AXIS Optimizer

AXIS Optimizer for XProtect®
AXIS Optimizer for Siemens Siveillance™

ユーザーマニュアル

目次

AXIS Optimizer 7
AXIS Optimizerの意図する使用 7
システム要件 7
統合システムに対応 7
相互接続されたシステムのサポート 7
リリースノート 7
AXIS Optimizerのインストール、または更新 8
AXIS Optimizerのインストール 8
システムにインストールされているバージョンは何ですか? 8
高度なインストールオプション 8
VMSの移行 9
インストーラーの完全性 9
AXIS Optimizerを更新する 9
手動更新 10
システムを自動的にアップグレードする 10
自動アップグレードをオンにする 11
自動アップグレードをオフにする 11
詳細情報 11
AXIS Optimizerをアンインストールする 12
Factory default (工場出荷時設定): 12
安全な運用停止 12
ユーザー権限 12
デバイス設定にアクセス 14
装置アシスタント 14
Axisデバイスを設定する 14
Axis装置でのアプリケーションのインストール 14
Axis装置でのアプリケーションの設定 14
Axisデバイスのアプリケーションを更新する 14
Axisデバイスを再起動する 15
AxisデバイスのIPアドレスをコピーする 15
自動化を実行 16
Axis装置のアクションを作成 16
イベントサーバープラグイン 16
イベントサーバープラグインのインストール 16
ワンクリックで複数のカメラを乾燥 16
ワンクリックで複数のカメラのオートフォーカスをオンにする 17
ワンクリックで複数のストロボサイレンをトリガーする 18
複数のカメラのプライバシーマスクを自動的にオフにする 19
カメラが動きを検知したときにストロボサイレンが作動するようにする 22
カメラが動きを検知したときに、スピーカーまたはスピーカーゾーンで音声クリップを再生する 23
ルールのトラブルシューティング 25
ナンバープレートリストを一元管理 25
リストを作成する 25
リスト権限を設定する 26
リストの編集 26
リストのインポート 26
リストのエクスポート 27
リストの詳細について 28
ライブイベントに応答 29
装置コントロールの使用 29
オペレーターコントロール 29
オペレーターコントロールにアクセスする 29

PTZカメラのフォーカスエリアの保存 29
カメラのオートフォーカス 30
スピードドライ、またはワイパーをオンにする 30
スポット温度の測定 31
自動的にズームインし、動く物体を追跡します 31
カスタムオペレーターコントロールを作成する 32
オペレーターコントロールへのアクセスを設定する 32
スピーカーを介したやり取り 33
スピーカーマネージャー 33
モード 33
AXIS Audio Manager Proモード 33
AXIS Audio Manager Edgeモード 35
レガシーモード 36
スピーカーでの音声の再生 37
カメラビューでスピーカーから音声を再生する 38
アラームでスピーカーから音声を再生する 38
スピーカーインタラクションのビジュアル挙動を設定する 38
カメラビューまたはアラームの音声クリップブックマーク 39
訪問者の管理 39
インターカムプラグイン 39
インターカムの設定 39
インターカムの権限を設定する 40
テスト呼び出しを実行する 41
呼び出し中のエコー防止 41
ライブビューからインターカムを制御する 42
ライブビューからの呼び出しに応答する 44
呼び出しウィンドウに複数のカメラを表示する 46
呼び出しウィンドウのアクション 46
呼び出しウィンドウにページを表示する 46
呼び出し内線によるフィルタリング 47
呼び出し履歴の表示 48
アクティブな呼び出しがない場合にマイクをオフにする 49
ドアが強制的に開けられた場合にアラームを受け取る 49
ドアが長時間開いたままの場合にアラームを受信する 49
クライアントが呼び出しを受信できないようにする 49
音声の視覚化 50
マイクビュー 50
VMSをマイクビュー向けに設定する 50
Smart Clientにマイクビューを追加する 50
マイクビューの使用 51
複数のマイクを同時に聞く 51
音声によるインシデントの検知 51
発生後にインシデントを調査する 52
フォレンジック検索 53
フォレンジック検索 53
開始する前に 53
フォレンジック検索の設定 53
検索の実行 54
検索を微調整する 55
制限事項 56
車両検索 56
車両検索を設定する 58
車両の検索 58
検索を微調整する 58
検索速度の最適化 59
ゾーン速度検索 59

ゾーン速度検索の設定 59
ゾーン速度イベントの検索 60
検索を微調整する 60
コンテナ検索 61
コンテナ検索の設定 61
コンテナの検索 61
検索を微調整する 62
高品質なPDFレポートの作成 62
Axisナンバープレート 63
開始する前に 63
Axisナンバープレートの設定 63
ナンバープレートを検索する 63
ナンバープレートのライブ検索 64
検索を微調整する 64
検索速度の最適化 64
ナンバープレート検索をPDFレポートとしてエクスポートする 64
ナンバープレート検索をCSVレポートとしてエクスポートする 65
Axis insights 65
Axis insightsへのアクセス 65
新しいダッシュボードを作成する 66
ダッシュボードのドロップダウンリストを設定する 66
特定のカメラビューのインサイトを表示する 66
Axis insightsの設定 66
Axis insightsのトラブルシューティング 67
ビデオの歪み補正 68
歪み補正ビューを作成する 68
マルチセンサーパノラマカメラ用の歪み補正ビューを作成する 69
ワイドビュー 70
ホームポジションを設定する 70
オペレーターによる歪み補正ビューの制御と編集を可能にする 71
パフォーマンスとトラブルシューティング 71
Body worn integration 73
詳細情報 73
アクセスコントロール 74
アクセスコントロールの設定 74
システムにAxisネットワークドアコントローラーを追加する 74
ドアのライセンスを有効にする 75
アクセスコントロールを設定する。 75
アクセスコントロール統合 76
ドアとゾーン 76
ドアとゾーンの例 77
ドアを追加する手順については、 78
ドア設定 79
ドアセキュリティレベル 80
時間のオプション 81
「ドアモニターの追加」 82
監視ドアを追加する 82
「リーダーの追加」 83
REX装置の追加 84
ゾーンの追加 85
ゾーンセキュリティレベル 86
監視入力 86
手動アクション 87
カードフォーマットとPIN 88
カードフォーマットの設定 90
識別プロファイル 91

暗号化通信 ... 92
OSDPセキュアチャンネル ... 92
マルチサーバーBETA ... 93
ワークフロー ... 93
サブサーバーから設定ファイルを生成する ... 93
設定ファイルをメインサーバーにインポートする ... 93
サブサーバーを無効にする ... 93
サブサーバーを削除する ... 94
アクセス管理 ... 94
アクセス管理のワークフロー ... 94
カード所持者の追加 ... 95
認証情報の追加 ... 96
「グループの追加」 ... 98
アクセスルールを追加します。 ... 98
手動でドアとゾーンのロックを解除する ... 99
システム設定レポートをエクスポートする ... 99
カード所持者活動レポートの作成 ... 100
アクセス管理の設定 ... 100
インポートとエクスポート ... 101
バックアップとリストア ... 102
Smart Clientのアクセス管理 ... 102
AXIS Secure Entryのロール設定 ... 103
システム管理とセキュリティコントロール ... 104
オペレーター向けに機能へのアクセスをカスタマイズする ... 104
役割設定 ... 104
役割設定の定義 ... 104
デバイスの管理 ... 105
AXIS Device Manager Extend ... 105
エッジホストをインストールする ... 105
エッジホストの申し立てと装置の同期 ... 106
AXIS Device Manager Extendを使って装置を設定する ... 107
エッジホストに装置を追加する際のトラブルシューティング ... 107
AXIS Site Designerのインポート ... 107
設計プロジェクトをインポートする ... 108
インポートされた設定 ... 108
制限事項 ... 109
アカウントの管理 ... 109
XProtectサービスアカウントで装置に接続する ... 109
Axisイベント ... 110
複数の装置でイベントを設定する ... 110
イベント情報 ... 110
メタデータと検索 ... 110
メタデータ設定を行う ... 110
Axis検索カテゴリの設定 ... 111
サイバーセキュリティ ... 113
脆弱性の管理 ... 113
セキュリティ通知 ... 113
安全な製品ライフサイクル管理 ... 113
強化ガイド ... 113
さらに支援が必要ですか? ... 114
FAQ ... 114
トラブルシューティング ... 114
サポートに問い合わせる ... 114
ヒント ... 115
Smart ClientビューでのWebページの追加 ... 115
検索機能が内蔵されたビデオのエクスポート ... 115

ビデオをXProtect形式でエクスポートする 115
受信側コンピューターでエクスポートのブロックを解除する 115
エクスポートされたAxis歪み補正表示の再生 115

AXIS Optimizer

AXIS Optimizerにより、XProtectまたはSiemens Siveillance VideoでAxisの機能を直接利用できるようになります。このアプリケーションは、これらのビデオ管理システムにおけるAxis装置のパフォーマンスを最適化し、システム構成時や日々の運用時の時間と労力の両方を節約することができます。このアプリケーションは無料でご利用いただけますです。

AXIS Optimizerの意図する使用

この製品は、ビデオ管理ソフトウェア (VMS) の動作について豊富な知識を持つ専門家の方を対象としています。

システム要件

AXIS Optimizerは、以下のプラットフォームに完全に対応しています:

- XProtect Essential+
- XProtect Express+
- XProtect Professional+
- XProtect Expert
- XProtect Corporate
- Siemens Siveillance Video Pro
- Siemens Siveillance Video Advanced
- Siemens Siveillance Video Core Plus
- Siemens Siveillance Video Core

Management ClientとSmart Clientの最新バージョンを使用することをお勧めします。AXIS Optimizerの最新バージョンは、常にテストが実施されているため、VMSの最新バージョンと互換性があります。詳細については、*リリースノート, on page 7*を参照してください。

注

対応プラットフォームの最低要件

- VMSバージョン2019 R3。

ヘルプ内でSmart Clientと記載している箇所については、Siemensのシステムでは、XProtect Smart Clientとビデオクライアントの両方を指します。

統合システムに対応

AXIS Optimizerは、統合システムで完全にサポートされています。

相互接続されたシステムのサポート

AXIS Optimizerは、相互接続されたシステムで完全にサポートされています。

注

要件

- VMSバージョン2022 R3以降。

リリースノート

最新のリリースノートは、*axis.com/ftp/pub_soft/cam_srv/optimizer_milestone/latest/relnote.txt*を参照してください。

AXIS Optimizerのインストール、または更新

AXIS Optimizerのインストール



注

AXIS Optimizerを更新するには、管理者権限が必要です。

1. VMSのクライアントバージョンが正しいことを確認してください。
2. お使いのMyAxisアカウントにログインします。
3. *axis.com/products/axis-optimizer-for-milestone-xprotect*から、Management ClientまたはSmart Clientを実行する各デバイスにAXIS Optimizerをダウンロードします。
4. ダウンロードしたファイルを実行し、ステップバイステップガイドの指示に従います。

システムにインストールされているバージョンは何ですか?

[System overview (システム概要)] では、システム内の異なるサーバーおよびクライアントにインストールされている、AXIS OptimizerとAXIS Optimizer Body Worn Extensionのバージョンを確認できます。

注

[System overview (システムの概要)] にシステムのクライアントまたはサーバーを表示するには、AXIS Optimizerバージョン3.7.17.0、AXIS Optimizer Body Worn Extensionバージョン1.1.11.0以降が必要です。

アクティブなサーバーとクライアントを表示する方法:

1. Management Clientで、[Site Navigation > AXIS Optimizer > System overview (サイトナビゲーション > AXIS Optimizer > システムの概要)] に移動します。

特定のサーバーまたはクライアントをアップグレードする方法:

1. 特定のサーバーまたはクライアントに移動し、ローカルでアップグレードします。

高度なインストールオプション

ユーザーの介入なしでAXIS Optimizerを複数の装置に同時にインストールするには:

1. [Start (スタート)] メニューを右クリックします。
2. [実行] をクリックします。
3. ダウンロードしたインストールファイルを参照し、[Open (開く)] をクリックします。
4. パスの末尾に1つ以上のパラメーターを追加します。

パラメーター	説明
`/SILENT`	サイレントインストール中は、ステップバイステップガイドと背景ウィンドウは表示されません。代わりに、インストールの進行状況ウィンドウが表示されます。

/VERYSILENT	完全なサイレントインストールでは、ステップバイステップガイド、背景ウィンドウ、インストールの進行状況ウィンドウのいずれも表示されません。
/FULL	すべてのコンポーネント (オプションのイベントサーバープラグインやSecure Entryプラグインなど) をインストールします。このオプションは/VERYSILENTと組み合わせて使用すると便利です。
/SUPPRESSMSGBOXES	すべてのメッセージボックスを非表示にします。このオプションは通常、/VERYSILENTと組み合わせて使用します。
/log=<filename>	ログファイルを作成します。
/NORESTART	インストール中にコンピューターが再起動しないようにします。
/EVENTSERVERPLUGIN	対象マシンがイベントサーバーの場合は、イベントサーバープラグインをインストールします。
/SECUREENTRY	対象マシンがイベントサーバーの場合は、Secure Entryアクセスコントロールサービスをインストールします。

5. Enterキーを押します。

例:
コンピューターを再起動せず、ログをoutput.txtに出力する、完全なサイレントインストール

```
.\AxisOptimizerXProtectSetup.exe /VERYSILENT /log=output.txt /NORESTART
```

VMSの移行

AXIS Optimizerはデータの大部分をVMSデータベースに保存するため、VMSを別のサーバーに移行しても情報は保持されます。

VMSを別のサーバーに移行するには、*XProtect VMSのインストール//バージョンを古いサーバーから新規サーバーへ移行する方法*を参照してください。

インストーラーの完全性

AXIS Optimizerインストーラーの完全性を確認するには:

1. インストーラーファイルを右クリックし、**[Properties (プロパティ)]** を選択します。
2. **[Digital Signatures (デジタル署名)]** に移動し、**[Details (詳細)]** をクリックします。
3. 以下を確認します。
   - **[Digital Signature Information (デジタル署名情報)]** に、[This digital signature is OK (このデジタル署名は問題ありません)] と表示されている。
   - **[Signer information (署名者情報)]** > **[Name (名前)]** に、[Axis Communications AB] と表示されている。

AXIS Optimizerを更新する

AXIS Optimizerは、新規機能、機能改善、セキュリティのアップグレードなどによって定期的に更新されます。AXIS Optimizerは、1つのリリーストラック (最新かつ最高) のみを提供しており、

axis.comからダウンロードできるのはこの最新バージョンのみです。常にAXIS Optimizerの最新バージョンを使用することをお勧めします。

AXIS Optimizerには、VMS内のすべてのクライアントを更新できる機能も備わっています。詳細については、*システムの自動アップグレード*を参照してください。

注

AXIS Optimizerを更新するには、管理者権限が必要です。

通知の更新

AXIS Optimizerは、定期的に新しいバージョンをチェックし、新しい更新プログラムがある場合には通知します。ネットワークに接続している場合は、Smart Clientで更新通知を受け取ります。

受け取る通知のタイプを変更する:

1. Smart Clientで、[**Settings (設定)**] > [**Axis general options (Axis一般オプション)**] > [**Notification preference (通知設定)**] に移動します。
2. [**All (すべて)**]、[**Major (メジャー)**]、または [**None (なし)**] を選択します。

VMS内のすべてのクライアントに対してこれらの通知を設定する：

1. [**Management Client (管理クライアント)**] > [**Site Navigation (サイトナビゲーション)**] > [**AXIS Optimizer**] > [**System overview (システムの概要)**] に移動します。
2. [**System upgrade settings (システムアップグレードの設定)**] をクリックします。
3. [**Show upgrade notifications on all clients (すべてのクライアントのアップグレード通知を表示)**] をオンまたはオフにします。

手動更新

AXIS Optimizerは、Management ClientとSmart Clientの両方から手動で更新することができます。

注

AXIS Optimizerを更新するには、管理者権限が必要です。

マネジメントクライアントで：

1. [**Site Navigation > Basics > AXIS Optimizer (サイトナビゲーション > 基本 > AXIS Optimizer)**] に移動します。
2. **[更新]**をクリックします。

SMARTクライアントで：

1. [**Settings > Axis general options (設定 > Axisの一般的なオプション)**] に移動します。
2. **[更新]**をクリックします。

システムを自動的にアップグレードする

VMS管理サーバーから、ローカルのAXIS Optimizerバージョンをシステムに公開することができます。公開すると、AXIS Optimizerはすべてのクライアントマシンで自動的にアップグレードされます。自動アップグレードにより、オペレーターの作業が中断されることはありません。マシンまたはVMSクライアントの再起動中に、サイレントインストールが実行されます。自動アップグレードは、クライアントがインターネットに接続されていなくてもサポートされます。

注

自動アップグレードは、AXIS Optimizer 4.4以降を実行するクライアントでサポートされます。

自動アップグレードをオンにする



注

要件

- Management ClientがVMS管理サーバーと同じマシンで実行されているシステム。
- VMS管理サーバーのPC管理者権限。

自動アップグレードをオンにするには、特定のAXIS Optimizerバージョンをシステムに公開する必要があります。

1. VMS管理サーバーに、システム全体に公開するAXIS Optimizerのバージョンをインストールします。
2. VMS管理サーバーマシンで、Management Clientを開きます。
3. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [System overview (システムの概要)] に移動します。
4. [System upgrade settings (システムアップグレードの設定)] をクリックします。
5. [Local version (ローカルのバージョン)] が正しいことを確認し、[Publish (公開)] をクリックします。
   公開されているAXIS Optimizerのバージョンがすでに存在する場は、新しいバージョンに置き換えられます。

注

4.4より前のAXIS Optimizerバージョンがインストールされているクライアントマシンは、手動でアップグレードする必要があります。

自動アップグレードをオフにする

自動アップグレードをオフにするには、公開されたバージョンをリセットする必要があります。

1. VMS管理サーバーマシンで、Management Clientを開きます。
2. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [System overview (システムの概要)] に移動します。
3. [System upgrade settings > Reset published version (システムアップグレードの設定 > 公開されたバージョンのリセット)] をクリックします。

詳細情報

- AXIS Optimizerを使用しないSmart Clientは、インターネットに接続されていない場合でも、管理サーバーのWebページ (*http://[serveradress]/installation/*) で公開されたインストーラーファイルにアクセスできます。
- AXIS Optimizerインストールパッケージは、VMSのダウンロードマネージャーで利用および設定できます。
- 統合または相互接続されたシステムでは、それぞれの管理サーバーでAXIS Optimizerを公開する必要があります。
- 新バージョンのAXIS Optimizerを公開した後、どのクライアントが公開されたバージョンに更新しているかを監視できます。[System overview (システムの概要)] ページのマシンには、公開されたバージョンを実行しているときに緑色のチェック記号が表示されます。

- VMS管理サーバーを実行するマシンでは、自動アップグレードはオフになります。

AXIS Optimizerをアンインストールする

Factory default (工場出荷時設定):

AXIS Optimizerをデフォルトの状態にリセットするには、VMSからアンインストールしてから、もう一度インストールしてください。

安全な運用停止

VMSからAXIS Optimizerおよび保存されたデータを完全に削除するには、該当する場合は、ローカルコンピューターから削除する前にまず以下の手順を実行する必要があります。

1. ナンバープレートリストを削除する:
   - Management Clientを開き、**[AXIS Optimizer]** > **[License plate lists (ナンバープレートリスト)]** に移動します。
   - リストからすべてのサイトを削除します。
2. AXIS Audio Manager Proサーバーから切断する:
   - Management Clientを開き、**[AXIS Optimizer]** > **[Speaker manager (スピーカーマネジャー)]** に移動します。
   - [**Disconnect (切断)**] をクリックします。

ローカルコンピューターからAXIS Optimizerおよびローカルに保存されたデータを削除する:

1. **[Start menu (スタートメニュー)]** > **[Settings (設定)]** > **[Apps (アプリ)]** > **[Installed apps (インストール済みのアプリ)]** をクリックします。
2. **[AXIS Optimizer]** に移動します。
3. p,255mm,sfx)=″graphics:graphicF8543E623DBBE641C62ADEE8D132641F″ をクリックし、**[Uninstall (アンインストール)]** を選択します。

注

AXIS Optimizerをアンインストールした後、一部のVMSサービスを再起動する必要がある場合があります。

ユーザー権限

AXIS Optimizerには、特定のAXIS Optimizerユーザーの役割が含まれています。AXIS Optimizerの機能や性能を使用するために必要なSmart Client権限をユーザーに簡単に与えることができるようにすることが目的です。

XProtect 2018 R3、またそれ以前を実行する場合、この役割はXProtect Corporateでのみ使用できます。

XProtect 2019 R1以降を実行する場合、この役割は以下のエディションのXProtectで使用できます:

- 企業
- Expert
- Professional+
- Essential+
- Express+

権限を手動で設定する場合は、この設定を使用することで、Smart Clientのオペレーターが AXIS Optimizerに含まれるすべての機能を使用できるようになります。

- ハードウェア:ドライバーコマンド
- カメラ:AUXコマンド

注

さらに高度なユーザーの役割の処理については、*オペレーター向けに機能へのアクセスをカスタマイズする, on page 104*を参照してください。

デバイス設定にアクセス

装置アシスタント

装置アシスタントを使用すると、VMS Management ClientですべてのAxis装置の設定に直接簡単にアクセスできます。VMS内でAxis装置のWebページを簡単に見つけてアクセスし、さまざまな装置の設定を変更できます。装置にインストールされたアプリケーションを設定することもできます。

重要

- 装置アシスタントを使用するには、Axis装置がManagement Clientと同じネットワークに接続されている必要があります。
- 装置アシスタントはIPv6ネットワークではサポートされていません。

Axisデバイスを設定する

1. Management Clientで、[Site Navigation > AXIS Optimizer > Device assistant (サイトナビゲーション > AXIS Optimizer > 装置アシスタント)] に移動します。
2. 装置を選択し、[Device settings (装置の設定)] に移動します。デバイスのWebページが開きます。
3. 必要な設定を行います。

Axis装置でのアプリケーションのインストール

1. Management Clientで、[Site Navigation > AXIS Optimizer > Device assistant (サイトナビゲーション > AXIS Optimizer > 装置アシスタント)] に移動します。
2. 装置を選択し、[Device settings (装置の設定)] に移動します。デバイスのWebページが開きます。
3. [Apps] (アプリ) に移動します。Apps (アプリ) の機能は、装置のソフトウェアのバージョンによって異なります。詳細については、ご利用の装置のヘルプを参照してください。
4. 必要なアプリケーションをインストールします。

Axis装置でのアプリケーションの設定

1. Management Clientで、[Site Navigation > AXIS Optimizer > Device assistant (サイトナビゲーション > AXIS Optimizer > 装置アシスタント)] に移動します。
2. 装置を選択し、[Applications (アプリケーション)] に移動します。装置にアプリケーションがインストールされている場合は、ここに表示されます。
3. たとえば、AXIS Object Analyticsなど、該当するアプリケーションに移動します。
4. ニーズに合わせてアプリケーションを設定します。

Axisデバイスのアプリケーションを更新する

1. Management Clientで、[Site Navigation > AXIS Optimizer > Device assistant (サイトナビゲーション > AXIS Optimizer > 装置アシスタント)] に移動します。
2. 装置を右クリックして [Show updates (更新の表示)] を選択します。アプリケーションを更新できる場合は、適用可能な更新のリストが表示されます。
3. 更新ファイルをダウンロードします。
4. [How to update (更新方法)] をクリックし、手順に従います。

Axisデバイスを再起動する

1. Management Clientで、[Site Navigation > AXIS Optimizer > Device assistant (サイトナビゲーション > AXIS Optimizer > 装置アシスタント)] に移動します。
2. 装置を右クリックして [Restart device (装置の再起動)] を選択します。

AxisデバイスのIPアドレスをコピーする

1. Management Clientで、[Site Navigation > AXIS Optimizer > Device assistant (サイトナビゲーション > AXIS Optimizer > 装置アシスタント)] に移動します。
2. 装置を右クリックし、[Copy device address (装置アドレスのコピー)] を選択します。

自動化を実行

Axis装置のアクションを作成

イベントサーバープラグイン

AXIS Optimizerのイベントサーバープラグインを使用すると、Axis装置のカスタムアクションを作成することができます。XProtectのルールエンジンとイベントサーバーのプラグインを使用すると、以下のようなことが可能になります:

- オペレーターがSmart Clientのボタンをクリックすると、カスタムアクションを実行する。設定例については、*ワンクリックで複数のカメラを乾燥, on page 16*を参照してください。
- 人とのやり取りなしでアクションを実行する (自動化)。設定例については、*複数のカメラのプライバシーマスクを自動的にオフにする, on page 19*を参照してください。

イベントサーバーのプラグインは、次の2つの部分で構成されています:

- イベントサーバーで実行される独立したプラグイン。これにより、ルールエンジンに新しいアクションが追加されます。
- 新しいアクションのプリセットを作成できる管理サーバーの [Axis actions (Axisアクション)] ページ。

Axis装置のカスタムアクションは次のとおりです:オペレーターコントロールの実行、レーダーのオン/オフ、インターカム通話の開始、カメラの乾燥 (SpeedDry/ワイパー)。

イベントサーバーのプラグインは、AXIS Optimizerに含まれています。マルチPCのシステムでは、Management Clientマシンとイベントサーバーマシンの両方にAXIS Optimizerをインストールする必要があります。

イベントサーバープラグインのインストール

イベントサーバープラグインは、AXIS Optimizerのインストーラーに含まれているオプションのコンポーネントです。ビデオ管理システム (VMS) イベントサーバーにのみインストールできます。要件を満たしている場合、AXIS Optimizerインストーラーを実行すると、イベントサーバープラグインをインストールするオプションが表示されます。

注

VMSイベントサーバーは、AXIS Optimizerのインストール中およびアップグレード中に再起動が必要になる場合ががあります。この場合は、その旨の通知が表示されます。

ワンクリックで複数のカメラを乾燥

イベントサーバープラグインを使用すると、カスタムルールを設定してオペレーターの作業をより簡素化することができます。この例では、オーバーレイボタンをクリックして、特定のエリアのすべてのカメラを乾燥させる方法について説明します。



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

注

要件

- AXIS Optimizerバージョン4.0以降が搭載されたイベントサーバーとManagement Client
- AXIS Q86、Q87、Q61シリーズなど、SpeedDryまたはワイパーのいずれかに対応する1台以上のカメラ。

1. ユーザー定義のイベントを追加する:
   1.1. [Site Navigation > Rules and Events (サイトナビゲーション > ルールとイベント)] に移動し、[User-defined Event (ユーザー定義のイベント)] を右クリックします。
   1.2. [Add User-defined Event (ユーザー定義のイベントを追加)] を選択し、名前を入力します。この例では「すべてのカメラを乾燥」します。
2. 新しいルールを作成します:
   2.1. [Site Navigation > Rules and Events (サイトナビゲーション > ルールとイベント)] に移動し、[Rules (ルール)] を右クリックします。
   2.2. [Add Rule (ルールの追加)] を選択して名前を入力します。この例では「すべてのカメラを乾燥させるルール」を選択します。
   2.3. [Perform an action on <event> (イベントでアクションを実行)] を選択します。
   2.4. [Edit the rule description (ルール説明の編集)] フィールドで、[event (イベント)] をクリックします。
   2.5. [Events > External Events > User-defined Events (イベント > 外部イベント > ユーザー定義のイベント)] に移動し、[Dry all cameras (すべてのカメラを乾燥)] を選択します。
   2.6. [Next (次へ)] を、[Step 3: Actions (ステップ3：アクション)] が表示されるまでクリックします。
   2.7. アクション [Axis: Dry <camera> (Axis：カメラを乾燥)] を選択します。
   2.8. [Edit the rule description (ルール説明の編集)] フィールドで、[Axis: Dry camera (Axis：カメラを乾燥)] をクリックします。
   2.9. [Select Triggering Devices (トリガー装置の選択)] ウィンドウで、[Select devices (装置の選択)] を選択し、[OK] をクリックします。
   2.10. アクションをトリガーする装置を選択し、[OK] をクリックして、[Finish (完了)] をクリックします。
3. Smart Clientで、ユーザー定義のイベントをマップまたはビデオビューのオーバーレイボタンとして追加します。
4. オーバーレイボタンをクリックし、ルールが想定どおりに動作することを確認します。

ワンクリックで複数のカメラのオートフォーカスをオンにする

イベントサーバープラグインを使用すると、カスタムルールを設定してオペレーターの作業をより簡素化することができます。この例では、ワンクリックですべてのカメラのオートフォーカスをオンにする方法について説明します。

注

要件

- AXIS Optimizerバージョン4.1以降が搭載されたイベントサーバーとManagement Client
- オートフォーカスに対応した1台以上のカメラ

1. ユーザー定義のイベントを追加する:
   1.1. [Site Navigation > Rules and Events (サイトナビゲーション > ルールとイベント)] に移動し、[User-defined Event (ユーザー定義のイベント)] を右クリックします。
   1.2. [Add User-defined Event (ユーザー定義イベントの追加)] を選択します。この例では名前に「オートフォーカス」と入力します。
2. 新しいルールを作成します:

2.1. [Site Navigation > Rules and Events (サイトナビゲーション > ルールとイベント)] に移動し、[Rules (ルール)] を右クリックします。

2.2. [Add Rule (ルールの追加)]を選択します。この例では名前に「オートフォーカスの実行」と入力します。

2.3. [Perform an action on <event> (イベントでアクションを実行)] を選択します。

2.4. [Edit the rule description (ルール説明の編集)] フィールドで、[event (イベント)] をクリックします。

2.5. [Events > External Events > User-defined Events (イベント > 外部イベント > ユーザー定義のイベント)] に移動し、[Autofocus (オートフォーカス)] を選択します。[OK]をクリックします。

2.6. [Next (次へ)] を、[Step 3: Actions (ステップ3：アクション)] が表示されるまでクリックします。

2.7. アクション [Axis: Run autofocus on <camera> (Axis：カメラでオートフォーカスを実行)] を選択します。

2.8. [Edit the rule description (ルール説明の編集)] フィールドで、[Axis: Run autofocus on camera (Axis：カメラでオートフォーカスを実行)] をクリックします。

2.9. [Select Triggering Devices (トリガー装置の選択)] ウィンドウで、[Select devices (装置の選択)] を選択し、[OK] をクリックします。

2.10. アクションをトリガーする装置を選択して [OK] をクリックし、[Finish (完了)] をクリックします。

3. Smart Clientで、ユーザー定義イベント「オートフォーカス」をマップまたはビデオビューのオーバーレイボタンとして追加します。

4. オーバーレイボタンをクリックし、ルールが想定どおりに動作することを確認します。

ワンクリックで複数のストロボサイレンをトリガーする

イベントサーバープラグインを使用すると、カスタムルールを設定してオペレーターの作業をより簡素化することができます。この例では、Smart Clientでワンクリックで複数のストロボサイレンを作動させる方法について説明します。

注

要件

- AXIS Optimizerバージョン4.4以降が搭載されたイベントサーバーとManagement Client
- 1つまたは複数のAxisストロボサイレン
- Axisストロボサイレンの出力1が有効になり、管理クライアントの出力デバイスに追加されました。

1. ユーザー定義のイベントを作成します。

1.1. [Site Navigation > Rules and Events (サイトナビゲーション > ルールとイベント)] に移動し、[User-defined Event (ユーザー定義のイベント)] を右クリックします。

1.2. [Add User-defined Event (ユーザー定義イベントの追加)] を選択し、名前 (「Trigger all strobe sirens」など) を入力します。

2. 装置アシスタントで、ストロボサイレンプロファイルを作成します。

2.1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Device assistant (装置アシスタント)] に移動します。

2.2. ストロボサイレンを選択します。ストロボサイレンのWebページが開きます。

2.3. [Profiles (プロファイル)] に移動し、[Add profile (プロファイルの追加)] をクリックします。

2.4. Smart Clientで、オペレーターがストロボサイレンをトリガーしたときにストロボサイレンによって実行されるアクションを設定します。

2.5. 他のストロボサイレンにも同じプロファイルを作成します。すべてのデバイスで同じプロファイル名を使用する必要があります。

3. Axisアクションで、アクションプリセットを作成します。
   3.1. [Site Navigation (サイトナビゲーション)] > [Rules and Events (ルールとイベント)] > [Axis actionss (Axisアクション)] の順に移動します。
   3.2. [Add new preset (新しいプリセットを追加)] をクリックします。
   3.3. [Select strobe siren (ストロボサイレンの選択)] に移動し、[Strobe siren (ストロボサイレン)] をクリックします。
   3.4. 使用するストロボサイレンを選択し、[OK] をクリックします。
   ストロボサイレンのプロファイルのリストが表示されます。
   3.5. 前の手順で作成したストロボサイレンプロファイルを選択します。アクションプリセットは自動的に保存されます。
   3.6. F5を押して、サーバー設定を更新します。これで、作成した新しいアクションプリセットの使用を開始できます。
4. ルールの作成:
   4.1. [Site Navigation > Rules and Events (サイトナビゲーション > ルールとイベント)] に移動し、[Rules (ルール)] を右クリックします。
   4.2. [Add Rule (ルールの追加)] を選択し、名前 (「Trigger all strobe sirens rule」など) を入力します。
   4.3. [Perform an action on <event> (イベントでアクションを実行)] を選択します。
   4.4. [Edit the rule description (ルール説明の編集)] フィールドで、[event (イベント)] をクリックします。
   4.5. [Events (イベント)] > [External Events (外部イベント)] > [User-defined Events (ユーザー定義イベント)] に移動し、[Trigger all strobe sirens] を選択します。
   4.6. [Next (次へ)] を、[Step 3: Actions (ステップ3: アクション)] が表示されるまでクリックします。
   4.7. アクション Axis: Start or stop a profile on a strobe siren: <preset> (Axis：ストロボサイレンのプロファイルの実行プリセット)] を選択します。
   4.8. [Edit the rule description (ルール説明の編集)] フィールドで、[preset (プリセット)] をクリックします。
   4.9. 使用するプリセットを選択します。
   4.10. [Next (次へ)] をクリックし、[Finish (完了)] をクリックします。
5. Smart Clientで、ユーザー定義のイベントをマップまたはビデオビューのオーバーレイボタンとして追加します。
6. オーバーレイボタンをクリックし、ルールが想定どおりに動作することを確認します。

複数のカメラのプライバシーマスクを自動的にオフにする

イベントサーバープラグインを使用すると、特定のアクションを自動化できます。この例では、分析機能を使用するイベントが発生した際に、複数のカメラのプライバシーマスクを自動的にオフにする方法について説明します。この例では、本来ならば入ってはいけない場所に人間や車両が入り込むイベントを扱います。ここでは、プライバシーマスクを自動的にオフにして、現状を把握できるようにします。



以下の作業を行います:

1. AXIS Object Analytics (または任意の分析機能を搭載したアプリケーション) で *分析シナリオを設定する, on page 20*を行います。
2. *関連するカメラにオペレーターコントロールを追加する, on page 20*
3. *アクションプリセットを作成する, on page 21*
4. *分析イベントの発生時にプライバシーマスクをオフにするルールを作成する, on page 21*
5. *プライバシーマスクを再度オンにするルールを作成する, on page 21*
6. *ルールをテストします。, on page 22*を行い、すべてが想定どおりに動作することを確認します。

注

要件

- AXIS Optimizerバージョン4.0以降が搭載されたイベントサーバーとManagement Client
- AXIS OS 7.40以降を搭載したカメラ
- イベントを生成できるカメラ (この例では、AXIS Object Analyticsを搭載したカメラ)

分析シナリオを設定する

1. [Site Navigation > AXIS Optimizer > Device assistant (サイトナビゲーション > AXIS Optimizer > 装置アシスタント)] に移動し、使用する分析機能を搭載した装置を検索します。
2. [Applications (アプリケーション)] をクリックし、アクションをトリガーする分析シナリオを作成します。
3. [Devices > Cameras (装置 > カメラ)] に移動し、分析シナリオを作成したカメラを検索します。
4. [Properties (プロパティ)] ウィンドウで、[Events > Add (イベント > 追加)] をクリックします。
5. ドライバーイベントを選択します。この例では、「Object Analytics:Event test Rising (オブジェクト分析: イベントテスト上昇)」を選択し、[OK] をクリックします。
6. [Add (追加)] を クリックし、ドライバーイベント 「オブジェクト分析:イベントテスト下降」を選択します。[OK] をクリックします。
7. [Save (保存)] をクリックします。

関連するカメラにオペレーターコントロールを追加する

1. [AXIS Optimizer > Operator controls (AXIS Optimizer > オペレーターコントロール)] に移動し、コントロールライブラリを開きます。
2. [Configuration (設定)] ウィンドウで、該当するフォルダーを選択し、[Turn off privacy mask (プライバシーマスクをオフにする)] と [Turn on privacy mask (プライバシーマスクをオンにする)] の両方を有効にします。

アクションプリセットを作成する

1. [Rules and Events > Axis actions (ルールとイベント > Axisアクション)] に移動し、[Add new preset (新規プリセットの追加)] をクリックします。
2. [Cameras (カメラ)] をクリックし、該当するカメラを選択します。この例では:AXIS P1375とAXIS Q6075-Eです。次に、コントロール [Turn on privacy mask (プライバシーマスクをオンにする)] を選択します。
3. [Add new preset > Cameras (新規プリセットの追加 > カメラ)] をクリックし、該当するカメラを選択します。この例では:AXIS P1375とAXIS Q6075-Eです。次に、コントロール [Turn on privacy mask (プライバシーマスクをオフにする)] を選択します。

分析イベントの発生時にプライバシーマスクをオフにするルールを作成する

1. [Site Navigation > Rules and Events (サイトナビゲーション > ルールとイベント)] に移動し、[Rules (ルール)] を右クリックします。
2. [Add Rule (ルールの追加)] を選択して名前 (この例では「分析時にプライバシーマスクをオフにする」を入力します。
3. [Perform an action on <event> (イベントでアクションを実行)] を選択します。
4. [Edit the rule description (ルール説明の編集)] フィールドで、[event (イベント)] をクリックします。[Devices (デバイス)] > [Configurable Events (設定可能なイベント)] の順に移動し、[Object Analytics: Event test Rising (オブジェクト分析：イベントテスト上昇)] を選択します。
5. [Edit the rule description (ルール説明の編集)] フィールドで、装置を選択します (この例ではAXIS P1375)。
6. [Next (次へ)] を、[Step 3: Actions (ステップ3：アクション)] が表示されるまでクリックします。
7. アクション [Axis: Run operator control: <preset> (Axis：オペレーターコントロールの実行：プリセット)] を選択します。
8. [Edit the rule description (ルール説明の編集)] フィールドで、[preset (プリセット)] をクリックします。続いて、対象 [Turn off privacy mask on 2 cameras (2台のカメラでプライバシーマスクをオフにする)] 追加し、[OK] をクリックします。
9. Finish (終了) をクリックします。

プライバシーマスクを再度オンにするルールを作成する

1. [Add Rule (ルールの追加)] を選択して名前を入力します。この例では「分析の停止時にプライバシーマスクをオンにする」を選択します。
2. [Perform an action on <event> (イベントでアクションを実行)] を選択します。
3. [Edit the rule description (ルール説明の編集)] セクションで、[event (イベント)] をクリックします。[Devices (デバイス)] > [Configurable Events (設定可能なイベント)] の順に移動し、[Object Analytics: Event test Failing (オブジェクト分析：イベントテスト失敗)] を選択します。
4. [Edit the rule description (ルール説明の編集)] セクションで、装置を選択します (この例ではAXIS P1375)。
5. [Next (次へ)] を、[Step 3: Actions (ステップ3：アクション)] が表示されるまでクリックします。
6. アクション [Axis: Run operator control: <preset> (Axis：オペレーターコントロールの実行：プリセット)] を選択します。
7. [Edit the rule description (ルール説明の編集)] セクションで、[preset (プリセット)] をクリックします。続いて、対象 [Turn on privacy mask on 2 cameras (2台のカメラでプライバシーマスクをオンにする)] を追加し、[OK] をクリックします。

8. Finish (終了) をクリックします。

ルールをテストします。

1. [AXIS Optimizer > Device assistant (AXIS Optimizer > 装置アシスタント)] に移動し、自動化の作成に使用した分析機能を使用して装置を検索します。この例では、AXIS P1375を使用しています。
2. 該当するシナリオを開き、[Test alarm (アラームのテスト)] をクリックします。

カメラが動きを検知したときにストロボサイレンが作動するようにする

イベントサーバープラグインを使用すると、アクションを自動化するためのカスタムルールを設定できます。この例では、カメラによって動きが検知されたときに自動的にストロボサイレンを作動させる方法について説明します。

注

要件

- AXIS Optimizerバージョン4.4以降が搭載されたイベントサーバーとManagement Client
- 1つまたは複数のAxisストロボサイレン
- Axisストロボサイレンの出力1が有効になり、管理クライアントの出力デバイスに追加されました。
- VMSバージョン2022 R2より古いバージョンの場合、Axisアクションは停止アクションとして使用できません。旧バージョンでは、ストロボサイレンの実行と停止用に2つの別々のルールを作成する必要があります。

1. ストロボサイレンのプロファイルを作成する:
   1.1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Device assistant (装置アシスタント)] に移動します。
   1.2. [Axis output devices (Axis出力装置)] に移動し、ストロボサイレンを選択します。ストロボサイレンのWebページが開きます。
   1.3. [Profiles (プロファイル)] に移動し、[Add profile (プロファイルの追加)] をクリックします。
   1.4. すべてのサイレンに同じプロファイル名を選択してください。
   1.5. 動きが検知されたときにストロボサイレンが実行するアクションを設定します。
2. 開始/停止用のアクションプリセットを作成します。
   2.1. [Site Navigation (サイトナビゲーション)] > [Rules and Events (ルールとイベント)] > [Axis actionss (Axisアクション)] の順に移動します。
   2.2. 開始プリセットを作成するには、[Strobe siren (ストロボサイレン)] に移動し、[Add new preset (新しいプリセットの追加)] をクリックします。
   2.3. [Select strobe siren (ストロボサイレンの選択)] に移動し、[Strobe siren (ストロボサイレン)] をクリックします。
   2.4. リストから1つ以上のストロボサイレンを選択します。
   2.5. リストから先ほど作成したサイレンプロファイルを選択します。アクションプリセットは自動的に保存されます。
   2.6. 停止プリセットを作成するには、[Add new preset (新しいプリセットの追加)] をクリックします。
   2.7. [Select strobe siren (ストロボサイレンの選択)] に移動し、[Strobe siren (ストロボサイレン)] をクリックします。
   2.8. 開始プリセットに選択したものと同じストロボサイレンをリストから選択します。
   2.9. [Select action (アクションの選択)] に移動し、[Stop (停止)] を選択します。

2.10. 開始アクション用に作成したものと同じサイレンプロファイルを選択します。アクションプリセットは自動的に保存されます。

2.11. [click to refresh (クリックして更新)] をクリックするか、F5キーを押してサーバー設定を更新します。

3. ルールの作成:

3.1. [Site Navigation (サイトナビゲーション)] > [Rules and Events (ルールとイベント)] > [Rules (ルール)] の順に移動します。

3.2. [Rules (ルール)] を右クリックし、[Add Rule (ルールの追加)] を選択して、名前を入力します。

3.3. [Edit the rule description (ルール説明の編集)] で、[event (イベント)] をクリックします。

3.4. [Devices (装置)] > [Predefined Events (既定イベント)] の順に移動し、 [Motion Started (動き開始)] を選択します。

3.5. [Edit the rule description (ルール説明の編集)] で、[devices/recording_server/management_server (デバイス/録画サーバー/管理サーバー)] をクリックします。

3.6. ストロボサイレンをトリガーするカメラを選択します。

3.7. [Next (次へ)] を、[Step 3: Actions (ステップ3: アクション)] が表示されるまでクリックします。

3.8. アクション Axis: Start or stop a profile on a strobe siren: <preset> (Axis：ストロボサイレンのプロファイルの開始または停止：プリセット)] を選択します。

3.9. [Edit the rule description (ルール説明の編集)] で、[preset (プリセット)] をクリックします。

3.10. 先ほど作成した開始プリセットを選択します。

3.11. [Next (次へ)] をクリックして、[Perform stop action on <event> (イベントで停止アクションを実行)] を選択します。

3.12. [Next (次へ)] をクリックして、[Axis: Start or stop a profile on strobe siren: <event> (AXIS：ストロボサイレンのプロファイルの開始または停止：イベント)] を選択します。

3.13. [Edit the rule description (ルール説明の編集)] で、[preset (プリセット)] をクリックします。

3.14. 先ほど作成した停止プリセットを選択します。

3.15. [Finish (終了)] を選択します。

4. カメラで動きを検知したときにストロボサイレンが正しく動作することをテストします。

カメラが動きを検知したときに、スピーカーまたはスピーカーゾーンで音声クリップを再生する



イベントサーバープラグインにより、アクションを自動化するためのカスタムルール、いわゆるアクションプリセットを設定できます。この例では、カメラが動きを検知したときに、音声クリップを音声スピーカーまたはスピーカーゾーンで自動的に再生する方法を示します。

注

要件

- AXIS Optimizerバージョン4.6以降が搭載されたイベントサーバーとManagement Client.
- 1台または複数のAxis専用スピーカーまたはスピーカー内蔵のAxis装置.
- スピーカーゾーンで音声クリップを再生するには、正しく設定されたAXIS Audio Manager EdgeまたはAXIS Audio Manager Proシステムが必要です。これらのシステムの設定方法の詳細については、*設定モード, on page 33*を参照してください。

1. 音声クリップをアップロードするには:
   1.1. AXIS Audio Manager Edgeモードまたはレガシーモードでは、スピーカーにアップロードする音声クリップをデフォルトのフォルダー **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect - Audio Clips** に配置します。
   AXIS Audio Manager Proモードでは、AXIS Audi Manager Proのwebインターフェースから音声クリップをアップロードします。
   1.2. Management Clientで、**[Site Navigation (サイトナビゲーション)]** > **[AXIS Optimizer]** > **[Speaker manager (スピーカーマネージャー)]** に移動し、リストからスピーカー、デバイスグループ、またはスピーカーゾーンを選択します。

   注

   スピーカーマネージャーモードの選択方法の詳細については、*設定モード, on page 33*を参照してください。
   1.3. **[Audio clips (音声クリップ)]** に移動し、アップロードする音声クリップの前にある **[+]** をクリックします。
   1.4. レガシーモードでは、音声クリップを再生するスピーカーごとに、手順1.2～1.3を繰り返します。各スピーカーには必ず同じ音声ファイルをアップロードしてください。
2. スピーカーまたはスピーカーゾーンで音声クリップを再生するためのアクションプリセットを作成するには:
   2.1. **[Site Navigation (サイトナビゲーション)]** > **[Rules and Events (ルールとイベント)]** > **[Axis actions (Axisアクション)]** に移動します。
   2.2. プリセットを作成するには、**[Audio clips (音声クリップ)]** に移動し、**[Add new preset (新規プリセットの追加)]** をクリックします。
   2.3. AXIS Audio Manager EdgeまたはAXIS Audio Manager Proモードでは、**[Select playback destination (再生先を選択)]** に移動します。
   レガシーモードでは、**[Select speaker (スピーカーの選択)]** に移動します。
   2.4. スピーカーまたはスピーカーゾーンを選択します。
   2.5. リストから手順1でアップロードした音声クリップを選択します。アクションプリセットは自動的に保存されます。
   2.6. AXIS Audio Manager Proモードで、**[Select visual profile (ビジュアルプロファイルの選択)]** に移動し、ビジュアルプロファイルとテキストを設定します。

   注

   ビジュアルプロファイルリストから **[Default (デフォルト)]** を選択し、音声クリップアクションがトリガーされると、AXIS Audio Manager Proサーバーでデフォルトのビジュアルプロファイル動作を使用するようにします。
   2.7. **[refresh (更新)]** をクリックするか、F5を押してサーバー設定を更新します。
3. ルールを作成するには:
   3.1. **[Site Navigation (サイトナビゲーション)]** > **[Rules and Events (ルールとイベント)]** > **[Rules (ルール)]** の順に移動します。
   3.2. **[Rules (ルール)]** を右クリックし、**[Add Rule (ルールの追加)]** を選択して、名前を入力します。

3.3. [Edit the rule description (ルール説明の編集)] で、[event (イベント)] をクリックします。
3.4. [Devices (デバイス)] > [Predefined Events (既定イベント)] の順に移動し、[Motion Started (動き開始)] を選択します。
3.5. [Edit the rule description (ルール説明の編集)] で、[devices/recording_server/management_server (デバイス/録画サーバー/管理サーバー)] をクリックします。
3.6. アクションプリセットまたは音声クリップをトリガーするカメラを選択します。
3.7. [Next (次へ)] を、[Step 3: Actions (ステップ3: アクション)] が表示されるまでクリックします。
3.8. [Axis: Play audio clip: <preset> (Axis: オーディオクリップの再生: プリセット)] を選択します。
3.9. [Edit the rule description (ルール説明の編集)] で、[preset (プリセット)] をクリックします。
3.10. 前の手順で作成したプリセットを選択します。
3.11. [Finish (終了)] を選択します。
4. カメラで動きが検知されたときに音声クリップが正しく再生されるかをテストします。

ルールのトラブルシューティング

ルールが機能しない場合は、まずイベントサーバーのメッセージを確認し、イベントサービスが実行されていることを確認してください。

イベントサーバーでは、AXIS Optimizerのログを確認することもできます。Management ClientまたはSmart Clientが利用可能な場合は、それらを使用してログを有効にし、保存します。

ナンバープレートリストを一元管理

AXIS Optimizerのリストマネージャーを使用すると、すべてのカメラのナンバープレートリストを一元管理することができます。VMSから直接、許可リスト、ブロックリスト、カスタムリストを作成および管理できます。このシステムでは、リストの組み合わせに対応しています。システム内のすべてのカメラに適用されるグローバルリストと、特定のカメラに適用されるローカルリストを持つことができます。

駐車場の入退出を自動化する場合や、特定のナンバープレートの登録時にアラームを発生させる場合などで、リストの一元管理は便利です。

リストを作成および編集するには、管理者である必要があります。他の役割に読み取り権限と編集権限を与える方法については、*リスト権限を設定する, on page 26*のセクションを参照してください。

リストを作成する

注

要件

- カメラでAXIS License Plate Verifier 1.8以降が実行されている
- カスタムリストを作成するには、AXIS License Plate Verifier 2.0以降が必要です。

1. Management Clientで、[Site Navigation > AXIS Optimizer > License plate lists (サイトナビゲーション > AXIS Optimizer > ナンバープレートリスト)] に移動します。
2. 許可リスト、ブロックリスト、カスタムリストの送信先のカメラを選択します。
3. (オプション) 許可リスト、ブロックリスト、カスタムリストを表示および編集できるユーザーの役割を追加します。
4. 許可リスト、ブロックリスト、カスタムリストにナンバープレートを追加します。

既存のナンバープレートリストをインポートすることもできます。
リストのステータスが [Synchronized (同期済み)] になった場合、選択したカメラにプッシュされます。

リスト権限を設定する

許可リスト、ブロックリスト、カスタムリストを編集できるユーザーの役割を設定できます。たとえば、管理者がリストを設定している場合に、オペレーターが日々のニーズに応じて訪問者を追加できるようにする場合などに有効です。

マネジメントクライアントで：

リストを表示および編集する権限はすべて、リストごとに個別に選択できます。

1. [Security (セキュリティ)] > [Roles (役割)] に移動し、役割を選択します。
2. [AXIS Optimizer] タブに移動します。
3. [Role settings (役割設定)] > [AXIS Optimizer] > [License plate lists (ナンバープレートリスト)] に移動します。
4. [License plate lists (node) (ナンバープレートリスト、ノード)] のフィールドで [Read (読み取り)] を選択します。
5. [License plate lists (ナンバープレートリスト)] でリストを選択し、[Edit license plates (ナンバープレートの編集)] を選択します。
   - XProtect 2023 R2よりも古いバージョンの場合は、[MIP > AXIS Optimizer > AXIS Optimizer Security > License plate lists (MIP > AXIS Optimizer > AXIS Optimizer Security > ナンバープレートリスト)] に移動し、[Edit license plate lists (ナンバープレートリストの編集)] を選択します。

リストの編集

マネジメントクライアントで：

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [License plate lists (ナンバープレートリスト)] に移動します。
2. 編集するサイトを選択します。
3. 必要に応じて、[Cameras (カメラ)] または [License plates (ナンバープレート)] を更新します。
   リストのステータスが [Synchronized (同期済み)] になると、選択したカメラに変更が反映されたことになります。

SMARTクライアントで：

1. *Axisナンバープレート, on page 63*に移動し、[License plate lists (ナンバープレートリスト)] をクリックします。
   タブが表示されていない場合は、[Settings > Axis search options (設定 > Axis検索オプション)] に移動し、[Show license plate tab (ナンバープレートタブの表示)] を選択します。
2. 編集するサイトを選択します。
3. 許可リスト、ブロックリスト、カスタムリストにナンバープレートを追加します。
   既存のナンバープレートリストをインポートすることもできます。
   リストのステータスが [Synchronized (同期済み)] になった場合、選択したカメラにプッシュされます。

リストのインポート

リストは、さまざまなテキスト形式、またはCSV形式でインポートできます。

- 使用できるテキスト形式:各ラインにナンバープレート1枚

- 使用できるCSV形式:
  - 各ラインにナンバープレート1つ
  - 2つのフィールド:ナンバープレートと日付
  - 3つのフィールド:ナンバープレート、所有者、コメント
  - 4つのフィールド:ナンバープレート、所有者、コメント、「Active (アクティブ)」または「Inactive (非アクティブ)」の文字列。(リストをエクスポートする場合と同じ形式です。)

マネジメントクライアントで：

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [License plate lists (ナンバープレートリスト)] に移動します。
2. 編集するサイトを選択します。
3. [Allowed (許可)]、[Blocked (ブロック)]、または [Custom (カスタム)] に移動します。
4. ⋮ をクリックしてから、[Import to allow list (許可リストにインポート)]、[Import to block list (ブロックリストにインポート)]、[Import to custom list (カスタムリストにインポート)] のいずれかを選択します。
5. [Reset list (リストのリセット)] ダイアログで:
   - [Yes (はい)] をクリックすると、既存のナンバープレートがすべて削除され、新しくインポートされたナンバープレートのみがリストに追加されます。
   - [No (いいえ)] をクリックすると、新しくインポートされたナンバープレートがリスト上の既存のナンバープレートに統合されます。

SMARTクライアントで：

1. *Axisナンバープレート, on page 63*に移動し、[License plate lists (ナンバープレートリスト)] をクリックします。
   タブが表示されていない場合は、[Settings > Axis search options (設定 > Axis検索オプション)] に移動し、[Show license plate tab (ナンバープレートタブの表示)] を選択します。
2. 編集するサイトを選択します。
3. [Allowed (許可)]、[Blocked (ブロック)]、または [Custom (カスタム)] に移動します。
4. ⋮ をクリックしてから、[Import to allow list (許可リストにインポート)]、[Import to block list (ブロックリストにインポート)]、[Import to custom list (カスタムリストにインポート)] のいずれかを選択します。
5. [Reset list (リストのリセット)] ダイアログで:
   - [Yes (はい)] をクリックすると、既存のナンバープレートがすべて削除され、新しくインポートされたナンバープレートのみがリストに追加されます。
   - [No (いいえ)] をクリックすると、新しくインポートされたナンバープレートがリスト上の既存のナンバープレートに統合されます。

リストのエクスポート

注
ナンバープレートリストをエクスポートするには、管理者権限が必要です。

マネジメントクライアントで：

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [License plate lists (ナンバープレートリスト)] に移動します。
2. 編集するサイトを選択します。
3. [Allowed (許可)]、[Blocked (ブロック)]、または [Custom (カスタム)] に移動します。

4. ⋮ をクリックしてから、[Export allow list (許可リストをエクスポート)]、[Export block list (ブロックリストをエクスポート)]、[Export custom list (カスタムリストをエクスポート)] のいずれかを選択します。
エクスポートされたリストは、4つのフィールドを含むCSV形式で表示されます。ナンバープレート、所有者、コメント、「Active (アクティブ)」または「Inactive (非アクティブ)」のステータス。

SMARTクライアントで：

1. *Axisナンバープレート, on page 63*に移動し、[License plate lists (ナンバープレートリスト)] をクリックします。
タブが表示されていない場合は、[Settings > Axis search options (設定 > Axis検索オプション)] に移動し、[Show license plate tab (ナンバープレートタブの表示)] を選択します。
2. 編集するサイトを選択します。
3. [Allowed (許可)]、[Blocked (ブロック)]、または [Custom (カスタム)] に移動します。
4. ⋮ をクリックしてから、[Export allow list (許可リストをエクスポート)]、[Export block list (ブロックリストをエクスポート)]、[Export custom list (カスタムリストをエクスポート)] のいずれかを選択します。
エクスポートされたリストは、4つのフィールドを含むCSV形式で表示されます。ナンバープレート、所有者、コメント、「Active (アクティブ)」または「Inactive (非アクティブ)」のステータス。

リストの詳細について

- 複数のサイトを作成できます。
- 各サイトは、AXIS License Plate Verifierがインストールされている1台以上のカメラに関連付けられます。
- 各サイトは、1つ以上のVMSユーザーの役割に関連付けられます。ユーザーの役割は、誰がナンバープレートリストの読み取りと編集の権限を持つかを定義します。
- すべてのリストはVMSデータベースに保存されます。
- カメラをサイトに追加すると、カメラの既存のナンバープレートが上書きされます。
- 同じカメラが複数のサイトに存在する場合、すべてのサイトの合計がカメラに表示されます。
- 複数のリストに同じナンバープレートがある場合、「ブロック」の優先度が最も高くなり、「許可」は中程度、カスタムは最も低くなります。
- ナンバープレートごとに、車両の所有者に関する情報を追加することができます。ただし、この情報はカメラとは同期されません。

ライブイベントに応答

装置コントロールの使用

オペレーターコントロール

オペレーターコントロールを使用すると、Smart Clientから直接、Axisカメラの特定の機能にアクセスできます。どの機能を利用できるかは、システム内にあるカメラとそのカメラに搭載されている機能によって異なります。インストール済みのオペレーターコントロールに加えて、カスタムコントロールを作成できます。また、オペレーターがアクセスできるコントロールを設定できます。

オペレーターコントロールの例を以下に示します:

- ワイパーのオン/オフ
- ヒーターのオン/オフ
- IRのオン/オフ
- フォーカスリコール
- WDRのオン/オフ
- 電子動体ブレ補正 (EIS) のオン/オフ
- プライバシーマスクのオン/オフ。

カメラ固有のオペレーターコントロールについては、データシートを参照してください。

オペレーターコントロールにアクセスする

注

要件

- AXIS OS 7.10、7.40以降を搭載したAxis装置。(バージョン7.20、および7.30はオペレーターコントロールに対応していません。)

1. Smart Clientで、[**Live (ライブ)**] をクリックし、Axisカメラに移動します。
2. をクリックし、使用する機能を選択します。

PTZカメラのフォーカスエリアの保存

フォーカスリコール機能を使用すると、フォーカスエリアを保存し、PTZカメラがそのエリアに移動した際に自動的に戻るようにすることができます。この機能は、カメラがフォーカスを合わせるのが難しい低光量の条件下で特に有効です。



1. Smart Clientで、フォーカスが合うエリアにカメラを移動します。

注

フォーカスエリアを設定する場合は、良好な光条件が要求されます。

2. カメラのフォーカスを調節します。
3. [**Add Focus Recall Zone (フォーカスリコールゾーンの追加)**] を選択します。

その後、カメラをパンまたはチルトして、あるエリアにビューを移すと、そのビューのプリセットフォーカスが自動的に呼び出されます。ズームインまたはズームアウトしても、カメラは同じフォーカス位置を維持します。

ゾーンの設定が正しくない場合は、[Remove Focus Recall Zone (フォーカスリコールゾーンの削除)] を選択します。

カメラのオートフォーカス



オートフォーカス機能を搭載したカメラは、ビューを変更しても画像のフォーカスが対象範囲に合うように、レンズを機械的・自動的に調整することができます。

PTZカメラのオートフォーカス

1. Smart Clientで、カメラビューを選択します。
2. をクリックして、[Set Focus (フォーカスのセット)] > [AF] の順に移動します。[Focus Control (フォーカスコントロール)] を使用すると、フォーカスポイントを近づけたり遠ざけたりすることができます:
   - 大きなステップの場合は、大きなバーをクリックします。
   - 小さなステップの場合は、小さなバーをクリックします。

固定ボックス型カメラと固定ドームカメラのオートフォーカス

1. Smart Clientで、カメラビューを選択します。
2. をクリックして、[Autofocus (オートフォーカス)] に移動します。

スピードドライ、またはワイパーをオンにする



スピードドライ機能により、雨が降った時にドームの水滴を振り落とすことができます。ドームが高速で振動させることで、水の表面張力を崩して水滴をふるい落とします。この機能により、雨天時でも鮮明な映像が得られます。

スピードドライ機能をオンにするには

1. Smart Clientで、カメラビューを選択します。
2. をクリックして、[PTZ] > [Speed Dry (スピードドライ)] の順に移動します。

重要

スピードドライ機能は、AXIS Q61シリーズのカメラでのみご利用いただけます。

ワイパー機能をオンにする

Axisのポジショニングカメラのレンズに付着した余分な水や雨を除去するワイパーです。

1. Smart Clientで、カメラビューを選択します。
2. をクリックします。

重要

ワイパー機能は、AXIS Q86シリーズのカメラでのみ使用できます。

スポット温度の測定



システムにスポット温度測定を内蔵したカメラが搭載されている場合は、カメラビューで直接温度を測定できます。スポット温度測定を備えたAXISカメラはAXIS Q1961-TE、AXIS Q2101-E、およびQ2901-Eです。

1. Smart Clientで、スポット温度測定が内蔵されたカメラでカメラビューを開きます。
2. スポット温度を測定するには、 をクリックして選択します。
   - AXIS Q2901-Eの場合は、[**Measure spot temperature (スポット温度の測定)**]。
   - AXIS Q1961-TEおよびAXIS Q2101-Eの場合は、[**Enable temperature spot meter (温度スポットメーターを有効にする)**]。
3. ビュー内の任意のエリアをクリックすると、現在のスポット温度が表示されます。Q1961-TEおよびAXIS Q2101-Eの場合は、[**Done (完了)**] をクリックします。
4. AXIS Q1961-TEおよびAXIS Q2101-Eの場合は、スポット温度を無効化するまで画像上に表示されます。
   - > [**Disable temperature spot meter (温度スポットメーターを無効にする)**] の順に選択します。

注

デジタルズームを使用した場合、温度測定が正しく行われない場合があります。

自動的にズームインし、動く物体を追跡します

自動追跡 (オートトラッキング)

オートトラッキングを使用すると、カメラが車両や人物などの動く物体に自動的にズームインし、物体を追跡します。物体を手動で選択することも、トリガーエリアを設定して、カメラに動く物体を検知させることもできます。物体を追跡していないとき、カメラは5秒後にホームポジションに戻ります。

- PTZカメラのWebインターフェースでトリガーエリアを設定します。
- Smart Clientに、以下の情報が表示されます。
  - 赤の四角形:追跡対象の物体.
  - 青いゾーン:追跡されてない物体がトリガーゾーンに入った場合、または右クリックすると追跡できます。

オートトラッキングの設定

注

要件

- AXIS OS 12.0
- Autotracking 2をサポートする1台以上のAxisのカメラ (AXIS Q6075 PTZ Dome Network Cameraなど)

1. カメラとメタデータ装置が有効になっていることを確認します。
2. カメラのメタデータ1を選択し、[Settings (設定)] をクリックします。
3. [Metadata stream > Event data (メタデータストリーム > イベントデータ)] に移動し、[Yes (はい)] を選択します。
4. [Save (保存)] をクリックします。
5. PTZカメラのWebインターフェースでオートトラッキングを設定します。

オートトラッキングのオン/オフ

1. Smart Clientで、 をクリックします。
2. [Turn on autotracking (オートトラッキングをオンにする)] または [Turn off autotracking (オートトラッキングをオフにする)] を選択します。

注
オートトラッキングのオン/オフを切り替えるオプションが複数ある場合は、リストの最後のオプションを使用してください。

手動でオートトラッキングを開始する

マウスでカーソルを物体の上に合わせると、オーバーレイが塗りつぶされます。物体をマウスポインターで右クリックすると、その物体がターゲットとして設定され、カメラがターゲットとなる物体の追跡を開始します。物体を追跡できない場合、カメラは5秒後にリセットされます。

青いボックスの外側を右クリックすると、オートトラッキングが停止します。

カスタムオペレーターコントロールを作成する

1. Management Clientで、[Site Navigation > AXIS Optimizer > Operator controls (サイトナビゲーション > AXIS Optimizer > オペレーターコントロール)] に移動します。
2. 装置または装置のグループを選択します。
3. [Add new control (新規コントロールの追加)] をクリックします。
4. [名前] と [説明] を入力します。
5. 管理者権限を持つユーザーだけがオペレーターコントロールを使用できる場合は、[Administrator (管理者)] を選択します。
6. 特定のコントロールのVAPIX URLを追加します。
例:オペレーターコントロールにデフォッグを追加するには、次のURLを入力します:
`/axis-cgi/param.cgi?action=update&imageSource.IO.Sensor.Defog=on`
Axisネットワーク装置のAPIの詳細については、を参照してください。
7. Smart Clientに移動し、オペレーターのコントロールが想定どおりに機能するかをテストします。

オペレーターコントロールへのアクセスを設定する

Smart Clientのオペレーターがアクセスできるオペレーターコントロールを設定できます。

1. Management Clientで、[Site Navigation > AXIS Optimizer > Operator controls (サイトナビゲーション > AXIS Optimizer > オペレーターコントロール)] に移動します。
2. 装置または装置のグループを選択します。
3. Smart Clientでオペレーターが利用するオペレーターコントロールを選択します。

スピーカーを介したやり取り

スピーカーマネージャー

スピーカーマネージャーは、Axisの音声製品をVMSに統合し、Axisデバイスの全機能を利用できるようにします。

- カメラに関連するスピーカーにアクセスする
  カメラをスピーカーまたはスピーカーのグループに接続すると、ライブビューからスピーカーにアクセスすることができます。スピーカーを手動で検索する必要はありません。
- スピーカーグループに音声を送信する
  ワンクリックで多くのスピーカーに音声を送信します。
- 音声クリップの管理
  音声クリップを簡単に管理できます。
- スピーカーを使用した迅速なアクション
  アラーム管理機能から離れることなく、アラームに迅速に対応できます。
- 複数のスピーカー間で音声を同期する
  音声システムをバックグラウンドミュージックに使用する場合、スピーカーマネージャーを使用して、スピーカー間の音声を同期するゾーンを設定できます (AXIS Audio Manager ProおよびEdgeモードの場合のみ)。

モード

スピーカーマネージャーは、さまざまなスピーカー設定に対応する3つの異なるモードをサポートしています。

- Pro、AXIS Audio Manager Proシステム向け
  大規模または高度な公共放送システム向けに設計された包括的なソフトウェアソリューションです。最大5,000台以上のスピーカーと500以上のゾーンに対応し、ライセンスや設置に関して柔軟な選択肢を提供しています。大規模なシステムや高度なスケジュール機能が必要なユーザーに推奨されます。
- Edge、AXIS Audio Manager Edgeシステム向け
  20ゾーンで最大200台のスピーカーを管理する効率的なソフトウェアソリューションです。Axisのネットワークスピーカーに直接組み込まれており、サーバーや追加のライセンスは不要です。高度なスケジュール機能が必要ない小規模なシステムに推奨されます。
- レガシー
  レガシーモードでは、ネイティブスピーカーの統合により複数のスピーカーに音声を配信したり、音声クリップを再生したりします。同期放送には対応していません。同期放送が必要なく、個別のスピーカーを使用するシステムに推奨されます。

設定モード

このページに初めて入るとモードの選択を求められますが、モードはいつでも変更できます。各モードで行う設定は個別ですが、モードを切り替えても設定は保持されます。

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Speaker manager (スピーカーマネージャー)] に移動します。
2. [Mode (モード)] で、現在選択されているモードをクリックし、ポップアップウィンドウから希望のモードを選択します。
3. [Switch mode (モードの変更)] をクリックします。

AXIS Audio Manager Proモード

このモードは以下の手順に従って使用します。

- AXIS Audio Manager Proソフトウェアを、録画サーバーなどのサーバーマシンにインストールします。

- APIアクセスでAXIS Audio Manager Proのライセンスを取得し、設定します。
- オプション:Webインターフェースのサーバー証明書を設定します。*証明書*を参照してください。
- VMSサーバーマシンにインストールされている場合は、ポート443からAXIS Audio Manager Proサーバーを変更します。

このモードは、スピーカーの接続やVMSのライセンス取得を必要としませんが、AXIS Audio Manager Proサーバーへの接続用のハードウェアが自動的に作成されます (VMSデバイスライセンスが1つ必要です)。AXIS Audio Manager Proの詳細については、*AXIS Audio Manager Proユーザーマニュアル*を参照してください。

注

AXIS Audio Manager Proモードは、シングルローカルサイトでのサポートに限定されています。マルチサイト、フェデレーテッド、および相互接続されたサイトアーキテクチャは、この統合の範囲外です。

ProモードでAXIS Audio Manager Proサーバーに接続する

1. Management Clientで、[**Site Navigation**] > [**AXIS Optimizer**] > [**Speaker manager (スピーカーマネージャー)**] に移動します。
2. [**Connect (接続)**] をクリックします。
3. ダイアログで、次のように実行します。
   - AXIS Audio Manager Proサーバーハードウェアを追加する録画サーバーを選択します。
   - AXIS Audio Manager ProサーバーのアドレスとHTTPSポートを入力します。
   - APIのユーザー名とパスワードを入力します (AXIS Audio Manager ProサーバーでAPIアクセスを有効にする必要があります)。
   - [**Connect (接続)**] をクリックします。

利用可能なすべての送信先とゾーンは、AXIS Audio Manager Proの左側に表示されています。[**AXIS Audio Manager Pro server (AXIS Audio Managerサーバー)**] をクリックすると、右側にAXIS Audio Manager ProサーバーのWebインターフェースが表示されます。

注

Webインターフェースにアクセスするには、Management ClientマシンとAXIS Audio Manager Proサーバー間の直接接続が必要です。

AXIS Audio Manager Proのwebインターフェースで、ゾーン、送信先、音声クリップ、またはビジュアルプロファイルに変更を加えた場合:

- [**Site Navigation (サイトナビゲーション)**] > [**AXIS Optimizer**] > [**Speaker manager (スピーカーマネージャー)**] に移動します。
- [**Update (更新)**] をクリックします。

カメラを送信先またはゾーンに関連付ける

カメラを特定の送信先またはゾーンに関連付けて、Smart Clientのカメラビューで直接使用することができます。

1. Management Clientで、[**Site Navigation (サイトナビゲーション)**] > [**AXIS Optimizer**] > [**Speaker manager (スピーカーマネージャー)**] に移動し、送信先またはゾーンを選択します。
2. [**Associated camera(s) (関連付けられたカメラ)**] で [**Add cameras... (カメラの追加)**] をクリックし、送信先またはゾーンに関連付けるカメラを選択します。

カメラが送信先またはゾーンに関連付けられると、Smart Clientのカメラビューのツールバーに が表示されます。

ビジュアルプロファイルを作成する

- Management Clientで、[Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Speaker manager (スピーカーマネージャー)] に移動します。
- [Audio Manager Pro server (Audio Manager Proサーバー)] をクリックして、webインターフェースを表示します。
- [Visual profiles (ビジュアルプロファイル)] をクリックして、ビジュアルプロファイルを作成または編集します。

ビジュアルプロファイルの詳細については、*AXIS Audio Manager Proユーザーマニュアル*を参照してください。

AXIS Audio Manager Edgeモード

AXIS Audio Manager Edge は、ほとんどのAxisスピーカーにプリインストールされており、このモードを選択すると自動的に検出されます。AXIS Audio Manager Edgeモードが正常に動作するには、サイトリーダー、ページングソース用の中間デバイス、スタンドアロン型スピーカーをVMSに追加する必要があります。

注

AXIS Audio Manager Edgeモードでは、カメラの内蔵音声出力やその他の互換性のない音声装置は使用できません。

AXIS Audio Manager Edgeの詳細については、*AXIS Audio Manager Edgeユーザーマニュアル*を参照してください。

AXIS Audio Manager Edgeモードでのスピーカーとゾーンの設定

音声クリップを再生してライブで話す場合は、まずゾーンのページングをオンにする必要があります。

1. Management Clientで、[Site Navigation (サイトナビゲーション)] > [Devices (デバイス)] > [Speakers (スピーカー)] に移動し、デバイスグループの追加、デバイスグループに対するスピーカーの追加・削除を行います。
2. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Speaker manager (スピーカーマネージャー)] に移動し、Edgeモードが選択されていることを確認します。次に、スピーカーマネージャーがVMSシステム内のすべてのスピーカーを検索し、Smart Clientで使用できるすべてのAXIS Audio Manager Edgeサイトとゾーンを表示します。
3. サイトリストで、ページングオフのゾーンを選択します。
4. [Turn on paging for the zone. (ゾーンのページングをオンにする)] を選択します。

ゾーンまたはページングソースに変更を加えた場合:

5. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Speaker manager (スピーカーマネージャー)] に移動します。
6. [Update (更新)] をクリックします。

注

設定が失敗した場合は、AXIS Audio Manager Edgeの設定を確認して再試行してください。



カメラをスピーカーまたはゾーンに関連付ける

特定のスピーカーまたはゾーンをSmart Clientのカメラビューで直接使用するために、それらをカメラに関連付けることができます。

1. Management Clientで、[Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Speaker manager (スピーカーマネージャー)] に移動し、スピーカーまたはゾーンを選択します。
2. [Associated cameras (関連付けられたカメラ)] 画面で [+ Add cameras (カメラの追加)] をクリックし、スピーカーまたはゾーンを関連付けるカメラを選択します。

カメラがスピーカー、デバイスグループ、またはゾーンに関連付けられると、Smart Clientのカメラビューのツールバーに が表示されます。

スピーカーにオーディオクリップをアップロードする

Smart Clientからスピーカーまたはゾーンで音声クリップを再生するには、まず、Management Clientで音声クリップをスピーカーにアップロードする必要があります。

1. スピーカーにアップロードする音声クリップをデフォルトのフォルダーC:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect - Audio Clips\に配置します。
2. Management Clientで、[Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Speaker manager (スピーカーマネージャー)] に移動し、スピーカーまたはゾーンを選択します。
3. [Audio clips (音声クリップ)] に移動し、スピーカーにアップロードするクリップの前にある [+] をクリックします。

レガシーモード

レガシーモードは、VMSに追加されたAxisスピーカーやその他の音声対応Axisデバイスのネイティブ機能を拡張します。他のモードとは異なり、レガシーモードでは複数のスピーカーへの同期ブロードキャストには対応していません。

レガシーモードでスピーカーを設定する

1. Management Clientで、[Site Navigation (サイトナビゲーション)] > [Devices (デバイス)] > [Speakers (スピーカー)] に移動し、デバイスグループの追加、デバイスグループに対するスピーカーの追加・削除を行います。
2. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Speaker manager (スピーカーマネージャー)] に移動し、レガシーモードが選択されていることを確認します。
3. をクリックします。
   3.1. [Manage Side Panel (サイドパネルの管理)] ウィンドウで、Smart Clientに表示するスピーカーを選択します。
   3.2. [Add (追加)] をクリックし、[OK] をクリックします。
   [Visible (表示)] パネルのスピーカーがSmart Clientに表示されるようになり、スピーカーにアクセスできるすべてのユーザーが表示されます。
4. スピーカーを削除するには、以下の手順に従います。
   4.1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Speaker manager (スピーカーマネージャー)] に移動し、 をクリックします。
   4.2. [Manage Side Panel (サイドパネルの管理)] ウィンドウで、削除するスピーカーを選択します。
   4.3. [Remove (削除)] をクリックし、[OK] をクリックします。

カメラをスピーカーまたはスピーカーグループに関連付ける

カメラを特定の送信先またはゾーンに関連付けて、Smart Clientのカメラビューで直接使用することができます。

1. Management Clientで、**[Site Navigation (サイトナビゲーション)]** > **[AXIS Optimizer]** > **[Speaker manager (スピーカーマネージャー)]** に移動し、スピーカーまたはスピーカーグループを選択します。
2. **[Associated camera(s) (関連付けられたカメラ)]** で **[Add cameras... (カメラの追加)]** をクリックし、スピーカーまたはスピーカーグループに関連付けるカメラを選択します。

カメラがスピーカーまたはスピーカーグループに関連付けられると、Smart Clientのカメラビューのツールバーに が表示されます。

スピーカーにオーディオクリップをアップロードする

Smart Clientからスピーカーまたはゾーンで音声クリップを再生するには、まず、Management Clientで音声クリップをスピーカーにアップロードする必要があります。

1. スピーカーにアップロードする音声クリップをデフォルトのフォルダー**C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect - Audio Clips**に配置します。
2. Management Clientで、**[Site Navigation (サイトナビゲーション)]** > **[AXIS Optimizer]** > **[Speaker manager (スピーカーマネージャー)]** に移動し、スピーカーまたはスピーカーグループを選択します。
3. **[Audio clips (音声クリップ)]** に移動し、スピーカーにアップロードするクリップの前にある [+] をクリックします。



音量の変更

スピーカーの音量を変更するには、以下の手順に従います。

1. Management Clientで、**[Site Navigation (サイトナビゲーション)]** > **[Speaker manager (スピーカーマネージャー)]** に移動し、スピーカーまたはスピーカーグループを選択します。
2. **[Volume (音量)]** に移動し、必要な音量に調整します。



スピーカーでの音声の再生

1. Smart Clientで、**[Live (ライブ)]** > **[MIP plug-ins (MIPプラグイン)]** > **[Axis speaker control (Axisスピーカーコントロール)]** に移動し、ドロップダウンリストでスピーカーまたはゾーンを選択します。

2. マイクからスピーカーに音声が送信されるようにする:
   2.1. を押しながら話します。
   マイクレベルメーターに音声アクティビティが表示されていることを確認します。
3. スピーカーで音声クリップを再生する:
   3.1. [Media clip (メディアクリップ)] に移動し、ドロップダウンリストから音声クリップを選択します。
   3.2. 選択したスピーカーで音声クリップの再生を開始するには、再生をクリックします。

カメラビューでスピーカーから音声を再生する

1. Smart Clientで、カメラビューに移動します。
2. スピーカー、装置グループ、ゾーンへの関連付けがある場合、ツールバーに が表示されます。
3. をクリックして、[Axis speaker control (Axisのスピーカーコントロール)] ウィンドウを開きます。
4. マイクからスピーカーに音声が送信されるようにする:
   4.1. を押しながら話します。
   マイクレベルメーターに音声アクティビティが表示されていることを確認します。
5. スピーカーで音声クリップを再生する:
   5.1. [Media clip (メディアクリップ)] に移動し、ドロップダウンリストから音声クリップを選択します。
   5.2. 選択したスピーカーで音声クリップの再生を開始するには、再生をクリックします。

アラームでスピーカーから音声を再生する

1. Smart Clientで、[Alarms (アラーム)] に移動します。
2. カメラをソースとするアラームを選択します。
スピーカーまたはゾーンに関連付けられている場合、スピーカーコントロールが表示されます。
3. マイクからスピーカーに音声が送信されるようにする:
   – を押しながら話します。
   マイクレベルメーターに音声アクティビティが表示されていることを確認します。
4. スピーカーで音声クリップを再生する:
   – [Media clip (メディアクリップ)] に移動し、ドロップダウンリストから音声クリップを選択します。
   – 選択したスピーカーで音声クリップの再生を開始するには、再生をクリックします。

スピーカーインタラクションのビジュアル挙動を設定する

Smart Clientでは、Axis speaker control (Axisスピーカーコントロール) で、またはカメラビューから直接、あるいはAlarm Manager (アラームマネージャ) でデバイスのビジュアル挙動を設定することができます。

注

ビジュアルプロファイルは、AXIS Audio Manager Proモードでのみサポートされています。

- [Axis speaker control (Axisスピーカーコントロール)] サイドパネルで、

  - をクリックします。
  - ドロップダウンリストからビジュアルプロファイルを選択します。
  - 選択したビジュアルプロファイルに関連付けられている現在のテキストを上書きする場合は、テキストボックスに入力します。
- カメラビューで:
  - 特定のカメラビューに移動します。
  - スピーカー、装置グループ、ゾーンへの関連付けがある場合、ツールバーに が表示されます。
  - をクリックして、[Axis speaker control (Axisのスピーカーコントロール)] ウィンドウを開きます。
  - をクリックします。
- Alarm Manager (アラームマネージャ) で、
  - イベントを選択し、カメラビューに移動して、をクリックします。

カメラビューまたはアラームの音声クリップブックマーク

カメラビューまたはアラームのスピーカーコントロールから音声クリップを再生すると、誰がどのデバイスで音声クリップを再生したかの情報を含むブックマークが作成されます。

音声クリップのブックマークを検索するには、以下の手順に従います。

1. Smart Clientで、[Search (検索)] に移動します。
2. 時間の間隔と1台または複数のカメラを選択します。
3. [Search for (検索)] > [Bookmarks (ブックマーク)] > [New search (新規検索)] をクリックします。

訪問者の管理

インターカムプラグイン

Axisネットワークインターカムは、通信からビデオ監視、リモート入場管理を1台の装置で実行します。AXIS Optimizerを使用すると、VMSと連携してAxisインターカムを簡単に設定し、使用できるようになります。たとえば、呼び出しに応答し、ドアのロックを解除する設定などです。

インターカムの設定



通常、ドアロックはインターカムの最初の中継器に接続する必要があります。AXIS Optimizerは、[Usage (使用)] の情報に基づいて、使用する出力ポートを決定します。[Usage = Door (使用 = ドア)] の最初のポート (デフォルトではRELAY1) を使用します。

注

要件

- Axisインターカム
- 呼び出しを受け取るPCにインストールされたマイク
- Smart Clientの稼働と運用

注

バージョン5.0.X.X以降、AXIS Optimizerは以前のバージョンとは異なる方法を使用してVMS内のインターカムを設定します。メタデータデバイスは入力1の代わりに通話検知に使用できます。従来の設定方法は引き続きサポートされていますが、新規インストールについては新しい設定方法をお勧めします。

1. 呼び出しを受信し、そこからドアを制御する各クライアントに、最新バージョンのAXIS Optimizerをインストールします。
2. Management Clientにログインします。
3. Axisインターカムを録画サーバーに追加します。
4. Management Clientで、必要なすべての装置を有効にします。Smart Clientで呼び出しを受けるには、以下が必要です。
   - カメラ1
   - マイク
   - スピーカー
   - Metadata (メタデータ):
   - 入力2 (ポート2のインターカムにセキュリティ中継器が接続されている場合はオプションとなります)
   - ドアに接続された出力。ドアに接続されている出力が分かっている場合は、その出力を選択します。分からない場合はすべての出力を選択します。
5. [Site Navigation (サイトナビゲーション)] > [Devices (装置)] > [Metadata (メタデータ)] を開き、設置するインターカムのメタデータ装置を指定します。
6. [Settings (設定)] をクリックします。
7. [イベントデータ] を [はい] に設定します。
8. [Save (保存)] をクリックします。
9. [Input 2 (入力2)] を有効にしている場合は、[Input 2 (入力2)] も設定する必要があります。
   9.1. [Site Navigation (サイトナビゲーション) > [Devices (装置)] > [Input (入力)] に移動し、Input 2を選択します。
   9.2. [Events (イベント)] をクリックしてから、[Add (追加)] をクリックします。
   9.3. [Input Falling event (入力下降イベント) を選択し、有効な入力に追加します。[Input Rising event (入力上昇イベント)] についても同様の手順を繰り返します。
   9.4. [Save (保存)] をクリックします。
10. 特定の役割に対する権限の設定については、*インターカムの権限を設定する, on page 40*を参照してください。
11. *テスト呼び出しを実行する, on page 41*.

インターカムの権限を設定する

呼び出しを処理するには、まず権限を有効にする必要があります。

1. [Site Navigation (サイトナビゲーション)] > [Security (セキュリティ)] > [Roles (役割)] に移動します。
2. 役割を選択します。
3. [Overall Security (全般的なセキュリティ)] に移動します。

4. 各セキュリティグループに必要な権限が設定されていることを確認します。[Hardware (ハードウェア)] に移動し、[Driver commands (ドライバーコマンド)] を選択します。
5. システムレベルで権限を設定するには、[Overall Security (全体的なセキュリティ)] に移動します。
   装置レベルで権限を設定するには、[Device (装置)] に移動します。
6. セキュリティグループの権限を設定します。
   6.1. [Cameras (カメラ)] を開きます。[Read (読み取り)] と [View live (ライブの表示)] を選択します。
   6.2. [Microphones (マイク)] を開きます。[Read (読み取り)] と [Listen (聞く)] を選択します。
   6.3. [Overall Security (総合セキュリティ)] で [Speakers (スピーカー)] を開きます。[Read (読み取り)] と [Speak (話す)] を選択します。
   [Device (装置)] で、[Speakers (発言者)] を開き、[Read (読み取り)] を選択します。次に [Speech (発言)] タブを開き、[Speak (話す)] を選択します。
   6.4. [Metadata (メタデータ)] を開きます。[Read (読み取り)] と [Live (ライブ)] を選択します。
   6.5. [Input (入力)] を開きます。[Read (読み取り)] を選択します。
   6.6. [Output (出力)] を開きます。[Read (読み取り)] と [Activate (有効化)] を選択します。

特定のインターカムからの呼び出しを処理するオペレーターの制御権限を割り当てる方法は次のとおりです。

1. 対象のインターカムのメタデータ装置1について、[Read (読み取り)] 権限を選択します。
2. 他のすべての役割に対してこの権限をクリアします。権限がないユーザーは呼び出しを受信できません。

呼び出し履歴を表示するには、追加の権限が必要です。

1. システムレベルで権限を設定するには、[Overall Security (全体的なセキュリティ)] に移動します。
   装置レベルで権限を設定するには、[Device (装置)] に移動します。
2. 各セキュリティグループの次の権限を選択します。
   2.1. [Cameras (カメラ)] を開きます。[Playback (再生)] と [Read sequences (シーケンスの読み取り)] を選択します。
   2.2. [Microphones (マイク)] を開きます。[Playback (再生)] と [Read sequences (シーケンスの読み取り)] を選択します。
   2.3. [Speakers (スピーカー)] を開きます。[Listen (聞く)]、[Playback (再生)]、および [Read sequences (シーケンスの読み取り)] を選択します。

テスト呼び出しを実行する

1. Smart Clientで、[Settings (設定)] > [Axis intercom options (Axisインターカムのオプション)] を開きます。
2. [Test call (呼び出しのテスト)] をクリックします。
3. インターカムを選択し、[Make call (呼び出す)] をクリックします。

呼び出し中のエコー防止

Push-To-Talk機能の使用中は、インターカムを通じて一度に1方向のみ音声通信できます。通話中にエコーが発生する場合は、Push-To-Talkをオンにできます。

Push-To-Talkをオンにする手順は次の通りです。

- Smart Clientで、[Settings (設定)] > [Axis intercom options (Axisインターコムのオプション)] に移動します。
- [Call (呼び出し)]] に移動し、[Push-to-talk] を選択します。

ライブビューからインターカムを制御する

各インターカムとインターカムビューで



をクリックして、装置をすばやく制御します。

方法について	手順	コメント
ロックを解除する	 > [Access (アクセス)] または [Extended access (拡張アクセス)] の順にクリックします。	ロックが解除された場合、[Access (アクセス)] または [Extended access (拡張アクセス)] をクリックできません。
ドアのロック/ロック解除状態を確認する	 をクリックして、メニュー最下部にあるステータスを確認します。	-

方法について	手順	コメント
インターカムの前にいる人と話す	 > [Start call (呼び出し開始)] の順にクリックします。	呼び出しウィンドウが開き、インターカムとの双方向通信が開始します。
前日に呼び出しした人物を特定する	 > [Call history (呼び出し履歴)] の順にクリックします。	インターカムの現在の呼び出しリストが表示されます。

ライブビューからの呼び出しに応答する

訪問者がインターカムの呼び出しボタンを押すと、動作中の各Smart Clientに呼び出しウィンドウが表示されます。呼び出しウィンドウは、ウィンドウのサイズを変更すると、コリドールビューやランドスケープビューなど、適切なカメラビューが自動的に選択されます。

方法について	手順	コメント
呼び出しに応答する	[Accept (同意)] をクリックします。	インターカムの近くにいる人物とオペレーター間の双方向の音声チャンネルが開きます。
ビジー状態のため、他のオペレーターを呼び出しする	[X] をクリックしてウィンドウを閉じる	呼び出しを却下すると、別のオペレータが別のクライアントで呼び出しを受けることができます インターカムは、誰かが電話に出るまで鳴り続け、点滅します。誰も応答しない場合、呼び出し履歴のステータスが missed (不在着信) となります。
映像による確認をした上でドアを開けたため、相手と話す必要がないため、呼び出しに応答しません	[Decline (拒否)] をクリックします。	呼び出しを拒否すると、他のクライアントで通話ウィンドウが自動的に閉じられます。

方法について	手順	コメント
不要な訪問者と話したくないので呼び出しを拒否します		他のオペレーターは呼び出しを実行できません。 インターカムが鳴動・点滅を停止し、呼び出しウィンドウが閉じます。呼び出し履歴のステータスは応答済みとなります。
ドアを開ける	[**Access (アクセス)**] をクリックします。	インターカムのロックが7秒間開きます。ドアが開いたままにする時間を設定するには、以下の手順に従います。 1. Smart Clientで、**[Settings (設定)] > [Axis intercom options (Axisインターカムのオプション)] > [Door access (ドアアクセス)]** を開きます。 2. [**Access time (アクセス時間)**] を変更します。
オペレーターからドインターカムへの音声を一時的に停止します。	[**Mute (ミュート)**] をクリックします。	-
Push-To-Talkを有効にして、訪問者に話しかけます。	[**Talk (話す)**] をクリックします。	[Talk (話す)] ボタンを離すと、訪問者が発した音声が聞こえます。
呼び出しを終了します。	[**Hang up (通話終了)**] をクリックします	デフォルトの自動終了設定では、通話を拒否するか通話を終了すると、呼び出しウィンドウが閉じます。 デフォルトの呼び出しウィンドウの動作を変更するには、以下の手順に従います。 1. Smart Clientで、**[Settings (設定)] > [Axis intercom options (Axisインターカムのオプション)] > [Call (呼び出し)]** を開きます。 2. [**Auto-close window (ウィンドウの自動クローズ)**] をクリアします。

呼び出しウィンドウに複数のカメラを表示する

呼び出しウィンドウに最大3台のカメラを同時に表示できます。同じ通話ウィンドウ内で、インターカムのビデオストリームと他の2つのカメラのビデオストリームを表示することができます。たとえば、配達員と納品ドア周辺を同時に確認する必要がある場合などに便利です。

呼び出しウィンドウで複数のカメラを設定するには、以下の手順に従います。

1. Smart Clientで、**[Settings (設定)]** > **[Axis intercom options (Axisインターカムのオプション)]** を開きます。**[Call (通話)]** > **[Intercom settings (インターカム設定)]** に移動します。
2. **[Selected device (選択中の装置)]** に移動し、設定する装置を選択します。
3. **[Multiple cameras (複数のカメラ)]** を開きます。通話ウインドウで**[camera 1 (カメラ1)]** として表示するインターカムを選択します。
4. インターカム呼び出しの通話ウィンドウで [**camera 2 (カメラ2)**]、[**camera 3 (カメラ3)**] として表示する関連付け済みのカメラを選択します。
5. **[Intercom settings (インターカム設定)]** ウインドウを閉じます。

呼び出しウィンドウのアクション

呼び出しウィンドウのアクションを使用すると、XProtectルールエンジンのルールに紐付けされたユーザー定義イベントを設定できます。設定および使用できるイベントは、ユーザーの役割により異なります。

呼び出しウインドウアクションの設定手順は次のとおりです。

1. Smart Clientで、**[Settings (設定)]** > **[Axis intercom options (Axisインターカムのオプション)]** を開きます。
2. **[Call (通話)]** > **[Intercom settings (インターカム設定)]** に移動します。
3. **[Selected device (選択中の装置)]** に移動し、設定する装置を選択します。
4. **[Call window actions (通話ウインドウのアクション)]** を開き、使用する呼び出しウインドウアクションを選択します。

呼び出しウィンドウアクションには、次の2つのタイプがあります。

- **アクセスボタンのアクション**:アクセスボタンのアクションを設定すると、**[Access (アクセス)]** ボタンのデフォルトのアクションが上書きされます。たとえば、**[Access (アクセス)]** ボタンで複数のドアを開錠する設定を実行することができます。
- **カスタムアクション**:カスタムアクションを設定すると、呼び出しウィンドウにボタンが表示されます。このボタンをクリックすることにより、カスタムアクションをトリガーできます。カスタムアクションには、電子メールの送信やアラームのトリガー、連続録画の開始など、ドアの開閉に関係ないアクションも設定できます。

呼び出しウィンドウにページを表示する

AXIS I8307-VE Network Intercomの使用中に呼び出しウィンドウにページを表示できます。これはインターコムの前に立っている人に地図や営業時間などの情報を表示するのに便利です。

まず、インターコムのWebインターフェースでこれらのページを設定します。*AXIS I8307-VE Network Intercom*を参照してください。

インターコムから呼び出しがあった場合:

1. **[Show page (ページを表示)]** をクリックし、デバイスに設定されたすべてのページのダイアログを確認します。
2. **[Load previews (プレビューの読み込み)]** をクリックして、すべてのページのプレビューを確認します。

設定したページのプレビューを確認するには、そのページにカーソルを合わせ、画像アイコンをクリックします。

3. 設定したページをクリックすると、インターコムにページが表示されます。

インターコムカメラのフィードとページの両方を異なる関連付けられたカメラを使用して表示するように呼び出しウィンドウを設定できます (カメラ1をカメラのフィード、カメラ2をページの表示)。*呼び出しウィンドウに複数のカメラを表示する, on page 46*を参照してください。

ページは呼び出しが終了すると閉じます。上記の手順を繰り返して、新規呼び出しのページを表示します。

呼び出し内線によるフィルタリング

デフォルトでは、インターカムに接続されているすべてのPCが呼び出しを受信します。VMSで呼び出し内線を追加してそれらでフィルタリングすることで、VMSシステム内の特定のスマートクライアントに呼び出しを転送するようにインターカムを設定できます。呼び出しを転送するスケジュールを設定できるほか、予備の連絡先を追加できます。呼び出しをSIPベースの連絡先に転送し、予備の連絡先として追加することも可能です。

インターコムのwebインターフェースで次の操作を行います。

1. **[Communication (通信)]** > **[SIP]** を開きます。
2. [**Enable SIP (SIPの有効化)**] を選択します。
3. **[Save (保存)]** をクリックします。
4. **[Communication (通信)]** > **[Calls (呼び出し)]** を開きます。
5. **[Allow calls in the video management system (VMS) (ビデオ管理システムVMSで呼び出しを許可する)]** がオンになっていることを確認してください。
6. **[Communication (通信)]** > **[Contact list (連絡先リスト)]** に移動します。
7. **[Recipients (受信者)]** で、＋ をクリックして、新規の連絡先を追加します。新規の連絡先情報を入力し、[**Save (保存)**] をクリックします。複数の連絡先を追加できます。
   - [**SIP address (SIPアドレス)**] で、`VMS_CALL:<extension>`と入力します。`<extension>`は連絡先の内線名に置き換えてください (例: `ReceptionA`)。
   - この連絡先についてスケジュールを設定する場合は、連絡先の [**Availability (対応時間)**] を選択します。
   - 設定された元の連絡先がいずれも応答しない場合に呼び出しを受信する予備の連絡先を、`ReceptionB`などのように追加できます。
8. **[Communication (通信)]** > **[Calls (呼び出し)]** を開きます。
9. バージョン11.6より前のAXIS OSを搭載した装置では、**[Make calls in the video management system (VMS) (ビデオ管理システムVSMで呼び出す)]** をオフにしてください。
10. **[Recipients (送信先)]** で、連絡先VMSを削除し、作成した新規連絡先を追加します。

マネジメントクライアントで：

通話検知にメタデータ装置を使用するようにVMS内のインターカムを設定することをお勧めします。*インターカムの設定, on page 39*を参照してください。

SMARTクライアントで：
呼び出しを受信する必要があるすべてのユーザーの呼び出し内線を設定します。設定は、ユーザーレベルで保存されます。つまり、ユーザーは使用するPCに関わらず呼び出しを受信します。

1. 呼び出しを受信するユーザーとしてSmart Clientにログインします。
2. [**Settings (設定)**] > [**Axis intercom options (Axisインターカムオプション)**] に移動します。

3. **[Call (呼び出し)] > [Call extension (呼び出し内線)]** で、連絡先の呼び出し内線名 (`ReceptionA`など) を入力します。これで、ユーザーは呼び出し内線がフィルター値と一致する場合にのみ呼び出しを受信するようになります。
   複数の呼び出し内線名を追加するには、`ReceptionA;ReceptionC`のようにセミコロンで区切ります。

呼び出し履歴の表示

呼び出し履歴では、応答された呼び出し、不在呼び出し、ドアのロック解除を表示できます。通話内容を選択し、対応する再生ビデオがある場合は、これを表示することができます。

1. Smart Clientで、インターカムのビューを開きます。
2. 
   > **[Call history (呼び出し履歴)]** の順にクリックします。

注

呼び出し履歴は39件、アクセスログは1,000件に制限されます。頻繁に通話をミュートにした場合、呼び出しの件数が少なくなる場合があります。

ドアのロック解除を登録するには、Axisインターカムに対して保存期間 (日数) を設定する必要があります。

1. Management Clientで、**[Tools (ツール)] > [Options (オプション)] > [Alarm and Events (アラームとイベント)] > [Event retention (イベントの保持)]** に移動します。
2. **Output Activated (出力の有効化)** と **Output Deactivated (出力の無効化)** の時間を設定します。

アクティブな呼び出しがない場合にマイクをオフにする

Axisインターカムに呼び出しが入ってこない場合は、マイクをオフにできます。アクティブな呼び出しがある場合は、マイクがオンになります。

注

- マイクをオフにするには、管理者権限が必要です。
- これは、フェデレーテッドアーキテクチャの場合、または予備の連絡先を使用する場合はサポートされていません。

1. Smart Clientで、**[Settings (設定)]** > **[Axis intercom options (Axisインターコムのオプション)]** に移動します。
2. **[Turn off door station microphone when no active call (アクティブな呼び出しがない場合に、インターカムのマイクをオフにする)]** を選択します。

ドアが強制的に開けられた場合にアラームを受け取る

ドアにセキュリティリレー (入力2) がある場合、Smart Clientの呼び出しウィンドウのドアオーバーレイに、ドアが開いた時間や閉じられた時間が表示されます。つまり、ドアをロックした状態で誰かがドアを強制的に開けた場合、アラームを受信することができます。

注

アラームを受信するには、少なくとも1つのSmart Clientが実行されている必要があります。

アラームを設定するには、以下の手順に従います。

1. Smart Clientで、**[Settings(設定)]** > **[Axis intercom options (Axisインターカムオプション)]** > **[Administrator options (管理者オプション)]** を開きます。
2. **[Trigger an alarm when a door has been forced open (ドアが強制的に開けられた際にアラームをトリガーする)]** を選択します。

ドアが長時間開いたままの場合にアラームを受信する

ドアにセキュリティリレー (入力2) がある場合、Smart Clientの呼び出しウィンドウのドアオーバーレイに、ドアが開いた時間や閉じられた時間が表示されます。誰かがドアを開け、ドアが長時間開いたままになっている場合に、アラームを受け取ることができます。

注

アラームを受信するには、少なくとも1つのSmart Clientが実行されている必要があります。

アラームを設定するには、以下の手順に従います。

1. Smart Clientで、**[Settings(設定)]** > **[Axis intercom options (Axisインターカムオプション)]** > **[Administrator options (管理者オプション)]** を開きます。
2. **[Trigger an alarm when a door has been open longer than (s) (ドアが (秒) 以上開いている場合にアラームをトリガーする)]** を選択します。
3. アラームが鳴るまでにドアが開けた状態にできる時間を入力します。

クライアントが呼び出しを受信できないようにする

クライアントの設定をすることで、呼び出しを受信できないようにします。誰かが呼び出しを行った場合でも、特定のクライアントで呼び出しウィンドウが開きません。

1. Smart Clientで、**[Settings (設定)]** > **[Axis intercom options (Axisインターカムのオプション)]** > **[Call (呼び出し)]** を開きます。
2. **Receive calls on this client (このクライアントで呼び出しを受信する)]** をオフにします。

音声の視覚化

マイクビュー

Smart Clientに1つ以上のマイクビューを追加して、システム内の音声を視覚化することができます。これにより、ライブビューと再生の両方で音声を監視できます。Axis装置に内蔵された音声検知機能により、音声レベルが特定のレベルを超えたときにそれがわかります。一般的な使用事例は次のとおりです。

- *複数のマイクを同時に聞く, on page 51*
- *音声によるインシデントの検知, on page 51*
- *発生後にインシデントを調査する, on page 52*

注

要件

- VMS Smart Client 2020 R2以降。

VMSをマイクビュー向けに設定する

1. 検知レベルを設定する:
   1.1. Management Clientで、[Site Navigation > AXIS Optimizer > Device assistant (サイトナビゲーション > AXIS Optimizer > 装置アシスタント)] に移動し、装置を選択します。
   1.2. [Detectors (検知)] の設定を開きます。これらの設定を開く方法は、装置のソフトウェアのバージョンによって異なります。
   1.3. [Audio detection (音声検知)] に移動し、[Input 1 sound level (入力1のサウンドレベル)] をニーズに合わせて変更します。
2. カメラからのイベントをVMSに取得する:
   2.1. Management Clientで、[Site Navigation > Devices > Microphones (サイトナビゲーション > 装置 > マイク)] に移動します。
   2.2. マイクをクリックし、[Events (イベント)] をクリックします。
   2.3. [Audio Falling (音声下降)] および [Audio Rising (音声上昇)] イベントを追加します。
3. 次のように、検知された音声に関するメタデータをシステムが保持する時間を設定します。
   3.1. [Tools > Options > Alarm and Events > Device events (ツール > オプション > アラームとイベント > 装置イベント)] に移動します。
   3.2. [Audio Falling (音声下降)] を見つけ、保存期間を設定します。
   3.3. [Audio Raising (音声上昇)] を見つけ、保存期間を設定します。
4. 音声の録音を設定していることを確認します。音声を常に録音することも、音声上昇または音声下降イベントに基づいて録音ルールを作成することもできます。
5. マイクビューで使用するマイクごとに、上記の手順を繰り返します。
6. Smart Clientで、[Settings > Timeline > Additional data (設定 > タイムライン > その他のデータ)] に移動し、[Show (表示)] を選択します。

Smart Clientにマイクビューを追加する

1. Smart Clientを開き、[Setup (設定)] をクリックします。
2. [Views (ビュー)] に移動します。
3. [Create new view (新しいビューの作成)] をクリックし、形式を選択します。
4. [System overview > AXIS Optimizer (システムの概要 > AXIS Optimizer)] を開きます。

5. [Microphone view (マイクビュー)] をクリックし、ビューにドラッグします。
6. マイクを選択します。
7. [Setup (設定)] をクリックします。

マイクビューの使用

- ライブビュー
  - 音声レベルは棒グラフとして表示され、右側に現在のレベル、左側に動く最大60秒の音声履歴が表示されます。
  - ビュー内をクリックして、マイクからの音声を聞きます。
  - 各マイクビューにはヘッドフォンアイコンがあります。このアイコンをクリックすると、ビュー自体を選択せずに各ビューからの音声をミュートまたはミュート解除できます。これにより、複数のマイクを同時に聞くことができます。
- 再生
  - マイクに利用可能な検知された音声があると、アイコンがハイライト表示されます。
  - 黄色のバーは、装置に設定した検知レベルに従って音声が検知されたことを示します。
  - ビュー内をクリックして、マイクからの音声を聞きます。
  - 各マイクビューにはヘッドフォンアイコンがあります。このアイコンをクリックすると、ビュー自体を選択せずに各ビューからの音声をミュートまたはミュート解除できます。これにより、複数のマイクを同時に聞くことができます。

複数のマイクを同時に聞く

マイクビューを使用すると、ライブビューと再生の両方で複数のマイクを同時に聞くことができます。

1. *VMSをマイクビュー向けに設定する, on page 50*.
2. Smart Clientを開き、[Setup (設定)] をクリックします。
3. [Views (ビュー)] に移動します。
4. [Create new view (新しいビューの作成)] をクリックし、分割ビューを選択します。
5. [System overview > AXIS Optimizer (システムの概要 > AXIS Optimizer)] を開きます。
6. 聞きたいマイクごとに、以下の操作を行います。
   6.1. [Microphone view (マイクビュー)] をクリックし、ビューにドラッグします。
   6.2. マイクを選択します。
7. [Setup (設定)] をクリックします。
8. マイクごとに、各マイクビューのヘッドフォンアイコンをクリックして、マイクをミュートするかミュート解除するかを決定します。これで、ミュート解除されたすべてのマイクを同時に聞くことができます。

音声によるインシデントの検知

トイレなど、カメラの設置が許可されていないエリアからのアクションを監視したいことがあります。マイクビューでは、インシデントが発生したとき、つまり音声レベルが検知レベルを超えたときにすぐにわかります。

1. *VMSをマイクビュー向けに設定する, on page 50*.監視する装置とエリアに関連する検知レベルを忘れずに設定してください。
2. マイクビューを装置と共にSmart Clientのライブビューに追加します。*Smart Clientにマイクビューを追加する, on page 50*を参照してください。

発生後にインシデントを調査する

インシデントが発生した後、再生タイムラインでマイクで音声が検知された期間をすばやく特定できます。

1. *VMSをマイクビュー向けに設定する, on page 50*.
2. Smart Clientで再生するには、関連する装置が含まれる1つ以上のマイクビューを追加します。*Smart Clientにマイクビューを追加する, on page 50*を参照してください。

フォレンジック検索

AXIS Optimizerでは、一元検索でAxis装置に関する以下の4つの検索カテゴリを利用できます。

- *フォレンジック検索, on page 53* (物体検索)
- *車両検索, on page 56*
- *ゾーン速度検索, on page 59*
- *コンテナ検索, on page 61*

Smart Clientに別のナンバープレート検索タブを追加することもできます。*Axisナンバープレート, on page 63*を参照してください。

これらの検索カテゴリは、集中パネルで設定できます。*Axis検索カテゴリの設定, on page 111*を参照してください。

フォレンジック検索

AXIS OS 9.50以降を搭載したAxisカメラは、カメラの視野内で現在移動しているすべての物体を説明するメタデータを生成します。VMSは、このデータを対応するビデオおよび音声と共に記録できます。AXIS Optimizerの分析検索機能を使用すると、このデータを解析・検索できます。フォレンジック検索を使用して、シーンでのすべての活動の概要を把握したり、関心のある特定のオブジェクトやイベントをすばやく検索することができます。

開始する前に

1. カメラに搭載されているAXIS OSが最新バージョンであることを確認してください。
2. VMSのバージョンが正しいことを確認してください。
   - Corporate 2019 R3以降、またはExpert 2019 R3以降
   - Professional+ 2022 R3以降、またはExpress+ 2022 R3以降
3. カメラの時刻はNTPで同期されている必要があります。
4. 物体タイプ (**人**、**車両**、**バイク**、**バス**、**自動車**、**トラック**) でフィルタリングするには:
   4.1. AXIS Object Analyticsに対応しているAxisの装置を使用します。*プロダクトセレクターでAnalyticsフィルターを参照します。*
   4.2. **[System (システム)]** > **[Analytics metadata (Analyticsメタデータ)]** に移動し、カメラのWebページで **[Analytics Scene Description (Analyticsシーン説明)]** を有効にします。
5. **Vehicle color (車両の色)**、**Upper body clothing color (上の服の色)**、**Lower body clothing color (下の服の色)**でフィルタリングするには:
   5.1. AXIS Object Analyticsに対応しているAxisの装置を使用します。*プロダクトセレクターでAnalyticsフィルターを参照します。*
   5.2. ARTPEC-8またはCV25を搭載したAxisの装置を使用します。*プロダクトセレクターでシステムオンチップフィルターを参照します。*

フォレンジック検索の設定



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. Management Clientで、メタデータ装置がカメラで有効になっているかを確認します。
2. メタデータ装置がカメラに関連していることを確認します。
   - [Devices (デバイス)] > [Camera (カメラ)] に移動し、装置を選択します。
   - [Client (クライアント)] タブに移動し、[Related metadata (関連メタデータ)] でカメラのメタデータ装置が選択されていることを確認します。
3. [Site Navigation > Devices > Metadata (サイトナビゲーション > 装置 > メタデータ)] に移動します。
4. 装置を選択し、[Record (録画)] をクリックします。[Recording (録画)] が有効になっていることを確認します。
   デフォルトでは、VMSがシーン内の動きを検知した場合にのみ、メタデータが記録されます。物体の動きを見逃さないために、動きの閾値を環境に合わせて調整することをお勧めします。
5. [Settings (設定)] をクリックし、[Analytics data (分析データ)] が有効になっていることを確認します。
6. Smart Clientのライブビューを開き、オブジェクトの上に境界ボックスが表示され、ボックスが正しく表示されることを確認します。
   時計がNTP時間に適応するまでには、しばらく時間を要する場合があります。
7. ビデオとメタデータの記録には、少なくとも15分の待機が発生します。その後、検索を開始できます。*検索の実行, on page 54*を参照してください。
8. [Consolidated metadata (統合メタデータ)] をオンにすると、AXIS OS 11.10以降を実行している装置での検索の速度が向上します。「*メタデータと検索, on page 110*」を参照してください。

検索の実行



注

この検索機能を使用するには、Management Clientで設定する必要があります。これを行う方法については、*フォレンジック検索の設定, on page 53*を参照してください。

1. Smart Clientで、[Search (検索)] に移動します。
2. 時間の間隔と1台または複数のカメラを選択します。
3. [Search for > Forensic search > New search (検索 > フォレンジック検索 > 新規検索)] をクリックします。検索結果ごとに、オブジェクトとオブジェクトの移動経路がサムネイルで表示されます。
   - サムネイルには、物体が最も見やすかったときのビデオフレームが表示されます。
   - 緑色の点は、カメラが最初に物体を検出した場所を示しています。
   - 赤色の点は、カメラが最後に物体を検出した場所を示しています。
   - 検索結果の完全なビデオシーケンスを表示するには、その結果を選択し、プレビューパネルの [Play forward (再生)] をクリックします。
   - グラフィカルオーバーレイを非表示にする場合は、[Bounding boxes (境界ボックス)] に移動し、[Hide (非表示)] を選択します。

注

AXIS Object AnalyticsやAXIS Loitering Guardなど、カメラで実行される分析アプリケーションも、ビデオにオーバーレイを書き込む場合があります。これらのオーバーレイを削除するには、アプリケーションのWeb設定ページに移動してください。

4. 検索結果の数を絞り込むには、検索フィルターを選択します。
さまざまなフィルターの使用方法の詳細については、*検索を微調整する, on page 55*を参照してください。
5. 詳しく調査をする検索結果を選択します。たとえば、ブックマークを付ける、または *高品質なPDFレポートの作成, on page 62*。

検索を微調整する

検索結果の絞り込みには、1つ以上の検索フィルターを使用できます。

- [Region of interest (関心領域)]
特定のエリア内で移動した物体に絞り込みます。
- [Object direction (物体の向き)]
シーン内の特定のルートに沿って移動した物体に絞り込みます (左、右、下、または上方向)。
- 物体タイプ
特定のタイプの物体に絞り込みます (人、車両、バイク、バス、車、またはトラック)。

注

- 速度 (km/hまたはmph) およびナンバープレートは、AXIS Q1686–DLE Radar-Video Fusion Camera (レーダービデオ融合カメラ) でのみサポートされます。
- 使用する前に、速度 (km/hまたはmph) とナンバープレートをオンにする必要があります。これを行うには、*Axis検索カテゴリの設定, on page 111*を参照してください。
- Speed (km/h or mph) (速度 (km/hまたはmph))
特定の速度で移動している車両を検知します。
- ナンバープレート
特定のナンバープレートの車両を検知します。特定のアルファベットまたは数字を含むナンバープレートを検索するためにも使用できます。
- 車両の色
選択した色の車両に絞り込みます。
- Upper body clothing color (上の服の色)
選択した色の衣服を上半身に着用している人に絞り込みます。
- Lower body clothing color (下の服の色)
選択した色の衣服を下半身に着用している人に絞り込みます。
- [Time-of-day (時刻)]
1日の特定の時間帯で検知された物体に絞り込みます。このフィルターは、数日間に渡って検索を実行し、各日の特定の時間帯、たとえば午後の時間帯のオブジェクトに特化して調査する場合に有効です。
- Minimum time in scene (s) (シーン内の最小時間 (秒))
この秒数以上検知し、追跡した物体に絞り込みます。このフィルターは、たとえば遠くのオブジェクトや偽のオブジェクト (照明効果) など、関心の対象外となるオブジェクトをフィルタリングします。デフォルト値は1秒です。フィルターを設定しない場合、継続時間が1秒未満のオブジェクトは除外されます。
- Swaying objects (% of image) (揺らめいている物体 (%で指定))
たとえば、旗や木が風に吹かれて動くなど、制約のある領域でのみ動くオブジェクトを除外することができます。デフォルト値は5-100%です。つまり、フィルターが設定されていない場合は、画像領域内で5%以上移動しなかったオブジェクトを除外します。

制限事項

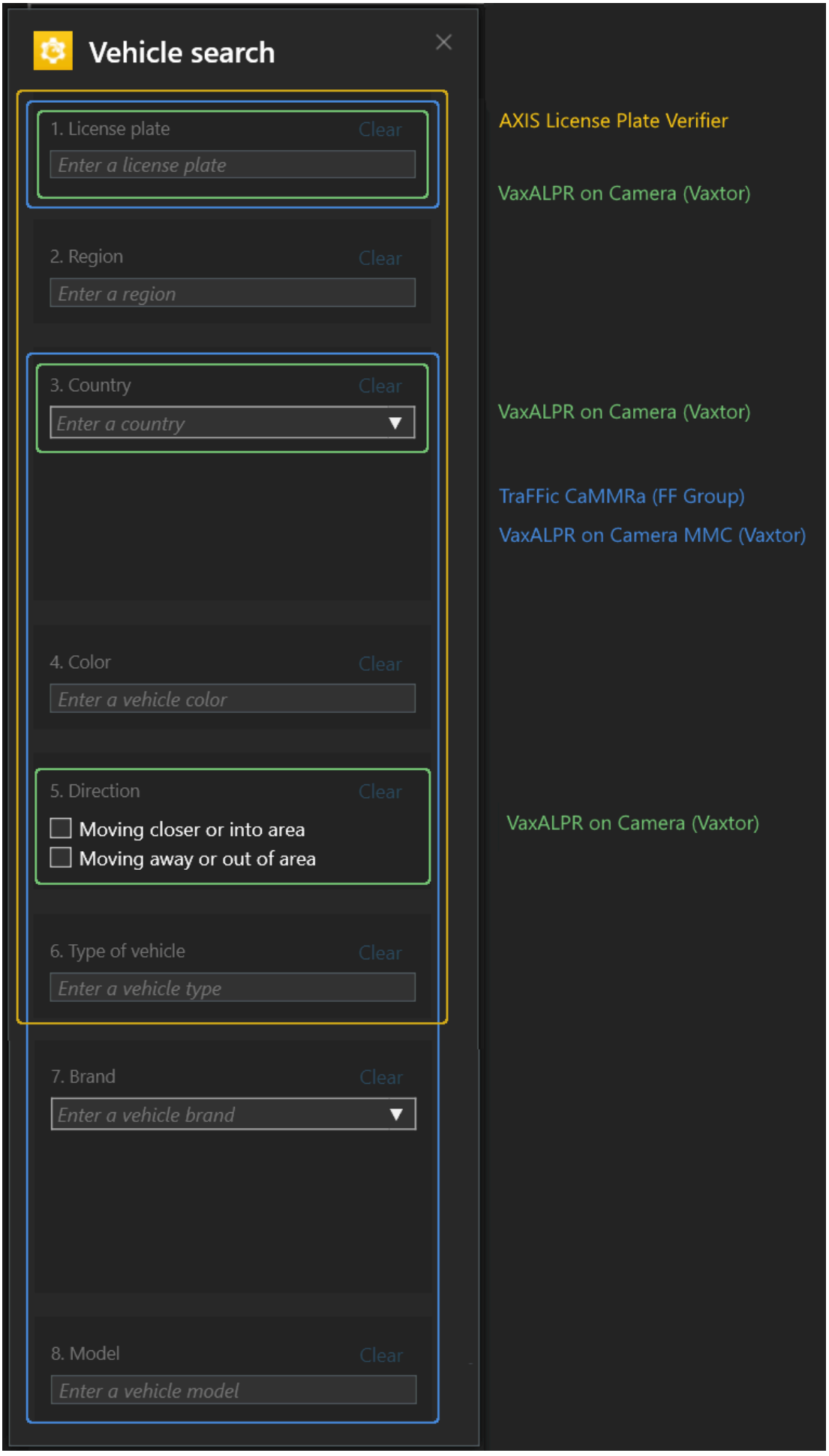
- 検索結果の正しいビデオ映像を取得するには、時刻の同期を正しくとることが重要です。
- フォレンジック検索プラグインで解析されたデータには、シーンの視点が考慮されません。つまり、物体のサイズと速度は、物体がカメラにどれだけ近いかによって異なります。
- 豪雨や豪雪などの気象条件により、検知精度が低下する場合があります。
- 低光量のシーンで物体のコントラストが良好であれば、分析はより正確になります。
- 状況によっては、1つの物体で複数の結果が生成される場合があります。たとえば、物体が別の物体によって一時的に隠されて追跡が失われた場合です。
- XProtectのバージョンにより、オーバーレイが異なる場合があります。例:ビデオプレビューのオーバーレイにはXProtect 2020 R3が、オーバーレイの色にはXProtect 2020 R2が必要です。
- 180度回転したビデオストリームに対してフォレンジック検索を実行するには、次の条件を満たしている必要があります。
  - カメラでAXIS OS 10.6以降を使用する、または
  - 録画サーバーでDevice Pack 11.0以降を使用する
- 適切な色検知を行うには、カメラのホワイトバランス設定が正確であることが必要です。

車両検索

AXIS Optimizerをカメラにインストールされた特定のアプリケーションと組み合わせて使用すると、車両に関する証拠ビデオを検索、識別、共有することができます。車両検索は、以下のアプリケーションによるナンバープレートデータに対応しています:

- Axis Communicationsが提供する*AXIS License Plate Verifier*
- *CAMMRA AI* by FF Group (バージョン1.3以上が必要)
- Vaxtor Recognition Technologiesが提供する*VaxALPR On Camera*
- Vaxtor Recognition Technologiesが提供する*VaxALPR On Camera MMC*

使用できる検索フィルターは、カメラにインストールされているアプリケーションによって異なります。詳細については、*検索を微調整する, on page 58*を参照してください。


Vehicle search
1. License plate
Clear
Enter a license plate
2. Region
Clear
Enter a region
3. Country
Clear
Enter a country
4. Color
Clear
Enter a vehicle color
5. Direction
Clear
Moving closer or into area
Moving away or out of area
6. Type of vehicle
Clear
Enter a vehicle type
7. Brand
Clear
Enter a vehicle brand
8. Model
Clear
Enter a vehicle model
AXIS License Plate Verifier
VaxALPR on Camera (Vaxtor)
VaxALPR on Camera (Vaxtor)
TraFFic CaMMRa (FF Group)
VaxALPR on Camera MMC (Vaxtor)
VaxALPR on Camera (Vaxtor)

車両検索を設定する

注

要件

- VMSシステム:
  - CorporateまたはExpert 2019 R3以降
  - Professional+またはExpress+ 2022 R3以降
- NTPと時刻同期されたカメラ
- に記載されているアプリケーションの1つ

1. Management Clientで、選択したアプリケーションを実行するカメラを追加します。
2. 必要なすべての装置を有効にします。AXIS License Plate Verifierを使用するには、カメラ1とメタデータ1が必要です。
3. メタデータ装置がカメラに関連していることを確認します。
   - **[Devices (デバイス)]** > **[Camera (カメラ)]** に移動し、装置を選択します。
   - **[Client (クライアント)]** タブに移動し、**[Related metadata (関連メタデータ)]** でカメラのメタデータ装置が選択されていることを確認します。
4. メタデータの設定:
   4.1. [**Site Navigation > Recording Server (サイトナビゲーション > 録画サーバー)**] に移動し、装置を検索します。
   4.2. メタデータ1を選択し、[**Settings (設定)**] をクリックします。
   4.3. [**Metadata stream > Event data (メタデータストリーム > イベントデータ)**] に移動し、[**Yes (はい)**] を選択します。
5. [**Record settings (録画の設定)**] タブに移動し、録画がメタデータに対して有効になっていることを確認します。
6. **[Save (保存)]** をクリックします。
7. 標準的なユーザーで動作するようにアプリケーションを設定する:
   7.1. 特定のカメラとユーザーに対して、読み取りと再生の権限を追加します。
   7.2. 特定のカメラとユーザーのメタデータに読み取りと再生の権限を追加します。

車両の検索

1. Smart Clientで、[**Search (検索)**] に移動します。
2. 時間の間隔と1台または複数のカメラを選択します。
3. [**Search for > Vehicle search > New search (検索 > 車両の検索 > 新規検索)** をクリックします。
4. 検索結果の数を絞り込むには、検索フィルターを選択します。
   さまざまなフィルターの詳細については、*検索を微調整する, on page 58*を参照してください。
5. 詳しく調査をする検索結果を選択します。たとえば、ブックマークを付ける、または *高品質なPDFレポートの作成, on page 62*。

検索を微調整する

検索結果の絞り込みには、1つ以上の検索フィルターを使用できます。アプリケーションによって、さまざまなフィルターオプションが利用できます。

- ナンバープレート
  特定のナンバープレート番号を検索します。
  アプリケーション：AXIS License Plate Verifier、VaxALPR On Camera, CAMMRA AI、またはVaxALPR On Camera MMC

- **地域**
  特定の地域の車両を検索します。
  アプリケーション：AXIS License Plate Verifier 2.9.19.

注

地域を正確に認識できるよう、Axis License Plate Verifierの設定でカメラの位置を設定します。

- **国名**
  特定の国の車両を検索します。
  アプリケーション：Axis License Plate Verifier 2.9.19、VaxALPR On Camera、CAMMRA AI、またはVaxALPR On Camera MMC。
- **カラー**
  特定の色の車両を検索します。
  アプリケーション：Axis License Plate Verifier 2.9.19、CAMMRA AI、またはVaxALPR On Camera MMC。
- **方向**
  特定の方向に移動する車両を検索します。
  アプリケーション：Axis License Plate Verifier 2.9.19、VaxALPR On Camera、CAMMRA AI、またはVaxALPR On Camera MMC。
- **Type of vehicle (車両の種類)**
  特定のタイプの車両を検索します。
  アプリケーション：Axis License Plate Verifier 2.9.19、CAMMRA AI、またはVaxALPR On Camera MMC。
- **ブランド**
  特定の銘柄の車両を検索します。
  アプリケーション：CAMMRA AI、またはVaxALPR On Camera MMC。
- **モデル**
  特定のモデルの車両を検索します。
  アプリケーション：CAMMRA AI、またはVaxALPR On Camera MMC。

検索速度の最適化

システムがVMSメタデータデバイスに保存するデータを管理することによって、検索速度を向上させることができます。

- 必要がない場合は、分析データを無効にします。
  - [**Devices (デバイス)**] > [**Metadata (メタデータ)**] に移動し、装置を選択します。
  - [**Settings (設定)**] をクリックし、[**Analytics data (分析データ)**] を無効にします。
- 分析データが必要な場合、利用可能であれば統合メタデータを使用することをお勧めします。「*メタデータと検索, on page 110*」を参照してください。
- AXIS License Plate Verifierで不要なイベントを無効にします。AXIS Optimizerを使用するには、**Lost**イベントのみが必要です。*AXIS License Plate Verifier*を参照してください。
- AXIS OS 12.8以降を使用してください。

ゾーン速度検索

AXIS Optimizerでは、ゾーン速度検索を使用して、カメラのビュー内の所定のゾーンに入ったときに検出された速度違反車両を検索することができます。ゾーン速度検索は、*AXIS Speed Monitor*と連携し、カメラのライブビューでレーダー検知ゾーン内の車両の速度を視覚化します。AXIS Zone speed searchを使用すると、特定のフィルターを設定して検索を絞り込み、調査中にビデオ証拠をエクスポートして共有できます。

ゾーン速度検索の設定

注

要件

- VMSシステム:
  - CorporateまたはExpert 2019 R3以降
  - Professional+またはExpress+ 2022 R3以降
- NTPと時刻同期されたカメラ

1. Management Clientで、選択したアプリケーションを実行するカメラを追加します。
2. 必要なすべての装置を有効にします。AXIS Zone速度検索を使用するには、カメラ1とメタデータ1が必要です。
3. メタデータ装置がカメラに関連していることを確認します。
   - **[Devices (デバイス)]** > **[Camera (カメラ)]** に移動し、装置を選択します。
   - **[Client (クライアント)]** タブに移動し、**[Related metadata (関連メタデータ)]** でカメラのメタデータ装置が選択されていることを確認します。
4. メタデータを設定するには:
   4.1. [**Site Navigation > Recording Server (サイトナビゲーション > 録画サーバー)**] に移動し、装置を検索します。
   4.2. メタデータ1を選択し、[**Settings (設定)**] をクリックします。
   4.3. [**Metadata stream > Event data (メタデータストリーム > イベントデータ)**] に移動し、[**Yes (はい)**] を選択します。
5. [**Record settings (録画の設定)**] タブに移動し、録画がメタデータに対して有効になっていることを確認します。
6. **[Save (保存)]** をクリックします。
7. 標準的なユーザーで動作するようにアプリケーションを設定:
   7.1. 特定のカメラとユーザーに対して、読み取りと再生の権限を追加します。
   7.2. 特定のカメラとユーザーのメタデータに読み取りと再生の権限を追加します。

ゾーン速度イベントの検索



1. Smart Clientで、[**Search (検索)**] に移動します。
2. 時間の間隔と1台または複数のカメラを選択します。
3. [**Search for > Zone speed search > New search (検索対象 > ゾーン速度検索 > 新規検索)**] をクリックします。
4. 検索結果の数を絞り込むには、検索フィルターを選択します。
   さまざまなフィルターの詳細については、*検索を微調整する, on page 60*を参照してください。
5. 詳しく調査をする検索結果を選択します。たとえば、ブックマークを付ける、または *高品質なPDFレポートの作成, on page 62*。

検索を微調整する

速度違反イベントの検索結果を絞り込むには、1つ以上の検索フィルターを使用できます。

- **最高速度**

イベント期間中にゾーン内の任意の物体の最大速度をフィルタリングします。最高速度の下限と上限の両方を設定できます。

- **物体タイプ**
  [**Vehicle (車両)**] を選択すると、ゾーン内の最速の物体が車両として分類される速度違反イベントのみが表示されます。
- **ゾーン名**
  名前でゾーンを検索およびフィルターします。

コンテナ検索

AXIS Optimizerを特定のアプリケーションと組み合わせて用すると、コンテナに関する証拠映像を検索、特定、共有することができます。コンテナ検索は、以下アプリケーションからのデータをサポートしています:

- Vaxtor Recognition Technologiesが提供する*VaxOCR コンテナ*

コンテナ検索の設定

注

要件

- VMSシステム:
  - CorporateまたはExpert 2019 R3以降
  - Professional+またはExpress+ 2022 R3以降
- NTPと時刻同期されたカメラ
- に一覧されているアプリケーション

1. Management Clientで、選択したアプリケーションを実行するカメラを追加します。
2. 必要なすべての装置を有効にします。
3. メタデータ装置がカメラに関連していることを確認します。
   - [**Devices (デバイス)**] > [**Camera (カメラ)**] に移動し、装置を選択します。
   - [**Client (クライアント)**] タブに移動し、[**Related metadata (関連メタデータ)**] でカメラのメタデータ装置が選択されていることを確認します。
4. メタデータの設定:
   4.1. [**Site Navigation > Recording Server (サイトナビゲーション > 録画サーバー)**] に移動し、装置を検索します。
   4.2. メタデータ1を選択し、[**Settings (設定)**] をクリックします。
   4.3. [**Metadata stream > Event data (メタデータストリーム > イベントデータ)**] に移動し、[**Yes (はい)**] を選択します。
5. [**Record settings (録画の設定)**] タブに移動し、録画がメタデータに対して有効になっていることを確認します。
6. [**Save (保存)**] をクリックします。
7. 標準的なユーザーで動作するようにアプリケーションを設定する:
   7.1. 特定のカメラとユーザーに対して、読み取りと再生の権限を追加します。
   7.2. 特定のカメラとユーザーのメタデータに読み取りと再生の権限を追加します。

コンテナの検索

1. Smart Clientで、[**Search (検索)**] に移動します。
2. 時間の間隔と1台または複数のカメラを選択します。
3. [**Search for > Container search > New search (検索 > コンテナ検索 > 新規検索)** をクリックします。

4. 検索結果の数を絞り込むには、検索フィルターを選択します。
さまざまなフィルターの詳細については、*検索を微調整する, on page 62*を参照してください。
5. 詳しく調査をする検索結果を選択します。たとえば、ブックマークを付ける、または *高品質なPDFレポートの作成, on page 62*。

検索を微調整する

検索結果の絞り込みには、1つ以上の検索フィルターを使用できます。すべてのフィルターオプションは、アプリケーションのVaxOCRコンテナーから取得されます。

- コンテナコード
特定のコンテナコードを検索します。
- オーナー
特定の所有者に属するコンテナを検索します。
- Owner code (所有者コード)
特定の所有者に属するコンテナを検索します。
- 大きさ
特定のサイズとタイプのコンテナを検索します。
- Size code (サイズコード)
特定のサイズとタイプのコンテナを検索します。
- City or country (都市または国)
特定の都市または国からコンテナを検索します。
- 検証
所有者コードまたはコントロールディジットを通じてすでに検証されているコンテナを検索します。

高品質なPDFレポートの作成



検索結果に基づいてレポートを作成します。この機能を使用すると、結果に高解像度の画像を含めることができます。

1. Smart Clientで、検索を実行します。
2. レポートに含める検索結果を選択します。
3. p,255mm,sfx)=″graphics:graphicF8543E623DBBE641C62ADEE8D132641F″ > [Create high quality PDF report (高画質のPDFレポートの作成)] の順にクリックします。
4. (オプション) [Report name (レポート名)]、[Report destination (レポートの送信先)]、[Notes (メモ)] を入力します。
5. 検索結果ごとに、レポートに含めるフレームを選択します。画像を拡大するには、ダブルクリックします。
6. [Create (作成)] をクリックします。レポートの準備が完了すると、通知が届きます。

Axisナンバープレート

Smart Clientで、ナンバープレートの検索および管理用の別のタブを追加できます。このタブは、LPR対応のAxisカメラが提供する情報に基づいて、ナンバープレートの管理、検索、エクスポートに関連するすべてのオペレータータスクを一元化します。



開始する前に

- VMSのバージョンが2018 R3以降であることを確認してください。
- VMS Device Packのバージョンが10.1以降であることを確認してください。
- カメラの時刻はNTPで同期されている必要があります。
- に記載されているアプリケーションの1つを使用します。

Axisナンバープレートの設定

1. Management Clientで、選択したアプリケーションを実行するカメラを追加します。
2. 必要なすべての装置を有効にします。AXIS License Plate Verifierを使用するには、カメラ1とメタデータ1が必要です。
3. メタデータ装置がカメラに関連していることを確認します。
   - [Devices (デバイス)] > [Camera (カメラ)] に移動し、装置を選択します。
   - [Client (クライアント)] タブに移動し、[Related metadata (関連メタデータ)] でカメラのメタデータ装置が選択されていることを確認します。
4. メタデータの設定:
   4.1. [Site Navigation > Recording Server (サイトナビゲーション > 録画サーバー)] に移動し、装置を検索します。
   4.2. メタデータ1を選択し、[Settings (設定)] をクリックします。
   4.3. [Metadata stream > Event data (メタデータストリーム > イベントデータ)] に移動し、[Yes (はい)] を選択します。
5. [Record settings (録画の設定)] タブに移動し、録画がメタデータに対して有効になっていることを確認します。
6. [Save (保存)] をクリックします。

ナンバープレートを検索する

1. Smart Clientで、[Axis license plates (Axisナンバープレート)] に移動します。
   タブが表示されていない場合は、[Settings > Axis search options (設定 > Axis検索オプション)] に移動し、[Show license plate tab (ナンバープレートタブの表示)] を選択します。
2. [Add camera... (カメラの追加...)] をクリックし、該当するカメラを選択して、[Close (閉じる)] をクリックします。
   カメラをシステムに追加できるのは管理者のみです。カメラによってナンバープレートが検出されると、カメラで撮影されたナンバープレートの切り抜き画像を含め、ナンバープレートがリストにリアルタイムで表示されます。検索結果には5,000件を超える結果は表示されません。

3. ナンバープレートとTime interval (時間間隔) を入力して、検索結果をフィルターします。
   – 選択した2つの日付を [Time interval (カスタム時間間隔)] に入力して、検索結果をフィルタリングします。

ナンバープレートのライブ検索

1. Smart Clientで、[Axis license plates (Axisナンバープレート)] に移動します。
   タブが表示されていない場合は、[Settings > Axis search options (設定 > Axis検索オプション)] に移動し、[Show license plate tab (ナンバープレートタブの表示)] を選択します。
2. [Add camera... (カメラの追加...)] をクリックし、該当するカメラを選択して、[Close (閉じる)] をクリックします。
   カメラをシステムに追加できるのは管理者のみです。カメラによってナンバープレートが検出されると、カメラで撮影されたナンバープレートの切り抜き画像を含め、ナンバープレートがリストにリアルタイムで表示されます。検索結果には5,000件を超える結果は表示されません。
3. ナンバープレートを入力し、[Time interval (時間間隔)] > [Live (ライブ)] を選択して、検索結果をフィルタリングします。

検索を微調整する

検索結果の絞り込みには、1つ以上の検索フィルターを使用できます。

- 時間間隔
  一定の時間内における検索ヒットをフィルタリングします。
- ナンバープレート
  部分的または完全なナンバープレートテキストをフィルタリングします。
- カメラ
  特定のカメラにより検知された検索ヒットをフィルタリングします。
- 方向
  特定の方向に移動する車両をフィルタリングします。
- Lists (リスト)
  特定のサイトにおける検索ヒットをフィルター処理し、許可リスト、ブロックリスト、カスタムリストにおける検索ヒットをフィルター処理します。リストを設定する方法については、*ナンバープレートリストを一元管理, on page 25*を参照してください。

検索速度の最適化

システムがVMSメタデータデバイスに保存するデータを管理することによって、検索速度を向上させることができます。

- 必要がない場合は、分析データを無効にします。
  – [Devices (デバイス)] > [Metadata (メタデータ)] に移動し、装置を選択します。
  – [Settings (設定)] をクリックし、[Analytics data (分析データ)] を無効にします。
- 分析データが必要な場合、利用可能であれば統合メタデータを使用することをお勧めします。「*メタデータと検索, on page 110*」を参照してください。
- AXIS License Plate Verifierで不要なイベントを無効にします。AXIS Optimizerを使用するには、Lostイベントのみが必要です。*AXIS License Plate Verifier*を参照してください。
- AXIS OS 12.8以降を使用してください。

ナンバープレート検索をPDFレポートとしてエクスポートする

この機能を使用して、関心のある検索結果を高画質の画像付きPDFレポートとしてまとめます。

1. [Export... (エクスポート...)] をクリックします。

2. [PDF...] を選択します。
3. (オプション) [Report name (レポート名)]、[Report destination (レポートの送信先)]、[Notes (備考)] を入力します。
4. 検索結果ごとに、レポートに含めるフレームを選択します。画像を拡大するには、その画像をダブルクリックします。
5. [Create (作成)] をクリックします。レポートの準備が完了すると、通知が届きます。

ナンバープレート検索をCSVレポートとしてエクスポートする

この機能を使用して、大量の検索結果をCSVレポートとしてまとめます。

1. [Export... (エクスポート...)] をクリックします。
2. [CSV...] を選択します。
3. エクスポートするファイルの保存先を選択します。

Axis insights

Axis insightsは、チャートとダッシュボードを通じて、装置からのデータの概要を提供します。これにより、すべての装置のメタデータを表示できます。検知された物体、識別された車両、アラームに関するデータを表示できます。ダッシュボードを新規作成し、他のユーザーと共有することもできます。

Axis insightsは、デフォルトの管理者ビューとオペレータビューで利用できます。Axis Insightsのデフォルト管理者ビューは管理者権限を持つユーザーのみが利用でき、デフォルトオペレータービューは適切な権限を持つすべてのオペレーターが利用できます。*役割設定の定義, on page 104* を参照してください。オペレータービューでは、設定した選択したカメラ ビューからの特定のデータが提供され、管理者ビューではシステム全体のオーバービューが提供されます。

Axis insightsへのアクセス

- [Smart Client] に移動し、[Axis insights] をクリックします。
- Dashboard (ダッシュボード):ドロップダウンリストからDashboard (ダッシュボード)を選択します。
- カメラビュー:データオーバービューの特定のカメラビューを選択します。
- 時間範囲:特定の時間範囲を選択します。
- Auto recovery (自動更新):オンにすると、データが自動的に更新されます。

••• コンテキストメニューは以下を含みます。

- Edit dashboard (ダッシュボードの編集):ダッシュボードを編集、共有、または削除します。
- Add chart (チャートの追加):ダッシュボードに新規チャートを作成します。
- About Axis insights (Axis insightsについて):Axis insightsについての説明が表示されます。

••• 各チャートのコンテキストメニューには以下が含まれます：

- チャートの最大化：クリックするとチャートが拡大されます。
- 画像としてコピー：クリックするとチャートがクリップボードにコピーされます。
- Export (エクスポート):クリックしてチャートをPNGまたはCSVでエクスポートします。
- Edit chart (チャートの編集):クリックするとチャートを編集できます。
- Remove chart (チャートの削除):クリックするとチャートを削除できます。

注

- 一部のチャートでは数字をクリックすると、追加情報が表示されます。
- :ダッシュボードの各チャートに適用されるそれぞれの選択を表示します。

新しいダッシュボードを作成する

1. Dashboard (ダッシュボード):ドロップダウンリストから [Add dashboard(ダッシュボードを追加)] を選択します。
2. [Empty (空)] をクリックして、新しいダッシュボードを作成するか、[From existing dashboard (既存のダッシュボードから)] をクリックして、システムで利用可能なダッシュボードに類似するダッシュボードを作成します。
3. Name (名前):ダッシュボードの名前を入力します。
4. Allow other users to view this dashboard (このダッシュボードを他のユーザーが表示することを許可する):クリックし、ダッシュボードを読み取り専用モードで他のユーザーと共有します。
5. [適用] をクリックします。
6. Add chart (チャートの追加):クリックすると、新規チャートを追加できます。
   - Select chart type (チャートタイプの選択):希望するチャートのタイプを選択し、[Next (次へ)] をクリックします。ビデオ分析や車両、折れ線グラフなど、タグやチャートのタイトルを使ってチャートタイプを検索できます。
   - Modify data selections (データ選択の修正):各カテゴリーの下で、適用可能なフィルターを選択します。
   - Adjust appearance (外観の調整):テキストを編集し、チャートサイズを選択します。

ダッシュボードのドロップダウンリストを設定する

注

- デフォルトでは、作成したダッシュボードのみを表示できます。

[Dashboard (ダッシュボード)]のドロップダウンリストで、他のユーザーが共有しているダッシュボードを表示するには:

1. [Shared dashboards (共有ダッシュボード)]に移動します。
2. ドロップダウンリストに追加する共有ダッシュボードのそれぞれのトグルスイッチをオンにします。

特定のカメラビューのインサイトを表示する

カメラビューでライブビューや再生ビデオを表示する際、アクティブなカメラビューを事前に選択してAxis insightsを開くことができます。

特定のカメラビューに対してAxis insightsを開くには:

1. Smart Clientに移動し、ビューを開きます。
2. [Show insights (insightsを表示)] をクリックします。

Axis insightsの設定

1. カメラがAXIS Object Analyticsをサポートしているかを確認します(*Axisプロダクトセレクターで分析機能を参照*)。
2. カメラの日付と時刻が正しく設定されているかを確認します。
3. Management Clientで、メタデータ装置がカメラで有効になっているかを確認します。

4. メタデータ装置がカメラに関連していることを確認します。
   - [Devices (デバイス)] > [Camera (カメラ)] に移動し、装置を選択します。
   - [Client (クライアント)] タブに移動し、[Related metadata (関連メタデータ)] でカメラのメタデータ装置が選択されていることを確認します。
5. Axis Insightsで利用可能なすべてのデータを表示するには、以下の手順に従って、*AXIS Scene Metadata*を使用してカメラでシーン分析を有効にします。
   5.1. [Devices (デバイス)] > [Metadata (メタデータ)] に移動し、装置を選択します。
   - [Record (録画)] をクリックし、[Recording (録画)] が有効になっているかを確認します。
   - [Settings (設定)] をクリックし、[Analytics data (分析データ)] が有効になっていることを確認します。

   5.1. 使用可能であれば [Consolidated metadata (統合メタデータ)] をオンにして、読み込みがより高速になるようにします。「*メタデータと検索, on page 110*」を参照してください。
6. *AXIS Object Analytics*、*AXIS Image Health Analytics*、または*環境センサー*を使用してチャートタイプにデータを有効にするには:
   - [Devices (デバイス)] > [Metadata (メタデータ)] に移動し、装置を選択します。
   - [Record (録画)] をクリックし、[Recording (録画)] が有効になっているかを確認します。
   - [Settings (設定)] をクリックし、[Event data (イベントデータ)] が有効になっていることを確認します。
   - このデバイスからのメタデータを常に録画するよう、VMSでルールを作成することをお勧めします。
7. セキュリティグループの権限を設定します。
   7.1. [Site Navigation (サイトナビゲーション)] > [Security (セキュリティ)] > [Roles (権限)] に移動します。
   7.2. 権限を選択します。
   7.3. [Cameras (カメラ)] を開きます。[Read (読み取り)] を選択します。
   7.4. [Metadata (メタデータ)] を開きます。[Read (読み取り)]、[Live (ライブ)]、[Playback (再生)] を選択します。
8. Axis insightsにナンバープレートのメタデータを追加するには、「*Axisナンバープレートの設定, on page 63*」を参照してください。

Axis insightsのトラブルシューティング

問題	解決策
チャートに「no data (データなし)」と表示される。	Axis insightsを設定する必要があります。「*Axis insightsの設定, on page 66*」を参照してください。
オペレータービューの読み込みに時間がかかる。	• 時間範囲を短くしてください。 • シーン分析カメラの数を減らしてカメラビューを作成して使用してください。 • 統合メタデータを有効にしてください (「*メタデータと検索, on page 110*」を参照)。

ビデオの歪み補正

歪み補正は、広角レンズまたは魚眼レンズによって引き起こされた幾何学的歪み画像のパースペクティブを平坦化し、補正します。VMSのAxisの歪み補正は、Axisの360°各種パノラマカメラで使用することができます。歪み補正は、カメラ、Smart Clientで直接行います。

歪み補正の詳細:

- クライアントサイドの歪み補正を使用すると、ライブ映像でも録画映像でもスムーズな歪み補正が可能になります。
- ビューに戻ると、自動的に最新の歪み補正のポジションに移動します。
- ビデオをエクスポートする場合は、歪み補正が含まれます。
- ホームポジションの保存については、*ホームポジションを設定する, on page 70*を参照してください。
- オペレーターが歪み補正ビューの制御と編集を許可されている場合は、*オペレーターによる歪み補正ビューの制御と編集を可能にする, on page 71*を参照してください。

歪み補正ビューを作成する

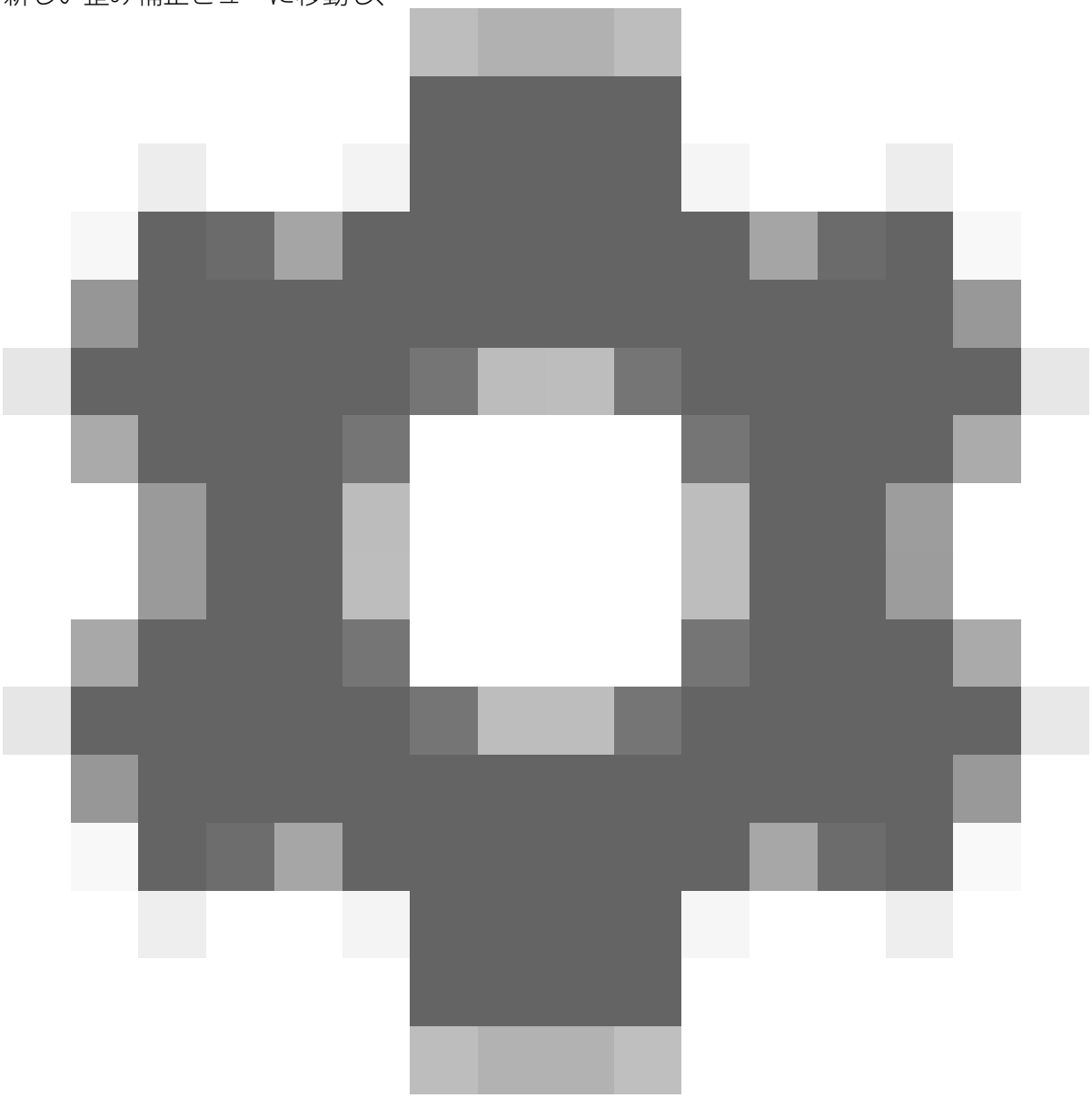


注

ストリームの歪み補正を最適化するには、Management Clientの [**Camera 1 (カメラ1)**] の [**Video stream 1 (ビデオストリーム1)**] で使用可能な最大解像度を選択します。詳細については、*パフォーマンスとトラブルシューティング, on page 71*を参照してください。

1. Smart Clientを開き、[**Setup (設定)**] をクリックします。
2. [**Views (ビュー)**] に移動します。
3. [**Create new view (新しいビューの作成)**] をクリックし、形式を選択します。
4. [**System overview > AXIS Optimizer (システムの概要 > AXIS Optimizer)**] を開きます。
5. [**Dewarping view (歪み補正ビュー)**] をクリックし、ビューにドラッグします。
6. カメラとカメラの現在の取り付け位置を選択します。
7. [**Setup (設定)**] をクリックします。

8. 新しい歪み補正ビューに移動し、



をクリックします。

9. [Set view type (ビュータイプの設定)] をクリックし、オプションを1つ選択します。カメラの取り付け方法に応じて、[Quad (4分割)]、[Normal (通常)]、[Normal with overview (通常と概要)]、または [Panorama (パノラマ)] を選択できます。

注

100 % DPIの使用を推奨します。解像度が100%以外の場合、2番目のディスプレイのAxisの歪み補正が完全に表示されない場合があります。

他のDPI設定を使用した場合、歪み補正ウィンドウが一部しか表示されない場合があります。この問題を解決するには、次の外部記事の手順に従ってください:

- *高解像度ディスプレイにおけるXProtectの問題 (4K以上)*
- *高DPIディスプレイでのクライアントGUIのサイズ変更*

マルチセンサーパノラマカメラ用の歪み補正ビューを作成する

AXIS P3807-PVE Network CameraやAXIS Q3819-PVE Panoramic Cameraなど、マルチセンサーパノラマカメラで歪み補正ビューを使用することができます。

- クライアント側のスティッチング。カメラがキャプチャーモードのクライアント歪み補正に設定されている場合、AXIS Optimizerは4つの画像を1つのシームレスなスパノラマにスティッチングします (AXIS P3807-PVEのみ)。
- 水平位置の調整。パノラマの水平位置を調整することができます。これは、カメラが地面に対して傾いており、地平線が湾曲している場合に役立ちます。これにより、バーチャルなPTZコントロールもさらに直感的に操作できるようになります。
- PTZコントロール。PTZカメラのような映像の拡大や移動が可能になります。



注

要件

- 以下のいずれかのユーザー権限を持つユーザーであること:
  - Optimizerの役割
  - ハードウェア > ドライバーコマンド = 許可
- Axisマルチセンサーパノラマカメラ

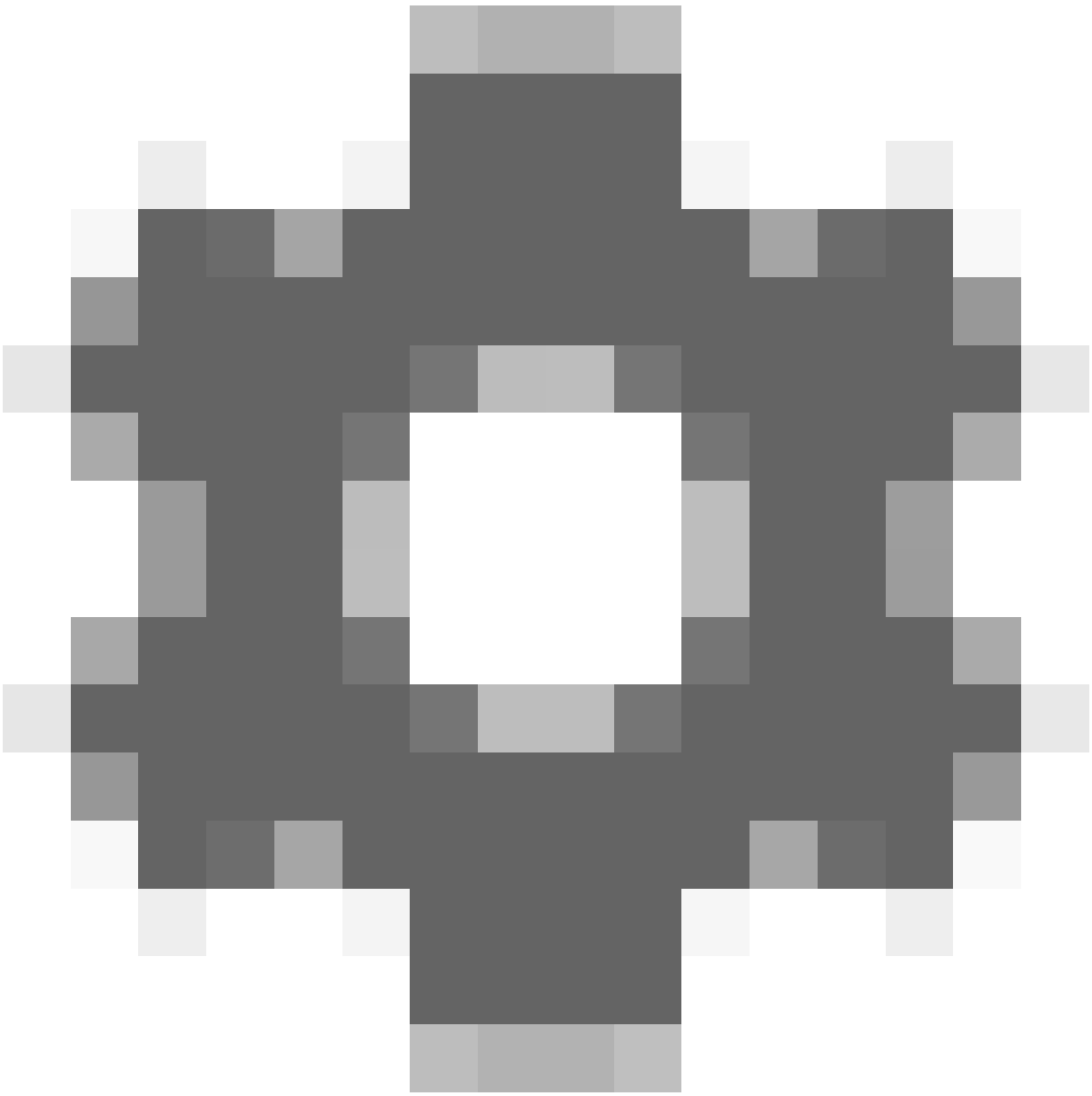
1. 該当する場合は、装置の初期設定時に、キャプチャーモードを [**Client Dewarp (クライアントの歪み補正)**] に設定します。
2. Smart Clientを開き、[**Setup (設定)**] をクリックします。
3. [**Views (ビュー)**] に移動します。
4. [**Create new view (新しいビューの作成)**] をクリックし、形式を選択します。
5. [**System overview > AXIS Optimizer (システムの概要 > AXIS Optimizer)**] を開きます。
6. [**Dewarping view (歪み補正ビュー)**] をクリックし、ビューにドラッグします。
7. マルチセンサーパノラマカメラを選択します。
   マルチセンサーパノラマカメラを初めて歪み補正ビューに追加すると、ビューの上に水平線キャリブレーションウィンドウが表示されます。
8. 矢印をクリックすると、赤い線が地平線に揃うようになります。
9. [**Done (完了)**] をクリックして設定を保存し、キャリブレーションモードを終了します。

ワイドビュー

ワイドビューはマルチセンサーパノラマカメラのビュータイプの1つです。通常の120°の視野では不十分な場合、**[wide view (ワイドビュー)]** をオンにします。ワイドビューを使用すると、常に画像に歪みが生じます。完全にズームアウトすると **[wide view (ワイドビュー)]** がオフになり、通常のビューに移行します。

ホームポジションを設定する

1. Smart Clientで、歪み補正ビューを開きます。
2. ホームポジションとして保存する位置に移動します。

3. 
をクリックしてから、[Set home position (ホームポジションの設定)] をクリックします。

オペレーターによる歪み補正ビューの制御と編集を可能にする

オペレーターが歪み補正ビューを制御・編集できるかどうかを設定できます。詳細は、*オペレーター向けに機能へのアクセスをカスタマイズする, on page 104*を参照してください。

パフォーマンスとトラブルシューティング

パフォーマンスに関する一般的な検討事項

- Axisのビデオの歪み補正は可能な限りGPUで行いますが、ビデオの歪み補正によってCPUに負荷がかかります。
- 多くの歪み補正ビューでフレームレートの低下を防ぐには、次の点に考慮してください:
  - カメラの解像度。カメラの解像度が2880x2880の高解像度の場合、1920x1920と比較して高い処理能力が必要となります。
  - カメラのフレームレート。高フレームレートが必要ない場合は、低フレームレートに変更することで、歪み補正ビューなどでのちらつきを防ぐことができます。

– モニターの解像度。高解像度モニター (4Kなど) では、映像の表示に多くのリソースが必要となります。高解像度が不要な場合は、モニターの解像度を低くすることで、より多くの歪み補正ビューをちらつきなしで実行できるようになります。

ダイナミック解像度

- ビデオストリームは、ビデオの質を低下させることなく、可能なかぎり自動的にダウンスケールされます。これにより、歪み補正ビューのパフォーマンスが向上します。
- オーバービューからのズームイン時に明滅が発生する場合は、ダイナミック解像度をオフにすると解消される場合があります。
- ダイナミック解像度のオン/オフを切り替えする方法:Smart Clientで、[**Settings (設定) > Axis dewarping options (Axis歪み補正オプション) > Rendering options (レンダリングオプション)**] の順に移動して、[**Dynamic resolution (動的解像度)**] を選択またはクリアします。
- **Dynamic resolution (ダイナミック解像度)** はデフォルトで有効になっています。

互換性レンダリング

- 歪み補正された画像に黒い画像などの視覚的エラーがある場合、またはパフォーマンスが想定よりも悪いと思われる場合は、互換性レンダリングを有効にしてください。互換性レンダリングの弊害として、ビュー間の遷移や再生時のスクラビングでちらつきが発生する場合があります。
- 互換性レンダリングのオン/オフを切り替する方法:Smart Clientを開いて、[**Settings (設定) > Axis dewarping options (Axis歪み補正オプション) > Rendering options (レンダリングオプション)**] の順に移動して、[**Use compatibility rendering (互換性レンダリングの使用)**] を選択またはクリアします。
- [**Use compatibility rendering (互換性レンダリングの使用)**] は、デフォルトでは無効になっています。

想定される動作

Intel Core i7 8700、NVIDIA Gefore 1050 GTX、3台の1920x1080モニターで構成されるリファレンスシステムで、次のことが可能です。

- 1920x1920の解像度で25fpsの7つの歪み補正ビューをフレーム低下なしで実行可能、また
- 解像度2880x2880、25fpsで4つの歪み補正ビューを実行

3台のディスプレイのうち1台が1920x1080ではなく4Kの解像度で動作している場合、次の動作が期待できます:

- 1920x1920の解像度で25fpsの5つの歪み補正ビューをフレーム低下なしで実行可能、また
- 解像度2880x2880、25fpsで3つの歪み補正ビューを実行。各モニターで歪み補正ビューを1個表示。

リニアなフレームレートと解像度のスケール。30fpsの歪み補正ビューを5個実行できるコンピューターでは、フレームレートを15fpsに下げると10個のビューを実行できます。

Body worn integration

AXIS Optimizer Body Worn Extensionは、現場カメラのユーザーがビデオを録画し、タグ付けし、オフィス内の調査員と共有できるため、調査員はVMSを使用して証拠ビデオを検索・管理することができます。このサービスにより、Axis装着式システムとVMS間の接続と転送を安全に行うことができます。AXIS Body Worn Extensionは、録画サーバーにインストールして使用する、無料のスタンドアロンサービスです。

注

対応しているバージョンは次のとおりです:

- VMSバージョン2020 R1 Corporate以降のバージョン
- VMSバージョン2020 R1 Professional+以降のバージョン
- VMSバージョン2020 R1 Expert以降のバージョン

最新のVMSホットフィックスおよび累積パッチインストーラーを必ず使用してください。

詳細情報

- サービス本体のダウンロードや、統合ガイド、ソリューションノートについては、*axis.com*にアクセスしてください。
- ユーザーマニュアルを参照するには、*axis.help.com*にアクセスしてください。

アクセスコントロール

アクセスコントロールは、物理アクセスコントロールと映像監視を組み合わせたソリューションです。この統合により、Management Clientから直接Axisアクセスコントロールシステムを設定できます。このシステムはXProtectとスムーズな統合を実現し、オペレーターがSmart Clientでアクセスを監視し、アクセスコントロールのアクションを実行できるようにします。

注

要件

- VMSバージョン2024 R1 以降。
- XProtect Accessライセンスについては、*アクセスライセンス*を参照してください。
- イベントサーバーとManagement ClientにInstall AXIS Optimizerをインストールします。

AXIS Secure Entry経由でAXIS Optimizerをインストールすると、ポート53459および53461が受信トラフィック (TCP) 用に開きます。

AXIS Secure Entryでドアを使用するには、ドアごとにライセンスを取得する必要があります。詳細については、*ドアのライセンスを有効にする, on page 75*を参照してください。

アクセスコントロールの設定

注

開始する前に、以下の手順を実行します。

- ドアコントローラーのソフトウェアをアップグレードする。以下の表でお使いのVMSバージョンに対応するAXIS OSの最小および推奨バージョンを確認してください。
- 日付と時刻が正しいことを確認してください。

AXIS Optimizerバージョン	最低限のAXIS OSバージョン	推奨AXIS OSバージョン
6.0	12.6.94.1	12.10.73.4
5.8	12.6.94.1	12.8.55.1
5.6	12.6.94.1	12.6.94.1

システムにAxisネットワークドアコントローラーを追加する

1. **[Site Navigation (サイトナビゲーション)]** > **[AXIS Optimizer]** > **[Access control (アクセスコントロール)]** に移動します。
2. **[Configuration (設定)]** で **[Devices (デバイス)]** を選択します。
3. **[Discovered devices (検出されたデバイス)]** を選択し、システムに追加できるユニットのリストを表示します。
4. 追加するユニットを選択します。
5. ポップアップウィンドウで **[+ Add (追加)]** をクリックし、コントローラーの認証情報を入力します。

注

- 追加されたコントローラーは、**[Management (管理)]** タブで確認できます。
- システムに手動でコントローラーを追加するには、**[Management (管理)]** タブで、**[+ Add (追加)]** をクリックします。
- ドアコントローラー名を追加、削除、または編集するたびに更新内容をVMSに統合するには:
  - **[Site Navigation (サイトナビゲーション)]** > **[Access control (アクセスコントロール)]** に移動し、[Access Control integration (アクセスコントロール統合)] をクリックします。

– [General settings (一般設定)] タブで [Refresh Configuration (設定を更新)] をクリックします。

ドアのライセンスを有効にする

ドアを追加する前に、システムに登録されているライセンスを有効にする必要があります。

1. [Site Navigation (サイトナビゲーション)] で [License Information (ライセンス情報)] に移動します。
2. [Activate License Manually (手動でライセンスを有効にする)] をクリックし、[Online (オンライン)] または [Offline (オフライン)] を選択します。
3. オンラインでドアのライセンスを有効にするには:
   – ユーザー名とパスワードを入力します。
4. ドアのライセンスをオフラインで有効にするには、*オフラインでドアのライセンスを有効にする*を参照してください。

有効にするドアライセンスの数を調整する必要がある場合は:

1. [AXIS Optimizer] > [Access control (アクセスコントロール)] に移動します。
2. [Configuration (設定)] で [Devices (デバイス)] を選択します。
3. [Allocated door licenses (割り当て済みのドアのライセンス)] > [Custom license allocation (ライセンス割り当てのカスタマイズ)] に移動し、使用するドアライセンス数を入力します。
4. [適用] をクリックします。
5. [License Information (ライセンス情報)] に移動し、ライセンスを再び有効にします。

アクセスコントロールを設定する。

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] に移動します。
2. 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, on page 91*を参照してください。
3. 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, on page 88*を参照してください。
4. ドアを追加し、識別プロファイルをドアに適用します。*ドアを追加する手順については、, on page 78*を参照してください。
5. 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, on page 85*を参照してください。

ドアコントローラー用デバイスソフトウェアの互換性

重要

ドアコントローラーのAXIS OSをアップグレードするときは、以下の点に注意してください。

- **対応AXIS OSバージョン:** 対応AXIS OSバージョンは、元の推奨VMSバージョンからアップグレードする場合、およびシステムにドアがある場合にのみ適用されます。システムがこれらの条件を満たしていない場合は、特定のVMSバージョンに対して推奨されるAXIS OSバージョンにアップグレードする必要があります。
- **最低対応AXIS OSバージョン:** システムにインストールされている最も古いAXIS OSバージョンによって、最低対応AXIS OSバージョンが決まります。2つ前のバージョンまでの制限があります。AXIS Optimizerバージョン6.0を使用しており、すべてのデバイスを推奨されるAXIS OS バージョン12.10.73.4にアップグレードするとします。すると、今後システムでサポートされる最低バージョンは、AXIS OSバージョン12.6.94.1となります。
- **推奨されるAXIS OSのバージョンを超えてアップグレードする場合:** 特定のVMSバージョンに対して推奨されているAXIS OSのバージョンよりも新しいバージョンにアップグレード

するとします。この場合は、VMSバージョンに設定されたサポート範囲内であれば、いつでも問題なく推奨のAXIS OSバージョンにダウングレードすることができます。

- **将来のAXIS OSの推奨:** システムの安定性と完全な互換性を確保するため、必ず各VMSバージョンに推奨されるAXIS OSバージョンに従ってください。

アクセスコントロール統合

VMSにアクセスコントロールを統合するには:

1. [Site Navigation (サイトナビゲーション)] > [Access Control (アクセスコントロール)] に移動します。
2. [Access Control (アクセスコントロール)] を右クリックし、[Create new... (新規作成)]をクリックします。
3. [Create Access Control System Integration (アクセスコントロールシステムシステム統合の作成)] のダイアログで:
   - 統合名を入力します。
   - [Integration plug-in (統合プラグイン)] のドロップダウンメニューから [AXIS Secure Entry] を選択します。
   - [Next (次へ)] をクリックし、[Associate cameras (カメラの関連付け)] のダイアログを表示します。
     ドアアクセスポイントにカメラを関連付けるには:
     - [Cameras (カメラ)] に表示されているお使いのデバイスをクリックし、XProtectシステムで設定されているカメラのリストを表示します。
     - カメラを選択し、関連付けるアクセスポイントにドラッグします。
     - [Close (閉じる)] をクリックし、ダイアログを閉じます。

注

- XProtectのアクセスコントロール統合の詳細については、*XProtect Smart Clientでアクセスコントロールを使用する*を参照してください。
- 一般設定、ドア、関連付けられたカメラ、アクセスコントロールイベントなどのアクセスコントロールのプロパティの詳細については、*アクセスコントロールのプロパティ* を参照してください。

ドアとゾーン

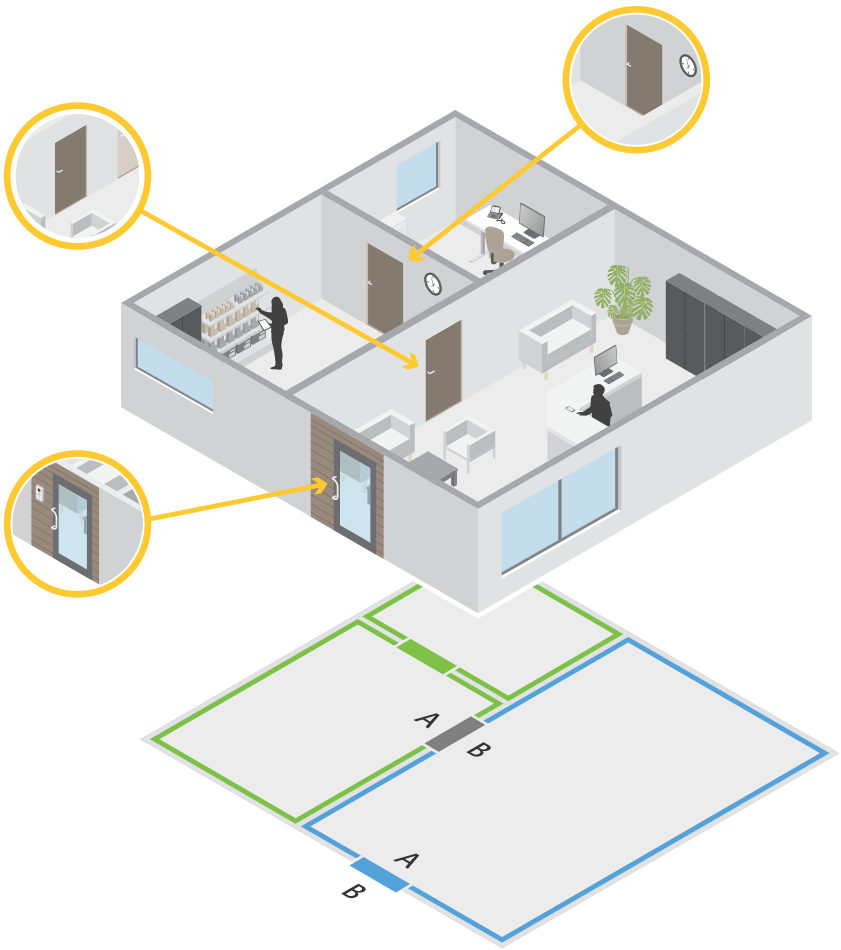
[Site Navigation (サイトナビゲーション)] > [Axis Optimizer] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] に移動して、概要を確認し、ドアとゾーンを設定します。

PINチャート	ドアに関連付けられたコントローラーのピン配置図の表示。ピン配置図を印刷する場合は、[Print (印刷)] をクリックします。
識別プロファイル	ドアの識別プロファイルを変更します。
セキュアチャンネル	特定のリーダーのOSDPセキュアチャンネルをオンまたはオフにします。

ドア	
名称	ドア名です。
ドアコントローラー	ドアに接続されているドアコントローラーです。
側面A	ドアのA面が面しているゾーンです。

側面B	ドアのB面が面しているゾーンです。
識別プロファイル	識別プロファイルはドアに適用されます。
カードフォーマットとPIN	カードのフォーマットまたはPINの長さを表示します。
ステータス	ドアのステータス。 • **オンライン:**ドアはオンラインで正しく機能しています。 • **リーダーオフライン:**ドア設定のリーダーがオフラインです。 • **リーダーエラー:**ドア設定のリーダーは、安全なチャンネルをサポートしていないか、セキュアチャンネルがリーダーに対してオフになっています。
ゾーン	
名称	ゾーン名です。
ドア数	ゾーンに含まれるドアの数です。

ドアとゾーンの例



- ゾーンは2色、つまり緑色と青色で表示されます。
- ドアは3色、つまり緑色、青色、茶色で表示されます。
- 緑色のドアは、緑色のゾーンにある内部ドアです。

- 青色のドアは、青色のゾーン専用の周辺ドアです。
- 茶色のドアは、緑色のゾーンと青色のゾーン共通の周辺ドアです。

ドアを追加する手順については、

注

- ドアコントローラーは、2つのロックがある1つのドア、またはそれぞれ1つのロックがある2つのドアで構成できます。
- ドアコントローラーにドアがなく、新バージョンのAxis Optimizerを使用しており、ドアコントローラーに古いソフトウェアが搭載されている場合、システムではドアの追加ができません。ただし、ドアがすでにある場合、システムコントローラーのソフトウェアが古くても、システムでは新しいドアを追加できます。

新しいドアの設定を作成してドアを追加する:

1. **[Site Navigation (サイトナビゲーション)]** > **[AXIS Optimizer]** > **[Access control (アクセスコントロール)]** > **[Doors and zones (ドアとゾーン)]** に移動します。
2. [+ **[Add door (ドアを追加)]**をクリックします。
3. ドア名を入力します。
4. [Controller (コントローラー)] ドロップダウンメニューで、ドアコントローラーを選択します。別のドアを追加できない場合、オフラインの場合、またはHTTPSがアクティブでない場合、コントローラーはグレー表示されます。
5. [Door type (ドアのタイプ)] ドロップダウンメニューで、作成するドアのタイプを選択します。
6. **[Next (次へ)]** をクリックして [Door configuration (ドアの設定)] ページに移動します。
7. [Primary lock (プライマリロック)] ドロップダウンメニューで、リレーポートを選択します。
8. ドアで2つのロックを設定するには、[Secondary lock (セカンダリロック)] ドロップダウンメニューからリレーポートを選択します。
9. 識別プロファイルを選択します。*識別プロファイル, on page 91*を参照してください。
10. ドアの設定に記載されている設定を行います。*ドア設定, on page 79*を参照してください。
11. 監視ドアを設定します。*監視ドアを追加する, on page 82*を参照してください。
12. **[Save (保存)]** をクリックします。

既存のドアの設定をコピーしてドアを追加する:

1. **[Site Navigation (サイトナビゲーション)]** > **[AXIS Optimizer]** > **[Access control (アクセスコントロール)]** > **[Doors and zones (ドアとゾーン)]** に移動します。
2. [+ **[Add door (ドアを追加)]**をクリックします。
3. ドア名を入力します。
4. [Controller (コントローラー)] ドロップダウンメニューで、ドアコントローラーを選択します。
5. **[Next (次へ)]** をクリックします。
6. [Copy configuration (設定のコピー)] ドロップダウンメニューで、既存のドアの設定を選択します。接続されているドアが表示され、コントローラーがグレー表示されている場合は、2つのドアが設定されているか、1つのドアに2つのロックが設定されています。
7. 必要に応じて設定を変更してください。
8. **[Save (保存)]** をクリックします。

ドアを編集するには:

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] > [Doors (ドア)] に移動します。
2. リストからドアを選択します。
3. [Edit (編集)]をクリックします。
4. 設定を変更して [Save (保存)] をクリックします。

ドアを削除するには:

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] > [Doors (ドア)] に移動します。
2. リストからドアを選択します。
3. [Remove (削除)]をクリックします。
4. [Yes (はい)] をクリックします。

ドア名を追加、削除、または編集するたびに更新内容をVMSに統合するには:

1. [Site Navigation (サイトナビゲーション)] > [Access control (アクセスコントロール)] に移動し、[Access Control integration (アクセスコントロール統合)] をクリックします。
2. [General settings (一般設定)] タブで [Refresh Configuration (設定を更新)] をクリックします。

ドア設定

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] に移動します。
2. 編集するドアを選択します。
3. [Edit (編集)]をクリックします。

アクセス時間 (秒)	アクセスが許可されてからドアのロック解除を継続する秒数を設定します。ドアが開くか設定時間が終了するまで、ドアのロックは解除されたままになります。ドアが閉まると、アクセス時間が残っていてもドアはロックされます。
Open-too-long time (sec) (長時間のドア開放 (秒))	ドアモニターを設定している場合にのみ有効です。ドアが開いたままになる秒数を設定します。設定時間が終了したときにドアが開いていると、長時間ドア開放アラームがトリガーされます。アクションルールを設定して、長時間ドア開放イベントでトリガーするアクションを設定します。
長いアクセス時間 (秒)	アクセスが許可されてからドアのロック解除を継続する秒数を設定します。Long access time (長いアクセス時間) は、この設定がオンになっているカード所持者のアクセス時間より優先されます。
Long open-too-long time (sec) (長い長時間のドア開放 (秒))	ドアモニターを設定している場合にのみ有効です。ドアが開いたままになる秒数を設定します。設定時間が終了したときにドアが開いていると、長時間ドア開放イベントがトリガーされます。[Long access time (長いアクセス時間)] 設定をオンにしている場合、[Long open-too-long time (長い長時間のドア開放)] は、カード所持者に対してすでに設定されている

	[Open too long time (長時間のドア開放)] 設定よりも優先されます。
再ロックの遅延時間 (ms)	ドアの開閉後にロック解除されたままになる時間 (ミリ秒) を設定します。
再ロック	• After opening (開けた後): ドアモニターを追加した場合のみ有効です。 • After closing (閉めた後): ドアモニターを追加した場合のみ有効です。

ドアセキュリティレベル

ドアに次のセキュリティ機能を追加できます。

2パーソンルール - 2人ルールでは、2人が有効な認証情報を使用してアクセスする必要があります。

ダブルスワイプ - ダブルスワイプにより、カード所持者はドアの現在の状態を無効にすることができます。たとえば、通常のスケジュール外でのドアのロックまたはロック解除に使用でき、システムにアクセスしてドアのロックを解除するよりも便利です。ダブルスワイプは既存のスケジュールには影響しません。たとえば、ドアが閉店時にロックされるようにスケジュールされていて、従業員が昼休みに店外に出ても、ドアはスケジュールに従ってロックされます。

セキュリティレベルは、新しいドアの追加時に、または既存のドアで設定できます。

既存のドアに2人ルールを追加するには:

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] に移動します。
2. セキュリティレベルを設定するドアを選択します。
3. [Edit] (編集) をクリックします。
4. [Security level (セキュリティレベル)] をクリックします。
5. 2人ルールをオンにします。
6. [適用] をクリックします。

2パーソンルール	
Side A (A面) とSide B (B面)	ルールを使用するドアの面を選択します。
スケジュール	ルールがいつアクティブになるかを選択します。
タイムアウト (秒)	タイムアウトは、カードのスワイプ間または他のタイプの有効な認証情報間で許容される最長時間です。

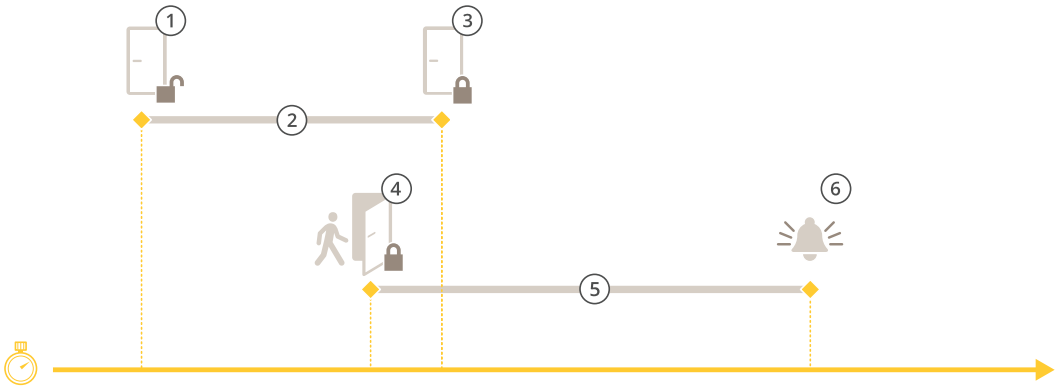
既存のドアにダブルスワイプを追加するには:

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] に移動します。
2. セキュリティレベルを設定するドアを選択します。
3. [Edit] (編集) をクリックします。
4. [Security level (セキュリティレベル)] をクリックします。
5. ダブルスワイプをオンにします。
6. [適用] をクリックします。

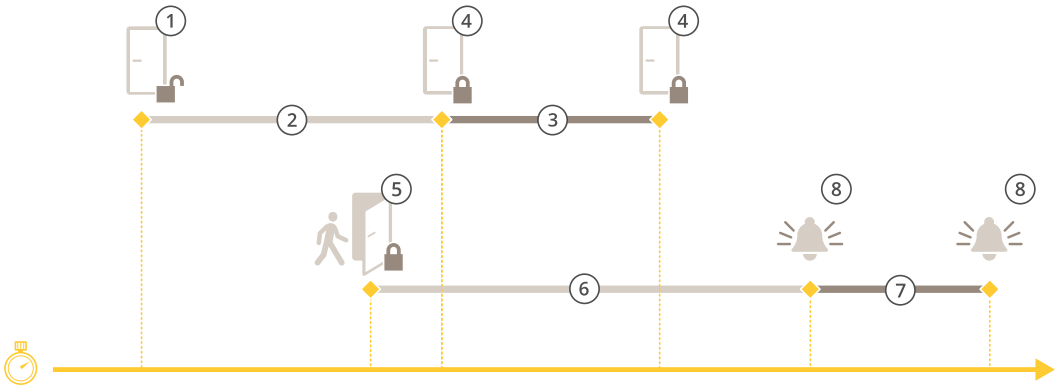
7. カード所持者に**ダブルスワイプ**を適用します。
   7.1. [Cardholder management (カード所持者の管理)] に移動します。
   7.2. 編集するカード所持者を選択し、[Edit (編集)] をクリックします。
   7.3. **詳細設定**] をクリックします。
   7.4. [Allow double-swipe (ダブルスワイプを許可する)] を選択します。
   7.5. [Save (保存)] をクリックします。

ダブルスワイプ	
タイムアウト (秒)	タイムアウトは、カードのスワイプ間または他のタイプの有効な認証情報間で許容される最長時間です。

時間のオプション



1 アクセス許可 - ロック解除
2 アクセス時間
3 アクションの実行なし - ロック施錠
4 アクションの実行 (ドアの開放) – ロック施錠、またはドアが閉じるまでロック解除状態を維持
5 長時間のドア開放
6 長時間のドア開放アラームの生成



1 アクセス許可 - ロック解除
2 アクセス時間
3 2+3:長いアクセス時間
4 アクションの実行なし - ロック施錠

5 アクションの実行 (ドアの開放) – ロック施錠、またはドアが閉じるまでロック解除状態を維持
6 長時間のドア開放
7 6+7:長い長時間のドア開放
8 長時間のドア開放アラームの生成

「ドアモニターの追加」

ドアモニターとは、ドアの物理的な状態を監視するドアポジションスイッチです。ドアにドアモニターを追加し、ドアモニターの接続方法を設定できます。

1. [Door configuration (ドアの設定)] ページに移動します。*ドアを追加する手順については、, on page 78*を参照してください。
2. [**Sensors (センサー)**] で、[**Add (追加)**] をクリックします。
3. [**Door position sensor (ドアポジションセンサー)**] を選択します。
4. ドアモニターを接続するI/Oポートを選択します。
5. [**Door open if (ドアが開く条件)**] で、ドアモニター回路の接続方法を選択します。
6. デジタル入力が新しい安定状態に移行するまで状態変化を無視するには、**[Debounce time (デバウンス時間)]** を設定します。
7. ドアコントローラーとドアモニターの間の接続が中断された場合にイベントをトリガーするには、[**Supervised input (状態監視入力)**] をオンにします。*監視入力, on page 86*を参照してください。

ドアが開く条件	
回路が開いている	ドアモニター回路はNC (Normally Closed) です。回路が開くと、ドアモニターはドアが開いている信号を送信します。回路が閉じると、ドアモニターはドアが閉じている信号を送信します。
回路が閉じている	ドアモニター回路はNO (Normally Open) です。回路が閉じると、ドアモニターはドアが開いている信号を送信します。回路が開くと、ドアモニターはドアが閉じている信号を送信します。

監視ドアを追加する

監視ドアは、開閉状態を表示できるタイプのドアです。たとえば、施錠は必要ないが開閉状態を知る必要がある防火扉に、このオプションを使用できます。

監視ドアは、ドアモニター付きの通常のドアとは異なります。ドアモニター付きの通常のドアは、ロックとリーダーをサポートしていますが、ドアコントローラーが必要です。監視ドアは、1つのドアポジションセンサーをサポートしていますが、ドアコントローラーに接続されたネットワークI/Oリレーモジュールのみが必要です。1つのネットワークI/Oリレーモジュールには、最大5つのドアポジションセンサーを接続できます。

注
監視ドアには、AXIS Monitoring Door ACAPアプリケーションを含む最新ソフトウェアが搭載されたAXIS A9210 Network I/O Relay Moduleが必要です。

監視ドアを設定するには:

1. AXIS A9210を設置し、AXIS OSの最新バージョンにアップグレードします。
2. ドアポジションセンサーを取り付けます。

3. VMSで、[Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] に移動します。
4. [Add door (ドアを追加)] をクリックします。
5. 名前)を入力します。
6. [Type (タイプ)] で、[Monitoring door (監視ドア)] を選択します。
7. [Device (デバイス)] で、ネットワークI/Oリレーモジュールを選択します。
8. [Next (次へ)] をクリックします。
9. [Sensors (センサー)] で、[+ Add (追加)] をクリックし、[Door position sensor (ドアポジションセンサー)] を選択します。
10. ドアポジションセンサーに接続されているI/Oを選択します。
11. [追加] をクリックします。

「リーダーの追加」

ドアコントローラーは2台の有線リーダーを使用するように設定できます。リーダーをドアの片面に追加するか、両面に追加するかを選択します。

カスタム設定のカードフォーマットやPIN長をリーダーに適用すると、そのことは [Configuration > Access control > Doors and zones (設定 > アクセスコントロール > ドアとゾーン)] の [Card formats (カードフォーマット)] で確認できます。*ドアとゾーン, on page 76*を参照してください。

1. [Door configuration (ドアの設定)] ページに移動します。*ドアを追加する手順については、, on page 78*を参照してください。
2. ドアのどちらかの面で [Add (追加)] をクリックします。
3. [Card reader (カードリーダー)] を選択します。
4. [Reader type (リーダータイプ)] を選択します。
5. このリーダーにカスタムのPIN長さ設定を使用するには:
   5.1. 詳細設定] をクリックします。
   5.2. [Custom PIN length (カスタムPIN長)] をオンにします。
   5.3. [Min PIN length (最小PIN長)]、[Max PIN length (最大PIN長)]、[End of PIN character (PIN文字の終端)] をそれぞれ設定します。
6. このリーダーにカスタムのカードフォーマットを使用するには:
   6.1. 詳細設定] をクリックします。
   6.2. [Custom card formats (カスタムカードフォーマット)] をオンにします。
   6.3. リーダーで使用するカードフォーマットを選択します。すでに同じビット長のカードフォーマットを使用している場合は、まずそれを無効にする必要があります。カードフォーマットの設定が現在のシステム設定と異なる場合、クライアントに警告アイコンが表示されます。
7. [追加] をクリックします。
8. ドアの反対側の面にリーダーを追加するには、この手順を再度行います。

リーダータイプ	
OSDP RS485 half duplex (OSDP RS485半二重)	RS485リーダーの場合は、[OSDP RS485 half duplex (OSDP RS485半二重)] とリーダーポートを選択します。
Wiegand	Wiegandプロトコルを使用するリーダーの場合は、[Wiegand] とリーダーポートを選択します。

Wiegand	
LEDコントロール	[Single wire (シングルワイヤー)] または [Dual wire (R/G) (デュアルワイヤー (R/G))] を選択します。デュアルLEDコントロールを備えたリーダーは、通常、赤、緑のLED用にさまざまな配線を使用します。
いたずら警告	リーダーに対するいたずら入力がアクティブになるタイミングを選択します。 • Open circuit (開路):リーダーは、回路が開いたときにいたずら信号を送信します。 • Closed circuit (閉路):リーダーは、回路が閉じたときにいたずら信号を送信します。
Tamper debounce time (いたずらのデバウンス時間)	リーダーへのいたずら入力が新しい安定状態に移行するまで状態変化を無視するには、[Tamper debounce time (いたずらのデバウンス時間)] を設定します。
状態監視入力	オンにすると、ドアコントローラーとリーダーの間の接続が中断されたときにイベントがトリガーされます。*監視入力, on page 86*を参照してください。

REX装置の追加

REX (退出要求) 装置は、ドアの片面に取り付けるか、両面に取り付けるかを選択できます。REX装置には、PIRセンサー、REXボタン、またはプッシュバーを使用できます。

1. [Door configuration (ドアの設定)] ページに移動します。*ドアを追加する手順については、, on page 78*を参照してください。
2. ドアのどちらかの面で [Add (追加)] をクリックします。
3. [REX device (REXデバイス)] を選択します。
4. REX装置を接続するI/Oポートを選択します。使用可能なポートが1つしかない場合、ポートは自動的に選択されます。
5. [Action (アクション)] で、ドアがREX信号を受信したときにトリガーするアクションを選択します。
6. [REX active (REXアクティブ)] で、ドアモニター回路の接続方法を選択します。
7. デジタル入力が新しい安定状態に移行するまで状態変化を無視するには、[Debounce time (ms) (デバウンス時間 (ミリ秒))] を設定します。
8. ドアコントローラーとREX装置の間の接続が中断された場合にイベントをトリガーするには、[Supervised input (状態監視入力)] をオンにします。*監視入力, on page 86*を参照してください。

アクション	
ドアロック解除	REX信号を受信したときにドアのロックを解除する場合に選択します。
なし	ドアがREX信号を受信したときにアクションをトリガーしない場合に選択します。

REX有効	
回路が開いている	REX回路がNC (Normally Closed) の場合に選択します。REX装置は、回路が開いたときに信号を送信します。
回路が閉じている	REX回路がNO (Normally Open) の場合に選択します。REX装置は、回路が閉じたときに信号を送信します。

ゾーンの追加

ゾーンとは、グループ化されたドアがある特定の物理的領域です。ゾーンを作成したり、ゾーンにドアを追加したりできます。ドアには 2 つのタイプがあります。

- Perimeter door (敷地周辺ドア): このドアを通ってカード所持者がゾーンに出入りします。
- Internal door (内部ドア): ゾーンの内部にあるドアです。

注

周辺ドアは、2つのゾーンに属することができますが、内部ドアは1つのゾーンにのみ属することができます。

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] > [Zones (ゾーン)] に移動します。
2. + [Add zone (ゾーンを追加)]をクリックします。
3. ゾーン名を入力します。
4. [Add door (ドアを追加)] をクリックします。
5. ゾーンに追加するドアを選択し、[Add (追加)] をクリックします。
6. デフォルトでは、ドアは敷地周辺ドアに設定されています。これを変更するには、ドロップダウンメニューで [Internal door (内部ドア)] を選択します。
7. 敷地周辺ドアでは、デフォルトでドアのA面がゾーンへの入口として使用されます。これを変更するには、ドロップダウンメニューで [Leave (退出)] を選択します。
8. ゾーンからドアを削除するには、ドアを選択し、[Remove (削除)] をクリックします。
9. [Save (保存)] をクリックします。

ゾーンを編集するには:

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] > [Zones (ゾーン)] に移動します。
2. リストからゾーンを選択します。
3. [Edit (編集)]をクリックします。
4. 設定を変更して [Save (保存)] をクリックします。

ゾーンを削除するには:

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] > [Zones (ゾーン)] に移動します。
2. リストからゾーンを選択します。
3. [Remove (削除)]をクリックします。

4. [Yes (はい)] をクリックします。

ゾーンセキュリティレベル

ゾーンに次のセキュリティ機能を追加できます。

アンチパスバック - ユーザーが自分より前にそのエリアに入った人と同じ認証情報を使用することを防ぎます。これにより、ユーザーは認証情報を再度使用する前に、まずそのエリアから退出する必要があります。

注

- 不正通行防止では、ゾーン内のすべてのドアにドアポジションセンサーが必要です。これにより、ユーザーがカードのスワイプ後にドアを開けたことをシステムが登録できます。
- ゾーン内のすべてのドアが同じドアコントローラーに属している場合、ドアコントローラーがオフラインになっても、不正通行防止は機能します。ただし、ゾーン内のドアが異なるドアコントローラーに属している場合は、ドアコントローラーがオフラインになると、不正通行防止は機能しなくなります。

セキュリティレベルは、新しいゾーンの追加時に、または既存のゾーンで設定できます。既存のゾーンにセキュリティレベルを追加するには:

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] に移動します。
2. セキュリティレベルを設定するゾーンを選択します。
3. [Edit] (編集) をクリックします。
4. [Security level (セキュリティレベル)] をクリックします。
5. ドアに追加するセキュリティ機能をオンにします。
6. [適用] をクリックします。

アンチパスバック	
Log violation only (Soft) (違反を記録のみ (ソフト))	2人目のユーザーが最初の人と同じ認証情報を使用してドアから入ることを許可する場合に、このオプションを使用します。このオプションでは、システムアラームのみが発生します。
アクセスを拒否 (ハード)	2人目のユーザーが最初のユーザーと同じ認証情報を使用してドアから入ることを禁止する場合に、このオプションを使用します。このオプションでも、システムアラームが発生します。
タイムアウト (秒)	この時間が経過するまで、ユーザーは再入場を許可されます。タイムアウトを設定しない場合は0と入力します。その場合、ユーザーがゾーンから退出するまで、そのソーンでアンチパスバックが維持されます。[Deny access (Hard) (アクセス拒否 (ハード))] でタイムアウトとして0を使用するのは、ゾーン内のすべてのドアの両側にリーダーがある場合に限ります。

監視入力

状態監視入力は、ドアコントローラーへの接続が中断されたときにイベントをトリガーできます。

- ドアコントローラーとドアモニターの接続。*「ドアモニターの追加」, on page 82*を参照してください。

- Wiegandプロトコルを使用するドアコントローラーとリーダー間の接続。*「リーダーの追加」, on page 83*を参照してください。
- ドアコントローラーとREX装置間の接続。*REX装置の追加, on page 84*を参照してください。

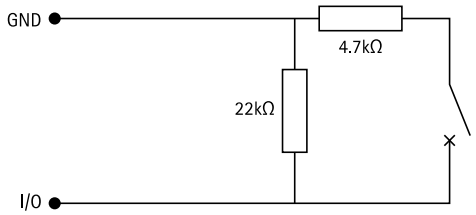
監視入力を使用するには:

1. 終端抵抗は、接続図にしたがって、できるだけ周辺機器の近くに設置してください。
2. リーダー、ドアモニター、またはREX装置の設定ページに移動し、[**Supervised input (監視入力)**] をオンにします。
3. 並列優先接続図に従った場合は、[**Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (22 KΩの並列抵抗器と4.7 KΩの直列抵抗器による並列優先接続)**] を選択します。
4. 直列優先接続図に従った場合は、[**Serial first connection (直列優先接続)**] を選択し、[**Resistor values (抵抗器の値)**] ドロップダウンメニューから抵抗器の値を選択します。

接続図

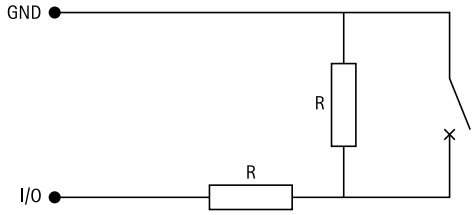
並列優先接続

抵抗器の値は 4.7 kΩ及び 22 kΩである必要があります。



直列優先接続

抵抗器の値は同じで、1~10 kΩの範囲内である必要があります。



手動アクション

ドアとゾーンには、以下の手動アクションを実行することができます。

リセット - 設定されたシステムルールに戻ります。

アクセスの付与 - ドアまたはゾーンのロックを7秒間解除し、再度ロックします。

ロック解除 - リセットするまでドアのロックが解除されます。

ロック - システムがカード所持者にアクセスを許可するまで、ドアをロックします。

施設や部屋の封鎖 - リセットするかロックを解除するまで、誰も出入りできません。

手動アクションを実行するには、以下の手順に従います。

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] に移動します。
2. 手動アクションを実行するドアまたはゾーンを選択します。
3. 手動アクションのいずれかをクリックします。

注

ドアは、通常のスケジュールにリセットするまで、手動アクションステータス (手動オーバーライドモードとも呼ばれます) のままになります。

カードフォーマットとPIN

カードフォーマットは、カードにデータを保存する方法を定義します。これは、システム内で入力データを検証済みデータにする変換テーブルです。カードフォーマットごとに、保存された情報を整理する方法に対する異なるルールがあります。カードフォーマットを定義することで、コントローラーがカードリーダーから取得する情報をどのように解釈するかがシステムに通知されます。

そのまま使用したり、必要に応じて編集して使用したりできる、汎用性の高い既定のカードフォーマットも用意されています。カスタムのカードフォーマットを作成することもできます。

[Site Navigation (サイトナビゲーション)] > AXIS Optimizer > [Access control (アクセスコントロール)] > [Card formats and PIN (カードフォーマットとPIN)] に移動して、カードフォーマットを作成、編集、または有効化します。PINの設定もできます。

カスタムカードフォーマットには、認証情報の検証に使用する以下のデータフィールドを含めることができます。

カード番号 - 認証情報のバイナリデータのサブセットであり、10進数または16進数としてエンコードされています。カード番号を使用して、特定のカードまたはカード所持者を識別します。

設備コード - 認証情報のバイナリデータのサブセットであり、10進数または16進数としてエンコードされています。設備コードを使用して、特定のエンドカスタマーまたはサイトを識別します。

カードフォーマットを作成する手順は、以下のとおりです。

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Card formats and PIN (カードフォーマットとPIN)] に移動します。
2. [Add card format (カードフォーマットの追加)] をクリックします。
3. カードフォーマットの名前を入力します。
4. [Bit length (ビット長)] フィールドに、1～256の間のビット長を入力します。
5. カードリーダーから受信したデータのビット順を反転するには、[Invert bit order (ビット順を反転する)] を選択します。
6. カードリーダーから受信したデータのバイト順を反転するには、[Invert byte order (バイト順を反転する)] を選択します。このオプションは、8で割り切れるビット長を指定している場合のみ使用できます。
7. カードフォーマットで有効にするデータフィールドを選択して設定します。カードフォーマットでは、[Card number (カード番号)] か [Facility code (設備コード)] のいずれかを有効にする必要があります。
8. [OK]をクリックします。
9. カードフォーマットを有効にするには、カードフォーマット名の前にあるチェックボックスをオンにします。

注

- 同一ビット長の2つのカードフォーマットを同時にアクティブにすることはできません。たとえば、32ビットカードフォーマットを2つ定義した場合、アクティブにできるのはそのうちの1つだけです。一方のカードフォーマットを無効にすると、もう一方のフォーマットが有効になります。
- 1つ以上のリーダーが接続されたドアコントローラーを設定している場合は、カードフォーマットを有効または無効にのみ設定できます。

ⓘ	ⓘをクリックすると、ビット順を反転した後の出力例が表示されます。
通信可能距離	データフィールドのデータのビット範囲を設定します。この範囲は、[Bit length (ビット長)]に指定した範囲内である必要があります。
出力形式	データフィールドのデータの出力形式を選択します。 **Decimal (10進数)**:10を底とする位取り記数法であり、0〜9の数字で構成されます。 **Hexadecimal (16進数)**:16を底とする位取り記数法であり、16個の固有の記号で構成されます。0〜9の数字とa〜fの文字を使用して表記されます。
ビット順のサブ範囲	ビット順を選択します。 **Little endian (リトルエンディアン)**:最初のビットが最小 (最下位) です。 **Big endian (ビッグエンディアン)**:最初のビットが最大 (最上位) です。

カードフォーマットを編集する手順は、以下のとおりです。

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Card formats and PIN (カードフォーマットとPIN)] に移動します。
2. カードフォーマットを選択して をクリックします。
3. 既定のカードフォーマットを編集する場合は、[Invert bit order (ビット順を反転する)] と [Invert byte order (バイト順を反転する)] のみを編集できます。
4. [OK]をクリックします。

削除できるのは、カスタムカードフォーマットのみです。カスタムカードフォーマットを削除する手順は、以下のとおりです。

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Card formats and PIN (カードフォーマットとPIN)] に移動します。
2. カスタムカードフォーマットを選択し、 と[Yes (はい)]をクリックします。

既定のカードフォーマットをリセットするには:

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Card formats and PIN (カードフォーマットとPIN)] に移動します。
2. をクリックすると、カードフォーマットをデフォルトのフィールドマップにリセットできます。

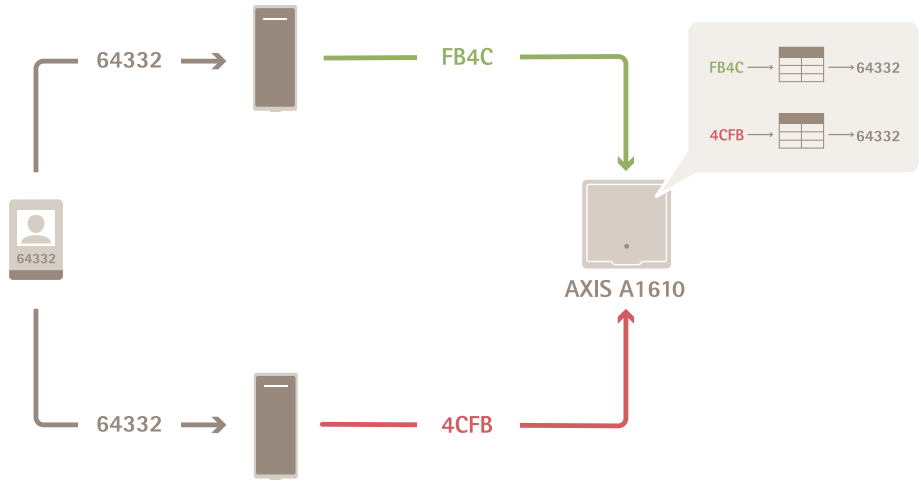
PIN長を設定する手順は、以下のとおりです。

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Card formats and PIN (カードフォーマットとPIN)] に移動します。
2. [PIN configuration (PIN設定)]で をクリックします。

3. [Min PIN length (最小PIN長)]、[Max PIN length (最大PIN長)]、[End of PIN character (PIN文字の終端)] をそれぞれ指定します。
4. [OK]をクリックします。

カードフォーマットの設定

概要



- カード番号は10進数で64332です。
- 1台のリーダーにより、カード番号が16進数のFB4Cに変換されます。別のリーダーにより、それが16進数の4CFBに変換されます。
- FB4Cを受信したAXIS A1610 Network Door Controllerは、それをリーダーのカードフォーマット設定に従って10進数の64332に変換します。
- 4CFBを受信したAXIS A1610 Network Door Controllerは、それをバイト順序を逆にしてFB4Cに変更し、リーダーのカードフォーマット設定に従って10進数の64332に変換します。

ビット順を反転する

ビット順の反転後、リーダーから受信したカードデータは、右から左にビット順に読み取られます。



バイト順を反転する

1バイトは8ビットです。バイト順の反転後、リーダーから受信したカードデータは、右から左にバイト順に読み取られます。



26ビット標準のWiegandカードフォーマット



1 *先頭のパリティ*
2 *設備コード*
3 *カード番号*
4 *末尾のパリティ*

識別プロファイル

識別プロファイルは、識別タイプとスケジュールを組み合わたものです。識別プロファイルを1つ以上のドアに適用して、カード所持者がドアにいつどのようにアクセスできるかを設定できます。

識別タイプは、ドアにアクセスするために必要な認証情報を運ぶものです。一般的な識別タイプには、トークン、個人識別番号 (PIN)、指紋、顔立ちマップ、REX装置があります。識別タイプは、1つ以上のタイプの情報を運ぶことができます。

スケジュールは**タイムプロファイル**とも呼ばれ、Management Clientで作成されます。タイムプロファイルの設定方法については、*タイムプロファイル (説明)* を参照してください。

サポートされる識別タイプ:カード、PIN、REX。

[Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Identification profiles (識別プロファイル)] に移動します。

そのまま使用したり、必要に応じて編集して使用したりできる、デフォルトの識別プロファイルが5つ用意されています。

カード - カード所持者がドアにアクセスする際に、カードを読み取らせる必要があります。

カードとPIN - カード所持者がドアにアクセスする際に、カードを読み取らせ、かつPINを入力する必要があります。

PIN - カード所持者がドアにアクセスする際に、PINを入力する必要があります。

カードまたはPIN - カード所持者がドアにアクセスする際に、カードを読み取らせるか、PINを入力する必要があります。

ナンバープレート - カード所持者は、承認済みのナンバープレートを付けた車両でカメラに向かって運転する必要があります。

識別プロファイルを作成する手順は、以下のとおりです。

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Identification profiles (識別プロファイル)] に移動します。
2. [Create identification profile (識別プロファイルの作成)] をクリックします。
3. 識別プロファイル名を入力します。
4. 設備コードを [Credential validation (認証情報の検証)] フィールドの1つとして使用するには、[Include facility code for card validation (カード検証用の機能コードを含める)] を選択します。このフィールドは、[Access management > Settings (アクセス管理 > 設定)] で [Facility code (設備コード)] をオンにしている場合のみ使用できます。
5. ドアの片側の面で識別プロファイルを設定します。
6. ドアの反対側の面で同じ手順を繰り返します。
7. [OK]をクリックします。

識別プロファイルを編集する手順は、以下のとおりです。

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Identification profiles (識別プロファイル)] に移動します。
2. 識別プロファイルを選択して をクリックします。
3. 識別プロファイル名を変更するには、新しい名前を入力します。
4. ドアの現在の面で編集をします。
5. ドアの反対側の面の識別プロファイルを編集するには、ここまでの手順を繰り返します。
6. [OK]をクリックします。

識別プロファイルを削除する手順は、以下のとおりです。

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Identification profiles (識別プロファイル)] に移動します。
2. 識別プロファイルを選択して をクリックします。
3. 識別プロファイルがドアで使用されている場合は、そのドア用に別の識別プロファイルを選択します。
4. [OK]をクリックします。

識別プロファイルの編集	
×	識別タイプとそれに関連するスケジュールを削除するには:
認証タイプ	識別タイプを変更するには、[Identification type (識別タイプ)] のドロップダウンメニューから1つ以上のタイプを選択します。
Schedule	スケジュールを変更するには、[Schedule (スケジュール)] ドロップダウンメニューから1つ以上のスケジュールを選択します。
+ 追加	識別タイプとそれに関連スケジュールを追加し、[Add (追加)] をクリックして、識別タイプとスケジュールを設定します。

暗号化通信

OSDPセキュアチャンネル

Secure Entryは、OSDP (Open Supervised Device Protocol) セキュアチャンネルに対応し、コントローラーとAxisリーダー間の回線暗号化をアクティブにします。

システム全体でOSDPセキュアチャンネルをオンにするには:

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Encrypted communication (暗号化通信)] に移動します。
2. メインの暗号化キーを入力し、[OK] をクリックします。
3. [OSDP Secure Channel (OSDPセキュアチャンネル)] をオンにします。このオプションは、メインの暗号化キーを入力した後にのみ使用できます。
4. デフォルトでは、メインの暗号化キーによってOSDPセキュアチャンネルキーが生成されます。OSDPセキュアチャンネルキーを手動で設定するには:
   4.1. [OSDP Secure Channel (OSDPセキュアチャンネル)]で、 をクリックします。
   4.2. [Use main encryption key to generate OSDP Secure Channel key (メイン暗号化キーを使用してOSDPセキュアチャンネルキーを生成する)] をクリアします。

4.3. OSDPセキュアチャンネルキーを入力し、[OK] をクリックします。

特定のリーダーでOSDPセキュアチャンネルをオンまたはオフにする方法については、*ドアとゾーン*を参照してください。

マルチサーバーBETA

マルチサーバーを使用すると、メインサーバー上のグローバルカード所持者およびカード所持者グループを接続されたサブサーバーで使用できます。

注

- 1つのシステムで最大64台のサブサーバーをサポートできます。
- 前提条件として、メインサーバーとサブサーバーは同じネットワーク上にある必要があります。
- メインサーバーとサブサーバーでかならず、WindowsファイアウォールがSecure Entryポートで入力TCP接続を許可するよう設定します。デフォルトポートは53461です。

ワークフロー

1. サーバーをサブサーバーとして設定し、設定ファイルを生成します。*サブサーバーから設定ファイルを生成する, on page 93*を参照してください。
2. サーバーをメインサーバーとして設定し、サブサーバーの設定ファイルをインポートします。*設定ファイルをメインサーバーにインポートする, on page 93*を参照してください。
3. メインサーバーでグローバルなカード所持者とカード所持者グループを設定します。*カード所持者の追加, on page 95*と *「グループの追加」, on page 98*を参照してください。
4. サブサーバーからグローバルなカード所持者およびカード所持者グループを表示および監視します。*アクセス管理, on page 94*を参照してください。

サブサーバーから設定ファイルを生成する

1. サブサーバーで、[AXIS Optimizer] > [Access control (アクセスコントロール)] > [Multi serverマルチサーバー)] に移動します。
2. [Sub server (サブサーバー)] をクリックします。
3. [Generate (生成)] をクリックします。設定ファイルが.json形式で生成されます。
4. [Download (ダウンロード)] をクリックし、ファイルを保存する場所を選択します。

設定ファイルをメインサーバーにインポートする

1. メインサーバーで、[AXIS Optimizer] > [Access control (アクセスコントロール)] > [Multi serverマルチサーバー)] に移動します。
2. [Main server (メインサーバー)] をクリックします。
3. ＋[Add (追加)]をクリックし、サブサーバーから生成された設定ファイルに移動します。
4. サブサーバーのサーバー名、IPアドレス、ポート番号を入力します。
5. [Import (インポート)] をクリックして、サブサーバーを追加します。
6. サブサーバーのステータスが [Connected] と表示されます。

サブサーバーを無効にする

サブサーバーは、設定ファイルをメインサーバーにインポートする前に限り無効にできます。

1. メインサーバーで、[AXIS Optimizer] > [Access control (アクセスコントロール)] > [Multi serverマルチサーバー)] に移動します。

2. [Sub server (サブサーバー)] をクリックしてから、[Revoke server (サーバーを無効化)] をクリックします。
これで、このサーバーをメインサーバーまたはサブサーバーとして設定できます。

サブサーバーを削除する

サブサーバーの設定ファイルをインポートすると、サブサーバーがメインサーバーに接続されます。

サブサーバーを削除するには、次の手順を実行します。

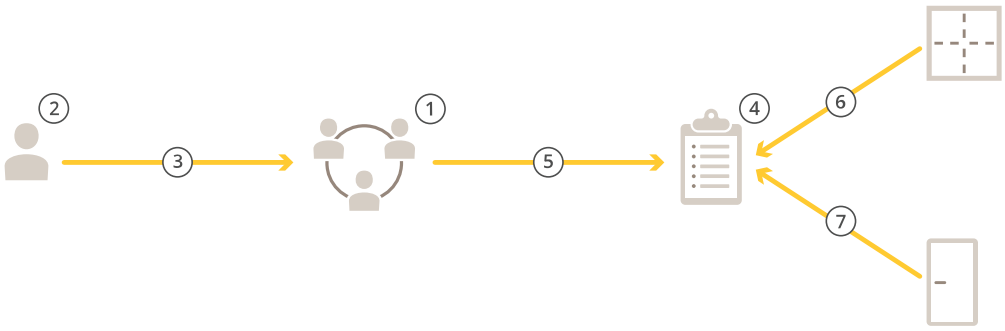
1. メインサーバーにアクセスします。
   1.1. [Access management (アクセス管理)] > [Dashboard (ダッシュボード)] を選択します。
   1.2. グローバルカード所持者とグループをローカルカード所持者とグループに変更します。
   1.3. [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Multi server (マルチサーバー)] に移動します。
   1.4. [Main server (メインサーバー)] をクリックすると、サブサーバーのリストが表示されます。
   1.5. サブサーバーを選択し、[Delete (削除)] をクリックします。
2. サブサーバーから:
   – [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Multi server (マルチサーバー)] に移動します。
   – [Sub server (サブサーバー)] をクリックしてから、[Revoke server (サーバーを無効化)] をクリックします。

アクセス管理

[Access management (アクセス管理)] タブでは、システムのカード所持者、グループ、アクセスルールの設定や管理ができます。

アクセス管理のワークフロー

アクセス管理の構造には柔軟性があり、ニーズに合わせてワークフローを開発することができます。以下はワークフローの例です。



1. グループを追加するワークフローについては、*「グループの追加」, on page 98*を参照してください。
2. カード所持者を追加するワークフローについては、*カード所持者の追加, on page 95*を参照してください。
3. カード所持者とグループの追加。

4. アクションルールを追加するワークフローについては、*アクセスルールを追加します。, on page 98*を参照してください。
5. アクセスルールへのグループの適用。
6. アクセスルールへのゾーンの適用。
7. アクセスルールへのドアの適用。

カード所持者の追加

カード所持者とは、システムに登録された一意のIDを持つ人物です。カード所持者に、個人を識別する認証情報と、その個人にドアへのアクセスを許可するタイミングと方法を設定します。

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Cardholder management (カード所持者の管理)] に移動します。
2. [Cardholders (カード所持者)] に移動し、[+Add (追加)] をクリックします。
3. カード所持者の名と姓を入力し、[Next (次へ)] をクリックします。
4. オプションとして [Advanced (詳細設定)] をクリックし、任意のオプションを選択します。
5. カード所持者に認証情報を追加します。*認証情報の追加, on page 96*を参照してください。
6. [Save (保存)] をクリックします。
7. グループにカード所持者を追加します。
   7.1. [Groups (グループ)] でカード所持者を追加するグループを選択し、[Edit (編集)] をクリックします。
   7.2. [+ Add (追加)] をクリックし、グループに追加するカード所持者を選択します。複数のカード所持者を選択できます。
   7.3. [追加] をクリックします。
   7.4. [Save (保存)] をクリックします。

高度	
長いアクセス時間	ドアモニターが設置されていて、カード所持者に長いアクセス時間と長い長時間のドア開放を許可する場合に選択します。
カード所持者の停止	カード所持者を停止する場合に選択します。
Allow double-swipe (ダブルスワイプを許可する)	カード所有者がドアの現在の状態を上書きできるようにする場合に選択します。たとえば、通常のスケジュール外にドアのロックを解除するために使用できます。
閉鎖の対象外	閉鎖中にカード所持者がアクセスできるようにする場合に選択します。
Exempt from anti-passback (不正通行防止からの免除)	カード所持者に不正通行防止ルールからの免除を与える場合に選択します。不正通行防止は、カード所持者が自分より前にそのエリアに入った人と同じ認証情報を使用することを防ぎます。最初の人は、認証情報を再度使用する前に、まずそのエリアから退出する必要があります。
グローバルカード所持者	サブサーバーでカード所持者を表示および監視できるようにする場合に選択します。このオプションは、メインサーバーで作成されたカード所持者にのみ使用できます。を参照してください。

認証情報の追加

カード所持者には、次のタイプの認証情報を追加できます。

- PIN
- カード
- ナンバープレート
- 携帯電話

カード所持者にナンバープレート認証情報を追加するには：

1. [Credentials (認証情報)] で [+ Add (追加)] をクリックし、[License plate (ナンバープレート)] を選択します。
2. 車両を表す認証情報名を入力します。
3. 車両のナンバープレート番号を入力します。
4. 認証情報の開始日と終了日を設定します。
5. [追加] をクリックします。

*認証情報としてナンバープレート番号を使用する, on page 97*の例を参照してください。

カード所持者にPIN認証情報を追加するには：

1. [Credentials (認証情報)] で [+ Add (追加)] をクリックし、[PIN] を選択します。
2. PINを入力します。
3. 強制PINを使用して無音アラームをトリガーするには、[Duress PIN (強制PIN)] をオンにして強制PINを入力します。
4. [追加] をクリックします。

PINの認証情報は常に有効です。ドアを開けてシステム内で無音アラームをトリガーする強制PINを設定することもできます。

カード所持者にカード認証情報を追加するには：

1. [Credentials (認証情報)] で [+ Add (追加)] をクリックし、[Card (カード)] を選択します。
2. カードデータを手動で入力するには、カード名、カード番号、ビット長を入力します。

注

ビット長は、システムに存在しない特殊なビット長のカードフォーマットを作成する場合にのみ設定可能です。

3. 前回読み取られたカードのカードデータを自動的に取得するには:
   3.1. [Select reader (リーダーの選択)] のドロップダウンメニューからドアを選択します。
   3.2. そのドアに接続されているリーダーにカードを読み取らせます。
   3.3. [Get last swiped card data from the door's reader(s) (ドアのリーダーから前回読み取ったカードデータを取得)] をクリックします。
4. 設備コードを入力します。このフィールドは、[Access management (アクセス管理)] > [Settings (設定)] で [Facility code (設備コード)] を有効にしている場合のみ使用できます。
5. 認証情報の開始日と終了日を設定します。
6. [追加] をクリックします。

有効期限	
発効日	認証情報が有効になる日時を設定します。
失効日	ドロップダウンメニューからオプションを選択します。

失効日	
終了日がありません	認証情報に有効期限を設けません。
日付	認証情報が失効する日時を設定します。
最初の使用から	認証情報を初めて使用してから失効するまでの期間を選択します。最初に使用してからの日数、月数、年数、または回数を選択します。
最後の使用から	認証情報を最後に使用してから失効するまでの期間を選択します。最後に使用してからの日数、月数、または年数を選択します。

認証情報としてナンバープレート番号を使用する

この例では、ドアコントローラーと共に、AXIS License Plate Verifierをインストールしたカメラを利用することで、車両のナンバープレート番号を認証情報として使用してアクセスを許可する方法を示します。

1. ドアコントローラーとカメラを AXIS Optimizerに追加します。
2. [Synchronize with server computer time (サーバーコンピューターの時刻と同期)] を使用して、新しい装置の日付と時刻を設定します。
3. 新しいデバイスのソフトウェアを利用可能な最新バージョンにアップグレードします。
4. ドアコントローラーに接続された新しいドアを追加します。*ドアを追加する手順*については、*, on page 78*を参照してください。
   4.1. リーダーを [Side A (A面)] に追加します。*「リーダーの追加」, on page 83*を参照してください。
   4.2. [Door settings (ドア設定)] で、[Reader type (リーダータイプ)] として [AXIS License Plate Verifier] を選択し、リーダーの名前を入力します。
   4.3. 必要に応じて、[Side B (側面B)] にリーダーまたはREX装置を追加します。
   4.4. Okをクリックします。
5. AXIS License Plate Verifierをカメラにインストールしてアクティブ化します。*AXIS License Plate Verifier*ユーザーマニュアルを参照してください。
6. AXIS License Plate Verifierを起動します。
7. AXIS License Plate Verifierを設定します。
   7.1. [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。
   7.2. [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。
   7.3. カメラのwebインターフェースからAXIS License Plate Verifierを開きます。
   7.4. 設定は行わないでください。
   7.5. [Settings (設定)] に移動します。
   7.6. [Access control (アクセスコントロール)] で、[Type (タイプ)] に [Secure Entry] を選択します。

7.7. [IP address (IPアドレス)] に、ドアコントローラーのIPアドレスを入力します。
7.8. [Authentication key (認証キー)] に、先ほどコピーした認証キーを貼り付けます。
7.9. [Connect (接続)] をクリックします。
7.10. [Door controller name (ドアコントローラー名)] で、使用するドアコントローラーを選択します。
7.11. [Reader name (リーダー名)] で、先ほど追加したリーダーを選択します。
7.12. 統合をオンにします。
8. アクセス権を付与するカード所持者を追加します。*カード所持者の追加, on page 95*を参照してください。
9. 新しいカード所持者にナンバープレートの認証情報を追加します。*認証情報の追加, on page 96*を参照してください。
10. アクセスルールを追加します。*アクセスルールを追加します。, on page 98*を参照してください。
10.1. スケジュールを追加します。
10.2. ナンバープレートへのアクセス権を付与するカード所持者を追加します。
10.3. AXIS License Plate Verifierリーダーのあるドアを追加します。

「グループの追加」

グループを使用すると、カード所持者とそのアクセスルールをまとめて効率的に管理することができます。

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Cardholder management (カード所持者の管理)] に移動します。
2. [Group (グループ)] に移動し、[+Add (追加)] をクリックします。
3. グループ名と、オプションとしてグループのイニシャルを入力します。
4. [Global group (グローバルグループ)] を選択すると、サブサーバーでカード所持者を表示および監視できるようになります。このオプションは、メインサーバーで作成されたカード所持者にのみ使用できます。*マルチサーバーBETA, on page 93*を参照してください。
5. 以下の手順に従ってグループにカード所持者を追加します。
5.1. [+ Add (追加)] をクリックします。
5.2. 追加するカード所持者を選択し、[Add (追加)] をクリックします。
6. [Save (保存)] をクリックします。

アクセスルールを追加します。

アクセスルールによって、アクセス権を付与されるための条件が定義されます。

アクセスルールの構成要素は以下のとおりです。

カード所持者とカード所持者グループ: - アクセス権が付与される人です。

ドアとゾーン - アクセス権が適用される場所です。

スケジュール - アクセス権が付与される期間です。

アクセスルールを追加するには:

1. [Access control (アクセスコントロール)] > [Cardholder management (カード所持者の管理)] に移動します。
2. [Access rules (アクセスルール)] で [+ Add (追加)] をクリックします。
3. アクセスルール名を入力し、[Next (次へ)] をクリックします。

4. カード所持者とグループを設定する:
   4.1. [Cardholders (カード所持者)] か [Groups (グループ)] で [+ Add (追加)] をクリックします。
   4.2. カード所持者またはグループを選択し、[Add (追加)] をクリックします。
5. ドアとゾーンを設定する:
   5.1. [Doors (ドア)] か [Zones (ゾーン)] で [+ Add (追加)] をクリックします。
   5.2. ドアまたはゾーンを選択し、[Add (追加)] をクリックします。
6. スケジュールを設定する:
   6.1. [Schedules (スケジュール)] で、[+ Add (追加)] をクリックします。
   6.2. 1つ以上のスケジュールを選択し、[Add (追加)] をクリックします。
7. [Save (保存)] をクリックします。

上記の構成要素の1つ以上が欠けているアクセスルールは、不完全です。すべての不完全なアクセスルールは、[Incomplete (不完全)] タブで確認することができます。

手動でドアとゾーンのロックを解除する

ドアの手動ロック解除などの手動アクションについては、*手動アクション, on page 87*を参照してください。

ゾーンの手動ロック解除などの手動アクションについては、*手動アクション, on page 87*を参照してください。

システム設定レポートをエクスポートする

システムに関するさまざまな種類の情報を含むレポートをエクスポートできます。AXIS Optimizer はレポートをCSV (カンマ区切り値) ファイルとしてエクスポートし、デフォルトのダウンロードフォルダーに保存します。レポートをエクスポートするには:

1. [Reports (レポート)] > [System configuration (システム設定)] に移動します。
2. エクスポートするレポートを選択し、[Download (ダウンロード)] をクリックします。

カード所有者の詳細	カード所持者、認証情報、カードの有効性、前回の利用状況についての情報が記載されています。
カード所有者のアクセス	カード所持者の情報と、カード所持者に関連するカード所持者グループ、アクセスルール、ドア、ゾーンについての情報が記載されています。
カード所持者グループのアクセス	カード所持者グループ名と、カード所持者グループに関連するカード所持者、アクセスルール、ドア、ゾーンについての情報が記載されています。
アクセスルール	アクセスルール名と、アクセスルールに関連するカード所持者、カード所持者グループ、ドア、ゾーンについての情報が記載されています。
ドアアクセス	ドアの名前と、ドアに関連するカード所持者、カード所持者グループ、アクセスルール、ゾーンについての情報が記載されています。
ゾーンアクセス	ゾーンの名前と、ゾーンに関連するカード所持者、カード所持者グループ、アクセスルール、ドアについての情報が記載されています。

カード所持者活動レポートの作成

点呼レポートは、指定されたゾーン内のカード所持者のリストを表示し、特定の時点にそこにいる人を特定するのに役立ちます。

集合レポートは、指定されたゾーン内のカード所持者のリストを表示し、緊急時に安全が確認された人と行方不明者の確認に役立ちます。建物の管理者が避難後にスタッフや訪問者の所在を確認する際に役立ちます。集合場所は、緊急時に職員が安否を報告し、現場にいる人と現場にいない人のリストを作成するために設けられたリーダーです。システムは、カード所持者が集合場所でチェックインするか、誰かが手動で安全であるとマークするまで、カード所持者を行方不明としてマークします。

点呼レポートと集合レポートはどちらも、カード所持者を追跡するためのゾーンを必要とします。

点呼または集合レポートを作成して実行するには、以下の手順に従います。

1. [**Reports (レポート)**] > [**Cardholder activity (カード所持者の活動)**] に移動します。
2. [**+ Add (追加)**] をクリックし、[**Roll call / Mustering (点呼/集合)**] を選択します。
3. レポート名を入力します。
4. レポートに含めるゾーンを選択します。
5. レポートに含めるグループを選択します。
6. 集合レポートが必要な場合は、[**Mustering point (集合場所)**] と集合場所のリーダーを選択します。
7. レポートのタイムフレームを選択します。
8. **[Save (保存)]** をクリックします。
9. レポートを選択し、[**Run (実行)**] をクリックします。

点呼レポートのステータス	説明
在席	カード所持者が指定ゾーンに入り、レポートを実行するまでに退出しなかった場合。
不在	カード所持者が指定ゾーンを退出し、レポートを実行するまでに再度入らなかった場合。

集合レポートのステータス	説明
安全	カード所持者が集合場所でカードをスワイプした場合。
行方不明	カード所持者が集合場所でカードをスワイプしなかった場合。

アクセス管理の設定

アクセス管理ダッシュボードで使用するカード所持者フィールドをカスタマイズする手順は、以下のとおりです。

1. [**Access Management (アクセス管理)**] タブで、[**Settings (設定)**] > [**Custom cardholder fields (カード所持者フィールドをカスタマイズ)**] をクリックします。
2. [**+ Add (追加)**] をクリックして名前を入力します。カスタムフィールドは最大6つまで追加できます。
3. [**追加**] をクリックします。

設備コードを使用してアクセスコントロールシステムを検証するには:

1. [Access Management (アクセス管理)] タブで、[Settings (設定)] > [Facility code (設備コード)] をクリックします。
2. [Facility code on (設備コードオン)] を選択します。

注

識別プロファイルを設定するときは、[Include facility code for card validation (カード検証用の設備コードを含める)] も選択する必要があります。を参照してください。

インポートとエクスポート

カード所持者のインポート

このオプションでは、CSVファイルからカード所持者、カード所持者グループ、認証情報、カード所持者の写真がインポートされます。カード所持者の写真をインポートするには、サーバーが写真にアクセスできることを確認してください。

カード所持者をインポートすると、アクセス管理システムは、すべてのハードウェア設定を含むシステム設定を自動的に保存し、以前に保存したものは削除します。

インポートオプション	
新規	このオプションを選択すると、既存のカード所有者が削除されてから、新しいカード所有者が追加されます。
更新	このオプションを選択すると、既存のカード所持者が更新され、新規のカード所持者が追加されます。
追加	このオプションを選択すると、既存のカード所持者が保持されたうえで、新しいカード所持者が追加されます。カード番号とカード所持者IDは一意であり、一度しか使用できません。

1. [Access Management (アクセス管理)] タブで、[Import and export (インポートとエクスポート)] をクリックします。
2. [Import cardholders (カード所持者をインポートする)] をクリックします。
3. [New (新規)]、[Update (更新)]、または [Add (追加)] を選択します。
4. [Next (次へ)] をクリックします。
5. [Choose a file (ファイルを選択する)] をクリックし、CSVファイルに移動します。[Open (開く)] をクリックします。
6. 列区切り文字を入力し、一意の識別子を選択して [Next (次へ)] をクリックします。
7. 各列に見出しを割り当てます。
8. [Import (インポート)] をクリックします。

インポート設定	
最初の行はヘッダー	CSVファイルに列ヘッダーが含まれている場合に選択します。
列区切り記号	CSVファイルの列区切り形式を入力します。

インポート設定	
一意の識別子	システムでは、デフォルトで**Cardholder ID (カード所持者ID)** を使用してカード所持者が識別されます。姓と名、またはメールアドレスを使用することもできます。一意の識別子により、重複するカード所持者レコードのインポートが防止されます。
カード番号の形式	デフォルトでは [**Allow both hexadecimal and number (16進数と数字の両方を有効にする)**] が選択されています。

: カード所持者をエクスポートする

このオプションを実行すると、システム内のカード所持者データがCSVファイルにエクスポートされます。

1. [**Access Management (アクセス管理)**] タブで、[**Import and export (インポートとエクスポート)**] をクリックします。
2. [**Export cardholders (カード所持者をエクスポートする)**] をクリックします。
3. ダウンロード先を選択し、[**Save (保存)**] をクリックします。

AXIS Optimizerは設定が変更されるたびに、`C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos`のカード会員写真を更新します。

インポートの取り消し

カード所持者をインポートすると、設定が自動的に保存されます。[**Undo import (インポートの取り消し)**] オプションを選択すると、カード所持者データとすべてのハードウェア設定が、最後にカード所持者をインポートした前の状態にリセットされます。

1. [**Access Management (アクセス管理)**] タブで、[**Import and export (インポートとエクスポート)**] をクリックします。
2. [**Undo import (インポートの取り消し)**] をクリックします。
3. [**Yes (はい)**] をクリックします。

バックアップとリストア

自動バックアップは毎日夜間に実行されます。最新のバックアップファイル3つは、C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\backup に保存されます。これらのファイルを復元する:

1. バックアップファイルを C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\restore に移動します。
2. AXIS Secure Entryを以下のいずれかの方法で再起動します。
   - MSC (Services) プログラムを起動し、"AXIS Optimizer Secure Entry Service" を探して再起動します。
   - コンピューターを再起動します。
3. イベントサーバーマシンで、AXIS Optimizerのインストーラーを再度実行します。

Smart Clientのアクセス管理

Smart Clientを通じて、オペレーターはアクセスコントロールシステムに関連する操作を行うことができます。手動によるドアコントロールなど、アクセスコントロールのほとんどの機能がSmart

Clientで利用できます。これらの機能の詳細については、*Smart Clientでアクセスコントロールを使用する*を参照してください。

Smart Clientで直接アクセスを管理することも可能です。Management Clientに搭載されている以下の機能は、Smart Clientでも利用できます。

- カード所持者の管理
- 一般設定
- カスタムカード所持者フィールド
- 設備コード
- 電子メールテンプレート
- バッジのテンプレート BETA

Smart ClientでAxisアクセス管理タブを表示するには:

1. Smart ClientマシンにAXIS Optimizerをインストールします。
2. まだ有効になっているドアがない場合は、1つのドアのライセンスを有効にします。ドアのライセンスを有効にするには、*ドアのライセンスを有効にする, on page 75*を参照してください。
3. サインイン中のユーザーがアクセス管理権限を持っていることを確認してください。*AXIS Secure Entryのロール設定, on page 103*を参照してください。

AXIS Secure Entryのロール設定

1. Management Clientで、**[Site Navigation (サイトナビゲーション)]** > **[Security (セキュリティ)]** > **[Roles (ロール)]** に移動します。
2. システムの特定のロールを選択します。
3. **[AXIS Optimizer]** を選択します。
4. リストを展開し、**[Access control (アクセスコントロール)]** をクリックします。
5. **[Read (読む)]** を選択してアクセスコントロールのセキュリティ設定を確認します。
6. そのロールに権限を付与する機能をクリックし、**[Grant (許可)]** をクリックします。
   - **Access control configuration (アクセスコントロール設定):** [Configuration (設定)] タブのすべての機能に対し、オペレーターロール権限が付与されます。
   - **Access management (アクセス管理):** [Access Management (アクセス管理)] タブのすべての機能に対し、オペレーターロール権限が付与されます。

システム管理とセキュリティコントロール

オペレーター向けに機能へのアクセスをカスタマイズする

役割設定

デフォルトでは、オペレーターはVMSの装置にもアクセスできる場合、Smart Clientのすべての AXIS Optimizer機能にアクセスできます。ただし、Management Clientでは、オペレーターがアクセスできる機能を [Role settings (ロール設定)] から設定できます。

役割設定の定義

[Role settings (役割の設定)] をオンにします。

1. Management Clientで、[Site Navigation > Security > AXIS Optimizer Security (サイトナビゲーション > セキュリティ > AXIS Optimizerのセキュリティ)] に移動します。

注

一度オンにした役割の設定をオフにすることはできません。この設定は永久的です。

2. [Turn on role settings (役割の設定をオンにする)] を選択します。
3. Management Clientを再起動します。

Role settings (役割設定) を定義する:

1. Management Clientで、[Site Navigation > Security > Roles (サイトナビゲーション > セキュリティ > 役割)] に移動します。
2. 役割を選択し、[Overall security (全体的なセキュリティ)] に移動します。
3. [AXIS Optimizer Security (AXIS Optimizerのセキュリティ)] をクリックします。
4. 役割がアクセスできる機能、アクセスできない機能を選択します。
   - Full control (フルコントロール)オペレーターの役割に、すべてのAXIS Optimizerへのフルアクセス権を割り当てます。
   - Edit (not applicable) (編集 (適用なし))AXIS Optimizerの役割設定に適用されないVMSの機能です。
   - Access AXIS Optimizer in Management Client (Management ClientでのAXIS Optimizerへのアクセス)。オペレーターがManagement Client内のすべてのAXIS Optimizerの管理機能を使用することができます。
   - Manage AXIS Optimizer security (AXIS Optimizerのセキュリティの管理)。オペレーターが [Site Navigation (サイトナビゲーション)] > [Security (セキュリティ)] > [AXIS Optimizer Security (AXIS Optimizerセキュリティ)] で設定を変更できます。
   - Dynamic camera operator controls (ダイナミックカメラオペレーターコントロール)。オペレーターが、システムがデバイス上で検出したすべてのプリインストール済み機能にアクセスできます。
   - Remote focus operator control (リモートフォーカスオペレーターコントロール)。オペレーターが固定ドームカメラにリモートフォーカスを設定できます。
   - PTZ operator controls (PTZオペレーターコントロール)。オペレーターの役割で、次のオペレーターPTZ コントロールにアクセスできます:フォーカスコントロール、PTZプリセット、Autotracking 2用オペレーターコントロール、ウォッシャー、SpeedDry/ワイパーボタン。
   - Temperature spot measurement control (温度スポット測定コントロール)。オペレーターの役割で、AXIS Q2901-Eでスポット温度を測定できます。
   - Speaker operator control (スピーカーオペレーターコントロール)。オペレーターが、Smart Clientのすべてのスピーカーマネージャー機能にアクセスできます。

- **Access visitor management (訪問者管理へのアクセス)。**オペレーターの役割で、訪問者管理に関するあらゆるものにアクセスでき、たとえば、呼び出しに応答したり、ライブビューでドアを開けたりすることができます。
- **Access call history (呼び出し履歴へのアクセス)。**オペレーターの役割で、インターコムの呼び出し履歴にアクセスできます。この設定を使用するには、**Access visitor management (訪問者管理へのアクセス)**を許可する必要があります。
- **Extended search functions (拡張検索機能)。[Deny (拒否)]** を選択すると、Smart Clientの [AXIS License Plate Verifier] タブが非表示になります。また、一元検索では車両とコンテナの検索を使用できません。
- **Control dewarping view (歪み補正ビューの制御)。**オペレーターが歪み補正ビュー内を移動できます。
- **Edit a dewarping view's home position (歪み補正ビューのホームポジションの編集)。**オペレーターがカメラのホームポジションを編集できます。
- **Web ページ**オペレーターが、Webブラウザを使用してビューを作成できます。
- **Axis insights dashboard**
  オペレーターの役割により、Axis Insights Dashboardにアクセスできます。

5. **[Save (保存)]** をクリックします。
6. システムで実行中のすべてのSmart Clientを再起動します。

デバイスの管理

AXIS Device Manager Extend

AXIS Optimizerでは、AXIS Device Manager Extendを使用して、複数のサイトの装置を管理することができます。録画サーバーにエッジホストを設定することで、AXIS Device Manager ExtendはVMS内の装置に接続できます。単一のユーザーインターフェースから、複数の装置やサイトの保証情報の確認やソフトウェアのアップグレードを簡単に行うことができます。

AXIS Device Manager Extendの詳細については、*ユーザーマニュアル*を参照してください。

注

要件

- お使いの*MyAxisアカウント*にログインします。
- 録画サーバーはインターネットにアクセスできる必要があります。
- AXIS OS 6.50を実行している装置でのみサポートされます。対応デバイスについては、*FAQ*を参照してください。

エッジホストをインストールする

エッジホストは、AXIS Device Manager ExtendがVMS内のローカル装置と通信できるようにするオンプレミス管理サービスです。

VMS内でAXIS Device Manager Extendを使用するには、エッジホストとデスクトップクライアントをインストールする必要があります。エッジホストとデスクトップクライアントの両方がAXIS Device Manager Extendのインストーラーに含まれています。

1. AXIS Device Manager Extendのインストーラーをダウンロードします。
   エッジホストは、VMS録画サーバーにインストールする必要があります。
2. 録画サーバーでインストーラーを実行し、エッジホストのインストールのみを選択します。

オープンネットワークポートやその他の要件の詳細については、*Axis Device Manager Extendユーザーマニュアル*を参照してください。

エッジホストの申し立てと装置の同期



1. Management Clientを開きます。
2. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [System overview (システムの概要)] に移動します。
3. を選択して、MyAxisにログインします。
4. 申し立てる準備が整っているエッジホストがインストールされている録画サーバータイルをクリックします。
5. サイドバーで、組織を新規作成するか、以前に作成した組織を選択します。
6. エッジホストをクリックし、申し立てをします。
7. ページが再読み込みされるまで待ち、[Synchronize (同期)] をクリックします。
   録画サーバー上のすべてのAxisデバイスがエッジホストに追加され、選択した組織に属するようになります。

注

AXIS Device Manager Extendは、VMS内のAxisハードウェアにアクセスできる必要があります。対応デバイスの詳細については、*エッジホストに装置を追加する際のトラブルシューティング, on page 107*を参照してください。

8. 録画サーバーに新しい装置を追加したり、装置の情報を変更したりする場合は、手順7を再度実行して、変更内容をAXIS Device Manager Extendシステムと同期します。
9. AXIS Device Manager Extendに追加する装置を持つすべての録画サーバーについて、手順4～7を繰り返します。

エッジホストのステータス

[System Overview (システムの概要)] の各録画サーバーで、エッジホストがインストール済み、または要求済みであるかどうか確認できます。[Show machines that need edge host action (エッジホストのアクションが必要なマシンを表示)] オンにして、ビューを絞り込むことができます。

- - 録画サーバーでエッジホストが検知されませんでした。
  - エッジホストがインストールされていない場合は、録画サーバーでエッジホストをダウンロードしてインストールします。*エッジホストをインストールする, on page 105*を参照してください。
  - エッジホストがインストールされている場合、エッジホストを検出するには、MyAxisアカウントにログインする必要があります。
- - エッジホストがインストール済みですが、申し立てされていません。新しい組織を作成するか、以前に作成した組織を選択することで、エッジホストの申し立てをします。*エッジホストの申し立てと装置の同期, on page 106*を参照してください。
- - エッジホストをインストール済みで、要求済みですが、要求が到達していません。録画サーバーがインターネットに接続しているか確認してください。

-  - エッジホストが同期されます。
-  – エッジホストの同期が必要です。エッジホストに追加可能なVMS内の新規デバイス、または、同期が必要な更新済みの装置情報である可能性があります。

AXIS Device Manager Extendを使って装置を設定する

装置がエッジホストに同期されると、AXIS Device Manager Extendで装置を設定できます。これは、インターネットに接続されている任意のPCから行うことができます。

注

また、リモート接続を介したデバイスを管理する場合は、*各エッジホストのリモートアクセス*をオンにする必要があります。

1. *AXIS Device Manager Extendデスクトップアプリケーション*をインストールして開きます。
2. エッジホストの申し立てに使用した組織を選択します。
3. 同期された装置は、VMS録画サーバーと同じ名前のサイトで見つけることができます。

エッジホストに装置を追加する際のトラブルシューティング

エッジホストに装置を追加する際に問題が発生した場合は、以下の手順に従ってください。

- AXIS Optimizerは、VMSから有効なハードウェアのみを追加します。
- VMS内のハードウェアとの接続が切れていないことを確認します。
- 装置にAXIS OS 6.50以上がインストールされていることを確認します。
- 装置がダイジェスト認証に設定されていることを確認します。デフォルトでは、AXIS Device Managementはベーシック認証に対応していません。
- AXIS Device Manager Extendアプリケーションから装置を直接追加します。
- AXIS Device Manager Extendからログを収集して、Axisのサポートにお問い合わせください。
  1. AXIS Device Manager Extendアプリケーションで、カメラがインストールされている録画サーバー上の特定のサイトに移動します。
  2. [**Settings (設定)**] に移動し、[**Download sitelog (サイトログのダウンロード)**] をクリックします。

AXIS Site Designerのインポート

AXIS OptimizerにAXIS Site Designerの設計プロジェクトをインポートし、1回の簡単なインポートプロセスでその設定をVMSに適用できます。*AXIS Site Designer*使用して、システムの設計と構成を行います。プロジェクトが完了した後は、AXIS Optimizerを使用してすべてのカメラ、および他の装置の設定をAXIS Site DesignerからManagement Clientにインポートできます。

AXIS Site Designerの詳細については、*ユーザーマニュアル*を参照してください。

注

要件

- VMSバージョン2020 R2以降

設計プロジェクトをインポートする



AXIS Site Designerにインポートする

1. プロジェクトを作成し、装置を設定します。
2. プロジェクトを完了し、コードを生成するか、設定ファイルをダウンロードしてください。

注

設計プロジェクトを更新するには、新しいコードを生成するか、新しい設定ファイルをダウンロードする必要があります。

マネジメントクライアントで：

1. 関連する装置がVMSに追加されていないことを確認します。
2. **[Site Navigation] > [AXIS Optimizer] > [設計プロジェクトのインポート]** に移動します。
3. ステップバイステップのガイドが開きます。アクセスコードを入力するか、プロジェクトの設定ファイルを選択してインポートするプロジェクトを選択します。**[Next (次へ)]** をクリックします。
4. **[Project overview (プロジェクトの概要)]** で、AXIS Site Designerプロジェクトで検出されたデバイス数と、VMSで検出されたデバイス数の情報を確認できます。**[Next (次へ)]** をクリックします。
5. 次の手順で、VMSの装置をAXIS Site Designer設計プロジェクトの装置に紐付けします。紐付け候補が1つしかないデバイスは自動的に選択されます。紐付けされたデバイスだけがインポートされます。紐付けが完了したら、[Next] (次へ) をクリック します。
6. 紐付けされたすべての装置の設定がインポートされ、VMSに適用されます。設計プロジェクトのサイズにより、このプロセスには数分かかる場合があります。**[Next (次へ)]** をクリックします。
7. [Results of import] (インポートの結果) で、インポートプロセスのさまざまな手順について詳細情報を確認できます。一部の設定がインポートできていない場合は、問題を解決し、再度インポートを実行してください。結果の一覧をファイルとして保存するには、[Export...] (エクスポート) をクリックします。[Done] (完了) をクリックして、ステップバイステップのガイドを終了します。

インポートされた設定

インポートには、VMSと設計プロジェクトにより相互に紐付けされた装置だけが含まれます。以下の設定がVMSにインポートされ、すべての装置タイプに適用されます。

- 設計プロジェクトで使用される装置名
- 設計プロジェクトで使用される装置の説明
- 装置がマップ上に配置されている場合の位置情報設定

装置がビデオ対応の場合、以下の設定も適用されます。

- VMSに構成された1~2つのビデオストリーム (解像度、フレームレート、コーデック、圧縮、Zipstream設定)

  - ビデオストリーム1は、ライブビューと録画用に設定されています。
  - ビデオストリーム2は、設計プロジェクトのライブビューと録画でストリーミング設定が異なる場合、録画用に設定されています。
- 動体検知や連続録画のルールは、設計プロジェクトに従って設定されます。VMS内蔵の動体検知が使用されています。ルールのタイムプロファイルが作成され、録画サーバー上に異なる保存期間のストレージプロファイルが作成されています。
- マイクは、設計プロジェクトの音声設定に従ってオンまたはオフになります。

制限事項

VMSにAXIS Site Designerの設計プロジェクトをインポートするにあたっては、いくつかの制限事項があります。

- VMSのデフォルトの動体録画ルールが、インポート時に作成された録画ルールを上書きする可能性があります。競合するルールをオフにするか、影響を受ける装置をルールから除外してください。
- VMSでの動きをトリガーとした録画の場合、録画の推定が不正確になる可能性があります。
- 現在のバージョンでは、間取り図はサポートされていません。
- 設計プロジェクトで、動きによるトリガーを使った録画と連続録画の両方が同時に設定されている場合、動きによるトリガーを使った録画設定のストリーミング設定のみ使用します。
- VMSでは、Zipstream向けに最小フレームレートを設定することはできません。

アカウントの管理

アカウントの管理は、XProtectで使用されるすべてのAxis装置のアカウントとパスワードを管理する上で役立ちます。

Axisのガイドラインに定められている通り、装置への接続にrootアカウントを使用しないでください。アカウント管理を使用して、XProtectサービスアカウントを作成できます。各装置に一意の16文字のパスワードが作成されます。すでにXProtectアカウントを持っている装置は、新規のパスワードを取得します。

XProtectサービスアカウントで装置に接続する

1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Account management (アカウントの管理)] を開きます。
   グラフは、オンラインの装置の数、XProtectサービスアカウントを持つ装置の数、およびXProtectサービスアカウントを持たない装置の数を示します。
2. [Show device details (装置の詳細を表示)] をクリックして、装置の情報を詳しく表示できます。オンラインの装置はリストの一番上に表示されます。特定の装置を選択して、パスワードを生成することができます。選択していない場合、オンラインになっているすべての装置が新規のパスワードを取得します。[OK]をクリックします。

注

ハードウェア構成でHTTPを選択した場合、パスワードは記録サーバーとAxisデバイス間でプレーンテキストで送信されます。VMSとデバイス間の通信を保護するためにHTTPSを設定することをお勧めします。

3. [Generate passwords (パスワードを生成する)] をクリックします。生成されたパスワードには、32～126文字の範囲の16個のASCII文字のランダムなテキストが含まれます。
   [Show device details (装置の詳細を表示)] をクリックして、プロセスのライブステータス更新を確認します。このプロセスを実行すると、アクティブなライブビューと保留中の録画がわずかな時間中断されます。

4. オンラインの装置は、XProtectサービスアカウントと新規パスワードを取得します。オンラインで、既存のXProtectサービスアカウントを持っている装置は、新規パスワードのみを取得します。

Axisイベント

Axisイベント機能は、VMS内のAxis装置で使用可能なイベントの概要を示します。特定の装置でイベントをテストしたり、イベントの詳細を表示したり、複数の装置にイベントを追加したりできます。

[Site Navigation (サイトナビゲーション)] で、[Rules and Events (ルールとイベント)] > [Axis events (Axisイベント)] に移動します。使用可能なすべてのイベントのリストが [Configuration (設定)] ウィンドウに表示されます。システム内でアクティブなイベントとアクティブでないイベントを確認できます。

イベントごとに、イベントが追加されている装置の装置名を確認できます。イベントの表示名、イベントの状態、イベントが最後にトリガーされた時間も確認できます。

注

要件

- VMSバージョン2023 R2以降。

複数の装置でイベントを設定する

1. [Configuration (設定)] に移動し、イベントを選択します。
2. Add devices (デバイスを追加) をクリックします。
3. [Add devices (デバイスの追加)] ウィンドウに、イベントを追加できる装置のリストが表示されます。1つ以上の装置を選択し、[Add devices (デバイスの追加)] をクリックします。

装置からイベントを削除するには、[Remove (削除)] をクリックします。

イベント情報

Axisイベントでは、ユーザーインターフェースで最後の既知のイベント、イベントの状態、リアルタイムの更新を表示できます。そのためには、Management Clientで保存期間を設定する必要があります。

1. [Tools (ツール)] > [Options (オプション)] > [Alarm and Events (アラームとイベント)] > [Event retention (イベントの保持)] に移動します。
2. 装置イベントグループ全体またはグループ内の特定のイベントの保存期間を設定します。

メタデータと検索

メタデータと検索では、VMSに追加したすべての装置、そのメタデータ機能、オペレーターに表示されるAxis検索カテゴリの概要が表示されます。

メタデータと検索を使用すると、これらの装置の特定の機能をオンにすることができます。つまり、複数の装置のイベントデータ、分析機能データ、統合データをオンにしたり、装置がサポートする分析機能を表示したりすることができます。Axisの検索カテゴリにより、すべてのオペレーターの検索オプションを制御して、VMSで利用可能な分析機能を反映することができます。検索カテゴリとフィルターのサポートは、カメラのモデルやインストールされている分析機能アプリケーションによって異なります。

メタデータ設定を行う

1. [Management Client (管理クライアント)] > [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Metadata and search (メタデータと検索)] に移動します。

- **イベントデータ**:VMSでオンにして、装置からイベントデータを取得します。これは、AXIS Optimizerのいくつかの機能に必要です。
- **Analytics data (分析データ)**:オンにすると、フォレンジック検索機能が使用され、ライブビューおよび再生で境界ボックスが表示されます。
- **Analytics features (分析機能)**:物体のタイプ (人、車) や物体の色など、装置が現在サポートしているビデオ分析機能を表示します。装置のソフトウェアをアップグレードすると、より多くの分析機能が利用できるようになります。
- **Consolidated metadata (統合メタデータ)**:オンにすると、フォレンジック検索を高速化し、Axis insightsの読み込み時間が速くなります。

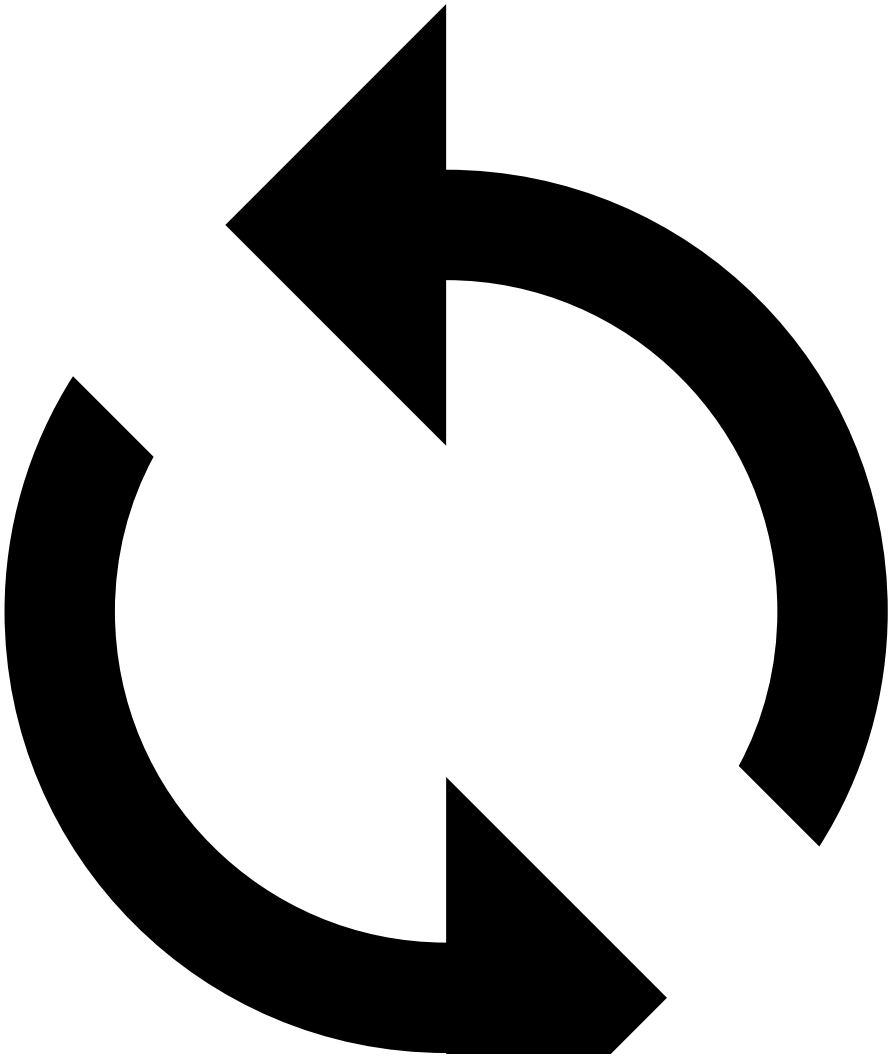
注

統合メタデータ要件

- AXIS OS 11.10以降のバージョンを搭載したAxis装置。

統合メタデータの制限

- ライブビューと録画の境界ボックス、およびVMS組み込みの検索オプションは使用できません。



- :デバイスの設定を変更したら、クリックして再読み込みしてください。

Axis検索カテゴリの設定

1. [Management Client (管理クライアント)] > [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Metadata and search (メタデータと検索)] に移動します。

2. [Axis search categories (Axis検索カテゴリ)] ダイアログで、使用する検索カテゴリをオンにします：
   - フォレンジック検索
   - 車両検索
   - ゾーン速度検索
   - コンテナ検索
3. 各検索カテゴリの下で、適用可能なフィルターを選択します。

注

Axis検索カテゴリの要件

- AXIS Optimizerバージョン5.3以降のSmart Client。

サイバーセキュリティ

サイバーセキュリティは、リスクを最小限に抑えながら、健全な製品ライフサイクルを支援します。当社のサイバーセキュリティへの取り組みに関する詳細な情報や資料は、*axis.com/about-axis/cybersecurity* でご覧いただけます。以下のサイバーセキュリティガイドラインに従ってAxisからの製品に関するセキュリティ通知を受け取り、製品の安全なライフサイクルおよび運用停止のための設定を行ってください。

*Axis Trust Center*では、Axisが実施するセキュリティコンプライアンス、透明性、データ保護、およびプライバシーについての情報をご覧いただけます。

脆弱性の管理

Axisは、*共通脆弱性識別子 (CVE) 採番機関 (CNA)*です。当社は、セキュリティリスクを最小限に抑えるため、当社のデバイス、ソフトウェア、およびサービスの脆弱性の特定と修正において業界標準に従って対応しています。当社の脆弱性管理ポリシーに関する詳細や、脆弱性の報告については、*axis.com/vulnerability-management*を参照してください。

セキュリティ通知

axis.com/security-notification-service から、Axisのセキュリティ通知電子メールを購読してください。お使いのAxis製品に関する脆弱性、関連するセキュリティアドバイザリ、およびその他のセキュリティ関連事項について情報をお送りします。

安全な製品ライフサイクル管理

Axisは、安全なライフサイクル管理を通じて、製品のライフサイクル全体でリスクを最小限に抑えています。*help.axis.com*に掲載されているハードニングガイドには、Axis製品のより安全な設定と操作に関する情報、および以下の情報が含まれています。

安全な初回使用 - Axis製品は、高度な保護機能がデフォルトで組み込まれているため、初回使用時から安全な初期化と暗号化された通信が可能です。

使用目的とよくある設定ミス - 当社のガイドには、Axis製品の使用目的について記載されています。これには、避けるべきよくあるセキュリティ関連の誤った使用や設定ミスについても含まれています。

脆弱性の管理とサプライチェーンの透明性 - 脆弱性の開示およびサプライチェーンの透明性向上を目的として、ソフトウェアのリリースごとに、*axis.com*でソフトウェア部品表 (SBOM) を公開しています。

利用停止とデータの安全な消去 - 製品のライフサイクル終了時に安全に利用を停止するために、工場出荷時の設定にリセットしてください。これにより、設定、保存されたデータ、およびセンシティブな情報が消去されます。

強化ガイド

VMSインフラストラクチャーに不可欠な構成要素であるAXIS Optimizerは、安全な環境を維持するために特定の設定が必要です。デバイスのパスワードを保護し、個人情報を守り、システムへの不正アクセスを防ぐために、推奨されるこれらの設定に従うことが極めて重要です。

- VMSにAxisデバイスを追加する場合はHTTPSを使用する。
- VMSクライアントとサーバー間の暗号化を有効にする。
- VMSで暗号化されたデータストレージを有効にする。
- すべてのVMSロールを確認し、必要以上の権限が割り当てられていないことを確認する。

さらに支援が必要ですか?

FAQ

問題	応答
クライアントPCがインターネット接続できない場合、AXIS Optimizerをどのように更新すればよいですか?	新しいバージョンをVMS管理サーバーに公開します。*システムを自動的にアップグレードする, on page 10*を参照してください。
AXIS Optimizerの新しいバージョンにアップグレードする前に設定をバックアップする必要がありますか ?	いいえ、バックアップする必要はありません。新しいバージョンへのアップグレードでは何も変更されません。
AXIS Optimizerを搭載しているクライアントPCが30台以上ある場合、1台ずつアップグレードする必要がありますか?	クライアントを個別にアップグレードできます。 ローカルのAXIS Optimizerバージョンをシステムに公開して、アップグレードを自動的にプッシュすることもできます。*システムを自動的にアップグレードする, on page 10*を参照してください。
AXIS Optimizer内の各プラグインは、個別に有効化/無効化できますか?	できません。ですが、これらを積極的に使っていない場合はリソースを消費することはありません。
AXIS Optimizerはどのポートを使用していますか?	ポート80と443です。このどちらもaxis.comとの通信に必要であり、システムが新しいリリースの情報を取得し、更新をダウンロードできるようになります。 AXIS Secure Entry経由でAXIS Optimizerをインストールすると、ポート53459および53461が受信トラフィック (TCP) 用に開放されます。

トラブルシューティング

技術的な問題がある場合は、デバッグログをオンにして問題を再現し、Axisサポートにログを提供してください。マネジメントクライアントまたはSMARTクライアントでデバッグログインをオンにすることができます。

マネジメントクライアントで：

1. **サイトナビゲーション** > **ベーシック** > **AXIS Optimizer**に移動します。
2. **デバッグロギングをオンにする**を選択します。
3. **レポートを保存する**をクリックして、ログを装置に保存します。

SMARTクライアントで：

1. **設定**> **Axis一般オプション**に移動します。
2. **デバッグロギングをオンにする**を選択します。
3. **レポートを保存する**をクリックして、ログを装置に保存します。

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。

ヒント

Smart ClientビューでのWebページの追加

AXIS Optimizerは、HTMLページだけでなく、ほとんどのWebページをSmart Clientで直接表示することができます。このWebビューは、最新のブラウザーエンジンを搭載しているため、ほとんどのWebページとの互換性があります。Smart ClientからAXIS Body Worn Managerにアクセスする場合や、ライブビューの横にAXIS Store Reporterのダッシュボードを表示したい場合などに便利です。

1. Smart Clientで、[**Setup (設定)**] をクリックします。
2. [**Views (ビュー)**] に移動します。
3. 新しいビューを作成するか、既存のビューを選択します。
4. [**System overview > AXIS Optimizer (システムの概要 > AXIS Optimizer)**] を開きます。
5. [**Web view (ウェブビュー)**] をクリックし、ビューにドラッグします。
6. アドレスを入力し、[**OK**] をクリックします。
7. [**Setup (設定)**] をクリックします。

検索機能が内蔵されたビデオのエクスポート

ビデオをXProtect形式でエクスポートする

内蔵されたAXIS Optimizerの検索機能および/またはAxis歪み補正機能でビデオを表示するには、必ずXProtect形式でビデオをエクスポートしてください。これはデモ目的などに便利です。

注

AXIS Optimizerバージョン5.3以降の場合は、手順3から開始します。

1. Smart Clientで、[**Settings (設定)**] > [**Axis search options (Axis検索オプション)**] に移動します。
2. [**Include search plugins in exports (エクスポートに検索プラグインを含める)**] をオンにします。
3. Smart Clientでエクスポートを作成するとき、[**XProtect format (XProtect形式)**] を選択します。

受信側コンピューターでエクスポートのブロックを解除する

別のコンピューターでエクスポートを正常に使用するには、エクスポートファイルのアーカイブのブロックを解除してください。

1. 受信側コンピューターで、エクスポートファイル (zip) を右クリックし、**[Properties (プロパティ)]** を選択します。
2. **[General (一般)]** で、**[Unblock (ブロック解除)]** > **[OK]** の順にクリックします。
3. エクスポートを抽出し、"SmartClient-Player.exe" ファイルを開きます。

エクスポートされたAxis歪み補正表示の再生

1. エクスポートしたプロジェクトを開きます。
2. Axis歪み補正表示を含む表示を選択します。

T10134385_ja

2026-09 (M61.2)

© 2021 – 2026 Axis Communications AB