

AXIS S3016 Recorder

デバイスについて

AXIS S3016 Recorderは、PoEスイッチと監視クラスのハードドライブを統合したネットワークビデオレコーダーです。また、ビデオ映像を簡単にエクスポートできるUSB 3.0ポートも搭載しています。レコーダーには、8 TB、16 TB、32 TBの3つのモデルがあります。

使用に当たって

装置にアクセスする

ネットワーク上のデバイスを検索する

Windows[®]でネットワーク上のAxis装置を見つけ、IPアドレスを割り当てるには、AXIS IP Utilityま たはAXIS Device Manager Extend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™	Firefox®	Edge™	Safari®
Windows®	推奨	推奨	\checkmark	
macOS®	推奨	推奨	\checkmark	\checkmark
Linux®	推奨	推奨	\checkmark	
その他のオペ レーティングシ ステム	1	√	✓	√*

* iOS 15またはiPadOS 15でAXIS OS Webインターフェースを使用するには、

[Settings (設定)] > [Safari] > [Advanced (詳細)] > [Experimental Features (実験的機能)]に移動 し、[NSURLSession Websocket]を無効にします。

装置のwebインターフェースを開く

- 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 Extend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

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

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

データを保護するために、次のことが強く推奨されています。

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

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。

webインターフェースの概要

このビデオでは、装置のwebインターフェースの概要について説明します。



Axis装置のwebインターフェース

使用に当たって

注

システムの設定を行うときはインターネットアクセスが必要です。

- 1.
- 2.
- 3.
- 4.
- 5.

インストールが完了したら:

- ・ システム内のすべてのAxis装置には最新のファームウェアが搭載されています。
- すべての装置にはパスワードがあります。
- デフォルト設定での録画が有効です。
- リモートアクセスが使用できます。

My Axisアカウントを登録する

axis.com/my-axis/loginでMy Axisアカウントを登録します。

My Axisアカウントの安全性を高めるため、多要素認証 (MFA) を有効にしてください。MFAは、 ユーザーの身元確認のために別の認証レイヤーを追加するセキュリティシステムです。

MFAを有効にするには:

- 1. axis.com/my-axis/loginに移動します。
- 2. My Axisの認証情報を使用してログインします。
- 3. ② に移動し、[Account settings (アカウント設定)] を選択します。
- 4. [Security settings (セキュリティ設定)] をクリックします。
- 5. [Handle your 2-factor authentication (2要素認証の処理)] をクリックします。
- 6. My Axisの認証情報を入力します。
- 7. 認証方法として [Authenticator App (TOTP) (認証アプリ(TOTP)] または [Email (電子メー ル)] のいずれかを選択し、画面の指示に従います。

ハードウェアのインストール

- 1. カメラのハードウェアをインストールします。
- 2. LANポート経由でレコーダーをネットワークに接続します。
- 3. カメラをレコーダー内蔵のPoEスイッチまたは外部PoEスイッチに接続します。
- 4. コンピューターをレコーダーと同じネットワークに接続します。
- 5. 電源をレコーダーに接続します。

重要

まずレコーダーに電源コードを接続し、電源ケーブルをコンセントに接続する必要がありま す。

6. 録画やカメラが起動するまで数分間待ってから、続行してください。

▲注意

オーバーヒートを避けるため、換気の良い環境にレコーダーを置き、レコーダーの周りに十分 なスペースを確保してください。

デスクトップアプリをインストールする

- 1. axis.com/products/axis-camera-station-edgeに移動し、[Download (ダウンロード)] をク リックして、Windows用の AXIS S3016 Recorderをダウンロードします。
- 2. 設定ファイルを開き、設定アシスタントに従います。
- 3. My Axisアカウントでサインインします。

サイトを作成する

サイトは、監視ソリューション (たとえば、店舗内のすべてのカメラ) への入り口です。1つのMy Axisアカウントで複数のサイトを追跡できます。

- 1. AXIS S3016 Recorderデスクトップアプリを起動します。
- 2. My Axisアカウントでサインインします。
- 3. [Create new site (新規サイトの作成)] をクリックして、サイト名を付けます。
- 4. [Next (次へ)] をクリックします。
- 5. サイトに追加するデバイスを選択します。

- 6. [Next (次へ)] をクリックします。
- 7. ストレージを選択します。
- 8. [Next (次へ)] をクリックします。
- 9. [Ready to install (インストールの準備完了)] ページでは、[Offline mode (オフライン モード)] と [Upgrade firmware (ファームウェアのアップグレード)] がデフォルトでオン になっています。オフラインモードにアクセスしたり、装置を最新のファームウェアバー ジョンにアップグレードしたりしない場合は、これらをオフにすることができます。
- 10. [Install (インストール)] をクリックし、AXIS S3016 Recorderで装置が設定されるまで待ち ます。 設定の完了までに数分かかる場合があります。

モバイルアプリをインストールする

AXIS S3016 Recorder モバイルアプリを使用すると、どこからでも装置や録画にアクセスできます。また、イベントが発生した場合や、インターカムから誰かが呼び出しを行った場合にも、通知を受け取ることができます。

Android版

[Download (ダウンロード)]をクリックするか、次のQR Code®をスキャンします。



iOS版

[Download (ダウンロード)]をクリックするか、次のQR Codeをスキャンします。



AXIS S3016 Recorderモバイルアプリを開き、Axisの認証情報を使用してログインします。

My Axisアカウントをお持ちでない場合は、*axis.com/my-axis*にアクセスして新しいアカウントを 登録できます。

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。

AXIS Camera Stationでの作業の開始

レコーダーを追加する

注

AXIS Camera Stationは、レコーダーを新しいシステムに追加するときに、以前のシステムから 録画を削除します。

- 1. [設定] [デバイス] [デバイスを追加] を選択します。
- 2. リストからレコーダーを選択し、[Add (追加)] をクリックします。レコーダーが表示されて いない場合は、[Manual search (手動検索)]を使用して手動で検索してください。
- 3. デフォルト設定を使用し、[Next (次へ)]をクリックします。
- ストレージ暗号化のパスワードを設定します。[Next (次へ)] をクリックします。このパス ワードは、レコーダーハードドライブにAXIS Camera Station外からアクセスする場合や、 装置のWebインターフェースからレコーダーを工場出荷時の設定にリセットする場合に必 要です。
- 5. [Configuration > Devices > Other devices (設定>デバイス>他のデバイス)] に移動し、 レコーダーが追加されているのを確認します。
- 6. [Configuration > Storage > Management (設定>ストレージ>管理)] に移動し、レコー ダーがストレージリストに追加されていることを確認します。

装置を追加し、録画ストレージとしてレコーダーを選択する

- 1. [設定] [デバイス] [デバイスを追加] を選択します。
- リストから装置を選択し、[Add (追加)] をクリックします。デバイスがリストされていない 場合は、[Manual search (手動検索)]を使用して手動で検索してください。
- 3. デフォルト設定を使用し、[Next (次へ)] をクリックします。
- 4. [Recording storage (録画ストレージ)] ドロップダウンリストからレコーダーを手動で選択し、[Install (インストール)] をクリックします。

注

[Automatic (自動)]を選択した場合、レコーダーは録画ストレージとして選択されません。

5. [設定] - [ストレージ] - [選択] を選択します。装置をクリックし、録画ストレージがレコー ダーか確認します。

録画を設定

- 1. [Configuration > Storage > Selection (設定 > ストレージ > 選択)] に移動し、デバイス を選択します。
- 2. [Retention time (保存期間)]を設定します。
 - ストレージが一杯になるまで録画を保存するには、保存期間に [Unlimited (無制限)]
 を選択します。
 - [Limited (制限付き)] を選択して、録画を保存する最大日数を設定します。
- 3. [適用]をクリックします。

注

[Fallback recording (フォールバック録画)] はデフォルトで有効になっており、AXIS Camera Stationとレコーダーの接続が失われたときに、録画がレコーダーに保存されます。フォール バック録画を参照してください。

デバイスを構成する

電力の割り当て

レコーダーはポートごとに一定の電力を確保しています。予約電力の合計は合計電源容量を超え ることはできません。レコーダーが使用可能な電力以上の電力を確保しようとした場合、ポート には電力が供給されません。これにより、接続されているすべての装置に確実に電源が供給され るようになります。

<mark>例:</mark> この例では:

- AXIS S3016 Recorderの合計電源容量は305 Wです。
- T PoE Class 3装置。要求する電力は15.5 Wですが、実際消費する電力は7.5 Wです。
- **v** PoE Class 4装置。要求する電力は30 Wですが、実際消費する電力は15 Wです。
- 確保する電力。
- 実際の消費電力。



実際の消費電力



- ・ 各ポートは、デバイスのPoEクラスに従って電力量を確保します。
- ・ レコーダーは、9台のPoE Class 4装置と2台のPoE Class 3装置を給電できます。
- 最大占有電力は (9 x 30) + (2 x 15.5) = 301 Wです。
- 実際に消費される電力は、(9×15)+(2×7.5)=150 Wです。

RAIDレベルの変更

▲注意

RAIDレベルを変更すると、ファイルシステムが再フォーマットされ、ディスクからすべての データが削除されます。

- 装置のwebインターフェースで、[System (システム)] > [Storage (ストレージ)] に移動し ます。
- 2. [Tools (ツール)] で、[Change RAID level (RAIDレベルの変更)] を選択し、[Use tool (ツー ルを使用)] をクリックします。
- 3. RAIDレベルを選択し、[Next (次へ)]をクリックします。

- 4. [Encrypt the disk (ディスクの暗号化)] を選択し、パスワードを入力します。[Next (次へ)] をクリックします。
- 5. [Yes (はい)] をクリックします。
- 6. ステータスメッセージが右上隅に表示されます。操作が完了し、RAID configuredが表示 されるまで待ってから、ページを閉じます。

ハードドライブの交換

注

静電放電を避けるために、システム内部のコンポーネントを操作するときは、常に静電マット と静電ストラップを使用することをお勧めします。

- 1. ベゼルの左右のネジを緩め、ベゼルを取り外します。
- 赤色のLEDで示される故障したハードドライブを見つけます。 RAIDに障害が発生した場合、すべてのLEDが赤色に点灯します。故障したハードドライブ を特定するには、装置のwebインターフェースにアクセスし、[System (システム)] > [Storage (ストレージ)] > [Hard drive status (ハードドライブのステータス)] に移動しま す。
- 3. ハードドライブスレッド (T10) のネジを緩めます。
- 4. ハードドライブスレッドをハードドライブベイから引き出します。
- 5. ハードドライブ (T8) の4本のネジを緩めます。
- 6. ハードドライブをハードドライブスレッドから取り出します。
- 7. 新しいハードドライブをハードドライブスレッドに挿入します。
- 8. ハードドライブの4本のネジを締めます。
- 9. ハードドライブスレッドをハードドライブベイの奥まで押し込みます。
- 10. ハードドライブスレッドのネジを締めます。LEDインジケーターが緑色になるまで待機して ください。
- 11. ベゼルを取り付け、ベゼルの左右のネジを締めます。

新しいRAIDの作成

▲注意

新しいRAIDを作成するのは、RAIDに障害が発生した場合のみです。新しいRAIDを作成すると、 ハードドライブからすべてのデータが削除されます。

- 1. 故障したハードドライブを交換します。を参照してください。
- 2. RAIDを設定します。を参照してください。
- 3. ビデオ管理システムで録画を設定します。「」および「」を参照してください。

レコーダーをハードリセットする

重要

レコーダーは電源がオンになっている間は慎重に動かしてください。突然動かしたり衝撃を与 えたりすると、ハードドライブが破損する場合があります。

注

- ハードリセットを行うと、IPアドレスを含むすべての設定がリセットされます。
 - ・ ハードリセットを行っても、録画は削除されません。
 - レコーダーの電源を切る: レコーダーの前面にある電源ボタンを、ビープ音が聞こえるまで4~5秒間押し続けます。
 - レコーダーがオフになるまで待ってから、裏返してコントロールボタンにアクセスします。

- 3. コントロールボタンを押し続けます。電源ボタンを押して放し、レコーダーを起動しま す。コントロールボタンを15~30秒間押し、LEDインジケーターがオレンジ色に光ったら リセットボタンを放します。
- 4. レコーダーを所定の場所に慎重に戻します。
- 5. プロセスが完了すると、ステータスLEDが緑色に変わります。これで本製品は工場出荷時の 設定にリセットされました。ネットワーク上に利用可能なDHCPサーバーがない場合、デ フォルトのIPアドレスは192.168.0.90になります
- 6. ハードドライブが暗号化されている場合は、レコーダーをリセットしてから手動でマウン トする必要があります。
 - 6.1. 装置のwebインターフェースに移動します。
 - 6.2. [System (システム)] > [Storage (ストレージ)] に移動し、[Mount (マウント)] をク リックします。
 - 6.3. ハードドライブを暗号化する際に使用する暗号化パスワードを入力します。

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。



・ 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。

ネットワークポート

ネットワークポートのステータス、および割り当てられた電力や合計PoE消費量などの電力情報 が表示されます。

Network ports settings (ネットワークポート設定):クリックすると、設定を変更できるネット ワークポートのページに移動します。

ストレージ

ストレージのステータス、および空き容量やディスク温度などの情報が表示されます。

Storage settings (ストレージ設定):クリックすると、設定を変更できるオンボードストレージのページに移動します。

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。

進行中の録画

ጦ

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。

録画

▷ _{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。

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。

⑪
 ヮリックすると、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



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。
 - 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。

ネットワーク

IPv4

Assign IPv4 automatically (IPv4自動割り当て):ネットワークルーターが自動的にデバイスにIP アドレスを割り当てる場合に選択します。ほとんどのネットワークでは、自動IP (DHCP) をお勧 めします。

IPアドレス:装置の固有のIPアドレスを入力します。孤立したネットワークの内部であれば、アドレスの重複がないことを条件に、静的なIPアドレスを自由に割り当てることができます。アドレスの重複を避けるため、固定IPアドレスを割り当てる前に、ネットワーク管理者に連絡することを推奨します。

サブネットマスク:サブネットマスクを入力して、ローカルエリアネットワーク内部のアドレス を定義します。ローカルエリアネットワークの外部のアドレスは、ルーターを経由します。

Router (ルーター):さまざまなネットワークやネットワークセグメントに接続された装置を接続 するために使用するデフォルトルーター (ゲートウェイ) のIPアドレスを入力します。

Fallback to static IP address if DHCP isn't available (DHCPが利用できない場合は固定IPアド レスにフォールバックする):DHCPが利用できず、IPアドレスを自動的に割り当てることができ ない場合に、フォールバックとして使用する固定IPアドレスを追加するときに選択します。

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。

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]:デフォルトの設定です。インターネットを介してO3Cサービスに接続するには、装置のコントロールボタンを押し続けます。コントロールボタンを押してから24時間以内に装置をO3Cサービスに登録する必要があります。登録しない場合、デバイスはO3Cサービスから切断されます。装置を登録すると、[Always (常時)] が有効になり、装置はO3Cサービスに接続されたままになります。
- [常時]:装置は、インターネットを介してO3Cサービスへの接続を継続的に試行します。装置を登録すると、装置はO3Cサービスに接続したままになります。デバイスのコントロールボタンに手が届かない場合は、このオプションを使用します。
- [なし]:O3Cサービスを無効にします。

Proxy settings (プロキシ設定): 必要な場合は、プロキシサーバーに接続するためのプロキシ設定を入力します。

[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。

ネットワークポート

Power over Ethernet

- ・ Allocated power (割り当てられた電力):現在割り当てられているワット数 (W)。
- Total PoE consumption (合計PoE消費電力):消費されるワット数(W)。
- Keep PoE active during recorder restart (レコーダーの再起動中もPoEを常にアクティブにする):レコーダーの再起動時に接続されたデバイスに電源を供給するには、オンにします。

- クリックして、ポートの画像を表示または非表示にします。

• 画像内のポートをクリックすると、ポートリストにポートの詳細が表示されます。

ポートリスト

- ポート:ポート番号。
- **PoE**: ポートのPoEをオンまたはオフにします。
- Network (ネットワーク):ポートのネットワークをオンまたはオフにします。
- Status (ステータス):このポートに装置が接続されているかどうかを示します。
- Friendly name (フレンドリ名):フレンドリ名は、[Network settings (ネットワーク設定)] で設定します。デフォルト名は、接続された装置のモデルとメディアアクセスコントロールアドレス (MACアドレス) の組み合わせです。
- 消費電力:接続されている装置によって現在消費され、割り当てられているワット数(W)。

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/en-us/axis-os#cryptographic-supportにアクセスしてください。
- Key type (キーのタイプ):ドロップダウンリストから、証明書の保護に使用する暗号化ア ルゴリズムとしてデフォルトかその他のいずれかを選択します。
- - コンテキストメニューは以下を含みます。
 - Certificate information (証明書情報):インストールされている証明書のプロパティを表示します。
 - Delete certificate (証明書の削除):証明書の削除。
 - ・ Create certificate signing request (証明書の署名要求を作成する):デジタルID証明書を 申請するために登録機関に送信する証明書署名要求を作成します。

セキュアキーストア:

- 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。

暗号化ポリシー

暗号化ポリシーは、データ保護のために暗号化がどのように使用されるかを定義します。

Active (アクティブ):デバイスに適用する暗号化ポリシーを選択します:

- ・ Default (デフォルト) OpenSSL: 一般的な使用向けのバランスの取れたセキュリティと パフォーマンス。
- FIPS FIPS 140-2に準拠したポリシー: 規制対象業界向けのFIPS 140-2に準拠した高セキュリティの暗号化。

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。

ファイアウォール

Activate (アクティブ化):ファイアウォールをオンにします。

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

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

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

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

十_{:クリックして、別のルールを作成します。}

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

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

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

注

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

Confirm rules (ルールを確認):クリックして、保留中のルールをアクティブにします。

Active rules (アクティブなルール):装置で現在実行中のルールの概要です。

 ⑪ :クリックして、アクティブなルールを削除します。

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

カスタム署名付きAXIS OS証明書

Axisのテストソフトウェアまたはその他のカスタムソフトウェアを装置にインストールするに は、カスタム署名付きAXIS OS証明書が必要です。証明書は、ソフトウェアが装置の所有者と Axisの両方によって承認されたことを証明します。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。

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。

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 (i [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。

ストレージ

オンボードストレージ

RAID

- Free (空き容量):ディスクの空き容量。
- Status (ステータス):ディスクがマウントされているかどうか。
- ・ File system (ファイルシステム):ディスクに使用されるファイルシステム。
- Encrypted (暗号化):ディスクが暗号化されているかどうか。
- Temperature (温度):ハードウェアの現在の温度。
- Overall heath test (総合的な健全性テスト):ディスクの状態を確認した結果。
- RAID level (RAIDレベル):ストレージに使用されているRAIDレベル。サポートされている RAIDレベルは0、1、5、6、10です。
- RAID status (RAIDスタータス):ストレージのRAIDステータス。表示される値は [Online (オンライン)]、[Degraded (劣化)]、[Syncing (同期中)]、または [Failed (失敗)]です。

ツール

注

次に示すツールを実行するときは、操作が完了するまでページを閉じないようにしてください。

- Check (チェック):ストレージデバイスにエラーがないかを確認し、ある場合は自動修復 を試みます。
- Repair (修復):ストレージ装置を修復します。修復中、アクティブな録画は一時停止されます。ストレージデバイスを修復すると、データが失われる場合があります。
- Format (形式):すべての録画を消去し、ストレージデバイスをフォーマットします。ファ イルシステムを選択します。
- Encrypt (暗号化):保存されているデータを暗号化します。ストレージ装置上のすべての ファイルは消去されます。
- Decrypt (復号化):保存されているデータを複合化します。ストレージ装置上のすべてのファイルは消去されます。
- Change password (パスワードの変更):ディスク暗号化のパスワードを変更します。パスフレーズを変更しても、進行中の録画には影響しません。
- ・ Change RAID level (RAIDレベルの変更):ストレージのRAIDレベルを変更します。
- ・ Use tool (ツールを使用)クリックして、選択したツールを実行します。

Hard drive status (ハードドライブのステータス):クリックすると、ハードドライブのステータス、容量、シリアル番号が表示されます。

Write protect (書き込み禁止):書き込み保護をオンにして、ストレージデバイスが上書きされな いように保護します。

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。

リモートシステムログ

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

┿ サーバー:クリックして新規サーバーを追加します。

[ホスト]:サーバーのホスト名またはIPアドレスを入力します。

Format (形式):使用するsyslogメッセージの形式を選択します。

- Axis
- RFC 3164
- RFC 5424

Protocol (プロトコル):使用するプロトコルを選択します。

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

ポート:別のポートを使用する場合は、ポート番号を編集します。

重大度:トリガー時に送信するメッセージを選択します。

CA証明書設定:現在の設定を参照するか、証明書を追加します。

メンテナンス

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。
- Autorollback (オートロールバック):設定した時間内にアップグレードを行い、アップグレードを確認します。確認しない場合、装置はAXIS OSの以前のバージョンに戻されます。

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

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

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。

署名付きOS

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

セキュアブート

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

Axis Edge Vault

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

TPMモジュール

TPM (トラステッドプラットフォームモジュール) は、不正アクセスから情報を保護するための暗 号化機能を提供するコンポーネントです。常に有効になっていて、変更できる設定はありません。

AxisデバイスID

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

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

仕様

製品概要





USB 3.0ポート
 製品ステータスLED
 ハードドライブステータスLED
 POE/ネットワークステータスLED
 電源コネクター
 POEポート
 AUX RJ45ポート
 LAN RJ45ポート
 LAN SFPポート
 USB 2.0ポート
 コントロールボタン
 電源ボタン

仕様

フロントLED

LED	カラー	説明
製品のステータス	禄	レコーダーがオンになってお り、ステータスは正常です。
	オレンジ	レコーダーの起動中か、 ファームウェアのアップグ レード中です。LEDインジケー ターが緑色になるまで待機し てください。
	赤	これは、PoEの予算を超えたこ とを意味している場合があり ます。装置をレコーダーに接

		続したばかりの場合は、削除 してみてください。
ハードドライブステータス	緑	ドライブはオンラインです。
	オレンジ	このドライブはオンラインで すが、別のドライブが故障し ています。
		RAIDが冗長性を失っていま す。
	赤	ドライブが故障しています。
	すべてが赤	RAIDに障害が発生しました。 システムは録画していませ ん。
		RAIDに障害が発生した場合、 故障したハードドライブを特 定するには、装置のwebイン ターフェースにアクセスし、 [System (システム)] > [Storage (ストレージ)] > [Hard drive status (ハードド ライブのステータス)] に移動 します。
	オフ	ハードドライブがありませ ん。
PoEのステータス	禄	装置が接続されています。
	オレンジ	PoEは使用中ですが、ネット ワークリンクがありません。
	赤	接続された装置が起動できま せん。
		PoE供給容量を超過していま す。
		PoEに障害が発生しています。
	オフ	ポートは使用されていない か、無効になっています。

リアLED

LED	カラー	説明
ネットワークポート	緑点滅	2.5ギガビット/秒
	黄点滅	1ギガビット/秒
	オフ	ネットワークなし
PoEポート	禄	PoEが使用されています。
左LED	赤	PoEに障害が発生しています。
		PoE供給容量を超過していま す。

	オフ	ポートは使用されていない か、無効になっています。
PoEポート	緑点滅	1ギガビット/秒
 右LED	黄点滅	100 Mbit/秒
	オフ	ネットワークなし

電源ボタン

- レコーダーをシャットダウンするには、電源ボタンを長押しすると、簡単な音が鳴ります。
- ・ ブザーを無音にするには、電源ボタンを少し押します。

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、ステータスLEDが緑色に点滅するまで約3秒間ボタンを押し続けます。

トラブルシューティング

技術的な問題、ヒント、解決策

問題	解決策
録画が利用できませ ん。	に移動します。
カメラに接続できま せん。	に移動します。
"No contact (接続で きません)" というエ ラー通知が表示され ます。	に移動します。
モバイルアプリに自 分のサイトが表示さ れません。	AXIS Companionモバイルアプリのバージョンが4であることを確認して ください。

一般的な問題を解決する

再起動する前に、装置を設定またはリセットします。

- 1. カメラとレコーダーに電力が供給されていることを確認します。
- 2. インターネットに接続されていることを確認します。
- 3. ネットワークが動作していることを確認します。
- リモートでない場合は、カメラがコンピューターと同じネットワークに接続されていることを確認します。
- まだ動作しませんか?
 - カメラ、レコーダー、およびAXIS Companionデスクトップアプリに最新のファームウェア とソフトウェア更新プログラムがインストールされていることを確認してください。
 「」を参照してください。
 - 6. AXIS Companionデスクトップアプリを再起動します。
 - 7. カメラとレコーダーを再起動します。
- まだ動作しませんか?
 - 8. カメラとレコーダーのハードリセットを行って、完全に工場出荷時の設定に戻します。 を参照してください。
 - 9. リセットしたカメラをもう一度サイトに追加します。
- まだ動作しませんか?
 - 10. 最新のドライバーを使用してグラフィックカードをアップデートしてください。
- まだ動作しませんか?
 - 11. システムレポートを保存し、Axisのテクニカルサポートに連絡してください。 を参照してください。

ファームウェアのアップグレード

新しいファームウェアの更新により、最新の改善された一連の機能、機能、およびセキュリティ 強化が提供されます。

- 1. リーダー装置のwebインターフェースに移動します。
- [Maintenance (メンテナンス) > Firmware upgrade (ファームウェアのアップグレード)] に移動し、[Upgrade (アップグレード)] をクリックします。

3. 画面上の指示に従ってください。

製品のwebインターフェースにログインできない

設定中に製品のパスワードを設定し、後でその製品をサイトに追加した場合、設定済みのパス ワードでは製品のwebインターフェースにログインできなくなります。これは、AXIS Companion ソフトウェアによってサイト内のすべてのデバイスのパスワードが変更されるためです。

サイト内の装置にログインするには、ユーザー名rootとサイトのパスワードを入力します。

すべての録画を消去する方法

- 1. 装置のwebインターフェースで、[System (システム)] > [Storage (ストレージ)] に移動し ます。
- 2. [Format (フォーマット)] を選択し、[Use tool (ツールを使用)] をクリックします。

注

この手順では、ハードドライブからすべての録画が消去されますが、レコーダーとサイトの設定は変更されません。

システムレポートを保存する

- 1. AXIS Companionでは、 V > [Save system report (システムレポートを保存)] に移動し ます。
- 3. Axisヘルプデスクに新しいサポート案件を登録する際には、システムレポートを添付してください。

さらに支援が必要ですか?

参考リンク

- AXIS Companion $\neg \forall \neg \neg \neg \neg \neg \nu$
- AXIS Camera Stationユーザーズマニュアル

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。

T10186767_ja

2025-04 (M6.2)

© 2022 – 2025 Axis Communications AB