表示することもできます。
  - : クリックすると、日付の修飾子%Fを追加して、yyyy-mm-ddを表示できます。
  - : クリックすると、時間の修飾子%Xを追加して、hh:mm:ss (24時間制) を表示できます。
  - **Modifiers (修飾子)**:クリックすると、リストに表示された修飾子から選択して、テキストボックスに追加できます。たとえば、%aを選択すると曜日が表示されます。
  - **サイズ**:フォントサイズを選択します。
  - **表示**:黒い背景に白いテキスト (デフォルト) など、背景色とテキストの色を選択します。
  - : 画像内でオーバーレイの位置を選択したり、オーバーレイをクリック＆ドラッグしてライブビュー内で移動させたりできます。
- **Image (画像)**:ビデオストリームに静止画像を重ねて表示する場合に選択します。.bmp、.png、.jpeg、または.svgファイルを使用できます。
  画像をアップロードするには、**画像**をクリックします。画像をアップロードする前に、以下の方法を選択できます。
  - **Scale with resolution (解像度に伴う拡大/縮小)**:選択すると、解像度に合わせてオーバーレイ画像のサイズを自動的に変更できます。
  - **Use transparency (透明色を使用する)**:その色のRGB 16進値を選択して入力します。RRGGBB形式を使用します。16進数値の例:FFFFFF - 白、000000 - 黒、FF0000 - 赤、6633FF - 青、669900 - 緑。.bmp画像の場合のみ。
- **シーンの注釈** :カメラが別の方向にパンまたはチルトした場合でも、ビデオストリームに同じ位置に留まるテキストオーバーレイを表示する場合に選択します。特定のズームレベル内でのみオーバーレイを表示するように選択できます。
  - : クリックすると、日付の修飾子%Fを追加して、yyyy-mm-ddを表示できます。
  - : クリックすると、時間の修飾子%Xを追加して、hh:mm:ss (24時間制) を表示できます。
  - **Modifiers (修飾子)**:クリックすると、リストに表示された修飾子から選択して、テキストボックスに追加できます。たとえば、%aを選択すると曜日が表示されます。
  - **サイズ**:フォントサイズを選択します。
  - **表示**:黒い背景に白いテキスト (デフォルト) など、背景色とテキストの色を選択します。
  - : 画像内でオーバーレイの位置を選択したり、オーバーレイをクリック＆ドラッグしてライブビュー内で移動させたりできます。オーバーレイは保存され、この位置のパンとチルトの座標に残ります。

- Annotation between zoom levels (%) (ズームレベル (%) 間に注釈を表示する): オーバーレイが表示されるズームレベルを設定します。
- Annotation symbol (注釈記号):カメラが設定したズームレベル内にない場合に、オーバーレイの代わりに表示される記号を選択します。

- ストリーミングインジケーター :ビデオストリームに重ね合わせてアニメーションを表示する場合に選択します。このアニメーションは、シーンに動きがなくても、ビデオストリームがライブであることを示します。
  - 表示:アニメーションの色と背景色を選択します。たとえば、透明な背景に赤いアニメーション (デフォルト) などです。
  - サイズ:フォントサイズを選択します。
  - : 画像内でオーバーレイの位置を選択したり、オーバーレイをクリック＆ドラッグしてライブビュー内で移動させたりできます。
- Widget:折れ線グラフ :測定値が時間の経過とともにどのように変化しているかを示すグラフを表示します。
  - タイトル:ウィジェットのタイトルを入力します。
  - Overlay modifier (オーバーレイ修飾子):データソースとしてオーバーレイ修飾子を選択します。MQTTオーバーレイを作成済みである場合、これらはリストの最後に配置されます。
  - : 画像内でオーバーレイの位置を選択したり、オーバーレイをクリック＆ドラッグしてライブビュー内で移動させたりできます。
  - サイズ:オーバーレイのサイズを選択します。
  - Visible on all channels (すべてのチャンネルで表示する):オフにすると、現在選択しているチャンネルのみに表示されます。オンにすると、アクティブなチャンネルすべてに表示されます。
  - Update interval (更新間隔):データの更新間隔を選択します。
  - Transparency (透明度):オーバーレイ全体の透明度を設定します。
  - Background transparency (背景の透明度):オーバーレイの背景のみの透明度を設定します。
  - Points (ポイント):オンにすると、データ更新時にグラフラインにポイントが追加されます。
  - X軸
    - ラベル:X軸のテキストラベルを入力します。
    - Time window (時間ウィンドウ):データが表示される時間の長さを入力します。
    - Time unit (時間単位):X軸の時間単位を入力します。
  - Y軸
    - ラベル:Y軸のテキストラベルを入力します。
    - Dynamic scale (ダイナミックスケール):オンにすると、スケールがデータ値に自動的に適応します。オフにして、固定スケールの値を手動で入力します。
    - Min alarm threshold (最小アラーム閾値) とMax alarm threshold (最大アラーム閾値):これらの値によってグラフに水平基準線が追加され、データ値が高すぎる場合や低すぎる場合に確認しやすくなります。
- Widget:メーター :最近測定されたデータ値を示す棒グラフを表示します。

- タイトル:ウィジェットのタイトルを入力します。
- Overlay modifier (オーバーレイ修飾子):データソースとしてオーバーレイ修飾子を選択します。MQTTオーバーレイを作成済みである場合、これらはリストの最後に配置されます。
- : 画像内でオーバーレイの位置を選択したり、オーバーレイをクリック＆ドラッグしてライブビュー内で移動させたりできます。
- サイズ:オーバーレイのサイズを選択します。
- Visible on all channels (すべてのチャンネルで表示する):オフにすると、現在選択しているチャンネルのみに表示されます。オンにすると、アクティブなチャンネルすべてに表示されます。
- Update interval (更新間隔):データの更新間隔を選択します。
- Transparency (透明度):オーバーレイ全体の透明度を設定します。
- Background transparency (背景の透明度):オーバーレイの背景のみの透明度を設定します。
- Points (ポイント):オンにすると、データ更新時にグラフラインにポイントが追加されます。
- Y軸
  - ラベル:Y軸のテキストラベルを入力します。
  - Dynamic scale (ダイナミックスケール):オンにすると、スケールがデータ値に自動的に適応します。オフにして、固定スケールの値を手動で入力します。
  - Min alarm threshold (最小アラーム閾値) とMax alarm threshold (最大アラーム閾値):これらの値によって棒グラフに水平基準線が追加され、データ値が高すぎる場合や低すぎる場合に確認しやすくなります。

プライバシーマスク

:クリックすると、新しいプライバシーマスクを作成できます。

Privacy masks (プライバシーマスク):クリックすると、すべてのプライバシーマスクの色を変更したり、すべてのプライバシーマスクを永久に削除したりすることができます。

マスクx: クリックすると、マスクの名前変更、無効化、永久削除を行うことができます。

コミュニケーション

連絡先リスト

連絡先

: クリックして、連絡先リストをjsonファイルとしてダウンロードします。

: クリックして、連絡先リスト (json) をインポートします。

Add contact (連絡先の追加)：クリックして、新しい連絡先を連絡先リストに追加します。

Upload image (画像のアップロード) :クリックして、連絡先を表す画像をアップロードします。

First name (名):連絡先の名を入力します。

Last name (姓):連絡先の姓を入力します。

Speed dial (短縮ダイヤル) ：連絡先に使用できる短縮ダイヤル番号を入力します。この番号は、装置から連絡先を呼び出すのに使用されます。

SIPアドレス:SIPを使用する場合は、連絡先のIPアドレスまたは内線番号を入力します。

：クリックして、テスト呼び出しを行います。応答があると、呼び出しは自動的に終了します。

SIPアカウント:SIPを使用する場合、装置から連絡先への呼び出しに使用するSIPアカウントを選択します。

Availability (対応可能):連絡先の対応可能スケジュールを選択します。[System (システム)] > [Events (イベント)] > [Schedules (スケジュール)] でスケジュールの追加や調整を行えます。連絡先が対応できないときに呼び出しが試行された場合、フォールバックがない限り、呼び出しはキャンセルされます。

Fallback (フォールバック):該当する場合は、リストからフォールバックを選択します。

Notes (メモ):連絡先に関する任意の情報を追加することができます。

コンテキストメニューは以下を含みます。

Edit contact (連絡先の編集):連絡先のプロパティを編集します。

Delete contact (連絡先の削除):連絡先を削除します。

SIP

設定

セッション開始プロトコル (SIP) は、ユーザー間でのインタラクティブな通信セッションに使用します。セッションには、音声およびビデオを含めることができます。

SIP setup assistant (SIP設定アシスタント):クリックすると、ステップバイステップでSIPを設定できます。

Enable SIP (SIP の有効化):このオプションをオンにすると、SIPコールの発着信が可能になります。

着信呼び出しを許可:このオプションにチェックマークを入れると、その他のSIPデバイスからの着信呼び出しを許可します。

呼び出し処理

- 呼び出しタイムアウト:誰も応答しない場合の呼び出しの最大継続時間を設定します。
- Incoming call duration (着信間隔):着信の最長時間 (最大10分) を設定します。
- End calls after (呼び出し終了):呼び出しの最長時間 (最大60分) を設定します。呼び出しの長さを制限しない場合は、[Infinite call duration (無限呼び出し期間)] を選択します。

ポート

ポート番号は1024～65535の間で指定する必要があります。

- SIPポート:SIP通信に使用するネットワークポートです。このポートを経由する信号トラフィックは暗号化されません。デフォルトポート番号は5060です。必要に応じて異なるポート番号を入力します。
- TLSポート:暗号化されたSIP通信に使用するネットワークポートです。このポートを経由する信号トラフィックは、Transport Layer Security (TLS) を使用して暗号化されます。デフォルトポート番号は5061です。必要に応じて異なるポート番号を入力します。
- RTP開始ポート番号:SIP呼び出しで最初のRTPメディアストリームに使用されるネットワークポートです。デフォルトの開始ポート番号は4000です。ファイアウォールは、特定のポート番号のRTPトラフィックをブロックします。

NATトラバーサル

NAT (ネットワークアドレス変換) トラバーサルは、プライベートネットワーク (LAN) 上にある装置を、そのネットワークの外部から利用できるようにする場合に使用します。

注

NATトラバーサルを機能させるには、ルーターがNATトラバーサルに対応している必要があります。また、UPnP®にも対応している必要があります。

NATトラバーサルプロトコルは個別に使用することも、ネットワーク環境に応じたさまざまな組み合わせで使用することもできます。

- ICE:ICE (双方向接続性確立) プロトコルを使用することで、ピアデバイス間の通信を成功させるために最も効率の良いパスを見つけやすくなります。STUNやTURNも有効にすると、さらにICEプロトコルで見つけやすくなります。
- STUN:STUN (NATのためのセッショントラバーサルユーティリティ) は、装置がNATまたはファイアウォールを経由して配置されているかどうかを特定し、経由していれば、リモートホストへの接続に割り当てるマッピングされるパブリックIPアドレスとポート番号を取得できるようにするクライアント/サーバーネットワークプロトコルです。IPアドレスなどのSTUNサーバーアドレスを入力します。
- TURN:TURN (NATに関するリレーを使用したトラバーサル) は、NATルーターまたはファイアウォールを経由するデバイスが、TCPやUDPを介して他のホストから着信データを受信できるようにするプロトコルです。TURNサーバーアドレスとログイン情報を入力します。

音声とビデオ

- 音声コーデックの優先度:望ましい音声品質で、SIP呼び出しの音声コーデックを1つ以上選択します。ドラッグアンドドロップして、優先順位を変更します。

注

呼び出しを行うと送信先のコーデックが決定されるため、選択したコーデックは送信先のコーデックと一致する必要があります。

- Audio direction (音声の方向):許可されている音声方向を選択します。

- H.264 packetization mode (H.264パケット化モード):使用するパケット化モードを選択します。
  - [オート]:(推奨) 使用するパケット化モードは本装置によって決定されます。
  - None (なし):パケット化モードは設定されません。このモードは、多くの場合、モード0と解釈されます。
  - 0: ノンインターリーブモード。
  - 1: シングルNALユニットモード。
- ビデオの方向:許可されているビデオの方向を選択します。
- Show video in call (通話中にビデオを表示) :受信したビデオストリームをデバイスの画面に表示します。

その他

- UDP-to-TCP switching (UDPからTCPへの切り替え):選択して、転送プロトコルをUDP (User Datagram Protocol) からTCP (Transmission Control Protocol) に一時的に切り替えます。切り替えるのはフラグメンテーションを避けるためであり、要求が200バイト以内または1300バイト以上の最大転送ユニット (MTU) の場合に実行されます。
- Allow via rewrite (経由のリライトを許可):選択して、ルーターのパブリックIPアドレスの代わりに、ローカルIPアドレスを送信します。
- Allow contact rewrite (接続のリライトを許可):選択して、ルーターのパブリックIPアドレスの代わりに、ローカルIPアドレスを送信します。
- Register with server every (サーバーに登録):既存のSIPアカウントで、装置をSIPサーバーに登録する頻度を設定します。
- DTMF payload type (DTMFのペイロードタイプ):DTMFのデフォルトのペイロードタイプを変更します。
- Max retransmissions (最大再送回数):装置が試行を停止するまでにSIPサーバーへの接続を試行する最大回数を設定します。
- Seconds until failback (フェイルバックまでの秒数):装置がセカンダリSIPサーバーにフェイルオーバーした後、プライマリSIPサーバーへの再接続を試みるまでの秒数を設定します。

アカウント

現在のSIPアカウントはすべて、[SIP accounts (SIPアカウント)] に一覧表示されます。登録済みのアカウントの場合、色付きの円でステータスが示されます。

- アカウントをSIPサーバーに正常に登録できました。
- アカウントに問題があります。原因として、アカウントの認証情報が正しくないため認証に失敗した、またはSIPサーバーでアカウントが見つからないことが考えられます。

[Peer to peer (default) (ピアツーピア (デフォルト))] アカウントは、自動的に作成されたアカウントです。他に少なくとも1つアカウントを作成し、デフォルトとしてそのアカウントを設定した場合、ピアツーピアアカウントを削除することができます。デフォルトのアカウントは、どのSIPアカウントから呼び出すか指定せずにVAPIX®アプリケーションプログラミングインターフェース (API) 呼び出しを行うと必ず使用されます。

＋ **アカウントを追加**:クリックすると、新しいSIPアカウントを作成できます。

- **Active (アクティブ)**:アカウントを使用できるようにします。
- [**デフォルトにする**]:このアカウントをデフォルトに設定します。デフォルトのアカウントは必須で、デフォルトに設定できるのは1つだけです。
- [**自動応答**]:着信呼び出しに自動的に応答するにはこれを選択します。
- **IPv4よりIPv6を優先** :IPv6アドレスをIPv4アドレスより優先する場合に選択します。これは、IPv4アドレスとIPv6アドレスの両方で解決されるピアツーピアアカウントまたはドメイン名に接続する場合に便利です。IPv6アドレスにマッピングされているドメイン名にはIPv6のみを優先できます。
- **名前**:わかりやすい名前を入力します。姓名、権限、または場所などにすることができます。名前がすでに使用されています。
- **ユーザーID**:装置に割り当てられた一意の内線番号または電話番号を入力します。
- [**ピアツーピア**]:ローカルネットワーク上の別のSIP装置への直接的な呼び出しに使用します。
- **登録済み**:SIPサーバーを介して、ローカルネットワークの外部のSIPデバイスへの呼び出しに使用します。
- **ドメイン (Domain)**:利用可能な場合は、パブリックドメイン名を入力します。他のアカウントを呼び出したときにSIPアドレスの一部として表示されます。
- **パスワード**:SIPサーバーに対して認証するためのSIPアカウントに関連付けられたパスワードを入力します。
- **認証ID**:SIPサーバーに対して認証するために使用される認証IDを入力します。ユーザーIDと同じ場合、認証IDを入力する必要はありません。
- **呼び出し側ID**:装置からの呼び出しの送信先に表示される名前です。
- [**レジストラ**]:レジストラのIPアドレスを入力します。
- **伝送モード**:アカウントのSIP伝送モードを選択します。UPD、TCP、またはTLS。
- **TLS version (TLSバージョン)** (トランスポートモードTLSのみ):使用するTLSのバージョンを選択します。**v1.2**と**v1.3**が最も安全なバージョンです。[**Automatic (自動)**] では、システムが処理できる最も安全なバージョンが選択されます。
- **メディアの暗号化** (TLS伝送モードでのみ):SIP呼び出しでメディア暗号化 (音声およびビデオ) のタイプを選択します。
- **証明書** (TLS伝送モードでのみ):証明書を選択します。
- **サーバー証明書の検証** (TLS伝送モードでのみ):サーバー証明書を確認します。
- **セカンダリSIPサーバー**:プライマリSIPサーバーへの登録に失敗したときに、装置がセカンダリSIPサーバーへの登録を試みるようにする場合にオンにします。

- [SIPS (SIP secure)]:SIPS (Secure Session Initiation Protocol) を使用する場合に選択します。SIPSは、トラフィックを暗号化するためにTLS伝送モードを使用します。
- プロキシー
  - ＋ プロキシー:クリックしてプロキシを追加します。
  - 優先:2つ以上のプロキシーを追加した場合は、クリックして優先順位を付けます。
  - サーバーアドレス:SIPプロキシサーバーのIPアドレスを入力します。
  - Username (ユーザー名):必要であればSIPプロキシーサーバーで使用するユーザー名を入力します。
  - パスワード:必要であればSIPプロキシーサーバーで使用するパスワードを入力します。
- ビデオ
  - View area (ビューエリア):ビデオ通話に使用するビューエリアを選択します。[なし] を選択すると、ネイティブビューが使用されます。
  - 解像度:ビデオ通話に使用する解像度を選択します。解像度は、必要な帯域幅に影響します。
  - フレームレート:ビデオ通話1秒あたりのフレーム数を選択します。フレームレートは、必要な帯域幅に影響します。
  - H.264プロファイル:ビデオ通話に使用するプロファイルを選択します。

DTMF

＋ シーケンスを追加:クリックして、新しいDTMF (Dual-Tone Multi-Frequency) シーケンスを作成します。タッチトーンによって有効になるルールを作成するには、[Events (イベント)] > [Rules (ルール)] に移動します。

シーケンス:ルールを有効にする文字を入力します。使用できる文字:0〜9、A〜D、#、および *。

Description (説明):シーケンスによってトリガーされるアクションの説明を入力します。

Accounts (アカウント):DTMFシーケンスを使用するアカウントを選択します。[peer-to-peer (ピアツーピア)] を選択した場合、すべてのピアツーピアアカウントが同じDTMFシーケンスを共有します。

プロトコル

各アカウントに使用するプロトコルを選択します。すべてのピアツーピアアカウントは同じプロトコル設定を共有します。

RTP (RFC2833) を使用:RTPパケット内でDTMF (Dual-Tone Multi-Frequency) 信号などのトーン信号およびテレフォニーイベントを許可する場合は、オンにします。

[SIP INFO (RFC2976) を使用]:オンにして、SIPプロトコルにINFO方式を含めます。INFO方式で、必要に応じたアプリケーションのレイヤー情報 (通常はセッションに関連する情報) が追加されます。

呼び出しのテスト

SIPアカウント:テスト呼び出しを行うアカウントを選択します。

SIPアドレス:呼び出しのテストを行い、アカウントが動作していることを確認するには、SIPアドレスを入力し、をクリックします。

アクセスリスト

Use access list (アクセスリストを使用する):装置への呼び出しができるユーザーを制限する場合は、オンにします。

Policy (ポリシー):
- Allow (許可):アクセスリスト内のソースからの着信のみを許可する場合に選択します。
- Block (ブロック):アクセスリスト内のソースからの着信をブロックする場合に選択します。

＋ Add source (ソースの追加):クリックして、アクセスリストに新しいエントリを作成します。

SIP source (SIPソース):ソースの呼び出し元IDまたはSIPサーバーアドレスを入力します。

呼び出し

呼び出しボタン

Use call button (コールボタンを使用):オンにすると、呼び出しボタンが使用できるようになります。

Button functionality during a call (通話中のボタン機能):デバイスから通話が開始されたら、コールボタンの機能を選択します。

- End the call (通話を終了):訪問者が発信中にコールボタンを押すと、通話が終了します。訪問者がいつでも通話を終了できるようにするには、このオプションを使用してください。
- No functionality until the call has ended (通話が終了するまで機能しない):訪問者が発信中にコールボタンを押しても反応しません。訪問者が通話を終了できないようにするには、このオプションを使用してください。
- Delay before you can end the call (通話を終了できるまでの遅延):訪問者が通話を開始した後、[Delay (seconds) (遅延 (秒))] で設定された時間内は、コールボタンを押しても反応しません。遅延時間の経過後にコールボタンを押すと通話が終了します。このオプションを使用すると、訪問者が二度押しによって意図せず通話を終了するのを防ぐことができます。
  - Delay (seconds) (遅延 (秒)): コールボタンを2回目に押したときに通話が終了するようになるまでの時間を入力します。

Standby light (スタンバイライト):呼び出しボタン周辺の内蔵ライトのオプションを選択します。

- Auto (オート) ：装置は周囲の明るさに応じて内蔵ライトをオン/オフにします。
- On (オフ)：装置がスタンドバイモードのとき、内蔵ライトは常にオンになります。
- Off (オフ):装置がスタンドバイモードのとき、内蔵ライトは常にオフになります。

Recipients (送信先):誰かが呼び出しボタンを押したときに呼び出す連絡先を1つ以上選択または作成します。複数の送信先を追加すると、呼び出しは同時にすべての送信先に発信されます。SIP呼び出し送信先の最大数は6ですが、VMS呼び出し送信先の数は無制限です。

Fallback (フォールバック):送信先から応答がない場合に備えて、リストからフォールバックを追加します。

概要

音声

注

- 選択した音声クリップは、呼び出し時にのみ再生されます。
- 発信中に音声クリップやゲインを変更しても、その変更は次の呼び出しまで有効になりません。

Ringtone (着信音):装置に着信があったときに再生する音声クリップを選択します。スライダーを使用してゲインを調整します。

Ringback tone (発信音):装置から発信があったときに再生する音声クリップを選択します。スライダーを使用してゲインを調整します。

VMS呼び出し

VMS呼び出し

ビデオ管理ソフトウェア (VMS) での通話を許可する：装置からVMSへの通話を許可する場合に選択します。SIP がオフになっている場合も、VMS通話を行うことができます。

呼び出しタイムアウト:誰も応答しない場合の呼び出しの最大継続時間を設定します。

分析機能

メタデータの設定

RTSPメタデータプロデューサー

メタデータをストリーミングするデータチャネルと、それらが使用するチャネルを表示、管理します。

注

これらは、ONVIF XMLを使用しているRTSPメタデータストリームの設定です。ここで行った変更は、メタデータ視覚化ページには影響しません。

Producer (プロデューサー):リアルタイム・ストリーミング・プロトコル (RTSP) を使用してメタデータを送信するデータチャンネル。

チャンネル:プロデューサーからメタデータを送信するために使用されるチャネル。オンにすると、メタデータストリームが有効になります。互換性またはリソース管理の理由がある場合はオフにします。

MQTT

MQTT (Message Queuing Telemetry Transport) 上でメタデータを生成し、ストリーミングするプロデューサーを設定します。

- 作成:クリックして、新しいMQTTプロデューサーを作成します。
  - Key (キー):ドロップダウンリストから定義済みの識別子を選択して、メタデータストリームのソースを指定します。
  - MQTT topic (MQTTトピック):MQTTトピックの名前を入力します。
  - QoS (Quality of Service): メッセージ配信の保証レベル (0〜2) を設定します。

Retain messages (メッセージの保持):MQTTトピックの最後のメッセージを保持するかどうかを選択します。

Use MQTT client device topic prefix (MQTTクライアントデバイスのトピックプレフィックスを使用):ソースデバイスを識別するために、MQTTトピックにプレフィックスを追加するかどうかを選択します。

コンテキストメニューは以下を含みます。

- Update (更新):選択したプロデューサーの設定を変更します。
- 削除:選択したプロデューサーを削除します。

Object snapshot (オブジェクトスナップショット):オンにすると、検出された各オブジェクトのトリミング画像が含まれます。

Additional crop margin (トリミング余白):オンにすると、検出されたオブジェクトのトリミング画像の周りに余白が追加されます。

リーダー

接続

外部リーダー (入力)

Use external OSDP reader (外部OSDPリーダーを使用する):オンに設定すると、外部リーダーで装置を使用できます。リーダーをリーダーコネクター (IO1、IO2、12V、GND) に接続します。

Status (ステータス):
- Connected (接続済み):装置はアクティブな外部リーダーに接続されています。
- Connecting (接続中):装置は外部リーダーへの接続を試行しています。
- Not connecte (未接続)：OSDPがオフになっています。

リーダープロトコル

Reader protocol type (リーダープロトコルタイプ):リーダー機能に使用するプロトコルを選択します。

- VAPIX reader (VAPIXリーダー):Axisドアコントローラーでのみ使用できます。
  - Protocol (プロトコル):[HTTPS] または [HTTP] を選択します。
  - Door controller address (ドアコントローラーアドレス):ドアコントローラーのIPアドレスを入力します。
  - User name (ユーザー名):ドアコントローラーのユーザー名を入力します。
  - パスワード:ドアコントローラーのパスワードを入力します。
  - Connect (接続する):クリックしてドアコントローラーに接続します。
  - Select reader (リーダーの選択):該当するドア用の入口リーダーを選択します。
- OSDP:
  - OSDP address (OSDPアドレス):OSDPリーダーのアドレスを入力します。デフォルトの「0」は、シングルリーダーの最も一般的なアドレスです。
- Wiegand :
  - Beeper (ビーパー):オンにすると、ビーパー入力が有効になります。
  - Input for beeper (ビーパー用の入力):ビーパーに使用するI/Oポートを選択します。
  - Input used for LED control (LED制御用の入力):装置のLEDフィードバックの制御に使用するI/Oポートの数を選択します。
  - Input for LED1/LED2 (LED1/LED2用の入力)：LED入力に使用するI/Oポートを選択します。
  - Idle color (待機中の色):LEDの制御に使用するI/Oポートがない場合に、カードリーダーのインジケーターストライプに表示する静的な色を選択できます。
  - Color for state low/high (低/高の状態の色)：1つの入出力ポートをLED制御に使用する場合は、状態が低の場合と高の場合にそれぞれ表示する色を選択します。
  - Idle color/LED1 color/LED2 color/LED1 + LED2 color (待機中の色/LED1の色/LED2の色/LED1 + LED2の色):LED制御に2つのI/Oポートを使用する場合は、待機中、LED1、LED2、およびLED1 + LED2のそれぞれに表示する色を選択します。
  - Keypress format (キー操作の形式):PINをアクセスコントロールユニットに送信するときのPINの形式を選択します。
    - FourBit: PIN1234はエンコーダされ、0x1 0x2 0x3 0x4として送信されます。これがデフォルトで、最も一般的な動作です。
    - EightBitZeroPadded: PIN1234はエンコーダされ、0x01 0x02 0x03 0x04として送信されます。
    - EightBitInvertPadded: PIN 1234はエンコーダされ、0xE1 0xD2 0xC3 0xB4として送信されます。
    - Wiegand26：PINが8ビットの設備コードと16ビットのIDを使用してWiegand26形式でエンコードされます。
    - Wiegand34：PINが16ビットの設備コードと16ビットのIDを使用してWiegand34形式でエンコードされます。
    - Wiegand37PINが35ビットIDを使用してWiegand37形式 (H10302) でエンコードされます。
    - Wiegand37FacilityCode：PINが16ビットの設備コードと19ビットのIDを使用してWiegand37形式 (H10304) でエンコードされます。

– Facility code (設備コード):送信する設備コードを入力します。このオプションは一部のキー操作の形式でのみ使用できます。

出力形式

Select data format (データ形式を選択する):カードデータをアクセスコントロールユニットに送信するときの形式を選択します。

- Raw (未処理):カードデータをそのまま送信します。
- Wiegand26：カードデータが8ビットの設備コードと16ビットのIDを使用してWiegand26形式でエンコードされます。
- Wiegand34：カードデータが16ビットの設備コードと16ビットのIDを使用してWiegand34形式でエンコードされます。
- Wiegand37：カードデータが35ビットIDを使用してWiegand37形式 (H10302) でエンコードされます。
- Wiegand37FacilityCode：カードデータが16ビットの設備コードと19ビットのIDを使用してWiegand37形式 (H10304) でエンコードされます。
- カスタム:独自の形式を定義します。

\Facility code override mode (設備コード上書きモード):設備コードを上書きするオプションを選択します。

- [オート]:設備コードを上書きせず、入力データの自動検出から設備コードを作成します。カードの元の設備コードを使用するか、カード番号の余剰ビットから施設コードを生成します。
- Optional (オプション):入力データからの設備コードを使用するか、設定されたオプション値で上書きします。
- Override (上書き):指定された設備コードで常に上書きします。

PIN

PINの設定は、アクセスコントロールユニットで設定されたものと一致する必要があります。

長さ (0-32)：PINの桁数を入力します。ユーザーがリーダーを使用する際にPINの使用が不要の場合は、長さを「0」に設定します。

タイムアウト (秒、3-50)PINを受信しなかった場合に、装置が待機モードに戻るまでに経過する必要のある秒数を入力します。

エントリーリスト

エントリーリストを使用すると、認証情報保持者がカードやPINまたはQR Code® を使用してドアの開放などのさまざまなアクションを実行できるようにデバイスを設定できます。認証情報は装置にローカルで保存されます。この機能を外部のドアコントローラーと組み合わせることもできます。

QRコードは、日本およびその他の国々におけるデンソーウェイブ株式会社の登録商標です。

認証情報保持者

Use Entry list (エントリーリストを使用):エントリーリスト機能を使用するには、オンにします。

Use connected door controller (接続されたドアコントローラーを使用):装置がドアコントローラーにすでに接続されている場合は、オンにします。エントリーリストに存在しない認証情報が提示された場合、接続されたドアコントローラーに要求が送信されます。エントリーリストにある認証情報は送信されません。

Add credential holder (認証情報保持者を追加):クリックして、新しい認証情報保持者を追加します。

First name (名):名を入力します。

Last name (姓):姓を入力します。

Credential type (認証情報のタイプ):

- PIN:
  - PIN：一意のPINを入力します。または、[Generate (生成)] をクリックすると、PINが自動的に作成されます。
- Card (カード):
  - UID：カードのUIDとビット長を入力するか、[Get latest (最新データを取得)] をクリックして最新のカードスワイプからデータを取得します。
- QR Code®

Event condition (イベント条件):認証情報保持者が認証情報を使用するときにトリガーする条件を1つ以上選択します。結果のアクションを設定するには、[System (システム)] > [Events (イベント)] に移動し、ここで選択した条件を使用してルールを作成します。

Valid from (発効日):認証情報をすぐに有効にするには、[Current device time (現在のデバイス時刻)] を選択します。認証情報を有効にするタイミングを指定するには、クリアします。

Valid to (失効日):

- No end date (終了日なし):認証情報は無期限に有効です。
- End date (終了日):認証情報が無効になる日時を指定します。
- Number of times (回数):認証情報保持者が認証情報を使用できる回数を指定します。フィールドの値は、認証情報が使用されるたびに減り、残りの使用回数を示します。

Notes (メモ):任意の情報を入力します。

Suspend (停止):認証情報を一時的に無効にする場合に、選択します。

Download QR Code when saving (保存時にQR Codeをダウンロード):認証情報のタイプとしてQR Codeを選択した場合、このチェックボックスを選択すると、[Save (保存)] をクリックするとQR Codeをダウンロードできます。

イベントログ

イベントログには、エントリーリストのイベントのリストが表示されます。ログファイルの最大サイズは2MBで、これは約6000イベントに相当します。

Export all (すべてエクスポート):クリックすると、リスト内のすべてのイベントをエクスポートできます。サブセットのみをエクスポートするには、対象のイベントを選択してください。イベントはCSV形式でエクスポートされます。

フィルター:クリックすると、特定の時間帯に発生したイベントが表示されます。

🔍: 入力すると、リスト内の一致するすべてのコンテンツを検索できます。

音声

デバイスの設定

入力:音声入力のオン/オフを切り替えます。入力のタイプを表示します。

入力タイプ:内蔵マイクやライン入力など、入力のタイプを選択します。

電源タイプ:入力の電源タイプを選択します。

変更を適用する:選択した内容を適用します。

Noise cancellation (ノイズキャンセル):オンに設定すると、バックグラウンドノイズを除去して音質が向上します。

エコーキャンセル:オンにすると、双方向通信時のエコーが除去されます。

個別のゲインコントロール:オンにすると、入力タイプごとに個別にゲインを調整することができます。

自動ゲインコントロール:オンにすると、サウンドの変化に合わせてゲインが動的に調整されます。

Gain (ゲイン):スライダーを使用してゲインを変更します。マイクのアイコンをクリックすると、ミュート、ミュート解除ができます。

出力:出力のタイプを表示します。

Gain (ゲイン):スライダーを使用してゲインを変更します。スピーカーのアイコンをクリックすると、ミュート、ミュート解除ができます。

自動音量制御:これをオンにすると、デバイスで周囲の騒音レベルに基づいてゲインが自動的かつ動的に調整されるようになります。自動音量制御は、ラインとテレコイルを含め、すべての音声出力に影響します。

ストリーム

エンコード方式:入力ソースストリーミングに使用するエンコード方式を選択します。エンコード方式は、音声入力がオンになっている場合にのみ選択できます。音声入力がオフになっている場合は、[**Enable audio input (音声入力を有効にする)**] をクリックしてオンにします。

音声クリップ

クリップを追加:新しい音声クリップを追加します。au、.mp3、.opus、.vorbis、.wavファイルを使用できます。

音声クリップを再生します。

音声クリップの再生を停止します。

コンテキストメニューは以下を含みます。

- **Rename (名前の変更)**:オーディオクリップの名前を変更します。
- **Create link (リンクを作成)**:使用する場合は、音声クリップを装置上で再生するURLを作成します。クリップの音量と再生回数を指定します。
- **Download (ダウンロード)**:音声クリップをコンピューターにダウンロードします。
- **削除**:装置から音声クリップを削除します。

録画

進行中の録画:装置で進行中のすべての録画を表示します。

装置で録画を開始します。

保存先のストレージ装置を選択します。

装置で録画を停止します。

トリガーされた録画は、手動で停止したとき、または装置がシャットダウンされたときに終了します。

連続録画は、手動で停止するまで続行されます。装置がシャットダウンされた場合でも、録画は装置が再起動されるときまで続行されます。

録画を再生します。

録画の再生を停止します。

録画に関する情報とオプションを表示または非表示にします。

Set export range (エクスポート範囲の設定):録画の一部のみをエクスポートする場合は、時間範囲を入力します。装置の位置とは異なるタイムゾーンで作業する場合は、時間範囲が装置のタイムゾーンに基づくことに注意してください。

Encrypt (暗号化):エクスポートする録画のパスワードを設定する場合に選択します。エクスポートしたファイルをパスワードなしで開くことができなくなります。

クリックすると、録画が削除されます。

Export (エクスポート):録画の全体または一部をエクスポートします。

クリックして録画にフィルターを適用します。

From (開始):特定の時点以降に行われた録画を表示します。

To (終了):特定の時点までに行われた録画を表示します。

ソース:ソースに基づいて録画を表示します。ソースはセンサーを指します。

Event (イベント):イベントに基づいて録画を表示します。

ストレージ:ストレージタイプに基づいて録画を表示します。

アプリ

アプリを追加: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。

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*にアクセスします。ライセンスキーを入手するには、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ブラウザー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。
  - Trusted NTS KE CA certificates (信頼できるNTS KE CA証明書):安全なNTS KE時刻同期に使用する信頼できるCA証明書を選択するか、なしのままにします。
  - 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。
- 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。
  - 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。
- 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。
  - 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。真北が0です。
- **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。

設定の確認

インタラクティブな装置画像:画像内のボタンをクリックして、実際のキー押下をシミュレートします。これにより、装置に物理的にアクセスしなくても、設定の試行やハードウェアのトラブルシューティングを行うことができます。

最新の認証情報 ：最後に登録された認証情報に関する情報を表示します。

最新の認証情報データを表示します。

コンテキストメニューは以下を含みます。

- **Reverse UID (UIDを反転させる)**：UIDのバイト順を反転させます。
- **Revert UID (UIDを元に戻す)**：UIDのバイト順を元に戻します。
- **Copy to clipboard (クリップボードにコピーする)**:UIDをコピーします。

Check credentials (認証情報の確認) ：UIDまたはPINを入力し、送信して認証情報を確認します。システムは、装置で認証情報を使用した場合と同じように応答します。UIDとPINの両方が必要な場合は、まず、UIDを入力します。

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 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、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に選択します。

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の動的更新： IPアドレスの変更時に、デバイスでのドメインネームサーバーレコードの自動更新が可能となります。

DNS名の登録：デバイスのIPアドレスを指す一意のドメイン名を入力します。使用できる文字は、A～Z、a～z、0～9、-、_です。

TTL：TTL（Time to Live）とは、DNSレコードの更新が必要となるまでの有効期間を指します。

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。装置はポート80または1024～65535の範囲のポートを許可します。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。装置はポート443または1024～65535の範囲のポートを許可します。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 and CDP (LLDPおよび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。

グローバルプロキシー

Https proxy (HTTPプロキシー):許可された形式に従って、グローバルプロキシーホストまたはIPアドレスを指定します。

Https proxy (HTTPSプロキシー):許可された形式に従って、グローバルプロキシーホストまたはIPアドレスを指定します。

httpおよびhttpsプロキシーで許可されるフォーマット:

- http(s)://host:port
- http(s)://user@host:port
- http(s)://user:pass@host:port

注

装置を再起動し、グローバルプロキシー設定を適用します。

No proxy (プロキシーなし):グローバルプロキシーをバイパスするには、No proxy (プロキシーなし)を使用します。リスト内のオプションのいずれかを入力するか、コンマで区切って複数入力します。

- 空白にする
- IPアドレスを指定する
- CIDR形式でIPアドレスを指定する
- ドメイン名を指定する (www.<ドメイン名>.comなど)
- 特定のドメイン内のすべてのサブドメインを指定する (.<ドメイン名>.comなど)

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*を参照してください。

Allow O3C (O3Cを許可):

- [ワンクリック]:デフォルトの選択肢です。O3Cに接続するには、デバイスのコントロールボタンを押してください。ボタンの押し方は、デバイスモデルにより異なります。一度押して離し、ステータスLEDが点滅するまで待つか、またはステータスLEDが点滅するまで押し続けてください。[常時]を有効にして接続を維持するには、24時間以内にこのデバイスをO3Cサービスに登録してください。登録しないと、このデバイスはO3Cから切断されます。
- [常時]:デバイスは、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。一度デバイスを登録すれば、常時接続された状態になります。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。
- [なし]:O3Cを切断します。

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、プロキシー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]: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。
- [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) (オーナー認証キー、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、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):デバイスの起動時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。
    - Link down (リンクダウン):リンクの状態が接続から切断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、HTTPSを有効化し、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を有効化せずに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。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
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。

証明書を追加:クリックして証明書を追加します。ステップバイステップのガイドが開きます。

- **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**:[Trusted Execution Environment (SoC TEE)]、[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/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:

- **Trusted Execution Environment (SoC TEE)**: 安全なキーストアにSoC TEEを使用する場合に選択します。
- **セキュアエレメント (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場合に選択します。
- **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を使用する場合に選択します。

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デバイス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を使用):IEEE 802.1xプロトコルを使用する場合に選択します。

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

Firewall (ファイアウォール):オンにするとファイアウォールが有効になります。

Default Policy (デフォルトポリシー):ルールで定義されていない接続要求をファイアウォールがどのように処理するかを選択します。

- ACCEPT (許可): デバイス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。
- DROP (拒否): デバイスへのすべての接続をブロックします。

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、ポートからデバイスへの接続を許可またはブロックするルールを作成できます。

+ New rule (新規ルールの追加):クリックすると、ルールを作成できます。

Rule type (ルールタイプ):

- FILTER (フィルター): ルールで定義された条件に一致するデバイスからの接続を許可またはブロックする場合に選択します。
  - Policy (ポリシー)：ファイアウォールルールに [Accept (許可)] または [Drop (拒否)] を選択します。
  - IP range (IP範囲):許可またはブロックするアドレス範囲を指定する場合に選択します。[Start (開始)] と [End (終了)] にIPv4/IPv6を使用します。
  - IP address (IPアドレス):許可またはブロックするアドレスを入力します。IPv4/IPv6またはCIDR形式を使用します。
  - Protocol (プロトコル):許可またはブロックするネットワークプロトコル (TCP、UDP、または両方) を選択します。プロトコルを選択すると、ポートも指定する必要があります。
  - MAC: 許可またはブロックするデバイスのMACアドレスを入力します。
  - Port range (ポート範囲):許可またはブロックするポート範囲を指定する場合に選択します。[Start (開始)] と [End (終了)] にそれらを追加します。
  - ポート:許可またはブロックするポート番号を入力します。ポート番号は1～65535の間で指定する必要があります。
  - Traffic type (トラフィックタイプ):許可またはブロックするトラフィックタイプを選択します。
    - UNICAST (ユニキャスト): 1つの送信元から1つの送信先へのトラフィック。
    - BROADCAST (ブロードキャスト): 1つの送信元からネットワーク上のすべてのデバイスへのトラフィック。
    - MULTICAST (マルチキャスト): 複数の送信元から複数の送信先へのトラフィック。
- LIMIT (制限): ルールで定義された条件に一致するデバイスからの接続を許可しますが、過剰なトラフィックを軽減するために制限を適用する場合に選択します。
  - IP range (IP範囲):許可またはブロックするアドレス範囲を指定する場合に選択します。[Start (開始)] と [End (終了)] にIPv4/IPv6を使用します。
  - IP address (IPアドレス):許可またはブロックするアドレスを入力します。IPv4/IPv6またはCIDR形式を使用します。
  - Protocol (プロトコル):許可またはブロックするネットワークプロトコル (TCP、UDP、または両方) を選択します。プロトコルを選択すると、ポートも指定する必要があります。
  - MAC: 許可またはブロックするデバイスのMACアドレスを入力します。
  - Port range (ポート範囲):許可またはブロックするポート範囲を指定する場合に選択します。[Start (開始)] と [End (終了)] にそれらを追加します。
  - ポート:許可またはブロックするポート番号を入力します。ポート番号は1～65535の間で指定する必要があります。

- Unit (単位):許可またはブロックする接続のタイプを選択します。
- Period (期間):[Amount (量)] に関連する期間を選択します。
- Amount (量):設定した [Period (期間)] 内にデバイスの接続を許可する最大回数を設定します。上限は65535です。
- Burst (バースト):設定した [Period (期間)] に [Amount (量)] を1回超えることを許可する接続の数を入力します。一この数に達すると、設定した期間に設定した量のみ許可されます。
- Traffic type (トラフィックタイプ):許可またはブロックするトラフィックタイプを選択します。
  - UNICAST (ユニキャスト): 1つの送信元から1つの送信先へのトラフィック。
  - BROADCAST (ブロードキャスト): 1つの送信元からネットワーク上のすべてのデバイスへのトラフィック。
  - MULTICAST (マルチキャスト): 複数の送信元から複数の送信先へのトラフィック。

Test rules (テストルール):クリックして、定義したテストを追加します。

- Time in seconds (テスト時間、秒):ルールのテストに制限時間を設定します。
- Roll back (ロールバック):クリックすると、ルールをテストする前にファイアウォールを前の状態にロールバックします。
- Apply rules (ルールの適用):クリックすると、テストなしでルールが有効になります。これは推奨されません。

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。ソフトウェアは、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。署名用のキーはAxisが保有しており、カスタム署名付きAXIS OS証明書はAxisしか作成できません。

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

＋ **アカウントを追加**: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**):次のアクセス権を持っています:
  - ビデオストリームのスナップショットを見て撮影する。
  - 録画を再生およびエクスポートする。
  - PTZ**アカウント**アクセスをパン、チルト、ズームに使用します。

⋮ 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。

匿名アクセス

Allow anonymous viewing (**匿名の閲覧を許可する**):アカウントでログインせずに誰でも閲覧者として装置にアクセスできるようにする場合は、オンにします。

匿名のPTZ操作を許可する :オンにすると、匿名ユーザーに画像のパン、チルト、ズームを許可します。

SSHアカウント

＋ Add SSH account (SSHアカウントを追加):クリックして、新しいSSHアカウントを追加します。

- Enable SSH (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)

＋ Add virtual host (仮想ホストを追加):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。

クライアント認証情報付与設定

Admin claim (管理者請求):管理者権限の値を入力します。

Verification URL (検証URL): APIエンドポイント認証用のWebリンクを入力します。

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。

Save (保存):クリックして値を保存します。

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 (クライアント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。

Provider URL (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。

Enable OpenID (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。

イベント

ルール

ルールは、製品がアクションを実行するためのトリガーとなる条件を定義します。このリストには、本製品で現在設定されているすべてのルールが表示されます。

注

最大256のアクションルールを作成できます。

+ **ルールを追加**:ルールを作成します。

名前:アクションルールの名前を入力します。

Wait between actions (アクション間の待ち時間):ルールを有効化する最短の時間間隔 (hh:mm:ss) を入力します。たとえば、デイナイトモードの条件によってルールが有効になる場合、このパラメーターを設定することで、日の出や日没時のわずかな光の変化によりルールが反復的に有効になるのを避けられます。

Condition (条件):リストから条件を選択します。装置がアクションを実行するためには、条件を満たす必要があります。複数の条件が定義されている場合、すべての条件が満たされたときにアクションがトリガーされます。特定の条件については、「*イベントのルールの使用開始*」を参照してください。

Use this condition as a trigger (この条件をトリガーとして使用する):この最初の条件を開始トリガーとしてのみ機能させる場合に選択します。つまり、いったんルールが有効になると、最初の条件の状態に関わらず、他のすべての条件が満たされている限り有効のままになります。このオプションを選択しない場合、ルールは単純にすべての条件が満たされたときに有効化されます。

Invert this condition (この条件を逆にする):選択した条件とは逆の条件にする場合に選択します。

+ **条件を追加**:新たに条件を追加する場合にクリックします。

Action (アクション):リストからアクションを選択し、必要な情報を入力します。特定のアクションについては、「*イベントのルールの使用開始*」を参照してください。

送信先

イベントについて受信者に通知したり、ファイルを送信したりするように装置を設定できます。

注

FTPまたはSFTPを使用するように装置を設定した場合、ファイル名に付加される固有のシーケンス番号を変更したり削除したりしないでください。その場合、イベントごとに1つの画像しか送信できません。

このリストには、製品で現在設定されているすべての送信先とそれらの設定に関する情報が示されます。

注

最大20名の送信先を作成できます。

送信先を追加:クリックすると、送信先を追加できます。

名前:送信先の名前を入力します。

タイプ:リストから選択します:

- FTP
  - **[ホスト]**:サーバーのIPアドレスまたはホスト名を入力します。ホスト名を入力した場合は、必ず、[**System (システム) > Network (ネットワーク) > IPv4 and IPv6 (IPv4 と IPv6)**] で DNS サーバーを指定します。
  - **ポート**:FTPサーバーに使用するポート番号。デフォルトは21です。
  - **Folder (フォルダー)**:ファイルを保存するディレクトリのパスを入力します。FTPサーバー上に存在しないディレクトリを指定すると、ファイルのアップロード時にエラーメッセージが表示されます。
  - **Username (ユーザー名)**:ログインのユーザー名を入力します。
  - **パスワード**:ログインのパスワードを入力します。
  - **Use temporary file name (一時ファイル名を使用する)**:選択すると、自動的に生成された一時的なファイル名でファイルがアップロードされます。アップロードが完了した時点で、ファイル名が目的の名前に変更されます。アップロードが中止/中断されても、破損したファイルが発生することはありません。ただし、一時ファイルが残る可能性はあります。これにより、目的の名前を持つすべてのファイルが正常であると確信できます。
  - **Use passive FTP (パッシブFTPを使用する)**:通常は、製品がFTPサーバーに要求を送ることでデータ接続が開かれます。この接続では、対象サーバーとのFTP制御用接続とデータ用接続の両方が装置側から開かれます。一般に、装置と対象FTPサーバーの間にファイアウォールがある場合に必要となります。
- HTTP
  - **URL**:HTTPサーバーのネットワークアドレスと、要求の処理を行うスクリプトを入力します。たとえば、http://192.168.254.10/cgi-bin/notify.cgiと入力します。
  - **Username (ユーザー名)**:ログインのユーザー名を入力します。
  - **パスワード**:ログインのパスワードを入力します。
  - **Proxy (プロキシ)**:HTTPサーバーに接続するためにプロキシサーバーを渡す必要がある場合は、これをオンにし、必要な情報を入力します。
- HTTPS
  - **URL**:HTTPSサーバーのネットワークアドレスと、要求の処理を行うスクリプトを入力します。たとえば、https://192.168.254.10/cgi-bin/notify.cgiと入力します。
  - **Validate server certificate (サーバー証明書を検証する)**:HTTPSサーバーが作成した証明書を検証する場合にオンにします。
  - **Username (ユーザー名)**:ログインのユーザー名を入力します。
  - **パスワード**:ログインのパスワードを入力します。
  - **Proxy (プロキシ)**:HTTPSサーバーに接続するためにプロキシサーバーを渡す必要がある場合にオンにして、必要な情報を入力します。
- ネットワークストレージ
  NAS (network-attached storage) などのネットワークストレージを追加し、それを録画ファイルの保存先として使用することができます。ファイルは.mkv (Matroska) 形式で保存されます。
  - **[ホスト]**:ネットワークストレージのIPアドレスまたはホスト名を入力します。
  - **共有**:ホスト上の共有の名を入力します。

- Folder (フォルダー):ファイルを保存するディレクトリのパスを入力します。
- Username (ユーザー名):ログインのユーザー名を入力します。
- パスワード:ログインのパスワードを入力します。

- SFTP
  - [ホスト]:サーバーのIPアドレスまたはホスト名を入力します。ホスト名を入力した場合は、必ず、[System (システム) > Network (ネットワーク) > IPv4 and IPv6 (IPv4 と IPv6)] で DNS サーバーを指定します。
  - ポート:SFTPサーバーに使用するポート番号。デフォルトは22です。
  - Folder (フォルダー):ファイルを保存するディレクトリのパスを入力します。SFTPサーバー上に存在しないディレクトリを指定すると、ファイルのアップロード時にエラーメッセージが表示されます。
  - Username (ユーザー名):ログインのユーザー名を入力します。
  - パスワード:ログインのパスワードを入力します。
  - SSH host public key type (MD5) (SSHホスト公開鍵タイプ (MD5)):リモートホストの公開鍵のフィンガープリント (32桁の16進数) を入力します。SFTPクライアントは、RSA、DSA、ECDSA、およびED25519ホストキータイプによるSSH-2を使用するSFTPサーバーをサポートします。RSAは、ネゴシエーション時の推奨方式です。その後には、ECDSA、ED25519、DSAが続きます。SFTPサーバーで使用されている正しいMD5ホストキーを入力してください。AxisデバイスはMD5とSHA-256の両方のハッシュキーをサポートしていますが、MD5よりもセキュリティが強いため、SHA-256を使用することをお勧めします。AxisデバイスでSFTPサーバーを設定する方法の詳細については、*AXIS OSポータル*にアクセスしてください。
  - SSH host public key type (SHA256) (SSHホスト公開鍵タイプ (SHA256)):リモートホストの公開鍵のフィンガープリント (43桁のBase64エンコード文字列) を入力します。SFTPクライアントは、RSA、DSA、ECDSA、およびED25519ホストキータイプによるSSH-2を使用するSFTPサーバーをサポートします。RSAは、ネゴシエーション時の推奨方式です。その後には、ECDSA、ED25519、DSAが続きます。SFTPサーバーで使用されている正しいMD5ホストキーを入力してください。AxisデバイスはMD5とSHA-256の両方のハッシュキーをサポートしていますが、MD5よりもセキュリティが強いため、SHA-256を使用することをお勧めします。AxisデバイスでSFTPサーバーを設定する方法の詳細については、*AXIS OSポータル*にアクセスしてください。
  - Use temporary file name (一時ファイル名を使用する):選択すると、自動的に生成された一時的なファイル名でファイルがアップロードされます。アップロードが完了した時点で、ファイル名が目的の名前に変更されます。アップロードが中止/中断されても、ファイルが破損することはありません。ただし、一時ファイルが残る可能性はあります。これにより、目的の名前を持つすべてのファイルが正常であると確信できます。

- SIPまたはVMS :
  SIP:選択してSIP呼び出しを行います。
  VMS:選択してVMS呼び出しを行います。
  - 送信元のSIPアカウント:リストから選択します。
  - 送信先のSIPアドレス:SIPアドレスを入力します。
  - テスト:クリックして、呼び出しの設定が機能することをテストします。
- 電子メール
  - 電子メールの送信先:電子メールの宛先のアドレスを入力します。複数のアドレスを入力するには、カンマで区切ります。
  - 電子メールの送信元:送信側サーバーのメールアドレスを入力します。

- Username (ユーザー名):メールサーバーのユーザー名を入力します。認証の必要のないメールサーバーの場合は、このフィールドを空にします。
- パスワード:メールサーバーのパスワードを入力します。認証の必要のないメールサーバーの場合は、このフィールドを空にします。
- Email server (SMTP) (電子メールサーバー (SMTP)):SMTPサーバーの名前 (smtp.gmail.com、smtp.mail.yahoo.comなど) を入力します。
- ポート:SMTPサーバーのポート番号を0～65535の範囲で入力します。デフォルト設定値は587です。
- [暗号化]:暗号化を使用するには、SSL または TLS を選択します。
- Validate server certificate (サーバー証明書を検証する):暗号化を使用している場合にこれを選択すると、装置の身元を検証できます。この証明書は、自己署名または認証局 (CA) 発行の証明書のどちらでも可能です。
- POP authentication (POP認証):オンにすると、POPサーバーの名前 (pop.gmail.comなど) を入力できます。

注

一部の電子メールプロバイダーでは、大量の添付ファイルやスケジュール設定済みメールなどがセキュリティフィルターによって受信または表示できないようになっています。電子メールプロバイダーのセキュリティポリシーを確認し、メールアカウントのロックや、必要な電子メールの不着などが起こらないようにしてください。

- TCP
  - [ホスト]:サーバーのIPアドレスまたはホスト名を入力します。ホスト名を入力した場合は、必ず、[System (システム) > Network (ネットワーク) > IPv4 and IPv6 (IPv4 と IPv6)] で DNS サーバーを指定します。
  - ポート:サーバーへのアクセスに使用したポート番号を入力します。

Test (テスト):クリックすると、セットアップをテストすることができます。

⋮ コンテキストメニューは以下を含みます。

View recipient (送信先の表示):クリックすると、すべての送信先の詳細が表示されます。

Copy recipient (送信先のコピー):クリックすると、送信先をコピーできます。コピーする際、新しい送信先に変更を加えることができます。

Delete recipient (送信先の削除):クリックすると、受信者が完全に削除されます。

スケジュール

スケジュールとパルスは、ルールで条件として使用することができます。このリストには、製品で現在設定されているすべてのスケジュールとパルス、およびそれらの設定に関する情報が示されます。

＋ スケジュールを追加:クリックすると、スケジュールやパルスを作成できます。

手動トリガー

手動トリガーを使用すると、ルールを手動でトリガーできます。手動トリガーは、本製品の設置、設定中にアクションを検証する目的などで使用します。

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。

デバイスをMQTTクライアントとして設定します。MQTTの通信は、2つのエンティティ (クライアントとブローカー) 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ナレッジベース*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。ALPNは、HTTPなどの他のプロトコルで使用される同じポート経由で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通信のための専用ポートが開かれていない可能性があります。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オーバーSSLとMQTTオーバー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)：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。

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で構いません。

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で構いません。

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タメントメッセージ

最終意思テスタメント(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タ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。

＋ 条件を追加: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を追加**: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。

MQTTオーバーレイ

注

MQTTオーバーレイ修飾子を追加する前に、MQTTブローカーに接続します。

＋ **オーバーレイ修飾子を追加**:クリックして新しいオーバーレイ修飾子を追加します。

Topic filter (トピックフィルター):オーバーレイに表示するデータを含むMQTTトピックを追加します。

Data field (データフィールド):オーバーレイに表示するメッセージペイロードのキーを指定します。メッセージはJSON形式であるとします。

Modifier (修飾子):オーバーレイを作成するときに、生成された修飾子を使用します。

- **#XMP**で始まる修飾子は、トピックから受信したすべてのデータを示します。
- **#XMD**で始まる修飾子は、データフィールドで指定されたデータを示します。

ストレージ

ネットワークストレージ

使用しない:オンにすると、ネットワークストレージは使用されません。

Add network storage (ネットワークストレージの追加):クリックして、録画を保存できるネットワーク共有を追加します。

- アドレス:ホストサーバーのホスト名 (通常はNAS (network-attached storage) またはIPアドレスを入力します。DHCPではなく固定IPアドレスを使用するようにホストを設定するか (動的IPアドレスは変わる可能性があるため、DHCPは使用しない)、DNS名を使用することをお勧めします。Windows SMB/CIFS名はサポートされていません。
- Network share (ネットワーク共有):ホストサーバー上の共有場所の名前を入力します。各Axis装置にはそれぞれのフォルダーがあるため、複数の装置で同じネットワーク共有を使用できます。
- User (ユーザー):サーバーにログインが必要な場合は、ユーザー名を入力します。特定のドメインサーバーにログインするには、`DOMAIN\username` を入力します。
- パスワード:サーバーにログインが必要な場合は、パスワードを入力します。
- SMB version (SMBバージョン):NASに接続するSMBストレージプロトコルのバージョンを選択します。[Auto (自動)] を選択すると、装置は、セキュアバージョンであるSMB3.02、3.0、2.1 のいずれかにネゴシエートを試みます。1.0または2.0を選択すると、上位バージョンをサポートしない旧バージョンのNASに接続できます。Axis装置でのSMBサポートの詳細については、こちらをご覧ください。
- Add share without testing (テストなしで共有を追加する):接続テスト中にエラーが検出された場合でも、ネットワーク共有を追加する場合に選択します。サーバーにパスワードが必要な場合でも、パスワードを入力しなかったなど、エラーが発生する可能性があります。

ネットワークストレージを削除する:クリックして、ネットワーク共有への接続をマウント解除、バインド解除、削除します。これにより、ネットワーク共有のすべての設定が削除されます。

Unbind (バインド解除):クリックして、ネットワーク共有をアンバインドし、切断します。
Bind (バインド):クリックして、ネットワーク共有をバインドし、接続します。

Unmount (マウント解除):クリックして、ネットワーク共有をマウント解除します。
Mount (マウント):クリックしてネットワーク共有をマウントします。

Write protect (書き込み禁止):オンに設定すると、ネットワーク共有への書き込みが停止され、録画が削除されないように保護されます。書き込み保護されたネットワーク共有はフォーマットできません。

Retention time (保存期間):録画の保存期間を選択し、古い録画の量を制限したり、データストレージに関する規制に準拠したりします。ネットワークストレージがいっぱいになると、設定した時間が経過する前に古い録画が削除されます。

ツール

- 接続をテストする:ネットワーク共有への接続をテストします。
- Format (形式):ネットワーク共有をフォーマットします。たとえば、すべてのデータをすばやく消去する必要があるときです。CIFSをファイルシステムとして選択することもできます。

Use tool (ツールを使用)クリックして、選択したツールをアクティブにします。

オンボードストレージ

重要

データ損失や録画データ破損の危険があります。装置の稼働中はSDカードを取り外さないでください。SDカードを取り外す前に、SDカードをマウント解除します。

Unmount (マウント解除):SDカードを安全に取り外す場合にクリックします。

Write protect (書き込み禁止):オンにすると、SDカードへの書き込みが防止され、録画が削除されなくなります。書き込み保護されたSDカードはフォーマットできません。

Autoformat (自動フォーマット):オンにすると、新しく挿入されたSDカードが自動的にフォーマットされます。ファイルシステムをext4にフォーマットします。

使用しない:オンにすると、録画のSDカードへの保存が停止します。SDカードを無視すると、装置はカードがあっても認識しなくなります。この設定は管理者のみが使用できます。

Retention time (保存期間):録画の保存期間を選択し、古い録画の量を制限したり、データストレージの規制に準拠したりします。SDカードがいっぱいになると、保存期間が切れる前に古い録画が削除されます。

ツール

- **Check (チェック)**:SDカードのエラーをチェックします。
- **Repair (修復)**:ファイルシステムのエラーを修復します。
- **Format (形式)**:SDカードをフォーマットしてファイルシステムを変更し、すべてのデータを消去します。SDカードはext4ファイルシステムにのみフォーマットすることができます。Windows®からファイルシステムにアクセスするには、サードパーティ製のext4ドライバーまたはアプリケーションが必要です。
- **Encrypt (暗号化)**:このツールを使用して、暗号化ありでSDカードをフォーマットします。これにより、SDカードに保存されているデータはすべて削除されます。SDカードに保存する新規データはすべて暗号化されます。
- **Decrypt (復号化)**:このツールを使用して、暗号化なしでSDカードをフォーマットします。これにより、SDカードに保存されているデータはすべて削除されます。SDカードに保存する新規データは暗号化されません。
- **Change password (パスワードの変更)**:SDカードの暗号化に必要なパスワードを変更します。

Use tool (ツールを使用)クリックして、選択したツールをアクティブにします。

Wear trigger (消耗トリガー):アクションをトリガーするSDカードの消耗レベルの値を設定します。消耗レベルは0～200%です。一度も使用されていない新しいSDカードの消耗レベルは0%です。消耗レベルが100%になると、SDカードの寿命が近い状態にあります。消耗レベルが200%に達すると、SDカードが故障するリスクが高くなります。消耗トリガーを80～90%の間に設定することをお勧めします。これにより、SDカードが消耗し切る前に、録画をダウンロードしたり、SDカードを交換したりする時間ができます。消耗トリガーを使用すると、イベントを設定し、消耗レベルが設定値に達したときに通知を受け取ることができます。

ストリームプロファイル

ストリームプロファイルは、ビデオストリームに影響する設定のグループです。ストリームプロファイルは、たとえばイベントを作成するときや、ルールを使って録画するときなど、さまざまな場面で使うことができます。

ストリームプロファイルを追加:クリックして、新しいストリームプロファイルを作成します。

Preview (プレビュー):選択したストリームプロファイル設定によるビデオストリームのプレビューです。ページの設定を変更すると、プレビューは更新されます。装置のビューエリアが異なる場合は、画像の左下隅にあるドロップダウンリストでビューエリアを変更できます。

名前:プロファイルの名前を追加します。

Description (説明):プロファイルの説明を追加します。

Video codec (ビデオコーデック):プロファイルに適用するビデオコーデックを選択します。

解像度:この設定の説明については、を参照してください。

フレームレート:この設定の説明については、を参照してください。

圧縮:この設定の説明については、を参照してください。

Zipstream :この設定の説明については、を参照してください。

ストレージ用に最適化する :この設定の説明については、を参照してください。

ダイナミックFPS :この設定の説明については、を参照してください。

ダイナミックGOP :この設定の説明については、を参照してください。

ミラーリング :この設定の説明については、を参照してください。

GOP長 :この設定の説明については、を参照してください。

ビットレート制御:この設定の説明については、を参照してください。

オーバーレイを含める :含めるオーバーレイのタイプを選択します。オーバーレイを追加する作成方法については、を参照してください。

音声を含める :この設定の説明については、を参照してください。

ONVIF

ONVIFアカウント

ONVIF (Open Network Video Interface Forum) は、エンドユーザー、インテグレーター、コンサルタント、メーカーがネットワークビデオ技術が提供する可能性を容易に利用できるようにするグローバルなインターフェース標準です。ONVIFによって、さまざまなベンダー製品間の相互運用、柔軟性の向上、コストの低減、陳腐化しないシステムの構築が可能になります。

ONVIFアカウントを作成すると、ONVIF通信が自動的に有効になります。装置とのすべてのONVIF通信には、アカウント名とパスワードを使用します。詳細については、*axis.com*にあるAxis開発者コミュニティを参照してください。

+ アカウントを追加:クリックして、新規のONVIFアカウントを追加します。

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。

Role (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)]。
  - アプリを追加しています。
- Media account (メディアアカウント):ビデオストリームの参照のみを行えます。

⋮ 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。

ONVIFメディアプロファイル

ONVIFメディアプロファイルは、メディアストリーム設定の変更に使用する一連の設定から構成されています。独自の設定を使用して新しいプロファイルを作成することも、設定済みのプロファイルを使用してすばやく設定することもできます。

メディアプロファイルを追加:クリックすると、新しいONVIFメディアプロファイルを追加できます。

プロファイル名:メディアプロファイルに名前を付けます。

Video source (ビデオソース):設定に使用するビデオソースを選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択します。ドロップダウンリストに表示される設定は、マルチビュー、ビューエリア、バーチャルチャンネルなど、装置のビデオチャンネルに対応しています。

Video encoder (ビデオエンコーダ):設定に使用するビデオエンコード方式を選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、エンコード方式の設定を調整します。ドロップダウンリストに表示される設定は、ビデオエンコーダの設定の識別子/名前となります。ユーザー0～15を選択して、独自の設定を適用します。または、デフォルトユーザーのいずれかを選択して、特定のエンコード方式の既定の設定を使用します。

注

装置で音声を有効にすると、音声ソースと音声エンコーダ設定を選択するオプションが有効になります。

音声ソース:設定に使用する音声入力ソースを選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、音声設定を調整します。ドロップダウンリストに表示される設定は、装置の音声入力に対応しています。装置に1つの音声入力がある場合、それはuser0です。装置に複数の音声入力がある場合、リストには追加のユーザーが表示されます。

音声エンコーダ:設定に使用する音声エンコード方式を選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、音声エンコード方式の設定を調整します。ドロップダウンリストに表示される設定は、音声エンコーダの設定の識別子/名前として機能します。

音声デコーダ:設定に使用する音声デコード方式を選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、設定を調整します。ドロップダウンリストに表示される設定は、設定の識別子/名前として機能します。

音声出力:設定に使用する音声出力形式を選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、設定を調整します。ドロップダウンリストに表示される設定は、設定の識別子/名前として機能します。

Metadata (メタデータ):設定に含めるメタデータを選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、メタデータ設定を調整します。ドロップダウンリストに表示される設定は、メタデータの設定の識別子/名前となります。

PTZ: 設定に使用するPTZ設定を選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、PTZ設定を調整します。ドロップダウンリストに表示される設定は、PTZをサポートする装置のビデオチャンネルに対応しています。

[**Create (作成)**]:クリックして、設定を保存し、プロファイルを作成します。

Cancel (キャンセル):クリックして、設定をキャンセルし、すべての設定をクリアします。

profile_x:プロファイル名をクリックして、既定のプロファイルを開き、編集します。

検知器

カメラに対するいたずら

カメラに対するいたずら検知器は、レンズが覆われたり、スプレーをかけられたり、ひどいピンボケになったりしてシーンが変わり、[Trigger delay (トリガー遅延)] に設定された時間が経過したときにアラームが発生します。いたずら検知器は、カメラが10秒以上動かなかった場合にのみ作動します。この間に、映像からいたずらを比較検知するためのシーンモデルが検知器によって設定されます。シーンモデルを正しく設定するには、カメラのピントを合わせ、適切な照明状態にして、輪郭が乏しい情景 (殺風景な壁など) にカメラが向かないようにする必要があります。「カメラに対するいたずら」は、アクションを作動させる条件として使用できます。

Trigger delay (トリガー遅延):「いたずら」条件が有効になってからアラームがトリガーされるまでの最小時間を入力します。これにより、映像に影響する既知の条件に関する誤ったアラームが発せられるのを防ぐことができます。

Trigger on dark images (暗い画像でトリガー):レンズにスプレーが吹き付けられた場合にアラームを生成するのは困難です。照明の条件の変化などによって同じように映像が暗くなる場合と区別できないからです。映像が暗くなるすべての場合にアラームが発生させるには、このパラメーターをオンにします。オフにした場合は、画像が暗くなってもアラームが発生しません。

注

動きのないシーンや混雑していないシーンでのいたずら検知用。

音声検知

これらの設定は、音声入力ごとに利用できます。

Sound level (音声レベル):音声レベルは0～100の範囲で調整します。0が最も感度が高く、100が最も感度が低くなります。音声レベルの設定時には、アクティビティインジケーターをガイドとして使用します。イベントを作成する際に、音声レベルを条件として使用することができます。音声レベルが設定値より高くなった場合、低くなった場合、または設定値を通過した場合にアクションを起こすように選択できます。

衝撃検知

衝撃検知機能:オンにすると、装置が物が当たったり、いたずらされたときにアラームが生成されます。

感度レベル:スライダーを動かして、装置がアラームを生成する感度レベルを調整します。値を低くすると、衝撃が強力な場合にのみ、装置がアラームを生成します。値を大きな値に設定すると、軽いいたずらでもアラームが生成されます。

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などの外部デバイスを接続します。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webインターフェースから有効化できます。

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。

Usage (用途):リレーポートのデフォルトオプションは [Door (ドア)] です。インジケーターアイコンがある装置の場合、状態が変化してドアのロックが解除されると、 が緑色に点灯します。リレーをドア以外のものに使用し、状態が変化してもアイコンが点灯しないようにする場合は、ポートに他のオプションのいずれかを選択できます。

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。デバイス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、デバイス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。

監視済み :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。

エッジツーエッジ

[Camera pairing (カメラペアリング)] では、Axisインターコムを対応するAxisカメラとペアリングして、カメラのライブストリームをSIPおよびVMS通話の対象エリアに含めることができます。

+ Add (追加):ペアリングするデバイスを追加します。

Discover devices (デバイスの検索):クリックするとネットワーク上のデバイスが検索されます。ネットワークがスキャンされると、利用可能なデバイスの一覧が表示されます。

注

一覧にはペアリング可能なデバイスだけでなく、検索されたすべてのAxisデバイスが表示されます。

Bonjourが有効になっているデバイスのみ検索できます。デバイスのBonjourを有効にするには、デバイスのWebインターフェースを開き、[System (システム)] > [Network (ネットワーク)] > [Network discovery protocols (ネットワーク検索プロトコル)] に移動します。

注

すでにペアリングされているデバイスには情報アイコンが表示されます。アイコンにカーソルを合わせると、すでにアクティブになっているペアリングの情報が表示されます。

一覧からデバイスをペアリングするには、+ をクリックします。

(ペアリングタイプの選択):ドロップダウンリストから選択します。

アドレス:カメラのホスト名またはIPアドレスを入力します。

Username (ユーザー名):カメラのユーザー名を入力します。

パスワード:カメラのパスワードを入力します。

ストリーミングプロトコル:[RTSP] または [SRTSP] を選択します。

Verify certificate (証明書の検証):選択して検証します。

Close (閉じる)：クリックして、すべてのフィールドをクリアします。

Connect (接続する):これをクリックすると、カメラが接続されます。

ペアリングされたデバイスの詳細情報を表示するには、⌄ をクリックします。

ビデオチャンネル:表示するビデオチャンネルまたはビューエリアを選択します。

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。
- View the audit log (監査ログを表示):クリックすると、ユーザーやシステムのアクティビティに関する情報 (認証の成否や設定など) が表示されます。

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。

タイプ:送信するログのタイプを選択します。

Test server setup (テストサーバーセットアップ):設定を保存する前に、すべてのサーバーにテストメッセージを送信します。

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。

プレイン設定

[Plain Config] (プレイン設定) は、Axis装置の設定経験のある上級ユーザー向けのページです。ほとんどのパラメーターは、このページから設定、編集することができます。

メンテナンス

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、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*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*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。
- **Automatic rollback (自動ロールバック)**: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。

トラブルシューティング

Reset PTR (PTRのリセット) :何らかの理由で、**パン**、**チルト**、または**ロール**の設定が想定どおりに機能していない場合は、PTRをリセットします。新品のカメラの場合、PTRモーターは常にキャリブレーションされています。しかし、カメラの電源が失われたり、モーターが手で動かされたりした場合など、キャリブレーションが失われることがあります。PTRをリセットすると、カメラは再キャリブレーションされ、工場出荷時の設定の位置に戻ります。

Calibration (キャリブレーション) :[Calibrate (キャリブレート)] をクリックすると、パン、チルト、ロールモーターがデフォルト位置に再較正されます。

Ping：Pingを実行するホストのホスト名またはIPアドレスを入力して、**[開始]** をクリックすると、デバイスから特定のアドレスへの通信経路が適切に機能しているかどうかを確認することができます。

ポートチェック：チェックするホスト名またはIPアドレスとポート番号を入力して、**[開始]** をクリックすると、デバイスから特定のIPアドレスとTCP/UDPポートへの接続が可能かどうかを確認することができます。

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。

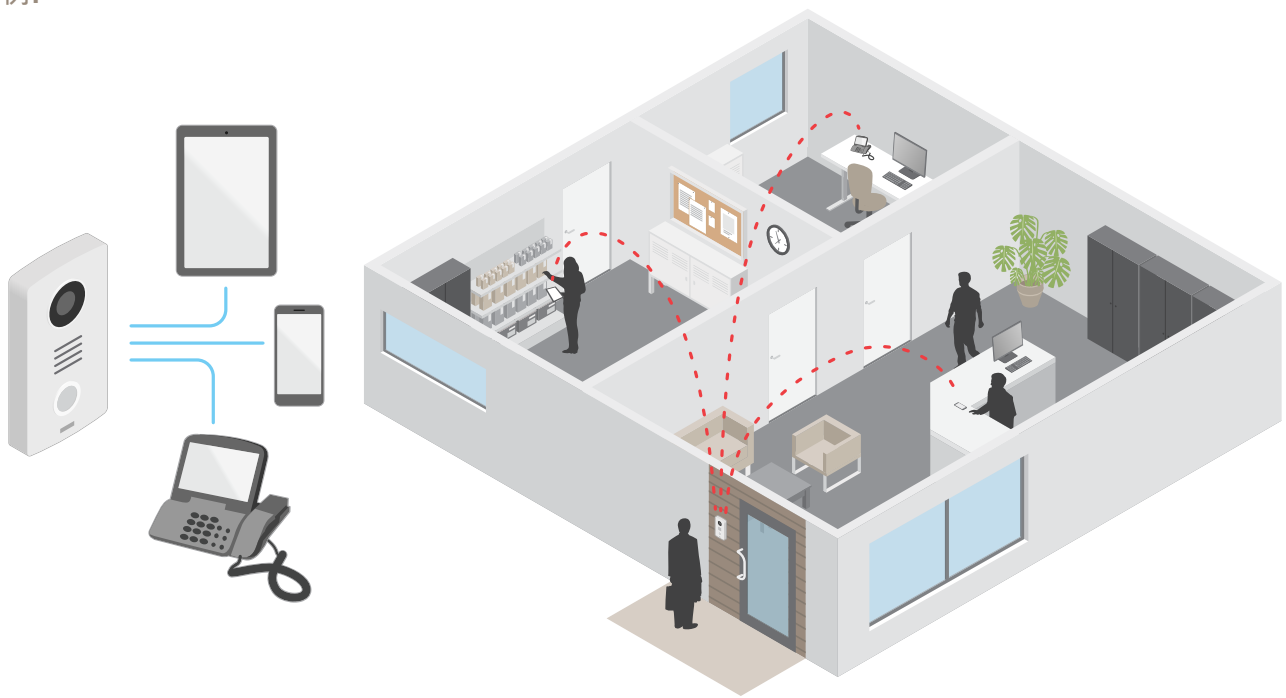
詳細情報

Voice over IP (VoIP)

Voice over IP (VoIP) は、インターネットなどのIPネットワーク上の音声通信とマルチメディアセッションを可能にするテクノロジー群です。従来の電話呼び出しでは、アナログ信号は公衆交換電話網 (PSTN) 経由のサーキット伝送を通じて送信されます。VoIP呼び出しでは、アナログ信号がデジタル信号に変換され、ローカルIPネットワークまたはインターネットを経由してデータパケットで信号を送信することができます。

本製品では、セッション開始プロトコル (SIP) およびDTMF (デュアルトーン多重周波数) 信号伝達によってVoIPが有効になっています。

例:



Axisインターカムで呼び出しボタンを押すと、1つ以上の既定の送信先への呼び出しが開始されます。送信先が応答すると、呼び出しが確立されます。VoIPテクノロジーで音声と映像が転送されます。

セッション開始プロトコル (SIP)

セッション開始プロトコル (SIP) を使用して、VoIP呼び出しを設定、維持、および終了します。2つ以上のグループ (SIPユーザーエージェント) の間で呼び出しを行うことができます。SIP呼び出しは、SIP電話、ソフトフォン、SIP対応Axisデバイスなどを使用して行うことができます。

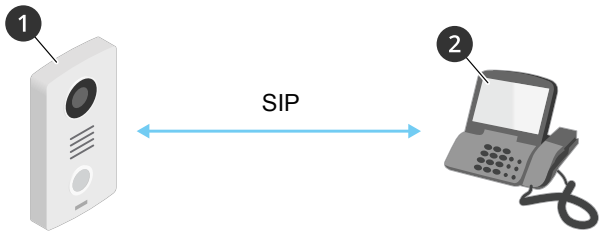
実際の音声またはビデオは、RTP (Real-time Transport Protocol) などのトランスポートプロトコルを使用して、SIPユーザーエージェントの間で交換されます。

ピアツーピア設定を使用するか、PBXを使用したネットワークを通じて、ローカルネットワークで呼び出しを行うことができます。

ピアツーピアSIP (P2PSIP)

最も基本的なタイプのSIP通信は、2つ以上のSIPユーザーエージェントの間で直接行われます。これは、ピアツーピアSIP (P2PSIP) と呼ばれます。ローカルネットワーク上で行われる場合、必要なのはユーザーエージェントのSIPアドレスだけです。この場合、通常のSIPアドレスは`sip:<local-ip>`です。

例:



1 ユーザーエージェントA - インターカム。SIPアドレス: sip:192.168.1.101
2 ユーザーエージェントB - SIPが有効な電話。SIPアドレス: sip:192.168.1.100

ピアツーピアSIP設定を使用して、同じネットワーク上でSIP対応電話などを呼び出すように、Axisインターカムを設定することができます。

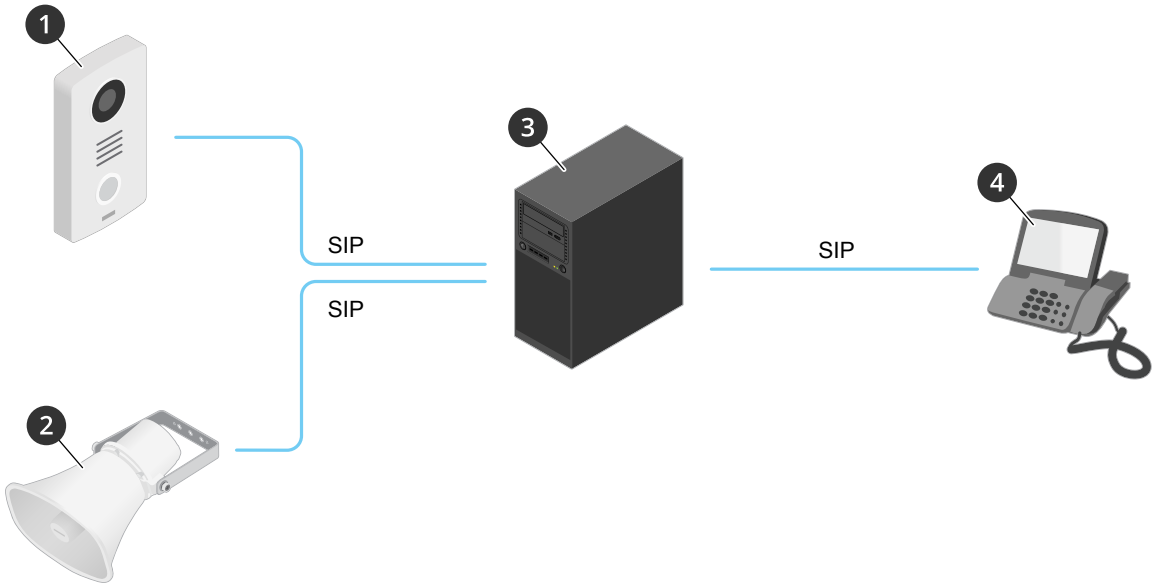
構内交換機 (PBX)

ローカルIPネットワークの外部でSIP呼び出しを行うときは、構内交換機 (PBX) をセンターハブとして機能させることができます。PBXの主要コンポーネントはSIPサーバーです。これは、SIPプロキシーまたはレジストラとも呼ばれます。PBXは従来の電話交換台のように動作します。クライアントの現在の状態を表示し、呼転送、ボイスメール、リダイレクトなどを行うことができます。

PBX SIPサーバーは、ローカルエンティティまたはオフサイトとして設定することができます。イントラネットまたはサードパーティのプロバイダーによってホストすることができます。ネットワーク間でSIP呼び出しを行うと、呼び出しは一連のPBXによって到達先のSIPアドレスの場所を照会し、ルーティングされます。

各SIPユーザーエージェントは、PBXに登録することで、正しい内線番号をダイヤすると該当のエージェントに到達できるようになります。この場合、通常のSIPアドレスは`sip:<user>@<domain>`または`sip:<user>@<registrar-ip>`です。SIPアドレスはそのIPアドレスとは無関係であり、PBXはデバイスがPBXに登録されている間は、そのデバイスをアクセス可能にします。

例:



1 sip:mydoor@company.com
2 sip:myspeaker@company.com
*3 **PBX** sip.company.com*
4 sip:office@company.com

Axisインターカムで呼び出しボタンを押すと、呼び出しが1つ以上のPBXを経由して、ローカルIPネットワークまたはインターネット上のSIPアドレスに転送されます。

NATトラバーサル

NAT (ネットワークアドレス変換) トラバーサルは、プライベートネットワーク (LAN) 上にあるAxisデバイスに、そのネットワークの外部からアクセスできるようにする場合に使用します。

注
ルーターが、NATトラバーサルとUPnP®に対応している必要があります。

NATトラバーサルプロトコルは個別に使用することも、ネットワーク環境に応じたさまざまな組み合わせで使用することもできます。

- **ICE** - ICE (双方向接続性確立) プロトコルを使用することで、ピアデバイス間の通信を成功させるために最も効率のよいパスを見つけやすくなります。STUNやTURNも有効にすると、さらにICEプロトコルで見つけやすくなります。
- **STUN** - STUN (NATのためのセッショントラバーサルユーティリティ) は、AxisデバイスがNATまたはファイアウォールを経由して配置されているかどうかを特定し、経由している場合に、リモートホストへの接続のために割り当てるマッピングされたパブリックIPアドレスとポート番号を取得できるようにする、クライアント/サーバーネットワークプロトコルです。IPアドレスなどのSTUNサーバーアドレスを入力します。
- **TURN** - TURN (NATに関するリレーを使用したトラバーサル) は、NATルーターまたはファイアウォールを経由するデバイスが、TCPやUDPを介して他のホストから着信データを受信できるようにするプロトコルです。TURNサーバーアドレスとログイン情報を入力します。

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の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。

Axisセキュリティ通知サービス

Axisは、Axis装置に関する脆弱性やその他のセキュリティ関連事項についての情報を提供する通知サービスを運営しています。通知を受け取るには、*axis.com/security-notification-service*で購読手続きを行うことができます。

脆弱性の管理

お客様の脆弱性リスクを最小限に抑えるため、Axisは**CVE (共通脆弱性識別子) 採番機関**として業界標準に従って、装置、ソフトウェア、およびサービスで発見された脆弱性の管理と対応を行っています。 Axisの脆弱性管理ポリシー、脆弱性の報告方法、すでに公開されている脆弱性、対応するセキュリティ勧告の詳細については、*axis.com/vulnerability-management*をご覧ください。

Axis装置のセキュアな動作

工場出荷時の設定のAxis装置は、セキュアなデフォルトの保護メカニズムで事前に設定されています。装置の設置時には、より多くのセキュリティ設定を使用することをお勧めします。装置のセキュリティを確保するためのベストプラクティス、リソース、ガイドラインなど、Axisのサイバーセキュリティに対する取り組みの詳細については、*https://www.axis.com/about-axis/cybersecurity*をご覧ください。

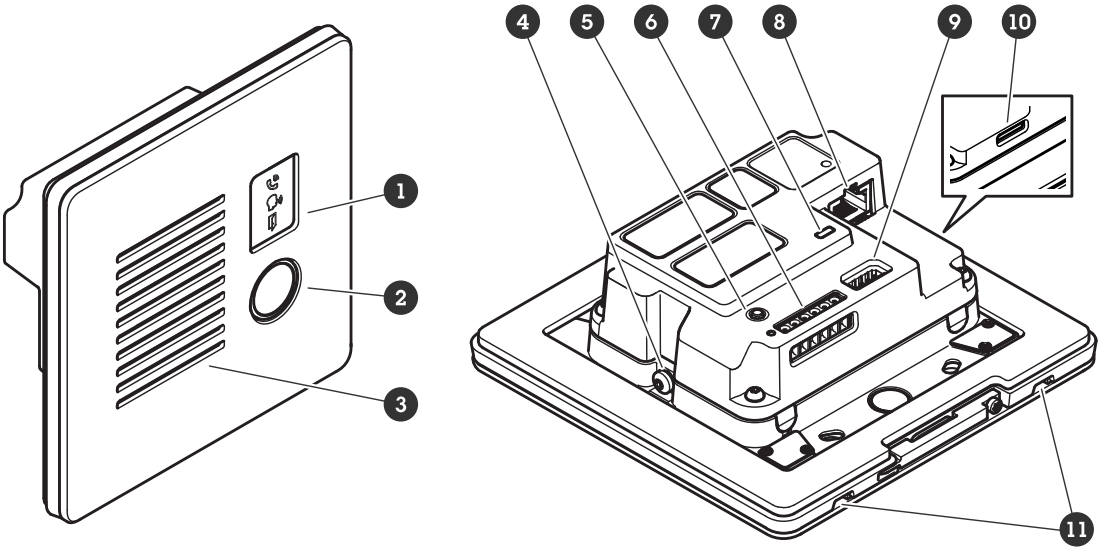
アプリケーション

アプリケーションを使用することで、Axis装置をより活用できます。AXIS Camera Application Platform (ACAP) は、サードパーティによるAxis装置向けの分析アプリケーションやその他のアプリケーションの開発を可能にするオープンプラットフォームです。アプリケーションとしては、装置にプリインストール済み、無料でダウンロード可能、またはライセンス料が必要なものがあります。

Axisアプリケーションのユーザーマニュアルについては、*help.axis.com*を参照してください。

仕様

製品概要



1
2 呼び出しボタン
3 スピーカー
4 アース端子ネジ
5
6
7 ステータスLED
8
9
10 (microSD/microSDHC/microSDXC)
11 マイクロフォン (x2)

フロントパネルインジケーターとコントロール

製品を電源に接続すると、フロントパネルのインジケーターが数秒間点灯します。

インジケーターアイコン

アイコン	説明
	発信が開始されると黄色に点灯します。 着信が開始されると黄色に点滅します。
	通話中は青色に点灯します。
	ドアが開いているときは緑色に点灯します。

LEDインジケーター

ステータスLED	説明
緑	正常動作であれば緑色に点灯します。

SDカードスロット

注意

- SDカード損傷の危険があります。SDカードの挿入と取り外しの際には、鋭利な工具や金属性の物を使用したり、過剰な力をかけたりしないでください。カードの挿入や取り外しは指で行ってください。
- データ損失や録画データ破損の危険があります。SDカードを取り外す前に、装置のwebインターフェースからマウント解除してください。本製品の稼働中はSDカードを取り外さないでください。

本装置は、microSD/microSDHC/microSDXCカードに対応しています。

推奨するSDカードについては、*axis.com*を参照してください。

microSD、microSDHC、およびmicroSDXCロゴは、SD-3C LLCの商標です。microSD、microSDHC、microSDXCは、米国および/または他の国々におけるSD-3C, LLCの商標または登録商標です。

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。
- インターネット経由でワンクリッククラウド接続 (O3C) サービスに接続します。接続するには、ボタンを押してから放し、ステータスLEDが緑色に3回点滅するまで待ちます。

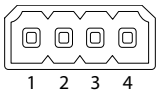
コネクター

ネットワーク コネクター

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

音声コネクター

音声入出力用4ピンターミナルブロック。

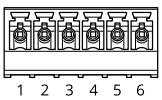


機能	ピン	メモ
ライン入力	1	ライン入力 (モノラル)
GND	2	音声アース
ライン出力端子	3	ライン出力 (モノラル)
GND	4	音声アース

I/O、リーダー、リレーコネクター

このコネクターは、I/Oおよびリレー、またはリーダーへの接続に使用できます。

6ピンターミナルブロック



1 -
2 12V
3 A/IO1
4 B/IO2
5 COM
6 NO/NC

機能	ピン	メモ	仕様
DCアース	1		0 V DC
DC出力	2	デバイスがPoE Class 4によって給電されている場合、補助装置への給電に使用できます。 注:このピンは、電源出力としてのみ使用できます。	12 V DC I/O ：最大負荷 = 50 mA リーダー/リレー：最大負荷 =350 mA
I/O：設定可能 (入力または出力) リーダー：A	3	I/O：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。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ともに使用する場合は、過渡電圧から保護するために、負荷と並列にダイオードを接続します。 リーダー：RS485 - A	I/O ：入力 - 0～最大 30 V DC 出力 - 0～30 V DC、オープンドレイン、100 mA
I/O：設定可能 (入力または出力) リーダー：B	4	I/O：PIN 3 と同じ リーダー：RS485 - B	I/O：PIN 3 と同じ
リレー：COM	5	コモン	
リレー：NO/NC	6	NO (Normally Open)/NC (Normally Closed)。リレー装置の接続用。2つのリレーピンは電気的に他の回路から絶縁されています。	最大電流700 mA、最大電圧30 V DC

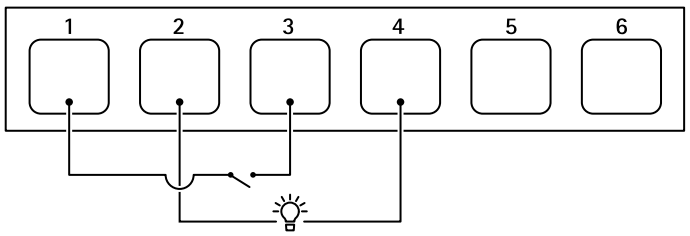
I/Oコネクター

1つのオプションは、I/Oコネクターに外部装置を接続し、いたずら警報、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です。I/Oコネクターは、0 V DC基準点と電力 (12 V DC出力) に加えて、以下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。

デジタル出力 - リレーやLEDなどの外部装置を接続します。接続した装置は、VAPIX®アプリケーションプログラミングインターフェース、イベント、または装置のインターフェースで起動することができます。

例:



1 *DCアース*
2 *DC出力12 V、最大50 mA*
3 *I/O (入力として設定)*
4 *I/O (出力として設定)*
5 *リレーのみ*
6 *リレーのみ*

リレーコネクタ

I/Oと組み合わせて使用すると、コネクターをリレーコネクターとして使用して、ソリッドステートリレーを接続し、次のように使用できます。

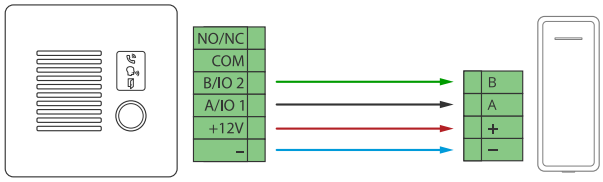
- 標準的なリレーとして補助回路を開閉します。
- ロックを直接制御します。
- 安全リレーを通してロックを制御します。ドアの安全な側で安全リレーを使用すると、ショートを防止することができます。

リーダーコネクター

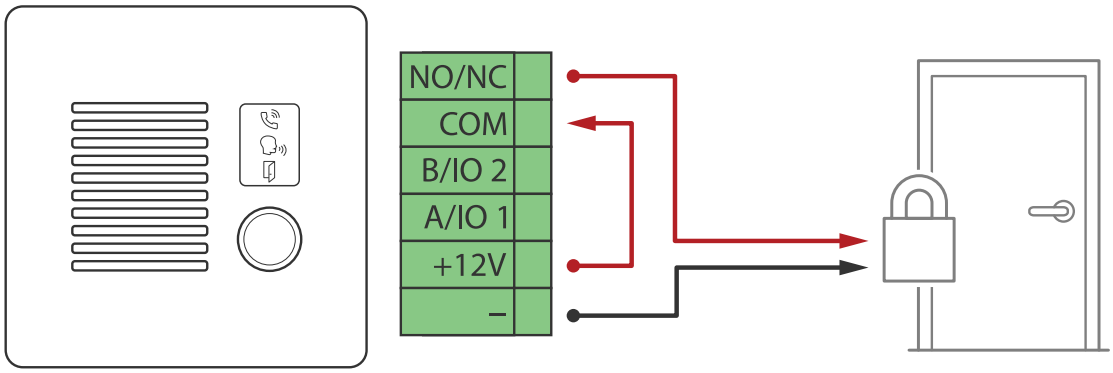
3つ目のオプションは、コネクターをリーダーコネクターとして使用して外部リーダーを接続する方法です。

機器の接続

Axisリーダー

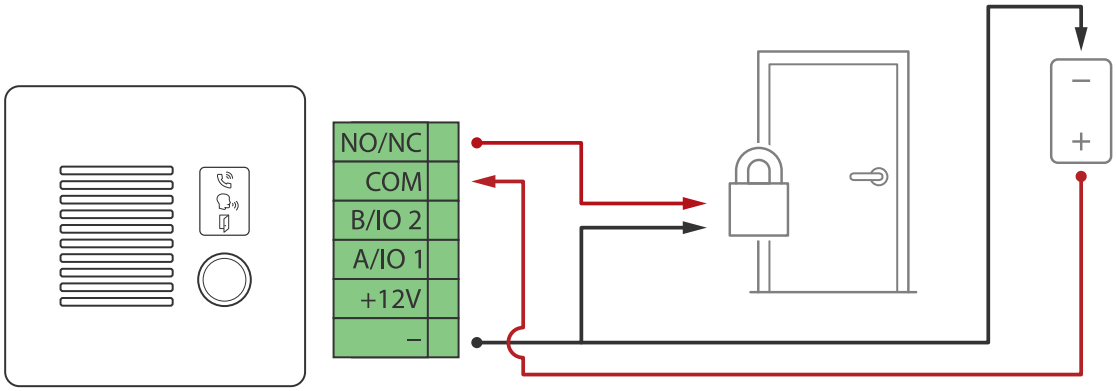


PoE (12V) で電力を供給されるリレー



1. リレーの状態を確認するには、[System > Accessories (システム > アクセサリー)] に移動し、リレーポートを検索します。
2. [Normal state (通常)] に設定します。
   - でフェイルセキュアをロックします。
   - でフェイルセーフをロックします。

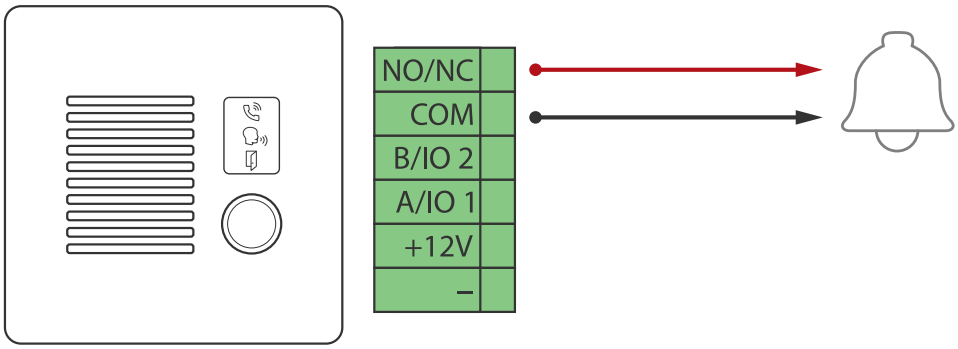
別の電源で電力を供給されるリレー



1. リレーの状態を確認するには、[System > Accessories (システム > アクセサリー)] に移動し、リレーポートを検索します。
2. [Normal state (通常)] に設定します。
   - でフェイルセキュアをロックします。

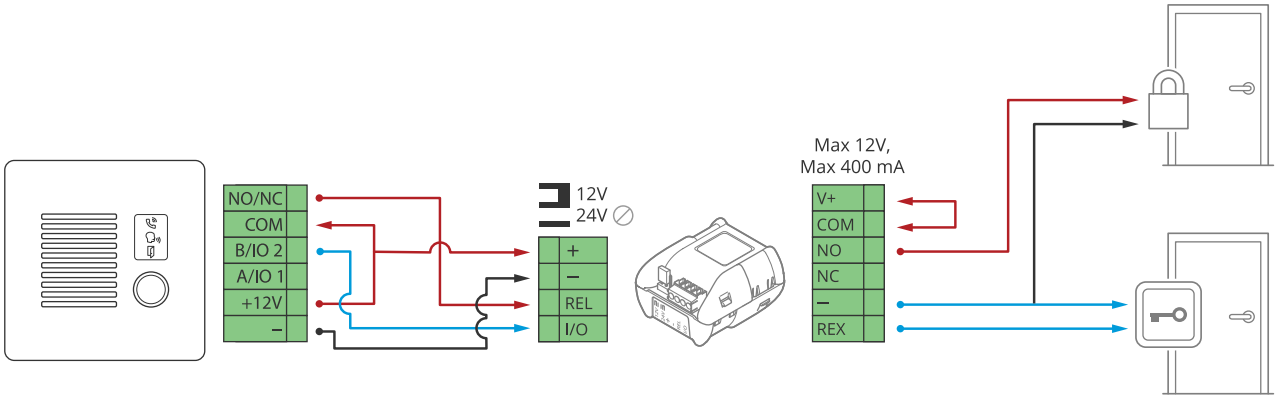
– でフェイルセーフをロックします。

無電圧リレー



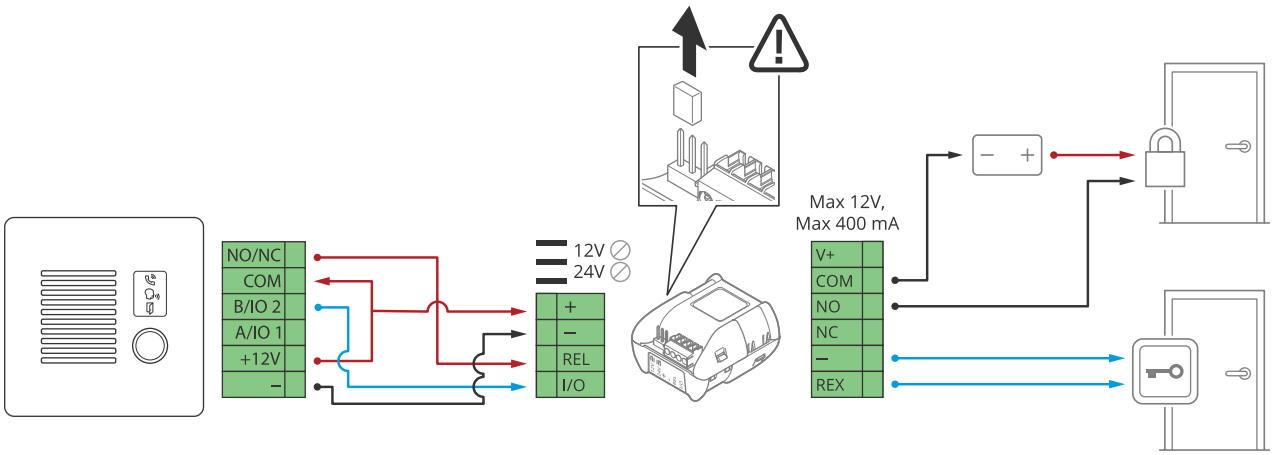
1. リレーの状態を確認するには、[System > Accessories (システム > アクセサリー)] に移動し、リレーポートを検索します。
2. [Normal state (通常)] に設定します。
   – でフェイルセキュアをロックします。
   – でフェイルセーフをロックします。

インターカムからのPoEで電力を供給される12 Vフェールセキュアロック



1. リレーの状態を確認するには、[System > Accessories (システム > アクセサリー)] に移動し、リレーポートを検索します。
2. [Normal state (通常)] に設定します。
   – でフェイルセキュアをロックします。
   – でフェイルセーフをロックします。

外部電源で電力を供給される12 Vフェールセキュアロック



1. リレーの状態を確認するには、[System > Accessories (システム > アクセサリー)] に移動し、リレーポートを検索します。
2. [Normal state (通常)] に設定します。
   - でフェイルセキュアをロックします。
   - でフェイルセーフをロックします。

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インジケーターがオレンジで点滅するまでコントロールボタンを15～30秒間押し続けます。
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、装置のIPアドレスのデフォルトは次のいずれかになります。
   - **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、装置へのアクセスを行います。
   *axis.com/support*のサポートページに、インストールおよび管理ソフトウェアツールが用意されています。

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*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、デバイス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*にアクセスしてください。

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*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。

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。

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、[**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

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。

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)。 • `Reply from <IP address>: bytes=32; time=10...`が表示された場合は、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。 • `Request timed out`が表示された場合は、Axisデバイスでその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。
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、*axis.com/support*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 Camera Station Edge：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 5:30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。
- AXIS Camera Station Pro:90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*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。 • 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て、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。 • サーバー/ブローカーがALPNをサポートしている場合、MQTTの使用は443などのオープンポートでネゴシエートできます。ALPNのサポートの有無、使用するALPNプロトコルとポートについては、サーバー/ブローカーのプロバイダーに確認してください。

パフォーマンスに関する一般的な検討事項

システムを設定する際には、さまざまな設定や条件がシステムのパフォーマンスにどのように影響するかを検討することが重要です。ある要因は必要な帯域幅の量 (ビットレート) に影響し、他の要因はフレームレートに影響し、帯域幅とフレームレートの両方に影響する事柄もあります。CPUの負荷が最大に達した場合も、フレームレートに影響を及ぼします。

最も重要な検討事項には次のようなものがあります。

- 画像解像度が高い、または圧縮レベルが低いと、画像のファイルサイズが増大し、結果的に帯域幅に影響を及ぼします。
- 多数のMotion JPEGクライアントまたはユニキャストH.264/H.265/AV1クライアントによるアクセスは帯域幅に影響します。
- 様々なクライアントが様々な解像度や圧縮方式が異なるストリームを同時に閲覧すると、フレームレートと帯域幅の両方に影響を及ぼします。フレームレートを高く維持するために、できる限り同一ストリームを使用してください。ストリームプロファイルを使用すると、ストリームの種類が同一であることを確認できます。
- 異なるコーデックのビデオストリームへの同時アクセスが発生すると、フレームレートと帯域幅の両方に影響が及ぼされます。最適な性能が実現するように、同じコーデックのストリームを使用してください。
- イベント設定を多用すると、製品のCPU負荷に影響が生じ、その結果、フレームレートに影響します。
- 特に、Motion JPEGのストリーミングでは、HTTPSを使用するとフレームレートが低くなる場合があります。
- 貧弱なインフラによるネットワークの使用率が高いと帯域幅に影響します。
- パフォーマンスの低いクライアントコンピューターで閲覧するとパフォーマンスが低下し、フレームレートに影響します。
- 複数のAXIS Camera Application Platform (ACAP) アプリケーションを同時に実行すると、フレームレートと全般的なパフォーマンスに影響する場合があります。

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*にアクセスしてください。

安全情報

危険レベル

⚠ 危険
回避しない場合、死亡または重傷につながる危険な状態を示します。

⚠ 警告
回避しない場合、死亡または重傷につながるおそれのある危険な状態を示します。

⚠ 注意
回避しない場合、軽傷または中程度の怪我につながるおそれのある危険な状態を示します。

注意
回避しない場合、器物の破損につながるおそれのある状態を示します。

その他のメッセージレベル

重要
製品を正しく機能させるために不可欠な重要情報を示します。

注
製品を最大限に活用するために役立つ有用な情報を示します。

T10208511_ja

2025-09 (M13.2)