AXIS Secure Entry for XProtect

ユーザーマニュアル

目次

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。

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
5.6	12.6.94.1	12.6.94.1

お使いのシステムに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)]** 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。

アクセスコントロールの設定方法

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、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、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。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。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。

- **サポートされているAXIS OSバージョン:** 上記の対応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。
- **対応する最低限の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、サポートされる最低限のAXIS OSバージョンが決まります。最大で2つ前のバージョンまで対応します。
- **推奨されるAXISOSバージョンを超えてアップグレードする場合:** 特定のVMSに推奨されているバージョンより上のAXIS OSバージョンにアップグレードしたとします。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。
- **今後のAXIS OSに関する推奨事項:** 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。

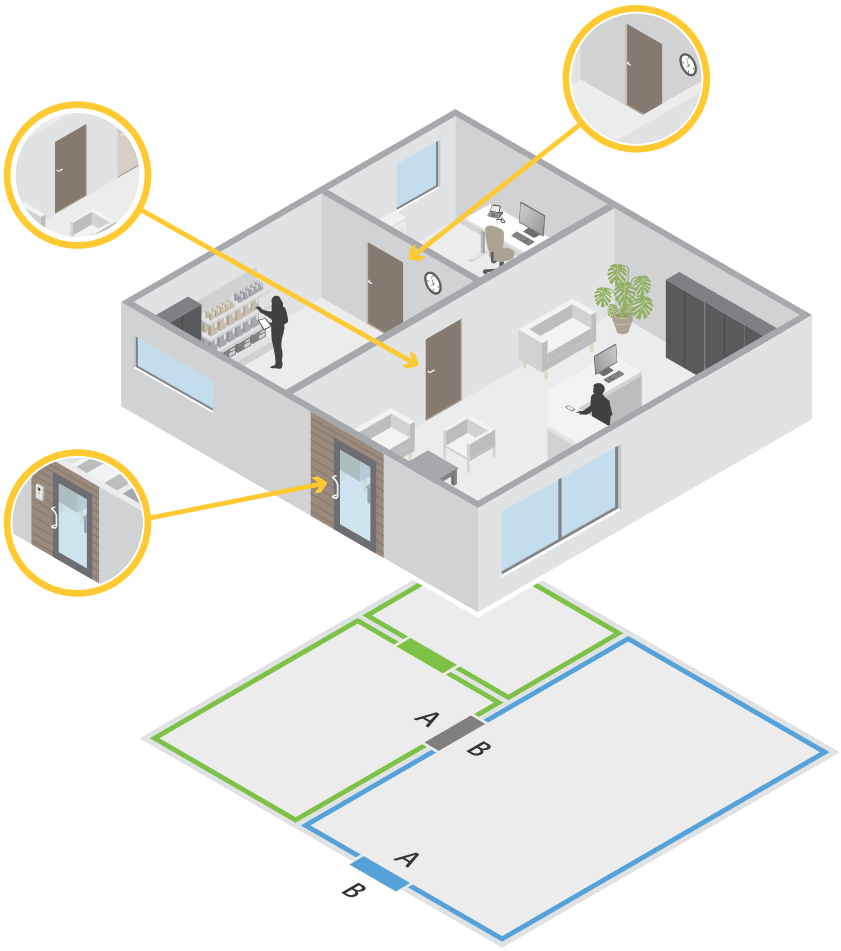
ドアとゾーン

[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。
カード形式と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



- グリーンゾーンとブルーゾーンの2つのゾーンがあります。
- 緑色のドア、青色のドア、茶色のドアの3つのドアがあります。
- 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。

ドアの追加

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い場合、新しいバージョンのAxis Optimizerを使用していて、ドアコントローラーのファームウェアが古いと、システムではドアを追加できません。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。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。を参照してください。
11. 監視ドアを設定します。を参照してください。
12. [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. [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 (閉じた後): 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。

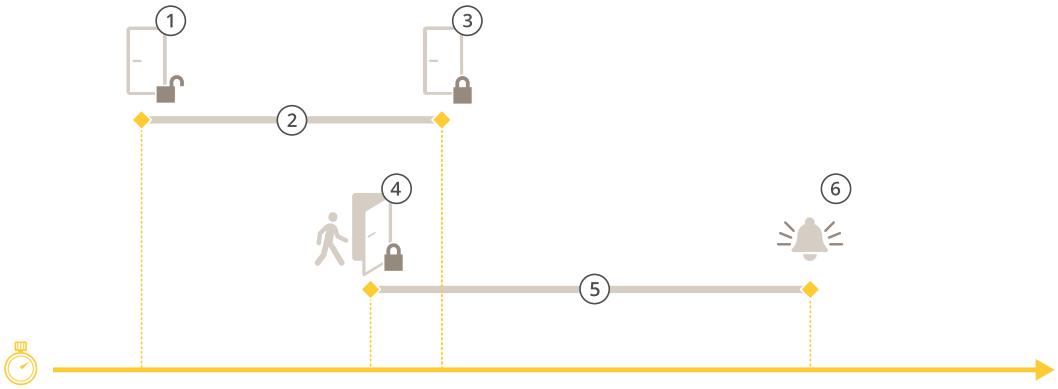
2パーソンルール	
Side A (A面) とSide B (B面)	ルールを使用するドアの面を選択します。
スケジュール	ルールがいつアクティブになるかを選択します。
タイムアウト (秒)	タイムアウトは、カードのスワイプ間または他のタイプの有効な認証情報間で許容される最長時間です。

既存のドアに**ダブルスワイプ**を追加するには:

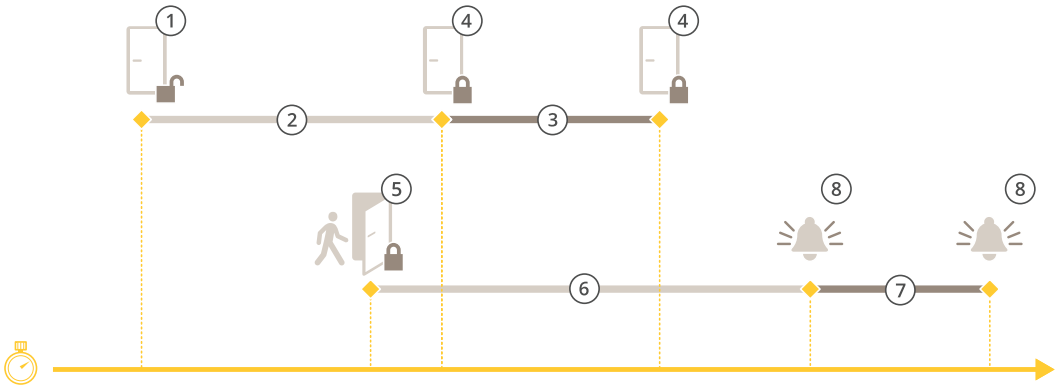
1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)] に移動します。
2. セキュリティレベルを設定するドアを選択します。
3. [Edit] (編集) をクリックします。
4. [Security level (セキュリティレベル)] をクリックします。
5. **ダブルスワイプ**をオンにします。
6. [適用] をクリックします。
7. カード所持者に**ダブルスワイプ**を適用します。
   7.1. [Cardholder 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の ⋮ をクリックし、[Edit (編集)]をクリックします。
   7.3. [More (詳細)] 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. [適用] 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。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 monitor sensor (ドアモニターセンサー)] 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。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。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。「ドアの追加」。
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。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。「ドアの追加」。
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。を参照してください。

動作	
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。
ありません	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。

- **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。

- **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. [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。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。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。を参照してください。

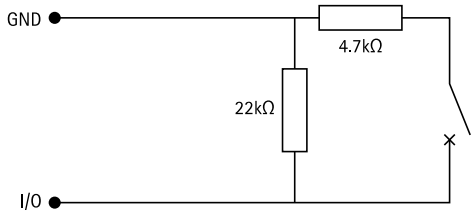
監視入力を使用するには:

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

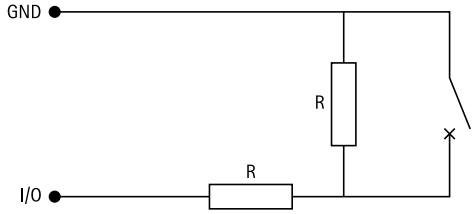
パラレルファースト接続

抵抗器の値は 4.7 kΩ及び 22 kΩである必要があります。



最初の直列接続

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。

カード形式と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。 **16進数**: 16進記数法としても知られ、0～9の数字とa～fの文字の16個の一意の記号で構成されます。
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:

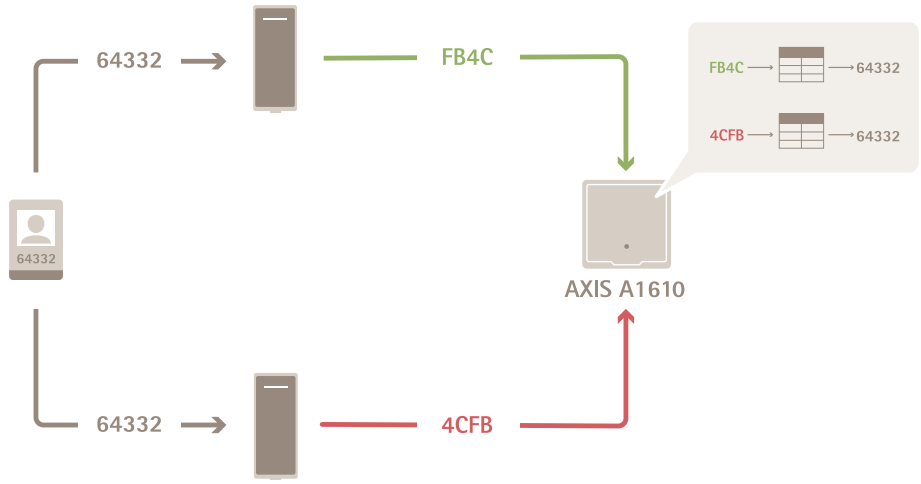
1. [Site Navigation (サイトナビゲーション)] > [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Card formats and PIN (カードフォーマットとPIN)] に移動します。
2. をクリックすると、カードフォーマットをデフォルトのフィールドマップにリセットできます。

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。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。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。と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。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。

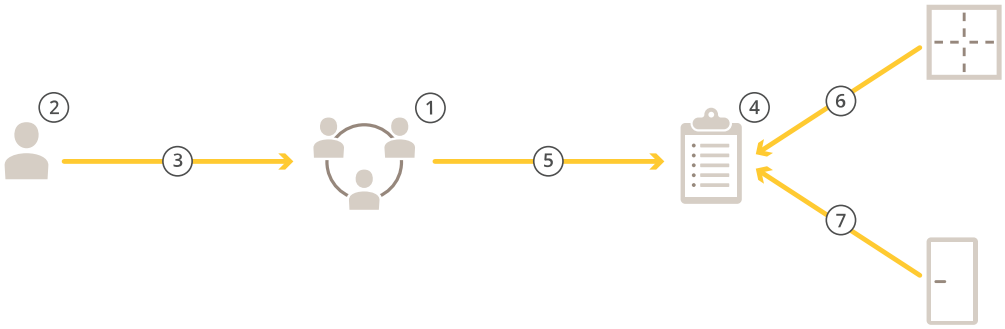
1. メインサーバーにアクセスします。
   1.1. [Access management (アクセス管理)] > [Dashboard (ダッシュボード)] を選択します。
   1.2. グローバルカード所持者とグループをローカルカード所持者とグループに変更します。
   1.3. [AXIS Optimizer] > [Access control (アクセスコントロール)] > [Multi server (マルチサーバー)] に移動します。
   1.4. [Main server (メインサーバー)] をクリックすると、サブサーバーのリストが表示されます。
   1.5. サブサーバーを選択し、[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、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、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、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。を参照してください
6. [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. [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。

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 Secure Entry for XProtect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。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。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. [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。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。を参照してください。
10. アクセスルールを追加します。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。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. [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. [保存] をクリックします。

「アクセスルールの追加」

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. [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、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、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 Secure Entry for XProtect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. [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。
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 Secure Entry for XProtect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リストアするには以下の手順に従います。

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。

T10234037_ja

2025-10 (M3.2)