AXIS D6310 Air Quality Sensor

ユーザーマニュアル

目次

インストール

重要

- 大きな通気口や汚染源のある場所からは、少なくとも1.5メートル (4.9フィート) 離して設置してください。これには、通気口やドア、窓、調理場などが含まれます。
- このデバイスは、空気が自由に流れる位置に設置してください。
- ベイピングや喫煙を効果的に検知するには、床から2.4〜2.7メートル (7.9〜8.9フィート) の高さの天井に設置してください。
- 空気品質や環境監視を効果的に行うには、床から0.9〜1.8メートル (3.0〜5.9フィート) の高さに設置してください。

取り付け方法の詳細については、インストールガイドを参照してください。

使用に当たって

⚠ 警告

光の点滅やちらつきは、光過敏性てんかんを持つ人の発作を引き起こすことがあります。

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。

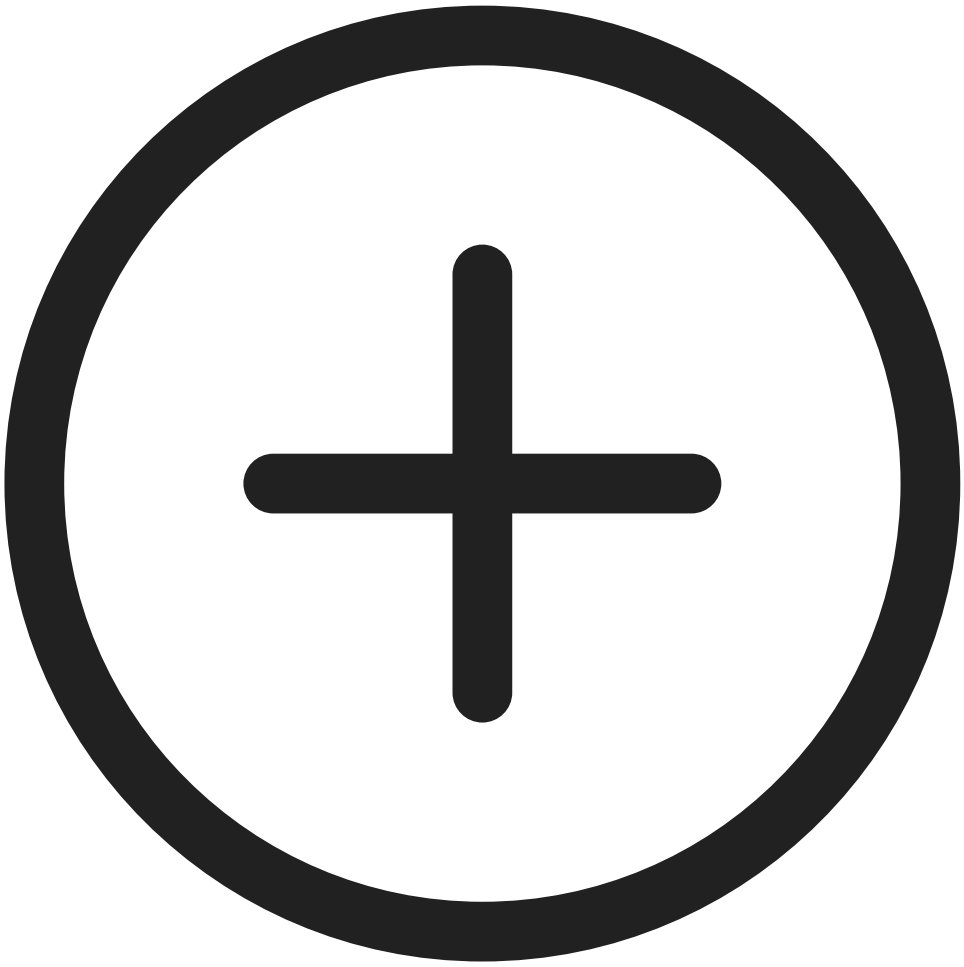
デバイスを構成する

空気質モニターの設定

空気質センサーのダッシュボードを設定する

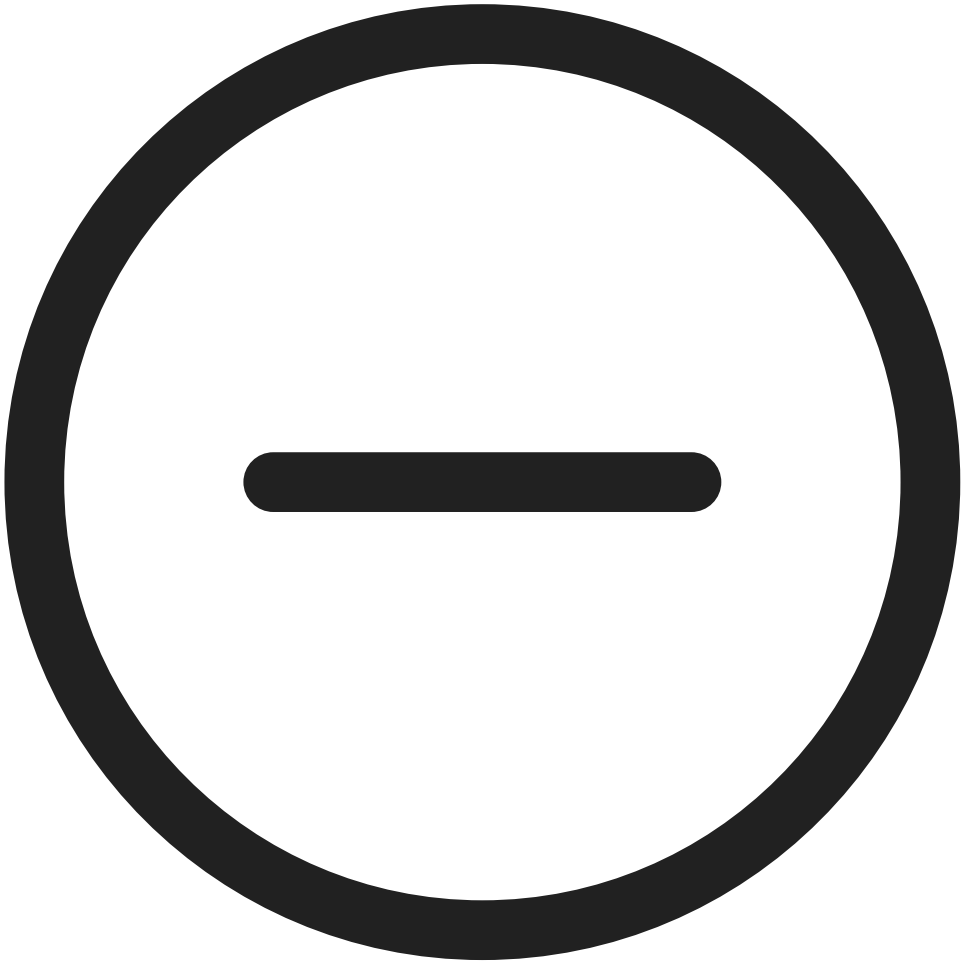
デバイスのWebページで、[Air quality monitor (空気質モニター)] > [Dashboard (ダッシュボード)] の順に移動します。

- ダッシュボードの名前を編集するには、左側の をクリックします。
- ダッシュボードにデータを表示するには、 [Edit (編集)] >



をクリックします。

- ダッシュボードでデータを非表示するには、 [Edit (編集)] >



をクリックします。

空気質センサーを設定する

デバイスのWebページで、[Air quality sensor (空気質モニター)] > [Settings (設定)] の順に移動します。

- 温度、湿度、CO2、NOx、PM1.0、PM2.5、PM4.0、PM10.0、VOC、AQIの閾値を設定します。詳細はを参照してください。
- 温度の単位を設定します。を参照してください。
- ベイピング検出ベイピング検知感度を設定します。を参照してください。
- ストレージの保持期間を設定します。を参照してください。
- クラウドメタデータ伝送周期を設定します。を参照してください。
- 検証期間を設定します。を参照してください。

センサーデータ統計情報のダウンロード

最大365日分のセンサー統計情報をCSVファイルにエクスポートし、Microsoft® Excelなどのアプリケーションで使用できます。

1. デバイスのWebページで、**[Air quality monitor (空気質モニター)]** > **[Statistics (統計)]** > **[Sensor Data Statistics (センサーデータ統計)]** の順に移動します。
2. 日付範囲を選択する:
   - **Custom range (カスタム範囲)**:**[From (開始)]** と **[To (終了)]** のリストから、開始日と終了日を選択します (最大365日)。
   - **Predefined range (あらかじめ定義された範囲)**:**[Predefined range (あらかじめ定義された範囲)]** のリストから期間を選択します。

   注
   カスタム範囲とあらかじめ定義された範囲の両方が選択されている場合、カスタム範囲が優先されます。

   注
   最大ダウンロード範囲は、で設定された保持期間に制限されます。
3. **[Source (ソース)]** のリストから希望のソースを選択します。すべてのソースのデータをエクスポートするには、**[Download all data (すべてのデータをダウンロード)]** をクリックします。
4. **[Download data (データをダウンロード)]** をクリックすると、選択した統計情報がエクスポートされます。

注
[Download all data (すべてのデータをダウンロード)] をクリックすると、選択した期間のすべてのソースのデータがエクスポートされます。

デバイスの初回動作のためのキャリブレーション

注
- 完全なCO2精度を得るには、デバイスの初回作動時には2日間が必要です。
- AQI (空気質指数) は、デバイスの初回作動時に機能するまでに12時間が必要です。AQIは、十分なデータが得られるまで、**Calculating (計算中)**と表示されます。デバイスが再起動するたびに、キャリブレーション時間が必要です。
- 完全なVOC精度は、デバイスを1時間作動させた後に得られます。デバイスが再起動するたびに、キャリブレーション時間が必要です。
- 完全なNOx精度は、デバイスを6時間作動させた後に得られます。デバイスが再起動するたびに、キャリブレーション時間が必要です。

プロファイルの設定

プロファイルとは、設定された構成の集合を意味します。優先順位やパターンの異なる最大30のプロファイルを設定できます。

新しいプロファイルを設定するには、以下の手順に従います。

1. **[Profiles (プロファイル)]** に移動し、[＋ **Create (作成)**] をクリックします。
2. **Name (名前)** と**Description (説明)** を入力します。
3. プロファイルに必要な **[Light (ライト)]** と **[Siren (サイレン)]** の設定を選択します。
4. ライトとサイレンの **[Priority (優先度)]** を設定し、**[Save (保存)]** をクリックします。

プロファイルを編集するには、 ⋮ をクリックして **[Edit (編集)]** を選択します。

カスタムサイレン音声ファイルでプロファイルを設定する

カスタム音声ファイルでプロファイルを設定できます。最大100MBまでの音声ファイルをデバイスに保存できます。これよりサイズが大きい音声ファイルは、デバイスにSDカードスロットが付いている場合はSDカードを使用してください。

音声ファイルのアップロード:

1. [Media (メディア)] に移動し、[+ Add (追加)] をクリックします。
2. コンピューターからファイルを選択します。
3. [Storage location (保存先)]を選択します。
4. [保存] をクリックします。

音声ファイルをプロファイル内で使用する：

1. [Profiles (プロファイル)] に移動し、プロファイルを作成します。詳細については、] を参照してください。
2. [Siren (サイレン)] を設定する際は、アップロードされた音声ファイルを[Pattern (パターン)] として選択します。

プロファイルのインポートまたはエクスポート

既定のプロファイルを使用する場合は、以下の方法でプロファイルをインポートできます。

1. [Profiles (プロファイル)] に移動し、[+ Import (インポート)] をクリックします。
2. 参照してファイルを見つけるか、インポートするファイルをドラッグアンドドロップします。
3. [保存] をクリックします。

1つ以上のプロファイルをコピーして他の装置に保存するには、以下の手順でプロファイルをエクスポートできます。

1. [profiles(プロファイル)] を選択します。
2. [エクスポート] をクリックします。
3. 参照して.jsonファイルを見つけます。

ダイレクトSIP (P2P) を設定する

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。P2Pの仕組みをよりよく理解するには、を参照してください 。

設定オプションの詳細については、を参照してください。

1. [System (システム)] > [SIP] > [SIP settings (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。
3. [Call handling (呼び出しの処理)] で、呼び出しのタイムアウトと継続時間を設定します。
4. [Ports (ポート)] で、ポート番号を入力します。
   - SIP port (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 port (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 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。メディア転送のデフォルトの開始ポートは4000です。ファイアウォールによっては、特定のポート番号のRTPトラフィックをブロックする場合があります。ポート番号は1024～65535の間で指定する必要があります。

5. [NAT traversal (NATトラバーサル)] で、NATトラバーサル用に有効にする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。

6. [Audio (音声)] で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。
7. [Additional (追加)] で、追加のオプションを選択します。
   - UDP-to-TCP switching (UDP からTCPへの切り替え) - 通話でトランスポートプロトコルをUDP (User Datagram Protocol) からTCP (Transmission Control Protocol) に一時的に切り替えることを許可するかどうかを選択します。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) - ルーターのパブリックIPアドレスではなく、ローカルIPアドレスを送信する場合に選択します。
   - Allow contact rewrite (連絡先書き換えの許可) - ルーターのパブリックIPアドレスではなく、ローカルIPアドレスを送信する場合に選択します。
   - Register with server every (サーバーへの登録を毎回行う) - 既存のSIPアカウントで、デバイスをSIPサーバーに登録する頻度を設定します。
   - DTMF payload type (DTMFの積載タイプ) - DTMFのデフォルトの積載タイプを変更します。
8. [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)

ユーザーエージェントどうしがIPネットワーク内外で通信する場合は、PBXサーバーを使用します。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。P2Pの仕組みをよりよく理解するには、を参照してください 。

設定オプションの詳細については、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. 新しいアカウントを追加するには、[System (システム)] > [SIP] > [SIP accounts (SIPアカウント)] に移動し、[+ Account (+ アカウント)] をクリックします。
3. PBXプロバイダーから受け取った詳細情報を入力します。

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. [保存] をクリックします。
7. ピアツーピアの場合と同じ方法でSIPを設定します。詳細については、を参照してください。

イベントのルールを設定する

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。

電子タバコの使用を検知したときにビデオを録画する

以下の例では、空気質センサーが電子タバコの使用を検知すると、ネットワークストレージへビデオを録画する設定方法を説明します。

1. 空気質センサーのWebページで、 [Settings (設定)] > [System (システム)] > [Storage (ストレージ)] の順に移動し、ネットワークストレージが設定されていることを確認します。
2. [Settings > System > Events (設定 > システム > イベント)] に移動し、ルールを追加します。以下の情報を入力します。
   - 名前:ルールの名前を入力します。
   - Condition (条件): Air quality monitor (空気質モニター) > Vaping or smoking detected (電子タバコまたはタバコの喫煙を検知)。
   - Action (アクション)： Recordings (記録) > Record video (ビデオの録画)。
   - ストレージ:Network storage (ネットワークストレージ)。ネットワークストレージが設定されていることを確認します。
   - カメラ:カメラのビューエリアを選択します。
   - Stream profile (ストリームプロファイル):ストリームプロファイルを選択するか、Create a stream profile (ストリームプロファイルを作成)します。
   - プリバッファとポストバッファ ：希望の値を設定します。
3. [保存] をクリックします。

CO2が過剰な場合に音声クリップを再生する

この例は、CO2が過剰な場合に音声クリップを再生する方法を説明します。

ルールを作成する

1. Webページで、**[Events (イベント)]** > **[Rules (ルール)]** > **[Add a rule (ルールを追加)]** の順に移動してルールを作成します。
2. 以下の情報を入力します。
   - **名前**:ルールの名前を入力します。
   - **条件**:Air quality monitor (空気質モニター) > Air quality outside acceptable range (許容範囲外の空気質)
   - Sensor (センサー): CO2
   - Action (アクション): オーディオクリップの再生
   - Clip (クリップ): 音声クリップを選択します。
3. [**保存**] をクリックします。

CO2アラーム範囲を設定する

- Webページで、**[Air quality monitor (空気質モニター)]** > **[Settings (設定)]** > **[CO2]** の順に移動します。
- **[MIN (最小)]** と **[MAX (最大)]** のデータ を入力し、CO2範囲を設定します。

PIRセンサー経由でライトとサイレンを作動させる

この例では、PIRセンサー経由でライトとサイレンを作動する方法を説明します。ライト (シグナリングLED) とサイレンの位置については、を参照してください。

ライトとサイレンのプロファイルを作成する:

1. デバイスのWebページで、**[Profiles (プロファイル)]** > **[Create (作成)]** の順に進みます。
2. 以下の情報を入力します。
   - **名前**:プロファイル1
   - **Description (説明)**:プロファイルの説明を追加します。
   - [Light (照明)]:**[Pattern (パターン)]**、**[Speed (速度)]**、**[Intensity (明るさ)]**、**[Color (色)]**、**[Duration (時間)]** を選択します。
   - [Siren (サイレン)]:**[Pattern (パターン)]**、**[Intensity (明るさ)]**、**[Duration (時間)]** を選択します。

   注

   番号の高いプロファイルは優先度が高くなります。
   - [Priority (優先度)]:**[Light priority (ライト優先度)]** と **[Siren priority (サイレン優先度)]** を選択します。

イベントを作成する:

1. **[System (システム)]** > **[Events (イベント)]** > **[Rules (ルール)]** の順に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - **名前**:シグナリングLEDとサイレンを作動させる
   - **Condition (条件)**: PIRセンサー
   - **Action (アクション)**:ライトとサイレンのプロファイルを実行
   - **Profile (プロファイル)**:プロファイル1
   - **Action (アクション)**:開始
3. [**保存**] をクリックします。

アラームがトリガーされたときにプロファイルを開始します

この例では、デジタル入力信号が変わったときにアラームをトリガーする方法について説明します。

ポートの方向入力を設定する手順:

1. [System (システム)]>[Accessories (アクセサリー)]>[I/O ports (I/Oポート)] に移動します。
2. [Port 1 (ポート1)]>[Normal state (通常状態)] に進み、[Circuit closed (閉回路)] をクリックします。

ルールの作成:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件の一覧で、[I/O] > [Digital input is active (デジタル入力がアクティブ)] を選択します。
4. [Port 1 (ポート1)] を選択します:
5. アクションのリストで、[Run light and siren profile while the rule is active (ルールがアクティブである間は、ライトとサイレンのプロファイルを実行)] を選択します。
6. [profile you want to start (開始するプロファイル)] を選択します。
7. [保存] をクリックします。

SIPを介したプロファイルの開始

この例では、SIPを介してアラームをトリガーする方法について説明します。

SIPを有効にする:

1. [System (システム)] > [SIP] > [SIP settings (SIP設定)] に移動します。
2. [Enable SIP (SIPの有効化)] と [Allow incoming calls (着信呼び出しを許可)] を選択します。
3. [保存] をクリックします。

ルールの作成:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件のリストで、[Call (呼び出し)]>[State (状態)] を選択します。
4. 状態のリストで、[Active (アクティブ)] を選択します。
5. アクションのリストで、[Run light and siren profile while the rule is active (ルールがアクティブである間は、ライトとサイレンのプロファイルを実行)] を選択します。
6. [profile you want to start (開始するプロファイル)] を選択します。
7. [保存] をクリックします。

SIP内線番号による複数のプロファイルの制御

SIPを有効にする:

1. [System (システム)] > [SIP] > [SIP settings (SIP設定)] に移動します。
2. [Enable SIP (SIPの有効化)] と [Allow incoming calls (着信呼び出しを許可)] を選択します。
3. [保存] をクリックします。

プロファイルを開始するルールを作成する:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。

3. 条件のリストで、[Call (呼び出し)] > [State change (状態変更)] を選択します。
4. 理由のリストで、[Accepted by device (装置で受け入れ)] を選択します。
5. [Call direction (呼び出し方向)] で [Incoming (着信)] を選択します。
6. [Local SIP URI] にsip:[Ext]@[IP address] と入力します。[Ext] はプロファイルに使用する内線番号で、[IP address] は装置のアドレスです。たとえば、sip:1001@192.168.0.90とします。
7. アクションのリストで、[Light and Siren (ライトとサイレン)] > [Run light and siren profile (ライトとサイレンのプロファイルを実行)] の順に選択します。
8. [profile you want to start (開始するプロファイル)] を選択します。
9. アクション [Start (開始)] を選択します。
10. [保存] をクリックします。

プロファイルを停止するルールを作成する:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件のリストで、[Call (呼び出し)] > [State change (状態変更)] を選択します。
4. 理由のリストで、[Terminated (終了した)] を選択します。
5. [Call direction (呼び出し方向)] で [Incoming (着信)] を選択します。
6. [Local SIP URI] にsip:[Ext]@[IP address] と入力します。[Ext] はプロファイルに使用する内線番号で、[IP address] は装置のアドレスです。たとえば、sip:1001@192.168.0.90とします。
7. アクションのリストで、[Light and Siren (ライトとサイレン)] > [Run light and siren profile (ライトとサイレンのプロファイルを実行)] の順に選択します。
8. 停止するプロファイルを選択します。
9. アクション [Stop (停止)] を選択します。
10. [保存] をクリックします。

この手順を繰り返して、SIPで制御する各プロファイルの開始と停止のルールを作成します。

優先度が異なる2つのプロファイルを実行する

優先度が異なる2つのプロファイルを実行すると、優先度の数字が高い番号のプロファイルが優先度の数字が低い番号のプロファイルに割り込みます。

注

同じ優先度の2つのプロファイルを実行した場合、最新のプロファイルによって前のプロファイルがキャンセルされます。

この例では、デジタルI/Oポートによってトリガーされたときに、優先度4のプロファイルを優先度3のプロファイルよりも先に表示するように設定する方法について説明します。

プロファイルの作成:

1. 優先度3のプロファイルを作成します。
2. 優先度4の別のプロファイルを作成します。

ルールの作成:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件の一覧で、[I/O] > [Digital input is active (デジタル入力がアクティブ)] を選択します。

4. [port (ポート)] を選択します。
5. アクションのリストで、[Run light and siren profile while the rule is active (ルールがアクティブである間は、ライトとサイレンのプロファイルを実行)] を選択します。
6. [the profile that has the highest priority number (優先度の数字が最も高いプロファイル)] を選択します。
7. [保存] をクリックします。
8. [Profiles (プロファイル)] に移動し、優先度の数字が最も低い番号のプロファイルを開始します。

カメラが動きを検知すると、HTTP postを使用してライトとサイレンのプロファイルを有効にする

この例では、空気質センサーにカメラを接続する方法と、カメラにインストールされているアプリケーションAXIS Motion Guardが動きを検知すると、空気質センサーのライトとサイレンのプロファイルを有効にする方法について説明します。

開始する前に、以下をご確認ください。

- 空気質センサーのオペレーター、または管理者のロールを持つ新しいユーザーを作成します。
- 名前を"Light and siren profile"として、空気質センサーのプロファイルを作成します。
- カメラでAXIS Motion Guardを設定し、「カメラプロファイル」というプロファイルを作成します。
- バージョン10.8.0以降のファームウェアでAXIS Device Assistantを使用してください。

カメラで送信先を作成する手順:

1. カメラの装置インターフェースで [System > Events > Recipients (システム > イベント > 送信先)] に移動し、送信先を追加します。
2. 以下の情報を入力します。
   - Name (名前): 空気質センサー
   - Type (タイプ): HTTP
   - URL: http://<IPaddress>/axis-cgi/siren_and_light.cgi
     <IPアドレス>を空気質センサーのアドレスに置き換えます。
   - これは新しく作成された空気質センサーのユーザー名とパスワードです。
3. [Test (テスト)] をクリックして、すべてのデータが有効であることを確認します。
4. [保存] をクリックします。

カメラに2つのルールを作成する:

1. [Rules (ルール)] に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - 名前:空気質センサーを動きの検知で起動する
   - Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (Motion Guard: カメラプロファイル)]
   - Action (アクション): Notifications > Send notification through HTTP (通知 > HTTPで通知を送信する)
   - Recipient (送信先): 空気質センサー。
     この情報は、[Events > Recipients > Name (イベント > 送信先 > 名前)] で入力した情報と同じである必要があります。
   - Method (メソッド): Post
   - Body (本文):

```
{  "apiVersion": "1.0",  "method": "start",  "params": {
"profile" : "Light and siren profile"  } }
```

空気質センサーのプロファイルを作成したときと同じ情報を [profile (プロファイル) : <>] に入力してください。この場合は“Light and siren profile”です。

3. [保存] をクリックします。
4. 次の情報を含む別のルールを追加します。
   - 名前:空気質センサーを動きの検知で解除する
   - Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (Motion Guard: カメラプロファイル)]
   - [Invert this condition (この条件を逆にする)] を選択します。
   - Action (アクション): Notifications > Send notification through HTTP (通知 > HTTPで通知を送信する)
   - Recipient (送信先): 空気質センサー
     この情報は、[Events > Recipients > Name (イベント > 送信先 > 名前)] で入力した情報と同じである必要があります。
   - Method (メソッド): Post
   - Body (本文):

```
{  "apiVersion": "1.0",  "method": "stop",  "params": {    "profile" : "Light and siren profile"  } }
```

空気質センサーのプロファイルを作成したときと同じ情報を [profile (プロファイル) : <>] に入力してください。この場合は“Light and siren profile”です。

5. [保存] をクリックします。

カメラが動きを検知すると、仮想入力を使用してライトとサイレンのプロファイルを有効にする

この例では、空気質センサーにカメラを接続する方法と、カメラにインストールされているアプリケーションAXIS Motion Guardが動きを検知すると、空気質センサーのライトとサイレンのプロファイルを有効にする方法について説明します。

開始する前に、以下をご確認ください。

- 空気質センサーでオペレーター、または管理者権限を持つ新しいアカウントを作成します。
- 空気質センサーのプロファイルを作成します。を参照してください。
- カメラでAXIS Motion Guardを設定し、「カメラプロファイル」というプロファイルを作成します。

カメラで2人の送信先を作成する:

1. カメラの装置インターフェースで [System > Events > Recipients (システム > イベント > 送信先)] に移動し、送信先を追加します。
2. 以下の情報を入力します。
   - 名前:Activate virtual port (仮想ポートのアクティブ化)
   - Type (タイプ): HTTP
   - URL: http://<IPaddress>/axis-cgi/virtualinput/activate.cgi
     <IPアドレス>を空気質センサーのアドレスに置き換えます。
   - これは新しく作成された空気質センサーのアカウントとパスワードです。
3. [Test (テスト)] をクリックして、すべてのデータが有効であることを確認します。
4. [保存] をクリックします。
5. 次の情報を含む2番目の送信先を追加します。
   - 名前:仮想ポートの非アクティブ化
   - Type (タイプ): HTTP
   - URL: http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi

<IPアドレス>を空気質センサーのアドレスに置き換えます。
- これは新しく作成された空気質センサーのアカウントとパスワードです。

6. [Test (テスト)] をクリックして、すべてのデータが有効であることを確認します。
7. [保存] をクリックします。

カメラに2つのルールを作成する:
1. [Rules (ルール)] に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - 名前:仮想IO1のアクティブ化
   - Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (Motion Guard: カメラプロファイル)]
   - Action (アクション): Notifications > Send notification through HTTP (通知 > HTTPで通知を送信する)
   - Recipient (送信先): Activate virtual port (仮想ポートのアクティブ化)
   - Query string suffix (クエリ文字列のサフィックス): schemaversion=1&port=1
3. [保存] をクリックします。
4. 次の情報を含む別のルールを追加します。
   - 名前:仮想IO1の非アクティブ化
   - Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (Motion Guard: カメラプロファイル)]
   - [Invert this condition (この条件を逆にする)] を選択します。
   - Action (アクション): Notifications > Send notification through HTTP (通知 > HTTPで通知を送信する)
   - Recipient (送信先): 仮想ポートの非アクティブ化
   - Query string suffix (クエリ文字列のサフィックス): schemaversion=1&port=1
5. [保存] をクリックします。

空気質センサーのルールを作成する:
1. 空気質センサーのWebインターフェースで、[System (システム)] > [Events (イベント)] に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - 名前:仮想入力1のトリガー
   - Condition (条件): [I/O] > [Virtual input is active (仮想入力有効)]
   - ポート: 1
   - Action (アクション): Light and siren > Run light and siren profile while the rule is active (ライトとサイレン > ルールがアクティブである間は、ライトとサイレンのプロファイルを実行)
   - Profile (プロファイル): 新しく作成したプロファイルを選択する
3. [保存] をクリックします。

カメラが動きを検知すると、MQTT経由でライトとサイレンのプロファイルを有効にする

この例では、カメラを空気質センサーに接続する方法と、カメラが動きを検知すると空気質センサーのライトとサイレンのプロファイルを有効にする方法を説明します。

開始する前に、以下をご確認ください。
- 空気質センサーのプロファイルを作成します。

- MQTTブローカーを設定し、ブローカーのIPアドレス、ユーザー名、パスワードを取得します。
- 動体検知アプリケーションが設定済みでカメラで実行中であることを確認してください。

カメラでMQTTクライアントを設定する:

1. カメラのWebインターフェースで、[System > MQTT > MQTT client > Broker (システム > MQTT > MQTTクライアント > ブローカー)] にアクセスし、以下の情報を入力します。
   - [ホスト]:ブローカーIPアドレス
   - Client ID (クライアントID)：例: カメラ1
   - Protocol (プロトコル):ブローカーが設定したプロトコル
   - ポート:ブローカーが使用するポート番号
   - ブローカーの Username (ユーザー名) と Password (パスワード)
2. [Save (保存)]をクリックし、[Connect (接続)]をクリックします。

カメラにMQTTパブリッシングの2つのルールを作成する:

1. [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。
2. 以下の情報を入力します。
   - 名前:動体を検知しました
   - Condition (条件): Applications > Motion alarm (アプリケーション > モーションアラーム)
   - Action (アクション):[MQTT] > [Send MQTT publish message (MQTT公開メッセージを送信)]
   - Topic (トピック):動き
   - Payload (ペイロード):オン
   - QoS:0、1、または2
3. [保存] をクリックします。
4. 次の情報を含む別のルールを追加します。
   - 名前:動きなし
   - Condition (条件): Applications > Motion alarm (アプリケーション > モーションアラーム)
     - [Invert this condition (この条件を逆にする)] を選択します。
   - Action (アクション):[MQTT] > [Send MQTT publish message (MQTT公開メッセージを送信)]
   - Topic (トピック):動き
   - Payload (ペイロード):オフ
   - QoS:0、1、または2
5. [保存] をクリックします。

空気質センサーにMQTTクライアントを設定する:

1. 空気質センサーのWebインターフェースで、[System (システム)] > [MQTT] > [MQTT client (MQTTクライアント)] > [Broker (ブローカー)] の順に移動して、以下の情報を入力します。
   - [ホスト]:ブローカーIPアドレス
   - Client ID (クライアントID)：サイレン1
   - Protocol (プロトコル):ブローカーが設定したプロトコル
   - ポート:ブローカーが使用するポート番号
   - Username (ユーザー名) と Password (パスワード)

2. [Save (保存)]をクリックし、[Connect (接続)]をクリックします。
3. [MQTT subscriptions (MQTTサブスクリプション)] に移動し、サブスクリプションを追加します。
   以下の情報を入力します。
   - サブスクリプションフィルター:動き
   - サブスクリプションの種類:ステートフル
   - QoS:0、1、または2
4. [保存] をクリックします。

MQTTサブスクリプションについて空気質センサーのルールを作成する:

1. [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。
2. 以下の情報を入力します。
   - 名前:動体を検知しました
   - Condition (条件):[MQTT] > [Stateful (ステートフル)]
   - サブスクリプションフィルター: 動き
   - Payload (ペイロード):オン
   - Action (アクション): Light and siren > Run light and siren profile while the rule is active (ライトとサイレン > ルールがアクティブである間は、ライトとサイレンのプロファイルを実行)
   - Profile (プロファイル):アクティブにするプロファイルを選択します。
3. [保存] をクリックします。

スピーカーテストが失敗した場合に電子メールを送信する

この例では、音声デバイスは、スピーカーテストが失敗したときに定義済みの送信先に電子メールを送信するように設定されています。スピーカーテストは、毎日18:00に実行するように設定されています。

1. スピーカーテストのスケジュールを設定する方法:
   1.1. [device interface (デバイスインターフェース)] > [System (システム)] > [Events (イベント)] > [Schedules (スケジュール)] に移動します。
   1.2. 毎日 18:00 に開始し、18:01 に終了するスケジュールを作成します。「毎日午後6時」と名付けます。
2. 電子メールの送信先を作成する:
   2.1. [device interface > System > Events > Recipients (デバイスインターフェース > システム > イベント > 送信先)] に移動します。
   2.2. [Add Recipient (送信先の追加)] をクリックします。
   2.3. 送信先に「スピーカーテストの送信先」と名前を付けます
   2.4. [Type (タイプ)] 配下で [Email (電子メール)] を選択します。
   2.5. [Send email to (電子メールの送信先)] で、送信先のメールアドレスを入力します。複数のアドレスを指定する場合は、カンマで区切ります。
   2.6. 送信者の電子メールアカウントの詳細を入力します。
   2.7. [Test (テスト)] をクリックして、テストメールを送信します。

注

一部の電子メールプロバイダーは、大量の添付ファイルの受信や表示を防止したり、スケジュールにしたがって送信された電子メールなどの受信を防止するセキュリティフィルターを備えています。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て、メールの送信の問題が発生したり、電子メールアカウントがロックされたりしないようにしてください。

2.8. [保存] をクリックします。

3. 自動スピーカーテストを設定します:
   3.1. [device interface > System > Events > Rules (デバイスインターフェース > システム > イベント > ルール)] に移動します。
   3.2. [Add a rule (ルールの追加)] をクリックします。
   3.3. アクションルールの名前を入力します。
   3.4. [Condition (条件)] で [Schedule (スケジュール)] を選択し、トリガーリストから選択します。
   3.5. [Schedule (スケジュール)] でスケジュールを選択します (「毎日午後6時」)。
   3.6. [Action (アクション)] で [Run automatic speaker test (自動スピーカーテストの実行)] を選択します。
   3.7. [保存] をクリックします。
4. スピーカーテストが失敗した場合に電子メールを送信する条件を設定します:
   4.1. [device interface > System > Events > Rules (デバイスインターフェース > システム > イベント > ルール)] に移動します。
   4.2. [Add a rule (ルールの追加)] をクリックします。
   4.3. アクションルールの名前を入力します。
   4.4. [Condition (条件)] で [Speaker test result (スピーカーテストの結果)] を選択します。
   4.5. [Speaker test status (スピーカーテストのステータス)] で、[Didn't pass the test (テストに不合格)] を選択します。
   4.6. [Action (アクション)] で [Send notification to email (電子メールで通知を送信する)] を選択します。
   4.7. [Recipient (送信先)] で、送信先を選択します (「スピーカーテストの送信先」)
   4.8. 件名とメッセージを入力し、[Save (保存)] をクリックします。

アラームトリガー時にカスタムクリップを再生する

この例では、デジタル音声入力信号が変化したときにカスタムオーディオファイルをトリガーする方法を説明します。

音声ファイルのアップロード:

1. [Media (メディア)] に移動し、[+ Add (追加)] をクリックします。
2. クリックしてコンピューターから音声ファイルを選択します。
3. [Storage location (保存先)]を選択します。
4. [保存] をクリックします。

音声ファイルでプロファイルを作成する:

1. [Profiles (プロファイル)] に移動し、[+ Create (作成)] をクリックします。
2. Name と入力し、プロファイルのライトパターンを選択します。
3. サイレンセクションで、アップロードされた音声ファイルを選択します。
4. [Intensity (強さ)] と[Intensity (持続時間)] を選択します。
5. [保存] をクリックします。

ポートの方向入力を設定する手順:

1. [System (システム)]>[Accessories (アクセサリー)]>[I/O ports (I/Oポート)] に移動します。

2. [Port 1 (ポート1)]>[Normal state (通常状態)] に進み、[Circuit closed (閉回路)] をクリックします。

ルールの作成:

1. [System (システム)]>[Events (イベント)] に移動し、ルールを追加します。
2. アクションルールの名前を入力します。
3. 条件の一覧で、[I/O>] [Digital input is active (デジタル入力がアクティブ)] を選択します。
4. [Port 1 (ポート1)] を選択します:
5. アクションのリストで、[Run light and siren profile while the rule is active (ルールがアクティブである間は、ライトとサイレンのプロファイルを実行)] を選択します。
6. アップロードした音声ファイルを含むプロファイルを選択します。
7. [保存] をクリックします。

DTMFで音声を停止する

この例では、次の方法について説明します。

- デバイスでDTMFを設定する。
- DTMFコマンドがデバイスに送信されたときに音声を停止するイベントを設定する

1. [System (システム)] > [SIP] > [SIP settings (SIP設定)] に移動します。
2. [Enable SIP (SIPの有効化)] がオンになっていることを確認します。
   オンにする必要がある場合は、必ず [Save (保存)] をクリックしてください。
3. SIP accounts (SIPのアカウント)に移動します。
4. SIPアカウントの横にある ⋮ > [Edit (編集)]をクリックします。
5. [DTMF] で [+ DTMFシーケンス] をクリックします。
6. [シーケンス] に「1」を入力します。
7. [Description (説明)] に「音声の停止」と入力します。
8. [保存] をクリックします。
9. [System > Events > Rules (システム > イベント > ルール)] に移動し、[+ Add a rule (ルールの追加)] をクリックします。
10. [Name (名前)] に「DTMF stop audio (DTMF音声の停止)」と入力します。
11. [Condition (条件)] で [DTMF] を選択します。
12. [DTMFイベントID] で [音声の停止] を選択します。
13. [Action (アクション)] で [Stop playing audio clip (オーディオクリップの再生を停止)] を選択します。
14. [保存] をクリックします。

着信SIP呼び出しの音声の設定

SIP呼び出しの受信時に音声クリップを再生するルールを設定できます。

音声クリップの終了後にSIP呼び出しに自動的に応答する追加ルールを設定することもできます。このルールは、アラームオペレーターが音声デバイスの近くの人に注意を促し、通信回線を確立したい場合に便利です。この操作は、音声デバイスにSIP呼び出しを行い、音声デバイスで音声クリップを再生してデバイスの近くの人に警告することで行われます。音声クリップの再生が停止すると、SIP呼び出しは音声デバイスによって自動的に応答され、アラームオペレーターと音声デバイスの近くの人の間の通信が行われます。

SIP設定を有効にする:

1. WebブラウザでIPアドレスを入力して、スピーカーのデバイスインターフェースに移動します。
2. **[System (システム)]** > **[SIP]** > **[SIP settings (SIP設定)]**に移動し、**[Enable SIP (SIPの有効化)]]**を選択します。
3. 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。
4. **[Save (保存)]**をクリックします。
5. **[SIP accounts (SIPのアカウント)]**に移動します。
6. SIPアカウントの横にある ⋮ > **[Edit (編集)]**をクリックします。
7. [**Answer automatically (自動応答)**] のチェックを外します。

SIP呼び出しの受信時に音声を再生する:

1. **[Settings (設定)]** > **[System (システム)]** > **[Events (イベント)]** > **[Rules (ルール)]**に移動して値を追加します。
2. ルールの名前を入力します。
3. 条件の一覧で**[State (状態)]**を選択します。
4. 状態の一覧で、[**Ringing (呼び出し中)**] を選択します。
5. アクションのリストで**[Play audio clip (音声クリップの再生)]**を選択します。
6. クリップのリストで、再生する音声クリップを選択します。
7. 音声クリップを繰り返す回数を選択します。0は「1回再生」を意味します。
8. **[Save (保存)]**をクリックします。

音声クリップの終了後、SIP呼び出しに自動的に応答する:

1. **[Settings (設定)]** > **[System (システム)]** > **[Events (イベント)]** > **[Rules (ルール)]**に移動して値を追加します。
2. ルールの名前を入力します。
3. 条件の一覧で**[Audio clip playing (音声クリップを再生中)]**を選択します。
4. [**Use this condition as a trigger (この条件をトリガーとして使用する)] をオンにします。**
5. [**Invert this condition (この条件を逆にする)**] をオンにします。
6. [**+ Add a condition (+ 条件の追加)**] をクリックして、イベントに2つ目の条件を追加します。
7. 条件の一覧で**[State (状態)]**を選択します。
8. 状態の一覧で、[**Ringing (呼び出し中)**] を選択します。
9. アクションの一覧で**[Answer Call (呼び出しに応答する)]**を選択します。
10. **[Save (保存)]**をクリックします。

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。

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。

装置を検索

シリアル番号やIPアドレスなど装置の検索情報を表示します。

Locate device (装置を検索):発言者を特定するための音声を再生します。一部の製品では、装置のLEDが点滅します。

電力状態

電力状態情報が表示されます。情報は製品によって異なります。

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。

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。

ビデオ

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。

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。

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。

空気質センサー

ダッシュボード

Real-time sensor data (リアルタイムのセンサーデータ)

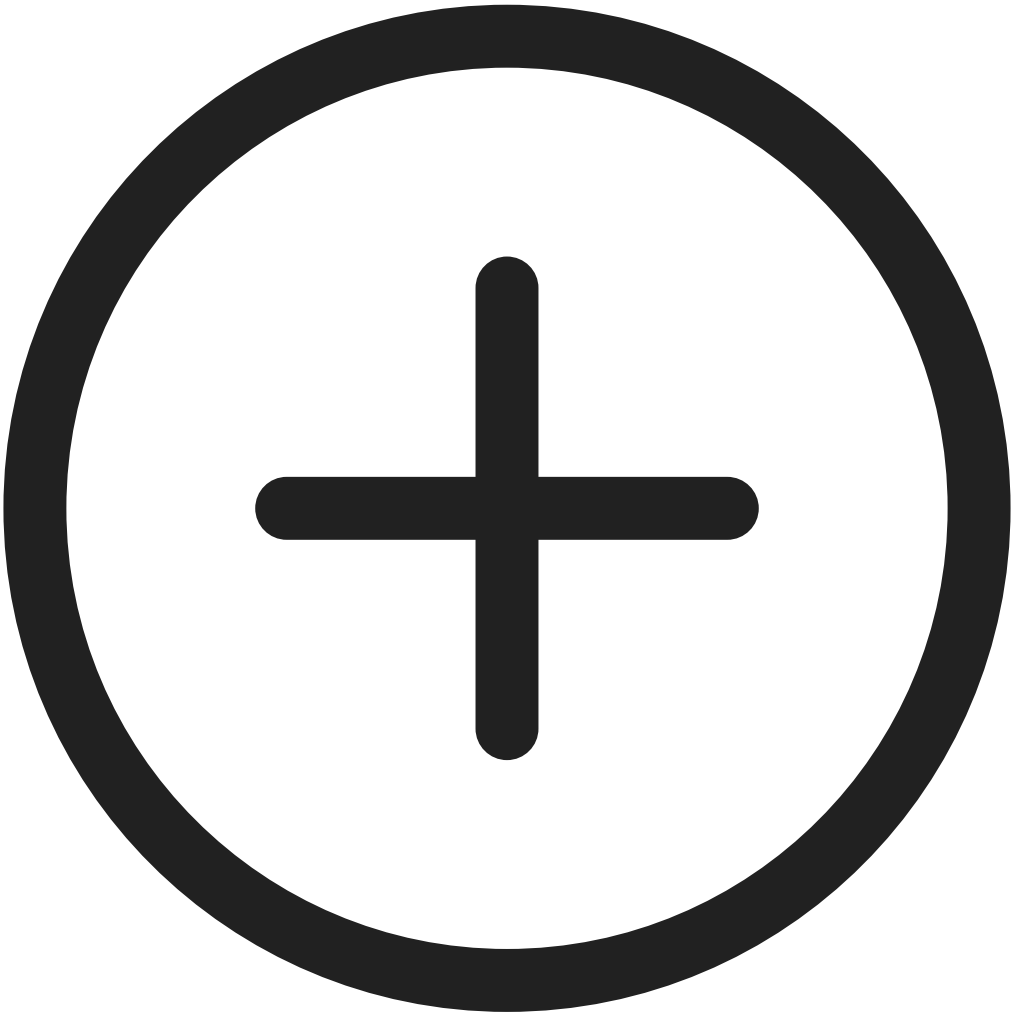
リアルタイムのセンサーデータを表示します。

注

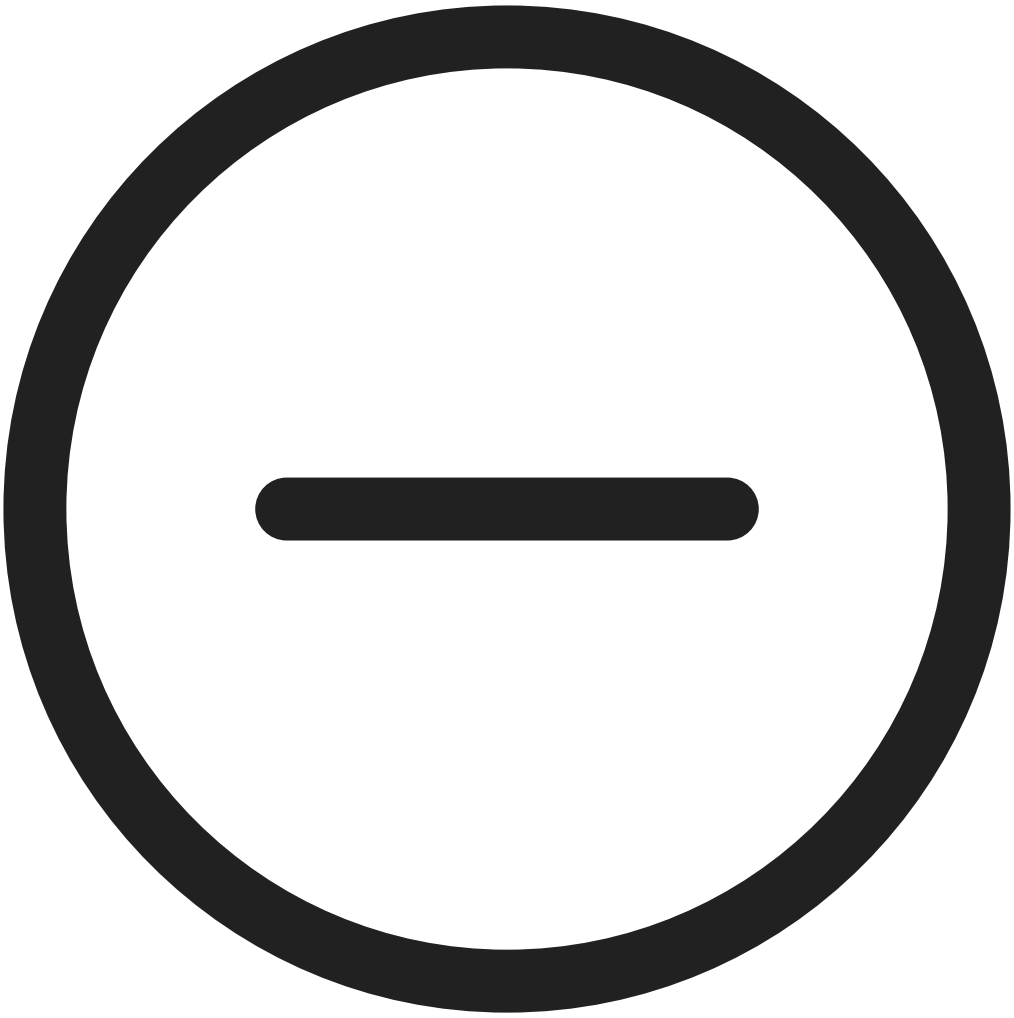
- 完全なCO2精度を得るには、デバイスの初回作動時には2日間が必要です。
- AQI (空気質指数) は、デバイスの初回作動時に機能するまでに12時間が必要です。AQIは、十分なデータが得られるまで、**Calculating (計算中)**と表示されます。デバイスが再起動するたびに、キャリブレーション時間が必要です。
- 完全なVOC精度は、デバイスを1時間作動させた後に得られます。デバイスが再起動するたびに、キャリブレーション時間が必要です。
- 完全なNOx精度は、デバイスを6時間作動させた後に得られます。デバイスが再起動するたびに、キャリブレーション時間が必要です。

: クリックするとダッシュボードの名前が設定されます。

編集:クリックして、データを表示または非表示にします。



: クリックするとダッシュボードにデータが追加されます。



: クリックするとダッシュボードからデータが削除されます。

Temperature (温度):空気質センサーによるリアルタイムの温度を表示します。

湿度:空気質センサーによるリアルタイムの湿度を表示します。

CO2: リアルタイムの二酸化炭素濃度を表示します。

CO2ステータスバーのカラーの意味は以下の通りです。

- **緑色 (0-1000)**:**良好**。データは良好とみなされます。
- **オレンジ色 (1001-2000)**:**感受性が高い人々にとっては有害**。感受性が高い人々にとっては有害な状態です一般的な人々が影響を受ける可能性は高くありません。
- **赤色 (2001-5000)**:**有害**.すべての人の健康に影響が及ぶ可能性があります。感受性が高い人々は、より深刻な影響を受ける可能性があります。
- **紫色 (5001-40000)**:**非常に有害**。健康に関する緊急事態の警告です。すべての人々が影響を受ける可能性がさらに高くなります。

NOx: 一酸化窒素と二酸化窒素をリアルタイムで表示。

NOxステータスバーのカラーの意味は以下の通りです。

- **緑色 (0-30):良好**。データは良好とみなされます。
- **黄色 (31-150):許容可能**。このデータは許容可能です。ごく少数の並外れて敏感な人には、許容範囲の健康上の懸念があるかもしれません。
- **オレンジ色 (151-300):感受性が高い人々にとっては有害**。すべての人の健康に影響が及ぶ可能性があります。感受性が高い人々は、より深刻な影響を受ける可能性があります。
- **赤色 (301-500):有害**。すべての人の健康に影響が及ぶ可能性があります。感受性が高い人々は、より深刻な影響を受ける可能性があります。

PM 1.0: リアルタイムの粒子状物質1.0を表示。

PM 2.5: リアルタイムの粒子状物質2.5を表示。

PM 2.5ステータスバーのカラーの意味は以下の通りです。
- **緑色 (0-9):良好**。データは良好とみなされます。
- **黄色 (9.1-35.4):許容可能**。このデータは許容可能です。ごく少数の並外れて敏感な人には、許容範囲の健康上の懸念があるかもしれません。
- **オレンジ色 (35.5-55.4):感受性が高い人々にとっては有害**。すべての人の健康に影響が及ぶ可能性があります。感受性が高い人々は、より深刻な影響を受ける可能性があります。
- **赤色 (55.5-125.4):有害**。すべての人の健康に影響が及ぶ可能性があります。感受性が高い人々は、より深刻な影響を受ける可能性があります。
- **紫色 (125.5-225.4):非常に有害**。健康に関する緊急事態の警告です。すべての人々が影響を受ける可能性がさらに高くなります。
- **栗色 (225.5-1000):危険**。緊急事態です。すべての人々が影響を受ける可能性がさらに高くなります。

PM 4.0: リアルタイムの粒子状物質4.0を表示。

PM 10.0: リアルタイムの粒子状物質10.0を表示。

PM 10.0ステータスバーのカラーの意味は以下の通りです。
- **緑色 (0-54):良好**。データは良好とみなされます。
- **黄色 (55-154):許容可能**。このデータは許容可能です。ごく少数の並外れて敏感な人には、許容範囲の健康上の懸念があるかもしれません。
- **オレンジ色 (155-254):感受性が高い人々にとっては有害**。すべての人の健康に影響が及ぶ可能性があります。感受性が高い人々は、より深刻な影響を受ける可能性があります。
- **赤色 (255-354):有害**。すべての人の健康に影響が及ぶ可能性があります。感受性が高い人々は、より深刻な影響を受ける可能性があります。
- **紫色 (355-424):非常に有害**。健康に関する緊急事態の警告です。すべての人々が影響を受ける可能性がさらに高くなります。
- **栗色 (425-1000):危険**。緊急事態です。すべての人々が影響を受ける可能性がさらに高くなります。

ベイピング/喫煙: 検知または未検知のベイピング/喫煙を表示します。

ベイピング/喫煙ステータスバーのカラーの意味は以下の通りです。
- **緑:非検知**。ベイピング/喫煙の疑いのある行為は検知されていません。
- **赤:検知**。ベイピング/喫煙の疑いのある行為が検知されています。

VOC: 揮発性有機化合物指数を表示します。

VOCステータスバーのカラーの意味は以下の通りです。
- **緑色 (0-100):良好**。データは良好とみなされます。

- **黄色 (101-300):許容可能**。このデータは許容可能です。ごく少数の並外れて敏感な人には、許容範囲の健康上の懸念があるかもしれません。
- **オレンジ色 (301-400):感受性が高い人々にとっては有害**。すべての人の健康に影響が及ぶ可能性があります。感受性が高い人々は、より深刻な影響を受ける可能性があります。
- **赤色 (401-500):有害**。すべての人の健康に影響が及ぶ可能性があります。感受性が高い人々は、より深刻な影響を受ける可能性があります。

AQI: 空気質指数を表示します。

空気質指数ステータスバーのカラーの意味は以下の通りです。

- **緑色 (0-50):良好**。データは良好とみなされます。
- **黄色 (51-100):許容可能**。このデータは許容可能です。ごく少数の並外れて敏感な人には、許容範囲の健康上の懸念があるかもしれません。
- **オレンジ色 (101-150):感受性が高い人々にとっては有害**。すべての人の健康に影響が及ぶ可能性があります。感受性が高い人々は、より深刻な影響を受ける可能性があります。
- **赤色 (151-200):有害**。すべての人の健康に影響が及ぶ可能性があります。感受性が高い人々は、より深刻な影響を受ける可能性があります。
- **紫色 (201-300):非常に有害**。健康に関する緊急事態の警告です。すべての人々が影響を受ける可能性がさらに高くなります。
- **栗色 (301-500):危険**。緊急事態です。すべての人々が影響を受ける可能性がさらに高くなります。

設定

閾値

空気質センサーのデータを設定する。

Temperature (温度):温度MIN (最小)とMAX (最大)を-10～45の範囲で設定します。

湿度：湿度MIN (最小)とMAX (最大)を0～100の範囲で設定します。

CO2：二酸化炭素MIN (最小)とMAX (最大)を0～40000の範囲で設定します。

NOx：一酸化窒素と二酸化窒素のMIN (最小)とMAX (最大) を0～500の範囲で設定します。

PM1.0：粒子状物質1.0MIN (最小)とMAX (最大)を0～1000の範囲で設定します。

PM2.5：粒子状物質2.5MIN (最小)とMAX (最大)を0～1000の範囲で設定します。

PM4.0：粒子状物質4.0MIN (最小)とMAX (最大)を0～1000の範囲で設定します。

PM10.0：粒子状物質MIN (最小)とMAX (最大)を0～1000の範囲で設定します。

VOC：揮発性有機化合物指数MIN (最小)とMAX (最大) を0～500の範囲で設定します。

AQI：空気質指数MIN (最小)とMAX (最大)を0～500の範囲で設定します。

温度の単位

Show temperature in (表示温度の単位)：Celsius (摂氏)またはFahrenheit (華氏)

ベイピング検知感度

ベイピング検知感度を設定します。

Low sensitivity (低感度)、High sensitivity (高感度)：スライダーを使用して、デバイスがアラームを発する低感度と高感度の差を調整します。高感度は、デバイスは電子タバコやタバコの喫煙量が微量でもそれを検知し、アラートをトリガーします。低感度は、デバイスは喫煙量が多い場合のみ反応するため、誤警報の可能性は低くなります。

ストレージ設定

- Retention time 1 month, frequency 1s (保持期間1か月、周期1秒): データは毎秒収集され、直近30日間のみ保持されます。
- Retention time 3 month, frequency 5s (保持期間3か月、周期5秒): データは5秒ごとに収集され、直近90日間のみ保持されます。
- Retention time 1 year, frequency 10s (保持期間1年、周期10秒): データは10秒ごとに収集され、直近365日間のみ保持されます。

注

ストレージオプションを変更すると、既存のデータが消去されます。

クラウドメタデータ伝送周期

クラウドメタデータ伝送周期は、センサーメタデータを調整可能な伝送周期でサブスクライブしたいサードパーティプラットフォームによって使用されます。クラウドメタデータには、ダッシュボードに表示されるすべてのセンサーデータが含まれます。

Cloud metadata (クラウドメタデータ):クラウドメタデータを使用する場合はオンにします。

注

デフォルトではこの機能は無効になっており、トピックのメタデータは送信されません。有効にすると、以下に設定した伝送周期でトピックのメタデータが送信されます。

Set frequency range (00:00:01 - 23:59:59) (周期の範囲の設定、00:00:01～23:59:59): 値を入力して周期の範囲を設定します。

検証期間

以下の空気質設定に検証期間を設定できます。検証期間は時間閾値の役割を果たし、アラームをトリガーするためには測定値が検証期間の範囲を上回っている必要があります。

例

CO_2検証期間が5秒の場合、アラームをトリガーするためにはCO_2レベルが5秒間、上限を上回る必要があります。

以下のデータに検証期間の範囲 (0秒～60秒) を設定します。

- 気温
- 湿度
- CO2
- NOx
- PM1.0
- PM2.5
- PM4.0
- PM10.0
- VOC
- AQI
- 電子タバコ/喫煙

統計情報

センサーデータの統計情報

最大365日分のセンサー統計情報をCSVファイルにエクスポートし、Microsoft® Excelなどのアプリケーションで使用できます。

- **Predefined date range (あらかじめ定義された日付範囲)**: あらかじめ定義された日付範囲をリストからダウンロードする場合に選択します。
- **From (開始)** と **To (終了)**: カスタム範囲をダウンロードする場合に選択します。データは最大365日分ダウンロードできます。

注

カスタム範囲とあらかじめ定義された範囲の両方が選択されている場合、カスタム範囲が優先されます。

注

最大ダウンロード範囲は、で設定された保持期間に制限されます。

- **Select a source (ソースを選択)**: ダウンロードするソースを選択します。
- **Download data (データをダウンロード)**: トップダウンメニューから **[Download selected sensor data (選択したセンサーデータをダウンロード)]** を選択します。
- **Download data for all sources (すべてのソースのデータをダウンロード)**: 選択した期間のすべてのソースのデータをエクスポートします。

ファイルはダウンロードフォルダーにダウンロードされます。ファイルサイズによっては、ダウンロードに時間がかかる場合があります。

分析機能

AXIS Audio Analytics

音圧レベル

Show threshold and events in graph (グラフに閾値とイベントを表示):オンにすると、音声スパイクが検知されるとグラフに表示されます。

Threshold (閾値):検知の閾値を調整します。アプリケーションは、この閾値から外れた音の音声イベントを登録します。

適応音声検知

Show events in graph (グラフにイベントを表示):オンにすると、音声スパイクが検知されるとグラフに表示されます。

Threshold (閾値):スライダーを動かして、検知の閾値を調整します。閾値を最小にするとわずかな音量のスパイクも検知対象となり、閾値を最大にすると顕著な音量のスパイクだけが検知対象となります。

Test alarms (アラームのテスト):テストを実行するために検知イベントをトリガーするには、[Test] (テスト) をクリックします。

Audio classification (音声分類)

Show events in graph (グラフにイベントを表示) :オンにすると、特定のタイプの音声が検知されるとグラフに表示されます。

Classifications (分類) :アプリケーションに検知させる音声タイプを選択します。

Test alarms (アラームのテスト) :[Test (テスト)] をクリックすると、テストを実行するために特定の音の検知イベントをトリガーします。

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。

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。

音声エンハンスメント

入力

Ten Band Graphic Audio Equalizer (10バンドグラフィック音声イコライザー):オンに設定して、音声信号内の異なる周波数帯域のレベルを調整します。この機能は、音声の設定経験のある上級ユーザー向けです。

トークバック範囲:音声コンテンツを収集する動作範囲を選択します。動作範囲を広げると、同時双方向通信機能が低下します。

音声強化:オンにすると、他の音声との関連で音声コンテンツが強化されます。

概要

シグナリングLEDステータス

デバイス上で動作中の、シグナリングLEDのさまざまなアクティビティを表示します。シグナリングLEDステータスリストには、同時に最大10個のアクティビティが表示されます。2つ以上のアクティビティが同時に実行されると、優先度が最も高いアクティビティがLEDステータスに表示されます。その行は、ステータスリストでハイライトされます。

音声スピーカーのステータス

デバイスで実行されている音声スピーカーのさまざまなアクティビティを表示します。音声スピーカーのステータスリスト内のアクティビティは同時に10個まで実行できます。2つ以上のアクティビティを同時に実行すると、優先度が最も高いアクティビティが実行されます。その行は、ステータスリストで緑色にハイライトされます。

プロファイル

プロファイル

プロファイルとは、設定された構成の集合を意味します。優先順位やパターンの異なる最大30のプロファイルを設定できます。プロファイルを一覧表示して、名前、優先度、ライトとサイレンの設定の概要を示します。

作成:クリックして、プロファイルを作成します。

- **Preview/Stop preview (プレビュー/プレビュー停止)**:プロファイルを保存する前に、プロファイルのプレビューを開始または停止します。

注

同じ名前のプロフィールが2つ存在することはできません。

- **名前**:プロファイルの名前を入力します。
- **Description (説明)**:プロファイルの説明を入力します。
- [Light (照明)]:ドロップダウンメニューから必要な照明の [Pattern (パターン)]、[Speed (速度)]、[Intensity (強度)]、[Color (色)] を選択します。
- [Siren (サイレン)]:ドロップダウンメニューから、必要なサイレンの [Pattern (パターン)] と [Intensity (強度)] を選択します。
- ライトまたはサイレンのみのプレビューを開始または停止します。
- [Duration (継続時間)]:アクティビティの継続時間を設定します。
  - [Continuous (連続性)]:起動すると、停止するまで実行されます。
  - Time (時刻):アクティビティが継続する時間を指定します。
  - [Repetitions (反復性)]:アクティビティを繰り返す回数を設定します。
- [Priority (優先度)]:アクティビティの優先順位を1～10の間で設定します。優先順位が10より高いアクティビティは、ステータスリストから削除できません。優先度が10よりも高いアクティビティには、**メンテナンス**(11)、**識別**(12)、**健全性チェック**(13)の3つのアクティビティがあります。

インポート:既定の設定を使用して、1つ以上のプロファイルを追加します。

- **Add (追加)**:新しいプロファイルを追加します。
- **Delete and add (削除して追加)**:古いプロファイルを削除し、新しいプロファイルをアップロードできます。
- [Overwrite (上書き)]:更新されたプロファイルは、既存のプロファイルを上書きします。

プロファイルをコピーして他の装置に保存するには、1つ以上のプロファイルを選択して [Export (エクスポート)] をクリックします。.jsonファイルがエクスポートされます。

プロファイルを開始します。プロファイルとそのアクティビティがステータスリストに表示されます。

[Edit (編集)]、[Copy (コピー)]、[Export (エクスポート)]、または[Delete the profile (プロファイルを削除)]を選択します。

録画

進行中の録画:進行中のすべての録画を表示します。

● 録画を開始します。

設定されたネットワークストレージを選択します。

● 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。

メディア

+ Add (追加):クリックして新規ファイルを追加します。

Storage location (保存先):内部メモリーまたはオンボードストレージ (SDカード、利用可能な場合) への保存を選択します。

⋮ コンテキストメニューは以下を含みます。

- Information (情報):ファイルに関する情報を表示します。
- Copy link (リンクをコピー):デバイス内のファイルの位置へのリンクをコピーします。
- 削除:保存先からファイルを削除します。

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 (信頼された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。

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)**:設定を変更するアクセス権を持っていません。

⋮ コンテキストメニューは以下を含みます。

Update account (アカウントの更新):アカウントのプロパティを編集します。

Delete account (アカウントの削除):アカウントを削除します。rootアカウントは削除できません。

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。

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。

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。

マルチキャストコントローラー

Use multicast controller (マルチキャストコントローラーを使用):オンにすると、マルチキャストコントローラーが有効になります。

Audio codec (音声コーデック):音声コーデックを選択します。

＋ **Source (ソース)**:新しいマルチキャストコントローラーソースを追加します。
- **ラベル**:ソースでまだ使用されていないラベルの名前を入力します。
- **Source (ソース)**:ソースを入力します。
- **ポート**:ポートを入力します。
- [**Priority (優先度)**]:優先度を選択します。
- **Profile (プロファイル)**:プロファイルを選択します。
- **SRTP key (SRTPキー)**:SRTPキーを入力します。

⋮ コンテキストメニューは以下を含みます。

Edit (編集):マルチキャストコントローラーソースを編集します。

削除:マルチキャストコントローラーソースを削除します。

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。

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

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。

PIRセンサー

PIRセンサーは、視野内の物体から放射される赤外線を測定します。

感度レベル:レベルを0～100の範囲で調整します。0は最も感度が低く、100は最も感度が高いとします。

電源の設定

電力状態

電力状態情報が表示されます。情報は製品によって異なります。

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。

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。

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

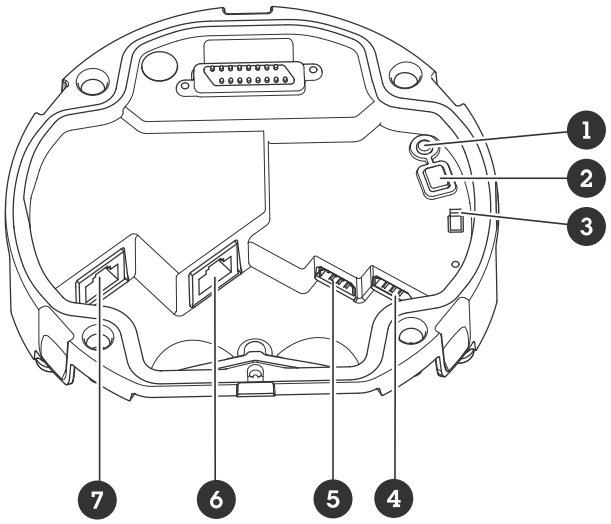
ネットワークトレースファイルには、証明書やパスワードなどの機密情報が含まれている場合があります。

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。

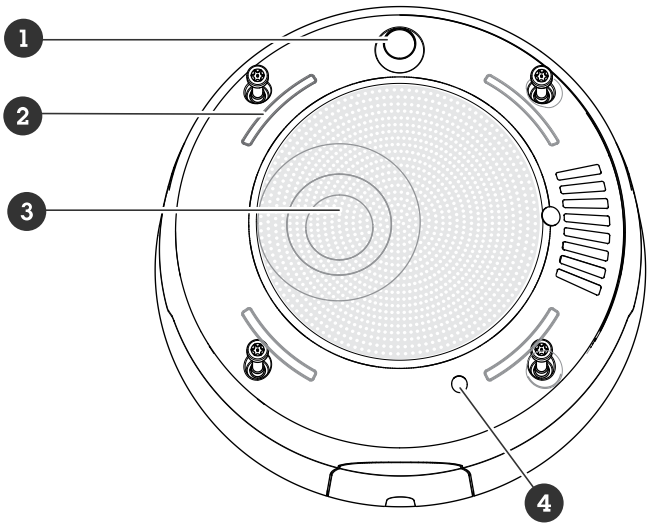
Trace time (追跡時間):秒または分でトレースの期間を選択し、[**ダウンロード**] をクリックします。

仕様

製品概要



1 ステータスLEDインジケーター
2 コントロールボタン
3 マイクスイッチ
4 I/Oコネクター
5 RS-485コネクター
6 ネットワークコネクタ (PoE出力)
7 ネットワークコネクタ (PoE入力)



1 PIRセンサー
2 シグナリングLED
3 スピーカー
4 内蔵マイク

ステータスLED

ステータスLED	説明
消灯	正常動作の場合消灯します。
緑	起動完了後、通常の操作では10秒間点灯します。
オレンジ	起動時に点灯し、装置のソフトウェアのアップグレード中、または工場出荷時の設定にリセット中に点滅します。
オレンジ/赤	ネットワーク接続が利用できないか、失われた場合は点滅します。

ボタン

コントロールボタン

コントロールボタンは、以下の用途で使用します。
- 製品を工場出荷時の設定にリセットする。を参照してください。

マイクスイッチ

マイクロフォンスイッチの場所については、を参照してください。

マイクロフォンスイッチを使用すると、マイクロフォンを機械的に**オン**または**オフ**にできます。工場出荷時の設定では、このスイッチは**オフ**になっています。

コネクター

ネットワーク コネクター

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

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

I/Oコネクター

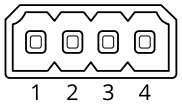
I/Oコネクターに外部装置を接続し、動体検知、イベントトリガー、アラーム通知などと組み合わせて使用することができます。I/Oコネクターは、0 VDC基準点と電力 (12 V DC出力) に加えて、以下のインターフェースを提供します。

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。

状態監視入力 - デジタル入力のいたずらを検知する機能が有効になります。

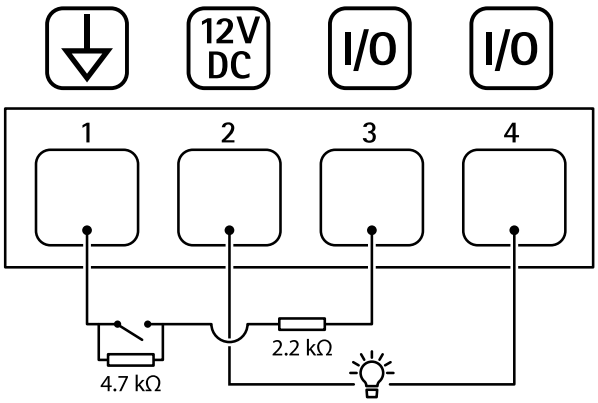
デジタル出力 - リレーやLEDなどの外部装置を接続します。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースを通じたイベントまたは本装置のwebインターフェースから有効にすることができます。

4ピンターミナルブロック



機能	ピン	メモ	仕様
DCアース	1		0 VDC
DC出力	2	⚠ 補助装置の電源供給に使用できます。 注:このピンは、電源出力としてのみ使用できます。	12VDC 最大負荷 = 25 mA
設定可能 (入力または出力)	3–4	デジタル入力/状態監視 – 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。状態監視を使用するには、終端抵抗器を設置します。抵抗器を接続する方法については、接続図を参照してください。	0～30 VDC (最大)
		デジタル出力 – アクティブ時はピン1 (DCアース) に内部で接続し、非アクティブ時はフロート状態 (未接続) になります。リレーなどの誘導負荷と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。	0～30 VDC (最大)、オープンドレイン、100 mA

例:

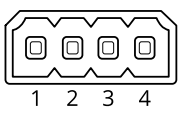


1 *DCアース*
2 *DC出力12 V、最大25 mA*
3 *I/O (状態監視として設定)*
4 *I/O (出力として設定)*

RS485/RS422コネクター

RS485/RS422シリアルインターフェース用2ピンターミナルブロック×2。シリアルポートの設定により、次のモードをサポート可能。

- 2ワイヤーRS485半二重
- 4ワイヤーRS485全二重
- 2ワイヤーRS422単方向
- 4ワイヤーRS422全二重ポイントツーポイント通信



機能	ピン	メモ
RS485/RS422 RX/TX A	1	(RX) 全二重RS485/RS422用 (RX/TX) 半二重用 RS485
RS485/RS422 RX/TX B	2	
RS485/RS422 TX A	3	(TX) 全二重RS485/RS422用
RS485/RS422 TX B	4	

ライトパターン名

オフ
点灯
代替
パルス
3つのステップでエスカレート
点滅
3回点滅
4回点滅
3回点滅して消える
4回点滅して消える
1回点滅
3回点滅

サイレンのパターン名

オフ
アラーム:高音アラーム
アラーム:低音アラーム
アラーム:鳥
アラーム:汽笛
アラーム:カーアラーム
アラーム:車のアラーム 高速
アラーム:クラシック時計
アラーム:初回出席者
アラーム:ホラー
アラーム:工業
アラーム:単一ビープ音
アラーム:ソフトクアッドビープ音
アラーム:ソフトトリプルビープ音
アラーム:トリプルハイピッチ

通知:許可
通知:呼び出し中
通知:却下
通知:完了
通知:エントリ
通知:失敗
通知:急ぐ
通知:メッセージ
通知:次へ
通知:オープン
[Siren (サイレン)]:代替
[Siren (サイレン)]:弾む
[Siren (サイレン)]:救急
[Siren (サイレン)]:下降調
[Siren (サイレン)]:ホームソフト

装置を清掃する

装置はぬるま湯で洗浄できます。

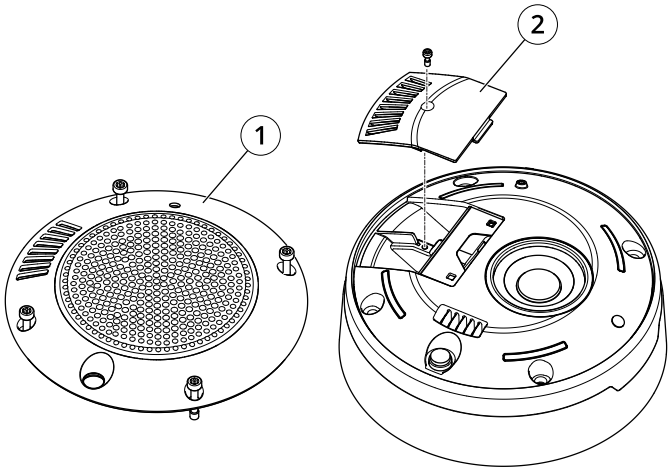
注意

- 強力な化学薬品は装置を損傷する可能性があります。窓ガラス用洗剤やアセトンなどの化学薬品を使用して装置をクリーニングしないでください。

1. 圧縮空気を使用すると、装置からほこりやごみを取り除くことができます。
2. 必要に応じて、ぬるま湯に浸した柔らかいマイクロファイバーの布で装置を清掃してください。
3. シミを防ぐために、きれいな非研磨性の布で装置から水分を拭き取ってください。

注

- カバー (1) とドア (2) を取り外します。
- ブラシを使ってほこりを取り除きます。



1 カバー
2 ドア

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。

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。

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。

別の製品に接続した後、デバイスが起動しない	
PoEクラスが誤っている	デバイスを別の製品に接続した場合、PoEクラス4の電源が使用されていることを確認してください。

センサーデータが正確でない	
センサーデータが不正確である	AQI (大気質指数)、CO2、VOC、NOxが機能するまでには時間がかかります。 を参照してください。

パフォーマンスに関する一般的な検討事項

最も重要な検討事項には次のようなものがあります。

- 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。

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。

T10222990_ja

2025-09 (M2.4)