

AXIS Camera Station 5

AXIS Camera Station Integrator Suiteについて

AXIS Camera Station Integrator Suiteは、監視システムのサービス提供を簡略化するツールボックスで、システム寿命のどの段階でもエラーを避け、時間と費用の両方を削減することができます。ツールボックスは、以下の機能で構成されます。

- **AXIS Site Designer**
簡略化された方法でシステム設計と製品の選択を行うブラウザーベースのツールです。このツールは、Axisのすべてのポートフォリオに即座にアクセスできます。帯域幅とストレージが自動計算され、これに適した録画ソリューションが推奨されます。システム設計ドキュメントが自動的に作成されるため、設計を簡単に共有できます。
- **自動設定**
インストール時間を短縮してインストールのミスを排除するために、AXIS Site Designerで完了した設定を AXIS Camera Station 5にインポートすることができます。
- **AXIS Installation Verifier**
アプリケーションが AXIS Camera Station 5に統合されています。これにより、現場のライブシステム検証を実行して、すべてが正しく機能していることを確認することができます。システムのパフォーマンスが検証されドキュメントが作成されます。このドキュメントは、初回のインストール時やサービス担当者の今後の訪問時に顧客に提供することができます。
- **AXIS System Health Monitoring**
AXIS Camera Station 5のインストールステータスを確認するには、AXIS System Health Monitoringを使用します。このポータルは、すべてのインストールを監視することができます。接続するいずれかのデバイスで問題が発生した場合に自動的に通知を受け取ることができます。

インテグレーターに役に立つリンク

使用を開始するのに役立つリンクをいくつか紹介します。ぜひお読みください。

- システムの設計, on page 5
- AXIS Camera Station 5の新機能
- AXIS Camera Station 5 ユーザーマニュアル
- AXIS Camera Station 5 インストールガイド

ワークフロー

Axisのエンドツーエンドソリューションを設計するワークフローは次のとおりです。

1. システムの設計, *on page 5*
2. システムの設定, *on page 6*
3. システムのテスト, *on page 13*

システムの設計

AXIS Site Designerについて

AXIS Site Designerは、システム設計と製品の選択を行うことができるWebベースのツールです。このツールは、Axisのすべてのポートフォリオにすばやくアクセスできます。帯域幅とストレージが自動計算され、これに適した録画ソリューションが推奨されます。システム設計ドキュメントが自動的に作成されるため、すべての設計を簡単に共有できます。

AXIS Site Designerでのプロジェクトの作成方法



この例では、AXIS Site Designerでソリューションをデザインおよび設定する方法について説明します。その後、AXIS Camera Station 5へこの設定をインポートできます。

注

前提条件:

- 有効なMy Axisアカウント

1. AXIS Site Designerにサインインします。
2. プロジェクトを新規作成します。
3. プロジェクトにカメラを追加します。
カメラの2Dビジュアル化ツールとフィルターで適切なカメラを検索してから、[Add (追加)] をクリックします。
4. カメラを設定します。
例えば、営業時間中は連続録画、営業時間外は動きに応じて録画を開始するような録画スケジュールを作成できます。録画を保持する日数を設定することもできます。
5. プロジェクトにデバイスを追加します。
スピーカーシステム、録画ソリューション、アクセサリ、ネットワークコンポーネントなどをプロジェクトに追加することができます。

次のステップ: AXIS Site Designerプロジェクトのインポート方法, on page 6

システムの設定

AXIS Site Designerプロジェクトのインポート方法

この例では、AXIS Site Designerプロジェクトを AXIS Camera Station 5へインポートする方法について説明します。

注

前提条件:

- 有効なMy Axisアカウント
- AXIS Site Designerプロジェクト

1. AXIS Site Designerにログインします。
2. プロジェクトを開きます。
3. **[Share with (と共有) AXIS Camera Station 5]** に移動し、以下のいずれかのオプションをクリックします。
 - **[Generate access code (アクセスコードの生成)]** - AXIS Camera Station 5サーバーでインターネットアクセスを利用する場合にこのオプションを使用します。
 - **[Download camera settings (カメラの設定をダウンロードする)]** - AXIS Camera Station 5サーバーでインターネットにアクセスできない場合にこのオプションを使用します。
4. AXIS Camera Station 5で、**[Configuration > Devices > Add devices (設定 > 装置 > 装置を追加)]** を選択します。
5. **[Add (追加)]** をクリックし、**[Site Designer configuration (Site Designer設定)]** を選択して、**[Next (次へ)]** をクリックします。
6. 以下のいずれかのオプションを選択してから、**[Import (インポート)]** をクリックします。
 - アクセスコードを生成した場合は、**[Access code (アクセスコード)]** を選択します。
 - ファイルをダウンロードした場合は、**[Choose file (ファイルの選択)]** を選択します。
7. **[インストール]** をクリックします。
このインポートで、AXIS Site Designerの設定に基づいた特定のモデルと、AXIS Camera Station 5のモデルとの設定のマッチングが自動的行われます。1つのカメラのモデルに複数の設定を行っている場合は、どの設定を使用するか手動で選択する必要があります。

次のステップ: システムのテスト, on page 13

AXIS Camera Station 5サーバーに接続する

このセクションでは、コンピューターやモバイルアプリから AXIS Camera Station 5サーバーに接続する方法について説明します。サーバーに接続するには、下記のように複数の方法があります。

注

この情報は、AXIS Camera Station 5.16以上に基づいています。これらの手順は以前のバージョンでも実行できますが、インターフェースの表示が異なる場合があります。

- ローカルネットワークからサーバーに接続する
- インターネットからサーバーに接続する:
 - Axis Secure Remote Access経由
 - ポートマッピング経由 (非推奨)

注

前提条件:

- 有効なMy Axisアカウント

AXIS Camera Station 5.16以降 (以前のバージョンでもほとんどのステップは実行できますが、ユーザーインターフェースが異なる可能性があります。)

システムを準備する

クライアント装置から AXIS Camera Station 5サーバーに接続するには、あらかじめシステムを準備しておく必要があります。全般的な設定の管理については、以下の手順を参考にしてください。

1. AXIS Camera Station 5 Windows®アプリをインストールしてください。
2. Windowsユーザーを作成します。「Windowsユーザーを作成する」を参照してください。
3. AXIS Camera Station 5 WindowsアプリにWindowsユーザーを追加します。
4. サーバーのファイアウォールを設定します。
5. AXIS Camera Station 5モバイルアプリをインストールします。

これらの手順は、お使いのシステムの設定、クライアントの設定、ネットワークインフラストラクチャーによって異なります。

ユーザーおよびユーザーグループについて

注

上級ユーザー向け:

Windowsと AXIS Camera Station 5のユーザーID/パスワードがあることを確認するために、ポートxxとyyを開放してモバイルアプリを設定してください。

クライアント装置から AXIS Camera Station 5サーバーに接続するには、適切な権限を持ったWindowsユーザーが必要です。サーバーがインストールされているWindowsデバイス上のデフォルトの管理者アカウントでも、作成されたユーザーでもかまいません。

AXIS Camera Station 5では、ローカルのWindowsユーザーとユーザーグループだけでなく、ドメインのユーザーとユーザーグループも使用できます。ドメインの設定を使用する場合は、サーバーをドメインに参加させる必要があります。これは通常、IT部門が行う作業となります。

現在のユーザーでログイン:

- サーバー上の権限リストに現在のWindowsユーザーを追加する場合は、[Current user (現在のユーザー)] を選択して [Log in (ログイン)] をクリックします。

他のユーザーでログイン:

1. 現在のWindowsユーザーがサーバー上の権限リストに追加されていない場合は、[Log in as current user (現在のユーザーでログイン)] の選択を解除し、[Log in (ログイン)] をクリックします。
2. 次のページで、[Other user (他のユーザー)] を選択します。
3. 認証情報を入力し、[Log in (ログイン)] をクリックします。

ユーザーまたはユーザーグループに、以下のいずれかの権限を与えることができます。

- **管理者:**
 - すべての機能およびすべてのデバイスにフルアクセスが可能です。
- **オペレーター:**
 - [Configuration (設定)] メニュー、[Configuration (設定)] ワークスペース、[Device management (デバイス管理)] ページ、[Audit log (監査ログ)] を除くすべての機能にフルアクセスが可能です。
 - 選択されたデバイスとI/Oポートへのフルアクセスが可能です。
 - 再生と録画エクスポートに制限付きでアクセスできます。
- **閲覧者:**
 - 選択したカメラからのライブビデオにアクセスできます。

- 選択されたI/Oポートにアクセスできます。

注

オペレーターアカウントと閲覧者アカウントをカスタマイズする詳細なオプションについては、各タブの **[Advanced (詳細設定)]** をクリックしてください。

AXIS Camera Station 5 Windows アプリ (クライアント) をインストールする

1. axis.com/products/axis-camera-station から Windows アプリをダウンロードします。
2. サーバーと同じバージョンの Windows アプリをインストールしてください。

注

AXIS Camera Station 5 バージョン 5 以降:

サーバーとクライアントが同じネットワークを共有し、最新バージョンが異なる場合、サーバーは、使用するバージョンについての情報を最初の接続時にクライアントに提供します。

Windows ユーザーを作成する

ローカルの Windows ユーザーとユーザーグループを使用するには、AXIS Camera Station 5 のインストール先 Windows サーバーにそれらのユーザーとグループを追加する必要があります。すべてのユーザーにそれぞれ独自のアカウントを与えることをお勧めします。

1. **[Computer Management (コンピューターの管理)] > [System tools (システムツール)] > [Local Users and Groups (ローカルユーザーとグループ)] > [Users (ユーザー)]** に移動します。
2. **[Users (ユーザー)]** フォルダーを右クリックし、**[New user (新しいユーザー)]** を選択します。
3. 必要な情報を入力します。
4. **[User must change password at next logon (ユーザーは次回ログオン時にパスワードの変更が必要)]** の選択を解除します。
5. **[Create (作成)]** をクリックします。

に Windows ユーザーを追加する AXIS Camera Station 5

Windows ユーザーをすでに作成している場合は、ユーザーを AXIS Camera Station 5 に追加する必要があります。

1. AXIS Camera Station 5 クライアントを開き、現在のユーザーでサーバーにログインします。
2. **[Configuration (設定)] > [Security (セキュリティ)] > [User permissions (ユーザー権限)]** に移動します。
3. **[add (追加)]** をクリックします。
4. アカウントの追加元となる範囲を選択します。
 - サーバー: ローカルユーザーとローカルグループが取得されます。
 - ドメイン: ドメインユーザーとドメイングループが取得されます。
5. ユーザーを選択し、**[Add (追加)]** をクリックします。
6. ユーザーのロールと権限レベルを選択し、**[OK]** をクリックします。

注

ローカルアカウントを使用する場合は、追加後のテストとして、そのユーザーでログインすることをお勧めします。

サーバーのファイアウォールを設定する

インストール中、受信トラフィックに対する Windows ファイアウォールの例外が AXIS Camera Station 5 によって自動的に設定されます。サードパーティのファイアウォールが表示された場合は、同様の一連の例外を設定に追加するよう要求する必要があります。ほとんどの場合、例外が必要なのは、**受信ポート範囲の 55752 と 55757** だけです。

この表は、一般的な AXIS Camera Station 5 の設定における各種ポートを示したものです。

ポート番号	プロトコル	受信/送信	次のデバイスによって使用中	コメント
80および443	HTTPおよびHTTPS	送信	サーバーおよびクライアントからインターネットまで	ライセンスの有効化、ファームウェアのダウンロード、接続サービスなど。
80	HTTP	送信	サーバーと装置	ビデオストリームおよびデバイスデータ
5353	UDP	マルチキャスト (受信+送信)	サーバーと装置	mDNS Discovery (Bonjour) がカメラを検索 (マルチキャスト 224.0.0.251)
1900	UDP	マルチキャスト (受信+送信)	サーバーと装置	SSDP Discoveryによるデバイスのupnp検索 (マルチキャスト 239.255.255.250)
3702	UDP	マルチキャスト (受信+送信)	サーバーと装置	WS-DiscoveryによるWebサービス探索 (Onvifマルチキャスト 239.255.255.250)
55752	TCP	受信	サーバーとクライアント	ビデオ、音声、メタデータストリーム (AES暗号化)。55754でTCPエラーが発生した場合、アプリケーションデータにはHTTPと55752が使用されます (AES暗号化)。
55754	TCP	受信	サーバーとクライアント	暗号化されたアプリケーションデータ (TLS 1.2暗号化)
55755	TCP	受信	サーバーとクライアント	サーバー探索 SSDP/UPNP
55756	TCP	受信	サーバーとモバイルアプリ	暗号化されたアプリケーションデータ、HTTPSビデオストリーム、MP4 over HTTPS
55757	TCP	受信	サーバーとモバイルアプリ	ビデオストリーム、RTSP over HTTP

*50333	TCP	受信	AXIS Camera Station 5 サーバーとサードパーティ製アプリケーション	ACS APIを使用するサードパーティ製アプリケーション用のアプリケーションデータ
*50334	TCP	受信	AXIS Camera Station 5 サーバーとサードパーティ製アプリケーション	AXIS Camera Station 5 API を使用するサードパーティ製アプリケーションで使用されるビデオポート

Axis Secure Remote Access経由でサーバーに接続する

セキュアリモートアクセスを使用すると、クライアントまたはモバイルアプリは、ポートフォワードなしでサーバーに接続できます。クライアント (またはモバイル) アプリとサーバーとの間で安全なピアツーピア接続が確立されている場合、データ転送の制限はありません。

直接の通信を確立できない場合、通信は仲介サーバーによって中継されます。中継データ転送は、My Axisユーザーごとに1か月あたり1 GBです。

Axisセキュアリモートアクセスの詳細については、axis.com/technologies/axis-secure-remote-accessを参照してください。

Axis Secure Remote Accessを管理するには、以下が必要です。

- AXIS Camera Station 5 5.12以上
- インターネットアクセス (プロキシサーバーを使用している場合は、*高度な設定, on page 11*を参照)
- My Axisアカウント

サーバーを設定する

1. 管理者ユーザーで AXIS Camera Station 5サーバーにログインします。ログイン時には、サーバーと同じネットワークを使用してください。
2. [Configuration (設定)] > [Connected services (接続中のサービス)] > [Axis Secure Remote Access (Axisセキュアリモートアクセス)] を選択します。
3. My Axisアカウントにログインします。

Windowsアプリ (クライアント) から接続する

1. AXIS Camera Station 5アプリを開きます。
2. [AXIS Secure Remote Access (Axisセキュアリモートアクセス)] をクリックします。
3. サーバーの設定時に使用したユーザー認証情報を入力します。
4. [Remote server (リモートサーバー)] を選択し、リストからサーバーを選択します。サーバーは、[ServerName (Secure Remote Access) (サーバー名 (セキュアリモートアクセス))] として表示されます。
5. [Log in (ログイン)] をクリックします。

モバイルアプリ (クライアント) から接続する

1. AXIS Camera Station 5モバイルアプリを開きます。
2. [Sign in (サインイン)] をクリックします。
3. My Axisアカウントのユーザー認証情報を入力します。

4. サーバーを選択します。
5. 設定したWindowsアカウントのユーザー認証情報を使用してログインします。認証情報の入力が必要になるのは、サーバーへの初回アクセス時のみです。ユーザー認証情報は、モバイルアプリによって保存されます。

注

システムの設定によっては、/ または / 形式を使用する必要があります。

ポートマッピングを使用してサーバーに接続する

▲ 警告

サイバーセキュリティ上の理由により、ポートマッピングを使用しないことをお勧めします。アクシスコミュニケーションズでは、代わりにAxisセキュアリモートアクセスを使用することを推奨しています。サイバーセキュリティとAxis Secure Remote Accessの詳細については、axis.comを参照してください。

ポートマッピングを使用すると、離れた場所からルーターでサーバーに接続することができます。お使いのネットワークのインフラストラクチャーによっては、この設定を行うためにネットワーク管理者の協力が必要な場合があります。

サーバーを設定する

- AXIS Camera Station 5サーバーをインターネットに接続しているルーター上で、次のポートを開放します。
 - Windowsクライアント接続を許可する: 55752および55754
 - モバイル接続を許可する: 55756および55757

Windowsアプリ (クライアント) から接続する

1. AXIS Camera Station 5 Windowsアプリを開きます。
2. [リモートサーバー] を選択します。
3. AXIS Camera Station 5サーバーがインストールされているネットワークのパブリックIPまたは完全修飾名を入力します。
4. ポートが転送ルールである場合に、デフォルトポートは使用しないでください。ポート60009に接続したい場合、アドレスに**60009**を追加します。

例:

myserver.axis.com:60009

モバイルアプリから接続する

- AXIS Camera Station 5モバイルアプリを開きます。
- [Add system (システムの追加)] をクリックし、パブリックIPまたはパブリックの完全修飾名を入力します。
- デフォルト値を使用しない場合は、必要に応じてポート番号を調整します。
- 設定したWindowsアカウントのユーザー認証情報を使用してログインします。認証情報の入力が必要になるのは、サーバーへの初回アクセス時のみです。ユーザー認証情報は、モバイルアプリによって保存されます。

高度な設定

サーバーのプロキシ設定

インターネットへの接続にプロキシの設定が求められるネットワーク上にサーバーがある場合、プロキシ情報をサービスに追加する必要があります。

1. AXIS Camera Station 5 Service Controlを開きます。
2. サーバーステータスの [Stop (停止)] をクリックします。

3. **[Modify settings (設定の変更)]** を選択します。
4. プロキシの設定を調整します。
5. **[保存]** をクリックします。
6. サービスを起動します。

クライアントのプロキシ設定

特定のWebサイトにアクセスするためにプロキシを必要とするWindowsアプリを使用する場合、同じプロキシサーバーを使用するように AXIS Camera Station 5クライアントを設定する必要があります。

- AXIS Camera Station 5 Windowsアプリを開きます。
- **[Change client proxy settings (クライアントのプロキシ設定を変更)]** をクリックします。
- 必要に応じて設定を調整し、**[OK]** をクリックします。

複数のサーバーのポートマッピングを実行する

同じネットワーク上で複数のサーバーを実行していてポートマッピングが必要である場合、AXIS Camera Station 5のデフォルトのポート (55752) を変更する必要があります。サーバーにはそれぞれ一意のポートを割り当てる必要があります。

各サーバーについて、以下の手順を実行します。

1. AXIS Camera Station 5 Service Controlを開きます。
2. サーバーステータスの **[Stop (停止)]** をクリックします。
3. **[Modify settings (設定の変更)]** を選択します。
4. HTTPポートを編集します。他のすべてのポートがしかるべき番号に調整されます。
5. 保存してサービスを再起動します。
6. 新しいポート範囲がポートフォワードに使用されます。

システムのテスト

AXIS Installation Verifierについて

AXIS Installation Verifierは、AXIS Camera Station 5バージョン5.02以降に組み込まれているツールです。システムのインストールと設定の終了後、一連のテストを実行して、システムが適切に作動しているか検証します。

AXIS Installation Verifierは、AXIS Camera Station 5サーバーの録画部分を模倣します。このツールは、現在の設定でテストを1回行い、低光量によるエミュレーションテストを1回行います。その後、システムのボトルネックを探し出すストレステストも行います。

AXIS Installation Verifierでは、顧客への提供が可能なPDF形式の検証レポートが生成されます。

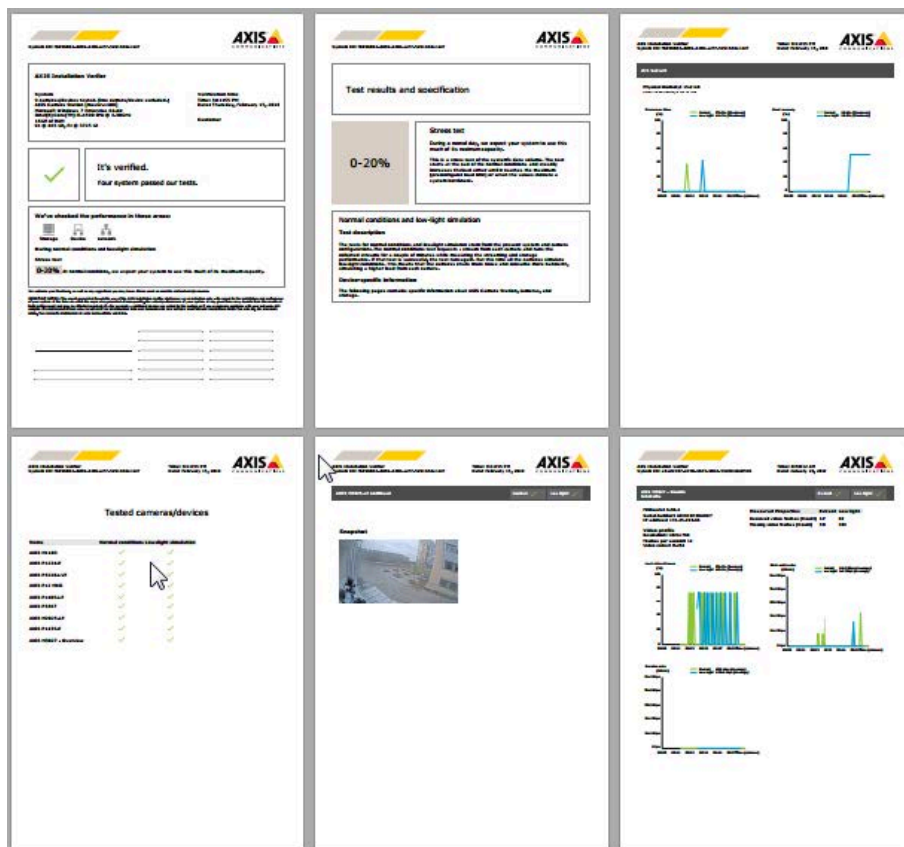
AXIS Installation Verifierの実行方法

1. AXIS Camera Station 5のインストールと設定を完了します。
2. AXIS Camera Station 5クライアントで、メインメニューに移動し、**[Help > Installation Verifier (ヘルプ > Installation Verifier)]** をクリックします。このテストは、完了までに約20分かかります。
テスト中、デバイスはメンテナンスモードに設定されるため、ライブビューや録画で使用するビデオストリームの機能は利用できません。テストのステータスには、次のようにさまざまな種類があります。
 - Running (実行中): テストが進行中です。しばらくお待ちください。
 - パスしました: テスト可能なすべてのデバイスがテストに合格しました。詳細については、レポートを参照してください。
 - パスしませんでした: テスト可能な一部のデバイスでテストに合格しませんでした。詳細については、レポートを参照してください。
 - 失敗しました: テストを完了できなかったため、レポートは生成されません。テストウィンドウのスナップショットを撮影し、AXIS Camera Station 5のシステムレポートを生成して、Axisサポートに問い合わせることをお勧めします。
3. 全テストの終了後、**[View Report (レポートの表示)]** をクリックするとレポートが開きます。**[Save Report (レポートの保存)]** をクリックするとファイルをクライアントPCに保存できます。

レポートの分析方法とレポートの見方

テスト結果: 一般情報

インストールの完了とシステム検証の終了後に、システムインテグレーターからエンドカスタマーにPDFファイル形式でレポートを手渡すことができます。

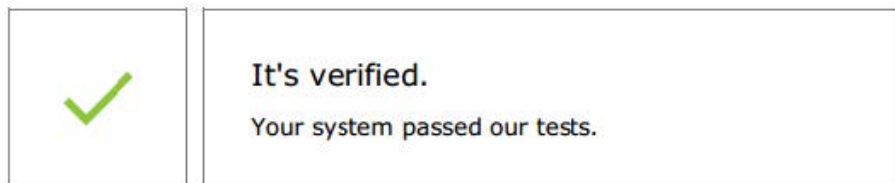


1ページ目の最初のセクションには、ハードウェア、オペレーティングシステムなどのシステムに関する情報とテストが実施された日付および時刻が記載されています。顧客名を記入できるエリアもあります。

AXIS Installation Verifier	
System 31 cameras/devices tested. (12 cameras/devices excluded.) AXIS Camera Station [master-1408] Microsoft Windows 7 Enterprise 64-bit Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz 16GB of RAM C: @ 465 GB, E: @ 3725 GB	Verification time Time: 8:16:51 AM Date: Friday, February 16, 2018 Customer

2番目のセクションには、テストの結果が表示されます。各テスト (通常条件、低光量、ストレステスト) の所要時間は5分間です。ストレージ、デバイス、およびネットワークがこのツールで検証する3つの領域です。検証では、次の2種類の結果が想定されます。

- システムがテストにパスし、検証される。システムは負荷および現在の設定に対応する必要があります。低光量シミュレーション時には負荷がかかることも想定されます。通常、これが最もリソースを必要とするシナリオです。
上記のストレステスト例では、システムの上限が特定され、通常および低光量の条件下では、リソースの4割〜6割が消費される見込みであるという結論が示されています。



We've checked the performance in these areas:

Storage

Device

Network

During normal conditions and low-light simulation

Stress test

40-60%

At normal conditions, we expect your system to use this much of its maximum capacity.

Test results and specification

40-60%

Stress test

During a normal day, we expect your system to use this much of its maximum capacity.

This is a stress test of the system's data volume. The test starts at the load of the normal conditions and steadily increases the load either until it reaches the maximum (preconfigured load limit) or when the values indicate a system bottleneck.

Normal conditions and low-light simulation

Test description

The tests for normal conditions and low-light simulation stem from the present system and camera configurations. The normal conditions test requests a stream from each camera and runs the collected streams for a couple of minutes while measuring the streaming and storage performance. If that test is successful, the test runs again. But this time all the cameras simulate low-light conditions. This means that the cameras create more noise and consume more bandwidth, simulating a higher load from each camera.

Device-specific information

The following pages contains specific information about AXIS Camera Station, cameras, and storage.

!

Issues found.

There's room for improvement.

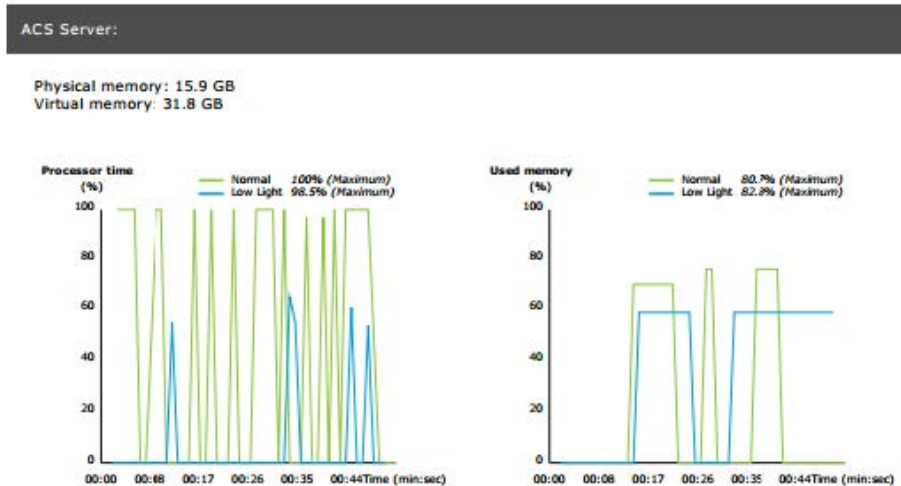
This is what we found:

Test Results		Error Messages
Current Mode Test	NOT PASSED	[RecEng] Could not connect to device
Low Light Simulation Test	PASSED	[RecEng] Device omitted from test due to previous errors
Load Test	PASSED	

- システムの安定性を改善するための問題点と、変更が必要ないいくつかの項目を明らかにしています。各テストの結果と検出された問題点は、エラーメッセージとともに一覧表示されます。さらに詳しい情報は、レポートの次のページで見ることができます。上記の例では、テスト中、デバイスの一つにアクセスできませんでした。おそらく、ネットワーク上の問題、デバイスの過負荷、返答不能が原因と思われます。

1ページ目の最下部に、顧客情報、テストに関するコメント、必要なその他の情報を記入できる場所があります。

テスト結果: AXIS Camera Station 5サーバー



このページの最上部に、物理メモリと仮想メモリが表示されています。

- ランダムアクセスメモリ (RAM) は、アプリケーション、ドキュメント、プロシーチャーをサーバーに保持する物理メモリです。
- 仮想メモリは、サーバーでRAMが不足した場合にハードドライブ上に一時的にファイルを保存し、必要に応じて取り出すためのストレージ領域です。仮想メモリは物理メモリよりはるかに低速であるため、絶対に使用しないでください。

AXIS Camera Station 5 サーバーは、次の2つのメトリックに対してテストされます。

- プロセッサ時間:** プロセッサがアイドル以外のスレッドの実行にかかった時間のパーセンテージを測定します。結果が85%を超える場合は、プロセッサの負荷が大きすぎることを表し、サーバーがより高速のプロセッサを必要とする可能性があるか、設定を調整する必要があります。
- 使用メモリ:** 実行中のすべてのプロセスで使用する物理メモリのパーセンテージを測定します。この値が85%を超える場合は、メモリが不足していることを表し、ページングアクティビティが増加する可能性があります。サーバーにメモリを追加してこの問題を解決するか、サーバーで実行するアプリケーション数を制限してください。

テスト結果: テストを実施したカメラとデバイス

Tested cameras/devices

Name	Normal conditions	Low-light simulation
AXIS M1103	✓	✓
AXIS M2025-LE	✓	✓
AXIS P1435-E	✓	✓
AXIS M3027 - Overview	✓	✓
AXIS M3027 (2) - Quad View	✓	✓
AXIS P1425-E	✓	✓
AXIS P5515	✓	N/A
AXIS M3005 (12)	!	N/A

次のページには、テストを実施したカメラとデバイスが一覧表示されています。複数のカメラを1台のデバイスに含めることができます。例: マルチセンサーデバイスやマルチチャンネルエンコーダは、3台、4台、さらには16台のカメラを装備していても (センサー/チャンネルごとにカメラ1台)、1台のデバイスとしてカウントされます。

- 緑色のチェックマークは、カメラが関連テストにパスしたことを示します。
- [N/A] は、カメラに対してテストを実施できなかったことを意味します。たとえば、低光量シミュレーション用の ExposureValue パラメーターをカメラがサポートしていない場合です。

- カメラがテストに合格しなかった場合は、赤色の記号が表示されます。カメラごとに異なるテスト結果の詳細情報は、以降の数ページに記載されます。

テスト結果: 注意事項と検討事項

テストに不合格にはならないが、設置を改善できる微調整がこのページに示されます。たとえば、デフォルトルーターがデバイスと同じサブネットにないときや、DNSまたはNTPサーバーがないときなどです。

テスト結果: 除外されたカメラとデバイス

Excluded cameras/devices

Name	Notes
AXIS 212 PTZ	Video codec not supported
AXIS T8508	Device has no enabled cameras
AXIS C8033	Device has no enabled cameras
AXIS A1001	Device has no enabled cameras
AXIS M1014	Device status is not OK
AXIS 216MFD	Video codec not supported
IPC-HD1200C	Device is not Vapix

デバイスがいずれかのテストに対応していない場合は、テストから除外されます。次のデバイスはテストされません。

- [Device is not Vapix® (デバイスがVapix®でない)]: サードパーティ製のデバイスはテストされません。
- [Device has no enabled cameras (デバイスに有効なカメラがない)]: ネットワークスイッチ、音声デバイス、ドアコントローラー、I/Oモジュールなど、ビデオセンサーのないデバイスです。
- [Video codec not supported (ビデオコーデック非対応)]: H.264に対応していないデバイスです (通常はファームウェア 4.x)。
- [Device status is not OK (デバイスのステータスがOKでない)]: デバイスがメンテナンスモードになっている、アクセス不能、または認証情報が正しくありません。

テスト結果: カメラ固有の結果

ファームウェア、シリアル番号、IPアドレス、映像プロファイルなど、録画に使用されるカメラのすべての情報が一覧表示されます。各テストでは、受信したか欠落した映像フレームについての概要も表示されます。

注

- デバイスが2種類の映像プロファイル (例: Medium for ContinuousおよびHigh for Motion Detection) で録画する設定の場合は、設定されているスケジュールに関わらず、最上位のプロファイルのみテストされます。
- ContinuousおよびMotionの両方の録画が無効の場合、現在アクティブでない場合でも、手動録画に選択されたプロファイルがテストに使用されます。

[デバイスの設定] セクションに、テストしたデバイスの最も重要な情報が示されます。一部のパラメーターが不適切な (設定されていないか、サブネットが異なる) 場合は、そのパラメーターの前に感嘆符が表示されます。

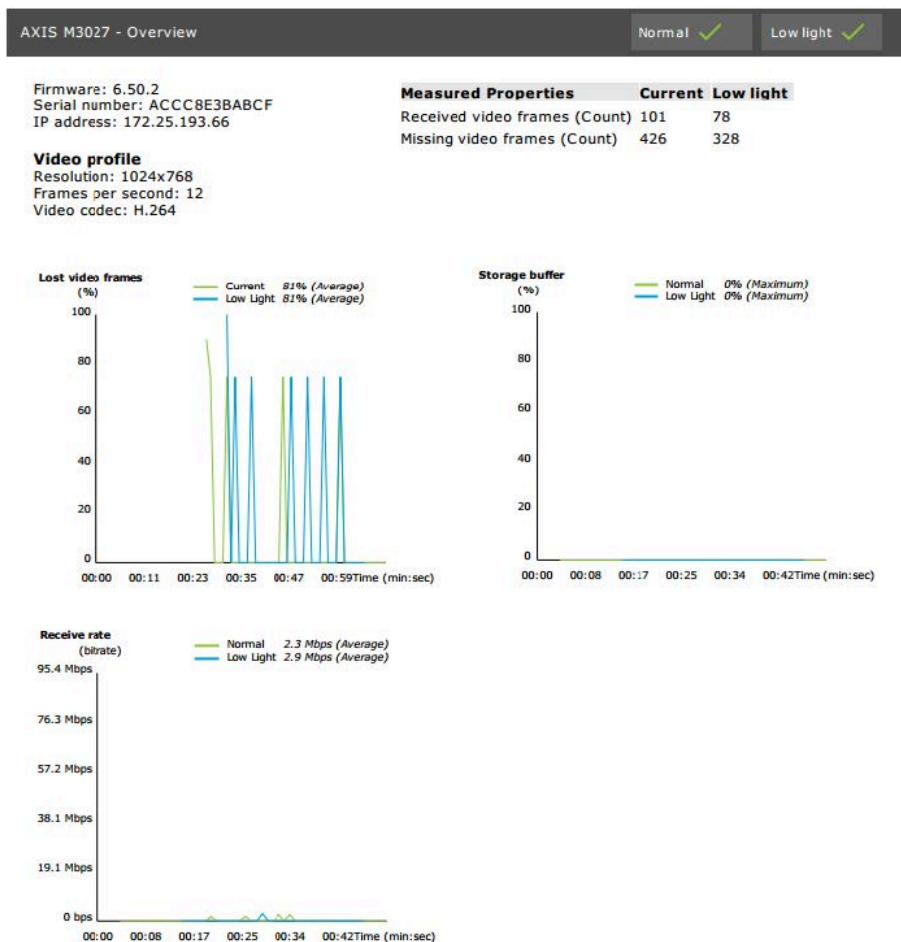
Device Configuration

Firmware: 8.40.1
 Serial number: ACCC8E02A96D
 IP address: 172.25.193.116
 Is Using Dhcp: Yes
 Subnet Mask: 255.255.255.0
 Default Router: ⚠192.168.0.1
 Primary DNS: ⚠0.0.0.0
 NTP Server: 10.0.2.201

グラフに示しているのは、通常および低光量の条件でのテスト中に測定された、3種類の指標です。

- **[Lost video frames (映像フレームの欠落)]**:1秒間隔で欠落した映像フレームのクォータ。平均値が高い場合、ネットワークのボトルネックまたはデバイスの過負荷を示しています。通常、映像フレームの平均欠落率は1パーセント未満です。
- **[Storage buffer (ストレージバッファ)]**:1秒間隔でのストレージバッファの使用量。ピーク値が高いと、ストレージに問題があることを示します。通常、ストレージバッファの使用率は20パーセント未満です。
- **[Received rate (受信速度)]**:カメラが送信してAXIS Camera Stationサーバーが受信するデータ速度 (オーバーヘッドを除く)。

以下のグラフでは、欠落した映像フレームのクォータは高くなっています。



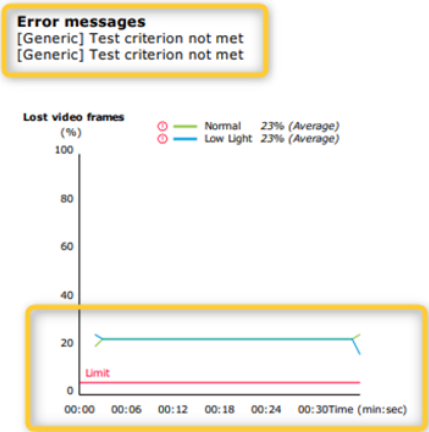
ほとんどの場合、次のような理由が考えられます。

- 使用するビューエリアが多すぎる (360度カメラなど) か、取り込んでいるストリームが多すぎるのが原因で、カメラが過負荷になっている。
- ネットワーク上のボトルネック、カメラと AXIS Camera Station 5サーバー間。
- ネットワークケーブルが故障しているか低品質である。
- PoEを含め、電力供給が不足しているか不安定である。

通常および低光量のテストの実行時は、追加のフレーム欠落基準が検討されます。

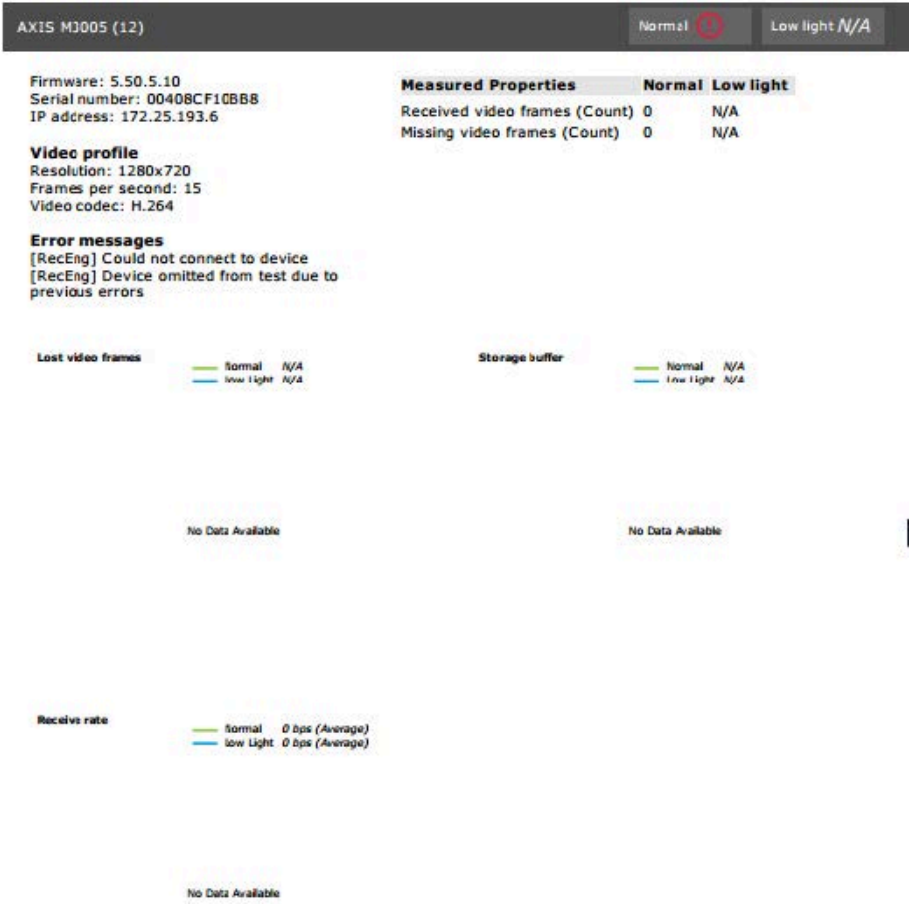
- 基準を満たさない (5%を超えるフレーム欠落) すべてのデバイスで検討事項が追加されます。これでテストは不合格にはなりません。
- テストで上記の基準を満たさないデバイスが5%を超える場合、テストステータスは「パスしませんでした」になります。

以下に、通常および低光量のテストのテスト基準が満たされなかった例を示します。



以下のグラフは、テストが完了できなかった例を示しています。ほとんどの場合、次のような理由が考えられます。

- テスト中にカメラが切断されたか、ネットワーク接続が中断された。
- テスト中にカメラに対して必要な電力供給ができなかった。
- カメラが過負荷となり、処理時間がかかり過ぎてサーバーのリクエストに応答できなかった。



カメラのテスト結果が出ると、カメラからのスナップショットが次のように表示されます。



Snapshot



テスト結果: ストレージデバイス

Tested storage devices

Path	Normal conditions	Low-light simulation
E:\Recording	✓	✓
\\172.25.192.20\nas\Recording	✓	✓

複数のストレージデバイスを同じ条件でテストします。

このツールは、次の2つの指標でローカルハードドライブをテストします。

- **[Disk write rate (ディスクの書き込み速度)]**: 1秒間隔でこのストレージに書き込まれる合計のデータ速度表示です。
- **[Used write buffers (count) (使用された書き込みバッファ (カウント))]**: 1秒間隔でのストレージバッファの使用量 (300サンプル)。ピーク値が高いと、ストレージに問題があることを示します。一般に、この値は1または2より小さくなります。

注

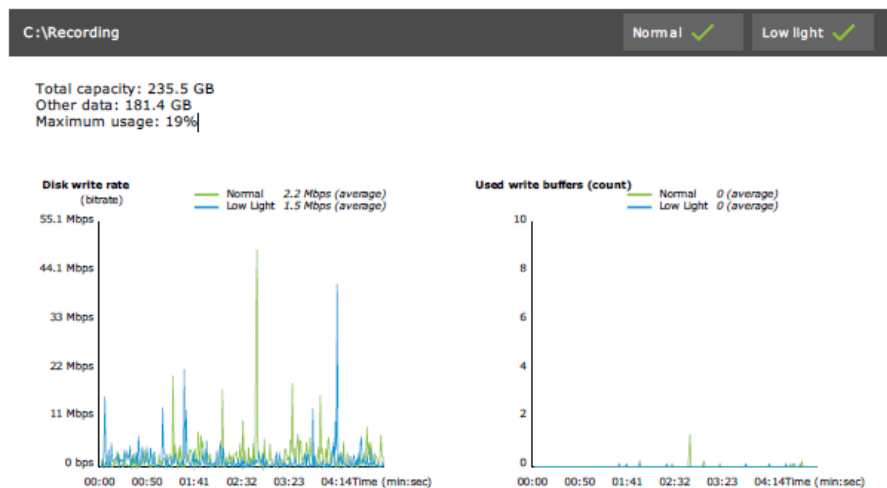
現在は、NAS (Network Attached Storage) はテストしません。

ストレージ使用量/容量については次の情報が利用できます。

[Total capacity (全容量)]: ストレージの合計サイズ。

[Other data (その他のデータ)]: AXIS Camera Station 5サーバーによってインデックス付けされていないデータ。これに当てはまる可能性があるのは、ランダムなドキュメント、オペレーティングシステムファイル、ゴミ箱内のファイルなどの外部ファイルです。

[Maximum usage (最大使用量)]: AXIS Camera Station 5で設定された録画容量の上限により、AXIS Camera Station 5は、ストレージ容量の最大限の割合を録画ファイルに割り当てます。この値は、OS以外のドライブで99%、OSドライブでは合計60GBがデフォルトで設定されます。

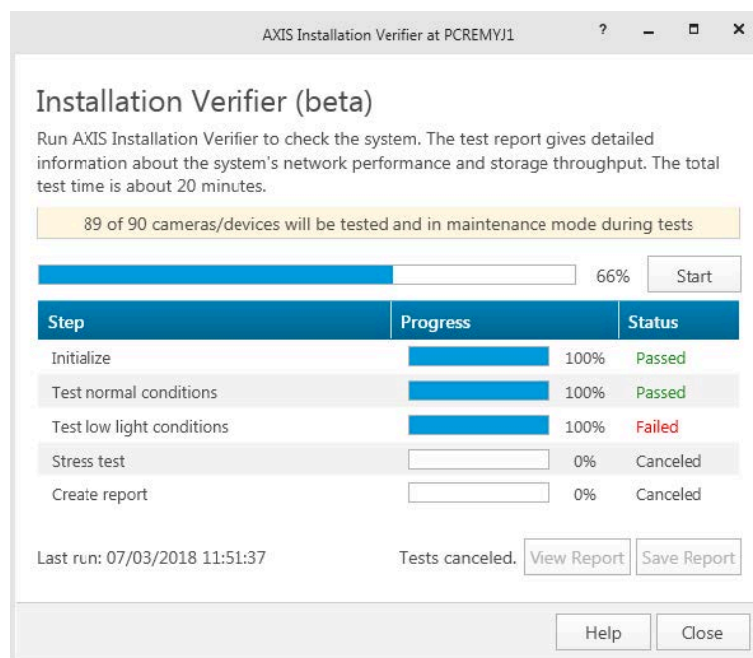


トラブルシューティング

いずれかのテストで失敗した場合は ([Failed (失敗)]、レポートは生成されません。テストウィンドウのスナップショットを撮影し、ヘルプメニューから AXIS Camera Station 5のシステムレポートを生成して、オンラインのヘルプデスクからのAxisサポートに問い合わせることをお勧めします。

注

- [Not passed (パスしませんでした)] と [Failed (失敗)] は同じではありません。
- [Not passed (パスしませんでした)] は、サーバー、一部のデバイス、またはストレージがテストの合格に必要な条件を満たしていないことを示します。
- [Failed (失敗)] は、テストが完了しなかったために、システムのパフォーマンスに関する結論を出せなかったことを意味します。



注意事項と制約事項

- ・ H.264のみサポートされます。H.264対応でないカメラは無視されます。
- ・ 低光量テストは、ExposureValueパラメーター対応のカメラにのみ実施されます。ExposureValue対応でないカメラにはN/Aと表示されます。

- WDR対応のカメラでは、低光量と通常の条件で、テストの結果が同じになる場合があります。
- サードパーティ製のカメラは無視されます。
- NAS (Network Attached Storage) はテストしませんが、検証済と表示されます。

システムの監視

AXIS System Health Monitoring ^{BETA}について

AXIS Camera Station 5のインストールの現在のステータスは、AXIS System Health Monitoringにログインして確認できます。AXIS System Health Monitoringを使用すると、すべてのインストールを監視でき、接続されているいずれかのデバイスに問題が発生した場合に自動的に通知を受け取ることができます。

AXIS System Health Monitoring ^{BETA}の設定方法

この例では、AXIS System Health Monitoringを設定する方法について説明します。

1. AXIS Camera Station 5axis.comから、利用可能な最新バージョンのをダウンロードしてインストールします。
2. AXIS System Health Monitoringを設定します。
 - 2.1. [Configuration > System Health Monitoring > Settings (設定 > システムの健全性監視 > 設定)] で、システムの健全性監視がWindows Defenderを通過できるようにファイアウォールルールを設定する必要があるかどうかを選択します。
 - 2.2. [Configuration (設定)] > [System Health Monitoring(システムの健全性監視)] > [Notification (通知)] で、SMTPサーバー、電子メールの送信先、さらに、電子メールの送信に関する通知ルールを設定します。
3. マルチシステムの設定に合わせてAXIS System Health Monitoringを設定します。
 - 3.1. [Configuration (設定)] > [System Health Monitoring] > [Multisystem (マルチシステム)] に移動します。
 - 3.2. [Generate system configuration (システム設定の生成)] で、[Generate (生成)] をクリックします。
 - 3.3. 設定をコピーし、データを収集するシステムに転送します。
 - 3.4. [Retrieve data from other systems (他のシステムからデータを取得する)] を展開し、先ほどコピーした設定を貼り付けて、[Add (追加)] をクリックします。システムごとに上記の手順を繰り返します。

機能

機能	説明
在庫	装置の概要が表示されたインベントリ。
装置情報	タイプ、モデル、ファームウェアバージョン、IPアドレス、MACアドレス、APIモード、録画タイプなど。
ビデオ管理システム (VMS) 情報	ソフトウェアバージョン、オペレーティングシステム、ハードウェア、CPUメモリ/ネットワーク使用状況など。
システムレポートのダウンロード	システムページから、AXIS Camera Station 5システムレポートまたはAXIS System Health Monitoringレポートを生成できます。
通知ログ	生成されたすべての通知ログの履歴を表示します。
ストレージ情報	カメラのストレージ使用量と保持時間、およびその他の録画関連情報を表示します。

トラブルシューティング

問題のタイプ	エラーメッセージ	解決策
駆動時間	システムがマルチシステム設定に表示されない。	<p>AXIS System Health Monitoringがシステムからデータを収集していません。新しいシステムを追加した後、AXIS System Health Monitoringがシステムからデータを収集できるようにしてください。[Manage servers (サーバーの管理)] ページにエラーアイコンが表示された場合は、次のことを確認してください。</p> <ul style="list-style-type: none"> • AXIS System Health Monitoringがシステムで実行されている。 • システムの健全性監視がシステムから表示できる。 • 指定した設定 (ホスト、ポート、トークン、証明書) が正しい。 • ネットワーク上でサーバーに到達できる。 • ファイアウォールの例外が有効になっている。 <p>エラーアイコンのツールチップも問題を解決するためのヒントになる場合があります。</p>

サポートログ

AXIS System Health Monitoringのデバッグログは、AXIS Camera Station 5サーバーの次の場所に保存されます。C:\ProgramData\Axis Communications\AXIS System Health Monitoring\logs

FAQ

Q: AXIS System Health Monitoringを使用するには、どのバージョンの AXIS Camera Station 5が必要ですか？

A: AXIS System Health Monitoringの公式サポートバージョンは5.41です。

Q: デバイスやVMSのステータスはどのくらいの頻度で更新されますか？

A: AXIS System Health MonitoringインターフェースでデバイスまたはVMSのステータスが更新されるまでに最大で60秒かかる場合があります。

注意事項と制約事項

- ストレージ:AXIS S3008に接続されたカメラの使用容量には対応していません。
- 非アクティブになったストレージ装置が表示され、収集されたデータは最大2週間保持されます。
- 通知設定はローカルのAXIS System Health Monitoringサーバーにのみ影響します。
- AXIS Camera Station 5でAXIS System Health Monitoringにアクセスするには、管理者権限が必要です。

- 保持警告は、動体検知の録画には対応していません。
- 「連続」または「動体検知」以外の方法 (手動/イベントなど) で作成された録画には、録画タイプとして[None (なし)] のフラグが付けられます。

システムにAxis製品を設定する

AXIS OS Recorderの設定

AXIS OS Recorderには、AXIS S30 SeriesとAXIS S40 Seriesが含まれます。

注

AXIS OS Recorderのファームウェアバージョン10.4以降と、Axisデバイスのファームウェアバージョン5.50以降が必要です。AXIS OS Recorderにはライセンスは不要です。

制限事項

AXIS OS Recorderをデバイスの録画ストレージとして AXIS Camera Station 5で使用する際は、次の制限事項に注意してください。

- AXIS OS Recorderは、装着式カメラの録画や、AXIS Camera Station 5でデモ用に使用されている事前録画済みビデオには対応していません。
- 録画ストリームは、カメラからAXIS OS Recorderへ直接伝送されます。カメラとAXIS OS Recorderが同じネットワークに接続され、すべてのデバイスが互いに通信可能なことを確認します。
- D1、CIF、4CIFなどの非数値ビデオ解像度のサードパーティ製カメラおよびデバイスはサポートされていません。
- AXIS OS Recorderを録画ストレージとして使用するカメラでは、フェイルオーバー録画はサポートされていません。
- AXIS OS Recorderからの内部イベントは、デバイスのイベントトリガーの設定ページに表示されません。
- ブックマークによる録画のロック機能はサポートされていません。
- カメラに接続された外部音声デバイスからの音声は録画されません。
- AXIS OS Recorderでは、シーン記述メタデータのストレージはサポートされていません。代わりに、AXIS Camera Station Proサーバーがメタデータを保存します。したがって、スマート検索2が正常に動作するためには、サーバーとカメラの接続が途切れないことが必須です。
- 自動動画編集およびスマート検索1に使用される分析データはサポートされていません。
- AXIS OS Recorderおよび接続されたデバイスでは、AXIS Installation Verifierはサポートされていません。
- 2N IP Intercomデバイスはサポートされていません。
- AXIS OS Recorder上でAXIS CompanionまたはAXIS Camera Station Edgeから作成した録画は、AXIS Camera Station 5で再生できません。
- AXIS S3008 RecorderおよびAXIS S3008 Mk II Recorderは、最大64の仮想入力に対応しています。
 - AXIS S3008 Mk II Recorderに録画する各カメラは、動体録画用、連続録画用、手動録画用に3つの仮想入力を使用します。
たとえば、8台のカメラでは64の仮想入力のうち24 (8×3) を使用し、残りの40の仮想入力はアクションルール用になります。
 - AXIS S3008 Mk II Recorderに録画する各ネットワークドアステーションは、動体録画用、連続録画用、手動録画用、デフォルトのアクションルール用に4つの仮想入力を使用します。
たとえば、7台のカメラと1台のドアステーションでは、64の仮想入力のうち25 (7×3 + 1×4) を使用し、残りの39の仮想入力は追加のアクションルール用になります。
 - AXIS OS Recorderで録画をトリガーする各アクションルールは、1つの仮想入力を使用します。
 - フォールバック録画では仮想入力は使用されません。

- AXIS S3016 Rack RecorderおよびAXIS S4000 Rack Recorderは、最大128の仮想入力に対応しています。

ワークフロー

1. レコーダーを追加する, on page 27
2. 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, on page 27
3. 録画を設定, on page 28

レコーダーを追加する

注

AXIS Camera Station 5 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] - [デバイスの追加]** 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。
4. ストレージ暗号化用に新しいパスワードを作成するか、現在のパスワードを使用します。詳細については、以下を参照してください。**[Next (次へ)]** をクリックします。
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。

重要

ストレージ暗号化用のパスワード

- ストレージ暗号化のパスワードは、レコーダーハードドライブに AXIS Camera Station 5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。
- 装置がフォーマットされていない場合は、ディスク暗号化用に新しいパスワードを選択する必要があります。これにより、ディスクがフォーマットされ、以前の録画が削除されます。
- 装置がすでにフォーマットされている場合は、現在のパスワードを使用するか、新しいパスワードを作成するかを選択できます。
 - 現在のパスワードを使用すると、システムはすべての録画を削除しますが、装置はフォーマットされません。このオプションにより時間を節約できます。
 - 新しいパスワードを作成する場合は、装置がフォーマットされ、すべての録画が削除されます。
- 複数の装置を選択し、新しいパスワードを作成する場合は、すべての装置がフォーマットされ、新しいパスワードが割り当てられます。
- 複数の装置を選択し、現在のパスワードを使用する場合は、パスワードが一致する装置のみが追加されます。

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] - [デバイスの追加]** を選択します。
2. 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 5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。

保存先の変更

装置の保存先を1つのレコーダーから別のレコーダーに変更して、すべての録画を保持できます。

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. 新しい保存先を選択します。
3. [適用] をクリックします。

注

選択したレコーダーが、録画アクションで最大数のアクションルールをすでに使用している場合は、次のいずれかを実行します。

- レコーダーをストレージとして使用している既存の装置から、アクションを録画するアクションルールを削除します。
- 録画アクションを含むアクションルールを使用して装置を別のストレージに移動します。

Axisネットワークドアコントローラーを設定する

このセクションでは、AXIS Camera Station 5でAXISネットワークドアコントローラーを設定する方法について説明します。設定方法に関するビデオを見るには、こちらのプレイリストにアクセスしてください。

注

- AXIS Camera Station 5.35以降が必要です。
 - AXIS Camera Station 5.37以降のコントローラーでは、HTTPSを有効にする必要があります。
1. AXIS Camera Station 5にAxisネットワークドアコントローラーを追加します。装置の追加を参照してください。
 2. ドアコントローラーのファームウェアをアップグレードする。ファームウェアのアップグレードを参照してください。
 3. 時刻同期をオンにして、AXIS Camera Station 5サーバーをNTPサーバーとして使用します。サーバーの設定を参照してください。
 4. コントローラーの日付と時刻を設定する。「日付と時刻の設定」を参照してください。
 5. コントローラーでHTTPSを有効にする。「セキュリティ」を参照してください。

6. アクセスコントロールを設定する。
 - 6.1. 既定の識別プロファイルを編集したり、新しい識別プロファイルを作成したりするには、「識別プロファイル」を参照してください。
 - 6.2. カスタム設定したカードフォーマットとPIN長を使用するには、「カードフォーマットとPIN」を参照してください。
 - 6.3. ドアを追加し、識別プロファイルをドアに適用します。「ドアの追加」を参照してください。
 - 6.4. ドアを設定します。
 - 「ドアモニターの追加」
 - 緊急入力追加
 - 「リーダーの追加」
 - REX装置の追加
 - 6.1. ゾーンを追加し、ゾーンにドアを追加します。「ゾーンの追加」を参照してください。
7. アクセスコントロールを管理する。
 - 7.1. スケジュールを追加する。「スケジュール」を参照してください。
 - 7.2. ワークフローを選択して、以下の要素を追加します。「アクセス管理」を参照してください。
 - カード所持者の追加
 - 認証情報の追加
 - 「グループの追加」
 - 「アクセスルールの追加」
 - 7.1. カード所持者、グループ、ドア、ゾーンをアクセスルールに適用します。
 - 7.2. レポートをエクスポートする。「レポートのエクスポート」を参照してください。
8. ドアダッシュボードでドアを手動で監視、管理する。「分割ビューのドアダッシュボード」を参照してください。
9. アクセスコントロールデータを検索する。
 - 9.1. ビューをドアに接続する。外部データソースを参照してください。
 - 9.2. 一定期間内のイベントデータや特定のキーワードを含むイベントデータを検索する。「データ検索」を参照してください。

注

AXIS Camera Station 5でドアコントローラーを取り外した場合、ドアコントローラーのデータは削除されません。そのデータを削除するには、デフォルトへのリセットを実行して工場出荷時の設定に戻してください。

2NデスクトップUSBカードリーダーの設定



このビデオを見るには、このドキュメントのWebバージョンにアクセスしてください。


1. <https://www.elatec-rfid.com/int/>にアクセスし、TWN4 DevPackをダウンロードして、任意のフォルダーに抽出します。
2. 抽出されたフォルダーに移動し、AppBlaster.exeを実行します。

- 2.1. リーダーをプログラムする**Multi keyboard V4.80**キーボードファームウェアを選択します。
- 2.2. プロジェクトを作成して、リーダーの形式を定義します。以下の項目を定義する必要があります。
 - 周波数、タイプ、およびサブタイプを含むトランスポンダータイプ。
例: MIFARE Classic (UID、任意の長さ)
 - トランスポンダータイプのビット操作。
例: 逆バイト順
 - トランスポンダータイプの出力形式。
例: 10進数
 - 出力データの既定のサフィックスを削除します。
- 2.1. プロジェクトファイルをリーダーに読み込みます。
3. AXIS Camera Station 5でカード認証情報を追加している場合は、アクセスコントロールカードをリーダーにかざして、カードの詳細を取得します。

Axis装着式システムの設定



Axis装着式ソリューションの詳細については、*Axis装着式ユーザーマニュアル*を参照してください。

1. 既存の AXIS Camera Station 5で、クライアントとの通信に使用されるサーバー証明書を更新します。
 - 1.1. AXIS Camera Station 5で、**[Configuration > Security > Certificates > Certificate renewal (設定 > セキュリティ > 証明書 > 証明書を更新)]**に移動します。
 - 1.2. **[Renew (更新)]** をクリックします。
 - 1.3. AXIS Camera Station 5サービスを再開します。
2. 接続ファイルを作成します。
 - 2.1. AXIS Camera Station 5で、 > **[Other (その他)]** > **[Connection file... (接続ファイル...)]** に移動します。
 - 2.2. 装着式システムに表示されているデフォルトのサイト名を変更するには、新しい名前を入力します。
 - 2.3. **[エクスポート]** をクリックします。
3. 装着式システムを設定します。「*Access AXIS Body Worn Manager for the first time (初めて AXIS Body Worn Managerにアクセスする)*」を参照してください。コンテンツの保存先を設定するように求められたら、AXIS Camera Station 5からエクスポートした接続ファイルを選択します。
4. AXIS Camera Station 5の **[Recordings (録画)]** タブで、仮想カメラがユーザー名と共に追加されていることを確認してください。
5. 保存期間を変更するには、**[Configuration (設定)]** > **[Storage (ストレージ)]** > **[Selection (選択)]** に移動します。
6. 装着式カメラで録画し、カメラの背面をドッキングステーションに合わせます。録画は、AXIS Camera Station 5に自動的にアップロードされます。

7. AXIS Camera Station 5で、装着式カメラからの録画の再生とエクスポートを行います。



重要

ユーザーの削除には、必ずAXIS Body Worn Managerを使用します。絶対に、AXIS Camera Station 5から装着式カメラのユーザーを削除しないでください。

Axisネットワークドアステーションを設定する

この例では、次の方法について説明します。

- AXIS Camera Station 5にAxisネットワークドアステーションを追加する
- クライアントで音声アラートを設定する
- 着信呼び出しの操作
- ドアステーション着信呼び出し通知を無効にする

制限事項:

- ドアステーションから AXIS Camera Station 5への通話は保留にできません。
- ドアステーションで動体検知を有効にできません。
- 呼び出し側からの録画のみを録画できます。オペレーターからの音声は録音できません。

AXIS Camera Station 5にAxisネットワークドアステーションを追加する

1. AXIS Camera Station 5で、[Configuration > Devices > Add devices (設定 > 装置 > 装置の追加)] に移動します。
2. ネットワークドアステーションを選択して [Add (追加)] をクリックします。
3. デフォルト設定を使用し、[Next (次へ)] と [Install (インストール)] をクリックします。
4. [Configuration > Devices > Cameras (設定>装置>カメラ)] に移動し、ドアステーションが追加 されていないか確認します。
5. [Configuration > Recording and events > Action rules (アクションルールの設定>録画とイベント>アクションルール)] に移動し、以下のアクションルールが自動的に追加されていないか確認します。
 - ドアルールを開く: [Open Door (ドアを開く)] アクションボタンが追加されます。ライブビューでボタンをクリックすると、デフォルトで7秒間、ドアステーションのI/Oポートが開きます。
 - 進行中の呼び出しがあるときに録画: 進行中の呼び出しがあると、ドアステーションでの録画を開始します。

着信音の設定

1. AXIS Camera Station 5で、[Configuration > Client > Settings (設定 > クライアント > 設定)] に移動します。
2. [Sound on incoming call (着信音)] で [Sound file (サウンドファイル)] を選択します。
3. [Browse (参照)] をクリックし、.wavまたは.mp3形式のサウンドファイルに移動します。
4. [Play (再生)] をクリックしてサウンドをテストすることができます。

着信呼び出しの操作

1. 呼び出しがアクティブになると、通知ウィンドウが表示されます。

2. サムネイルにマウスを置くと、呼び出し側の大きな画像が表示されます。
3. 呼び出しに回答するには、[Accept (同意)] をクリックします。ドアステーションからの表示を含む新規のタブが表示されます。[Open door (ドアを開く)] をクリックすると、デフォルトでドアステーションのI/Oポートが7秒間開きます。
4. このクライアントでの呼び出しのみを無視するには、[Ignore (無視)] をクリックします。この呼び出しには別のクライアントで応答できます。
5. 呼び出しを終了するには、[Decline (拒否)] をクリックします。呼び出しが終了し、すべてのクライアントで呼び出し通知が削除されます。

注

複数の呼び出しが発生した場合は、一度に1件の応答を行することをお勧めします。その他の呼び出しは、応答またはアウトになるまで表示されます。

ドアステーション通知を無効にする

1. クライアント用の別のユーザーを作成します。
 - 1.1. [Configuration > Security > User permissions (設定 > セキュリティ > ユーザー権限)] に移動します。
 - 1.2. [追加] をクリックします。
 - 1.3. リストからユーザーを選択し、[Add (追加)] をクリックします。
2. ユーザーを設定する。
 - 2.1. [Role (役割)] で [Operator (オペレーター)] を選択します。
 - 2.2. ドアステーションの [Access (アクセス)] を選択しますが、[Audio Listen (音声の聞き取り)] と [Audio Speak (音声、話す)] はクリアします。
 - 2.3. [保存] をクリックします。

AXIS Camera Station 5での音声の設定

この例では、次の方法について説明します。


- Axisネットワークの音声デバイスを AXIS Camera Station 5に追加し、Axisネットワークカメラと連動させる。
- AXIS Camera Station 5のカメラのライブビューにボタンを作成し、このボタンによって音声装置で音声クリップを再生できるようにする。

注意

このシステム設定は、侵入者アラームやスタッフ・顧客のアドレスなど、人命に関わるシステム以外に適しています。火災時の避難など人命に関わる重要システムに実装する場合は、特定のガイドラインや基準 (インストールの地域によって異なる) を満たす必要があります。

制限事項:

- AXIS Camera Station 5からAxisネットワーク音声装置に送信された音声は録画されません。
 - AXIS Camera Station 5で音声装置をカメラと関連付ける必要があります。
 - 関連付けることができるのは、カメラごとに音声デバイス1台のみです。
 - AXIS Camera Station 5.の音声装置には音量コントロール機能がありません。
1. 以下の手順に従って、AXIS Camera Station 5にAxisネットワーク音声装置を追加します。

- 1.1. AXIS Camera Station 5で  をクリックし、[Configuration (設定)] を選択します。
- 1.2. [デバイス] - [デバイスを追加] に移動します。
- 1.3. リストからネットワーク音声デバイスを選択して、[追加] をクリックします。
- 1.4. [他のデバイス] に移動し、音声デバイスがリストに追加されたことを確認します。

2. 音声デバイスをカメラと関連付ける:

- 2.1. AXIS Camera Station 5で、[Devices > Streaming profiles (装置 > ストリーミングプロファイル)] に移動し、音声装置に関連付けるカメラを選択します。
- 2.2. デバイスのストリーミングプロファイルで、[スピーカー] ドロップダウンから音声デバイスを選択します。
- 2.3. [適用] をクリックします。
- 2.4. 関連付けをテストするには、でカメラの [Live view (ライブビュー) AXIS Camera Station 5] に移動し、[Speak (話す)] ボタンをクリックします。コンピューターのマイクに向かって話すと、音声デバイスがその音声を再生します。
3. オーディオクリップのリンクを準備する:
 - 3.1. [Audio (音声)] > [Audio clips (音声クリップ)] に移動します。
 - 3.2. オーディオクリップのリンクアイコンをクリックします。
 - 3.3. クリップの音量と繰り返し回数を設定します。
 - 3.4. コピーアイコンをクリックして、リンクをコピーします。
4. オーディオクリップをトリガーするボタンを作成する:
 - 4.1. AXIS Camera Station 5で、[Configuration > Recording and events > Action rules (設定 > 録画とイベント > アクションルール)] を選択し、[New (新規)] をクリックします。
 - 4.2. [追加] をクリックしてトリガーを追加します。
 - 4.3. トリガーのリストから [アクションボタン] を選択し、[OK] をクリックします。
 - 4.4. ボタンが作成されている場合は、[Create new button (ボタンの新規作成)] を選択し、[Next (次へ)] をクリックします。
 - 4.5. [コマンドボタン] を選択し、[次へ] をクリックします。
 - 4.6. ボタンの詳細を次のように入力します。
 - ボタンのラベル: レジにスタッフを招集
 - ツールチップ: レジに来るようにスタッフを呼ぶ
 - カメラに追加: 音声装置に関連付けられたカメラを選択します。
 - マップに追加します。
 - 「OK」 をクリックします。

注

ボタンは複数のマップやカメラに関連付けることができます。

- 4.1. [Next (次へ)] をクリックします。
- 4.2. [追加] をクリックしてアクションを追加します。
- 4.3. アクションのリストから [HTTP通知を送信] を選択し、[OK] をクリックします。
- 4.4. 音声デバイスで設定したリンクを [URL] フィールドにペーストします。
- 4.5. [認証が必要] を選択し、音声デバイスの [ユーザー名] および [パスワード] を入力します。
- 4.6. [OK] をクリックします。
- 4.7. [次へ] を2回クリックします。
- 4.8. ルールの [名前] を入力し、[完了] をクリックします。

AXIS Camera Station 5のカメラのライブビューに、[Staff to till (レジにスタッフを招集)] というボタンが表示されるようになりました。このボタンをクリックすると、音声デバイスがオーディオクリップを再生します。

Axis分析機能の設定



分析機能 (AXIS Loitering Guard) による AXIS Camera Station 5の拡張

[AXIS Barcode Reader (AXISコードリーダー)]の設定してください。

このセクションでは、AxisのインターカムとカメラでAXIS Readerを設定する方法と、それをカメラで設定する方法AXIS Camera Station Secure Entry。AXIS Readerの詳細については、ユーザーズマニュアルを参照してください。

注

- これには、AXIS Camera Station 5 5.44以降、またはファームウェア10.11.9以降を搭載したAXIS A1601 Network Door Controllerが必要です。
- ライセンスが必要です。

制限事項

QRコードを送信できるのは、QR認証情報でカード所持者を保存した後のみです。


ワークフロー

1. AXISコードリーダーの取り付け, on page 34
2. AXIS Barcode Readerの設定, on page 34
3. ドアコントローラーとの接続を作成します, on page 35
4. QR認証情報の設定, on page 35
5. QR Code®の送信, on page 35

AXISコードリーダーの取り付け

1. axis.comからアプリケーションインストールをダウンロードします。
2. [webpage of your Axis intercom or camera (Axisインタカムまたはカメラのウェブページ)]に移動します。
3. アプリケーションをインストールします。
4. ライセンスをアクティブ化します。
5. アプリケーションを起動します。
6. QR精度を向上するには、以下のカメラ設定を変更することをお勧めします。
 - 6.1. カメラ設定に移動するには:
 - 6.2. [Image (画像) >Exposure (露出)]で、[Blur-noise trade-off (ブレとノイズのトレードオフ)]スライダーを中央に移動します。

AXIS Barcode Readerの設定

1. QR識別プロフィールを変更する場合、[Configuration (設定)] > [Access control (アクセス管理)] > [Identification profiles (識別プロファイル)] に移動して  をクリックします。識別プロファイルを参照してください。



2. ドアを追加する手順については、「[ドアの追加](#)」を参照してください。
3. このドアの識別プロファイルとして [QR]を選択します。ドア設定を参照してください。
4. 「バーコードのリーダーの追加。リーダーの追加を参照してください。
 - 4.1. ドアのどちらかの面で [Add reader (リーダーの追加)] をクリックします。
 - 4.2. [AXIS Barcode Reader (AXIS Barcode リーダー)]のドロップダウンリストから リーダータイプ を選択します。名前を入力し、[OK] をクリックします。

ドアコントローラーとの接続を作成します

ドアコントローラーとの接続を作成します

1. AXIS Camera Station 5で:
 - 1.1. [Configuration > Access control > Encrypted communication (設定 > アクセスコントロール > 暗号化通信)] に移動します。
 - 1.2. [External Peripheral Authentication Key (外部周辺機器認証)] キーで [Show authentication key (認証キーの表示)]、[Copy key (キーのコピー)] の順にクリックします。
2. AXISバーコードリーダーが実行されている装置のwebインターフェースで:
 - 2.1. AXIS Barcode Readerアプリケーションを開きます。
 - 2.2. サーバー証明書が AXIS Camera Station 5で設定されていない場合は、[Ignore server certificate validation (サーバー証明書の検証を無視する)] をオンにします。より詳細な情報については、[CA証明書](#) を参照してください。
 - 2.3. **AXIS Camera Station Secure Entry**に反対します。
 - 2.4. [追加] をクリックし、ドアコントローラーのIPアドレスを入力し、認証キーを貼り付けます。
 - 2.5. ドアのドロップダウンメニューからバーコードを読み取るリーダーを選択します。


QR認証情報の設定

1. カード所持者の追加。
2. QR認証情報の追加。
 - [Credentials (認証情報)]で  と  をクリックします。
 - 名前)を入力します。
 - 動的QRはデフォルトで有効になっています。動的QRはPIN認証情報と一緒に使用する必要があります。
 - 有効期限を設定し、[Add (追加)] をクリックします。
3. AXIS Barcode Readerを設定したドアにカード所持者のアクセスルールを追加します。

QR Code®の送信

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ーブ株式会社の登録商標です。

1. カード所持者が正しいメールアドレスで設定されていることを確認します。[カード所持者の追加](#)を参照してください。
2. メールを送信するには、SMTPサーバーを設定してください。サーバーの設定を参照してください。
3. 必要に合った場合は、メールテンプレートを編集します。アクセス管理設定を参照してください。
 - 3.1. [Access Management (アクセス管理)] > [Settings (設定)] を選択します。

- 3.2. [Email template 電子(メールテンプレート)]で、件名と本文のテキストを変更します。
- 3.3. デフォルトでは、電子メールに訪問時間を含めることが選択できます。
- 3.4. [適用] をクリックします。
4. QR Codeの送信。カード所持者の追加を参照してください。
 - 4.1. [Access Management (アクセス管理)] > [Dashboard (ダッシュボード)] > [Cardholders (カード所持者)] に移動します。
 - 4.2. カード所持者を選択して  と[Send QR code (QRコードを送信)]をクリックします。
 - 4.3. [OK] をクリックします。

AXIS Mobile Credentialの設定

動的QRコードを使用するには、AXIS Mobile Credentialを設定する必要があります。

受信した電子メールの手順に従います。

1. AXIS Mobile Credentialアプリをダウンロードします。
2. 電子メールのアクティブ化リンクをクリックします。
3. モバイル装置でアプリケーションを開くと、[My credentials (認証情報)] に認証情報が表示されます。
4. 表示された認証情報をクリックしてPINを入力し、動的QRコードを有効化します。


AXIS Perimeter Defender PTZ Autotrackingを設定する

AXIS Perimeter Defender PTZ Autotrackingを使用してAxis PTZカメラを設定すると、AXIS Camera Station 5のカメラを使用して、視野内の人や車両など、動く物体を自動的に検知して追跡することができます。屋内外を問わず、駐車場などの交通量の少ないエリアや、業務時間後の学校、オフィス、店舗での使用に適しています。

注

- AXIS Camera Station 5.38以降が必要です。
- 1度に追跡できるのは1つの物体のみです。

制限事項:


- 分割ビューでは、トリガーエリアと物体インジケーターが正しい位置に表示されない場合があります。
 - カメラの設定ページを更新するか、アプリケーション設定ページを再度開きます。
 - AXIS Camera Station 5でカメラのメンテナンスの後
 - カメラの向きが回転した場合
 - オートトラッキングプロファイルで使用しているプリセットポジションが削除されると、トリガーエリアは機能しなくなります。また、警告は AXIS Camera Station 5でトリガーされません。
1. カメラの設定ページに移動し、トリガーエリアを設定します。
 - 1.1. [Settings (設定)] > [Apps (アプリ)] に移動します。
 - 1.2. [AXIS PTZ Autotracking] をクリックして、アプリケーションを起動します。
 - 1.3. [Open (開く)] をクリックして、アプリケーションの設定ページを開きます。
 - 1.4. [Settings > Profiles (設定 > プロファイル)] を選択します。
 - 1.5.  をクリックしてプロファイル作成します。

- 1.6. トリガーエリアを移動し、アンカーポイントをドラッグしてサイズと形状を変更します。トリガーエリアごとに最大10個のプライマリアンカーポイントを設定できます。
- 1.7. 必要に応じて、さらにプロファイルとトリガーエリアを作成します。最大10個のプロファイルを作成できます。
- 1.8. アプリケーション設定ページを閉じます。
2. AXIS Camera Station 5で:
 - 2.1. **[設定] - [デバイス] - [デバイスの追加]** を選択します。
 - 2.2. PTZカメラを選択し、**[Add (追加)]** をクリックします。
 - 2.3. **[Next (次へ)]** をクリックし、**[Install (インストール)]** をクリックします。
3. カメラのライブビューに移動すると、以下が表示されます。
 - 黄色のエリア:カメラの設定ページで設定したトリガーエリア。黄色のトリガーエリアに入った物体は自動的に追跡されます。
 - 緑のエリア:カメラが検知した物体インジケーター。物体インジケーターは、**[Show PTZ autotracking object indicators (PTZオートトラッキング物体インジケーターを表示する)]** が選択されている場合にのみ使用できます。
 - 緑色のエリアをクリックすると、検知された物体の追跡が開始されます。
 - 物体をクリックして追跡を停止します。
4. オートトラッキングの開始時にアクションをトリガーするアクションルールを作成します。
 - 4.1. **[Configuration (設定)] > [Recording and events (録画とイベント)] > [Action rules (アクションルール)]** に移動して **[New (新規)]** をクリックします。
 - 4.2. オートトラッキングイベントのトリガーを追加します。
 - 4.2.1. **[追加]** をクリックし、**[デバイスイベント]** を選択します。**[OK]** をクリックします。
 - 4.2.2. **[Configure device event trigger (装置イベントトリガーを設定)]** で、以下のことを行います。
 - **[Device (装置)]** ドロップダウンリストからお使いのPTZカメラを選択します。
 - **[Event (イベント)]** ドロップダウンリストから **[PtzAutotracking > Autotracking is tracking (オートトラッキング > オートトラッキングが追跡中)]** を選択します。
 - **Trigger period (トリガー時間)**を設定し、**stateInfo**をyesに設定します。
 - 4.2.1. **[OK]** をクリックします。
 - 4.2. **[Next (次へ)]** をクリックします。
 - 4.3. 録画アクションを追加します。
 - 4.3.1. **[追加]** をクリックし、**[録画]** を選択します。**[OK]** をクリックします。
 - 4.3.2. **[Camera (カメラ)]** ドロップダウンリストからお使いのPTZカメラを選択します。
 - 4.3.3. **[Video setting (ビデオ設定)]** を設定します。
 - 4.3.4. **[OK]** をクリックします。
 - 4.5. **[Next (次へ)]** をクリックしてスケジュールを選択します。
 - 4.6. **Finish (終了)** をクリックします。

AXIS License Plate Verifierの設定

装置がAXIS License Plate Verifierで設定されている場合、その装置はビデオ管理システムの外部データソースと見なされます。表示をデータソースに接続し、装置でキャプチャーされたナンバープレートを検索して関連する画像を表示できます。

注

- AXIS Camera Station 5.38以降が必要です。
 - AXIS License Plate Verifierにはライセンスが必要です。
1. アプリケーションをダウンロードして装置にインストールします。
 2. アプリケーションの設定を行います。『AXIS License Plate Verifierユーザーマニュアル』を参照してください。
 3. 既存のAXIS Camera Stationインストールの場合は、クライアントとの通信に使用されるサーバー証明書を更新します。証明書の更新を参照してください。
 4. 時刻同期をオンにして、AXIS Camera StationサーバーをNTPサーバーとして使用します。サーバーの設定を参照してください。
 5. デバイスをAXIS Camera Stationに追加する。装置の追加を参照してください。
 6. 最初のイベントを受信すると、データソースは [Configuration > Devices > External data sources (設定 > デバイス > 外部データソース)] の下に自動的に追加されます。
 7. データソースをビューに接続します。外部データソースを参照してください。
 8. 装置によってキャプチャーされたナンバープレートを検索します。「データ検索」を参照してください。
 9.  をクリックして、検索結果を.txtファイルにエクスポートします。


AXIS Speed Monitorの設定

AXIS Speed Monitorアプリは、レーダーに接続された装置、またはレーダーに直接設置された装置にインストールできます。

装置またはレーダーがAXIS Speed Monitorで設定されている場合、その装置は AXIS Camera Station 5で外部データソースとみなされます。ビューをデータソースに接続し、装置でキャプチャーされた物体の速度を検索して関連する画像を表示できます。

注

- AXIS Camera Station 5.47以降が必要です。
1. アプリケーションをダウンロードして装置にインストールします。
 2. アプリケーションとレーダーを設定します。AXIS Speed Monitorユーザーマニュアルを参照してください。
 3. 既存のAXIS Camera Station 5インストールの場合、クライアントとの通信に使用されるサーバー証明書を更新します。証明書の更新を参照してください。
 4. 時刻同期をオンにして、AXIS Camera Station 5サーバーをNTPサーバーとして使用します。サーバーの設定を参照してください。
 5. 関連する装置をAXIS Camera Station 5に追加します。装置の追加を参照してください。
 - レーダーに接続された装置にアプリがインストールされている場合は、装置とレーダーを追加します。
 - アプリがレーダーにインストールされている場合は、レーダーを追加します。
 6. 最初のイベントを受信すると、データソースは [Configuration > Devices > External data sources (設定 > デバイス > 外部データソース)] の下に自動的に追加されます。
 7. データソースをビューに接続します。外部データソースを参照してください。

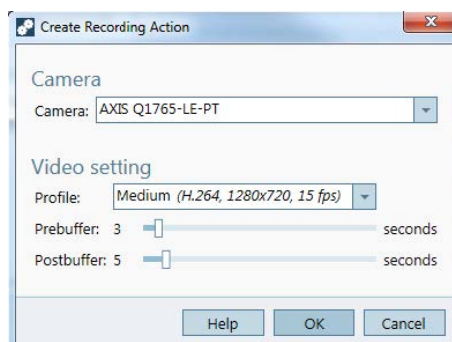
8. 装置によってキャプチャーされた物体の速度を検索します。「データ検索」を参照してください。
9.  をクリックして、検索結果を.txtファイルにエクスポートします。

AXIS Perimeter Defenderを設定する

AXIS Perimeter Defenderを設定する

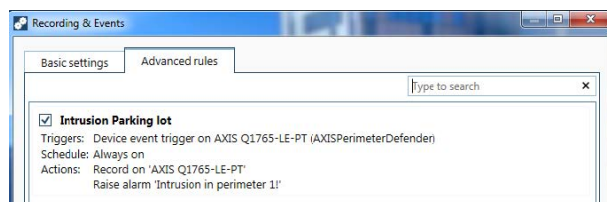
このセクションでは、AXIS Camera Station 5のイベントシステムを使用してAXIS Perimeter Defenderと統合する方法について説明します。以下に関する方法を習得します。

- 侵入発生時にトリガーする AXIS Camera Station 5ルールを設定します。
 - 設定が正しく行われたかどうか確認します。
1. AXIS Perimeter Defender SetupソフトウェアでAXIS Perimeter Defenderの設定およびキャリブレーションを行います。AXIS Perimeter Defenderのインストールとキャリブレーションの詳細については、AXIS Perimeter Defenderユーザーズマニュアル、または製品ページを参照してください。
 2. [AXIS Camera Station 5Add Camera (カメラを追加する)] ウィザードに従って、カメラを追加します。
 3. 次のようにデバイスイベントトリガーを設定します。
 - 3.1. [設定] - [録画とイベント] を選択し、[高度なルール] タブを開きます。
 - 3.2. 新しいルールを作成し、[デバイスイベント] トリガーを選択します。
 - 3.3. AXIS Perimeter Defenderがインストールされたカメラを選択します。
 - 3.4. [イベント] リストで [AXISPerimeterDefender] を選択します。
 - 3.5. [機能] リストで設定した侵入の名前を選択します (この場合は "Intrusion-1")。設定したすべてのシナリオでルールをトリガーする場合は、[ALL_SCENARIOS] を選択します。
 - 3.6. 侵入を検知した時点でトリガーをアクティブ化する場合、[はい] を選択します。侵入が検知されると、設定が正しいか確認できるステータスの変更が [アクティビティ] ウィンドウに表示されます。
 - 3.7. [OK] と [次へ] をクリックしてアクションを設定します。
 - 3.8. [アクションを追加] ダイアログで、ルールで使用するアクションを 1 つ以上追加できます。



この例では、録画のアクションとアラームのアクションを追加します。

- 3.9. Finish (終了) をクリックします。



例では、侵入発生時に2つのアクションをトリガーするルールを示します。

4. 監視対象エリアに実際に入ることによって侵入をシミュレーションして、想定したとおりに設定が機能するかをテストします。

さらに支援が必要ですか？

参考リンク

- インストールパラメーター - *AXIS Camera Station 5 Microsoft*インストーラー
- インストールスイッチ - *AXIS Camera Station 5* 実行可能ファイル
- *AXIS Camera Station 5* リリースノート
- *AXIS Camera Station 5* ユーザーマニュアル
- *AXIS Camera Station 5* チュートリアルビデオ

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。

T10128176_ja

2026-01 (M29.2)

© 2018 – 2026 Axis Communications AB