

AXIS Camera Station Pro Secure Entry

バージョン情報

Secure Entryは、AXIS Camera Station Proのコンポーネントです。デバイスを追加したり、スケジュールを管理したりするために使用します。詳細については、*AXIS Camera Station Pro*ユーザーマニュアルを参照してください。

アクセスコントロールを設定する。

Axisネットワークドアコントローラーをシステムに追加している場合、バージョン6.x以降のAXIS Camera Stationでアクセスコントロールハードウェアを設定できます。

AXIS Camera Station Pro Secure EntryでAxisネットワークドアコントローラーを設定する手順の詳細については、「Axisネットワークドアコントローラーを設定する」を参照してください。

注

開始する前に、以下の手順を実行します。

- **[Configuration (設定)] > [Devices (デバイス)] > [Management (管理)]** からコントローラーのAXIS OSバージョンをアップグレードします。
- **[Configuration (設定)] > [Devices (装置)] > [Management (管理)]** に移動し、コントローラーの日付と時刻を設定します。
- **[Configuration > Devices > Management (設定 > デバイス > 管理)]** に移動し、コントローラーでHTTPSをオンにします。

アクセスコントロール設定のワークフロー

1. あらかじめ定義された識別プロファイルの編集や、新しい識別プロファイルの作成を行うには、*識別プロファイル*, on page 22を参照してください。
2. カスタム設定したカードフォーマットとPIN長を使用するには、*カードフォーマットとPIN*, on page 25を参照してください。
3. ドアを追加し、識別プロファイルをドアに適用します。ドアを追加する手順については、, on page 8を参照してください。
4. ドアを設定する:
 - ドア位置センサーの追加, on page 14
 - 緊急センサーを追加する, on page 15
 - 「リーダーの追加」, on page 17
 - REX装置の追加, on page 18
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 21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際は、以下の点に留意してください。

- **サポートされているAXIS OSバージョン:** 以下の対応AXIS OSバージョンは、元の推奨 AXIS Camera Station Pro Secure Entry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 AXIS Camera Station Pro Secure Entry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 Camera Station Pro Secure Entryバージョン6.5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12.0.86.2にアップグレードするとします。これにより、その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12.0.86.2になります。
- **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 AXIS Camera Station Pro Secure Entry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、AXIS Camera

Station Pro Secure Entry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。

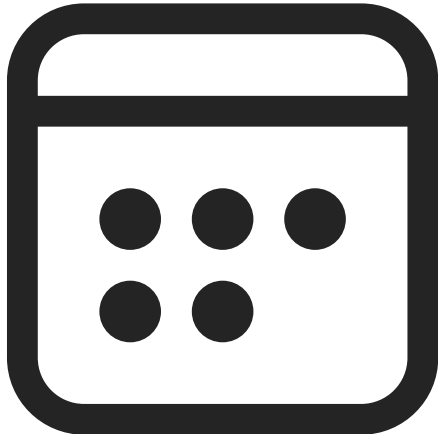
- 将来のAXIS OSの推奨:** システムの安定性と完全な互換性を確保するため、必ず各 AXIS Camera Station Pro Secure Entryバージョンに推奨されるAXIS OSバージョンに従ってください。
- トラックの変更:** ファームウェアのトラックを10.12.xxから11.0.xx以降に変更するには、工場出荷時の設定へのリセットが必要です。

以下の表は、AXIS Camera Station Proの各バージョンに対する最低限および推奨のAXIS OSバージョンを示しています。

AXIS Camera Station/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
Pro 6.17	12.6.102.1	12.9.65.3
Pro 6.16	12.6.102.1	12.9.65.3
Pro 6.15	12.5.68.1	12.8.55.1

ドアとゾーン

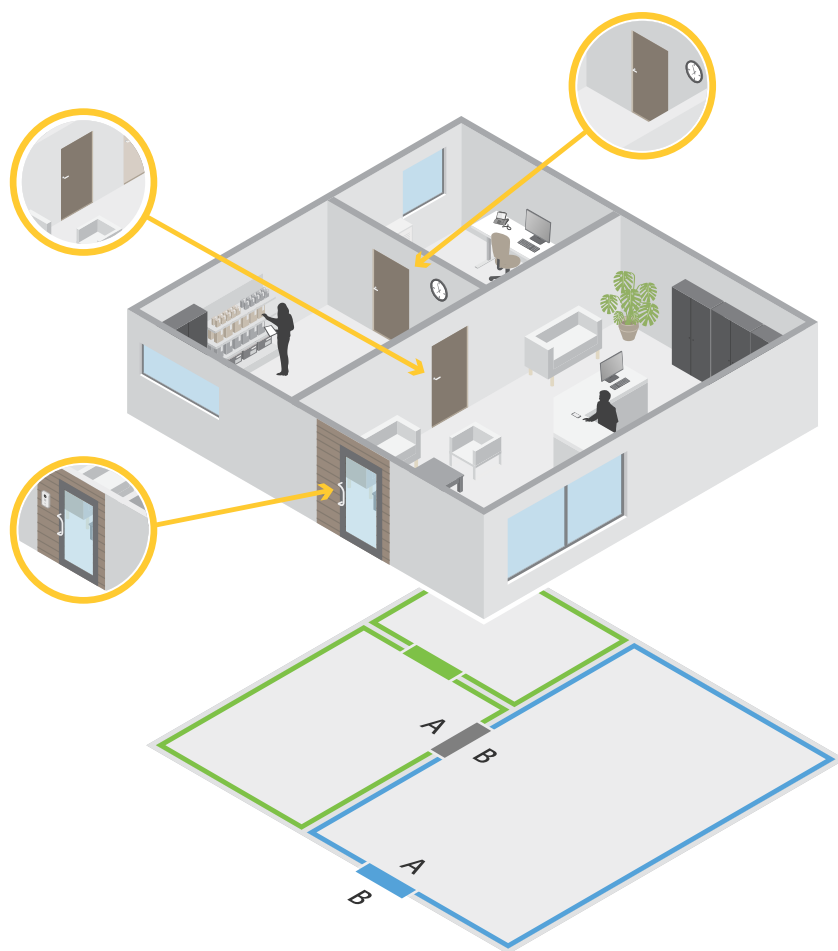
[Configuration > Access control > Doors and zones (設定 > アクセスコントロール > ドアとゾーン)] に移動して、概要を確認し、ドアとゾーンを設定します。

 手動アクション	ドアの状態を手動で設定します。[Reset (リセット)] (システムのルールに従う)、[Grant access (アクセスを許可)] (ドアを7秒間ロック解除)、[Unlock (ロック解除)] (ドアをロック解除したままにする)、[Lock (ロック)] (ドアをロックしたままにする)、[Lockdown (閉鎖)] (誰も出入りできないようにする) のオプションから選択します。
 スケジュールのロック解除	特定の時間にドアが自動でロック解除されるよう、スケジュールを設定します。それ以外の時間は、ドアはロックされたままです。スケジュールが有効になる前に、最初に入室する人が手動でドアのロックを解除できるようにするには、First person in (最初の人)をオンにします。
 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。
 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には、[Print (印刷)] をクリックします。
 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。
タイプ	ドア設定のタイプ。
デバイス	ドアに接続されているデバイス。

IPアドレス	ドアに接続されているドアコントローラーのIPアドレス。
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。
バッテリー	ドアコントローラーのバッテリー状態。
ステータス	ドアの状態。 • Online (オンライン): ドアはオンラインで、正常に動作しています。 • Reader offline (リーダーがオフライン): ドア設定のリーダーがオフライン状態です。 • Reader error (リーダーエラー): リーダーがセキュアチャンネルに対応していないか、リーダーに対してオフに設定されています。 • Old firmware (ファームウェアが古い): デバイスが古いバージョンのファームウェアを実行しています。最大限のパフォーマンスとセキュリティを確保するために、ファームウェアを更新してください。
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。
セキュリティレベル	そのゾーンに適用されるセキュリティレベル。

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。

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. [Configuration (設定)] > [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. 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。

ドア

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。マルチコントローラーは、追加のロック設定に対応しています。

ドアを追加する:

1. **[Configuration (設定)] > [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 (追加)]** をクリックし、ドロップダウンリストからドアのタイプを選択します。

ドアのタイプ	
ドア	ロックとリーダーに対応するドアモニター付きの標準的なドア。ドアコントローラーが必要です。
フロア	カードリーダーによってエレベーターの行き先階へのアクセス制御を行う、エレベーター制御向けのドアタイプです。詳細については、 <i>フロアの追加^{BETA}, on page 9</i> を参照してください。
監視ドア	開閉を通知できるドア。詳しくは、 <i>監視ドアを追加する, on page 10</i> を参照してください。
ワイヤレスドア	ASSA ABLOY Aperio® のワイヤレスロックと通信ハブで設定可能なドア。詳しくは、 <i>ワイヤレスロックの追加, on page 10</i> を参照してください。
設置済みドア	ハードウェアを選択せずにシステムに追加できる仮のドアです。

3. ドアの名前を入力し、**[Device (デバイス)]** の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てドアに関連付けます。ドアを追加できない場合、コントローラーがオフラインの場合、またはHTTPSがオンになっていない場合、コントローラーはグレー表示になります。
4. **[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。
5. **[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。
6. 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。
7. 識別プロファイルを選択します。 *識別プロファイル, on page 22*を参照してください。
8. **[Sensors (センサー)]**、**[Side A (A側)]**、**[Side B (B側)]** でセンサーやリーダーを追加してドアを設定します。
9. 特定のドアの設定を行います。「*ドア設定, on page 12*」を参照してください。
10. **[Save (保存)]** をクリックします。

ドア設定のコピー：

1. **[Configuration (設定)] > [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 (追加)]** をクリックします。
3. ドアの名前を入力し、**[Device (デバイス)]** の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てドアに関連付けます。
4. **[Next (次へ)]** をクリックします。
5. **[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。
6. 必要に応じて設定を変更してください。
7. **[Save (保存)]** をクリックします。



ドアとゾーンの追加と設定

フロアの追加^{BETA}

フロアはエレベーター各階へのアクセスを管理するために使用するドアタイプです。フロアを追加すると、そのエレベーターのすべての階をグループ化するエレベーターリソースが作成されます。各フロアは、ユーザーがその階へアクセスすることを許可する前に、エレベーター内に設置されたカードリーダーを使用してユーザーを認証します。

開始する前に以下が必要です。

- システムに追加された対応ネットワークドアコントローラー (AXIS A1610、AXIS A1710-B、AXIS A1810-Bなど)。
- 追加のリレー用のI/O拡張モジュール。AXIS A9920をお勧めします。

注

この機能はベータ版です。現在、最大64のフロアおよびカードリーダーのみに対応しています。

フロアを設定するには:

1. **[Configuration (設定)] > [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 (追加)]** をクリックし、**[Floor (フロア)]**^{BETA} を選択します。
3. フロアの名前を入力します。
4. コントローラーを選択します。
5. **[Elevator (エレベーター)]** で既存のエレベーターを選択するか、**[Create new elevator (エレベーターの新規作成)]** をクリックして新しいエレベーターを追加し、名前を入力します。
6. **[Side A (A面)]** で**[Card reader (カードリーダー)]** を選択し、リーダーを設定します。**[Side B (B面)]** は安全上の理由により設定できません。
7. **[Save and add new (保存して新規追加)]** をクリックして同じエレベーターにフロアを追加します。エレベーターとリーダーの設定は、次のフロア用に入力されたまま維持されます。このオプションは、コントローラーにリレーがある場合のみ利用できます。

8. フロアを追加したら、**[Save (保存)]** をクリックします。フロアは「エレベーター名 - フロア名」の形式で表示されます。例：「West Side - Floor 1」

注

- 複数のフロアで使用されているリーダーは、最初に追加されたフロアでのみ編集することができます。
- 関連するすべてのフロアが削除されると、エレベーターは自動的に削除されます。

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ファーム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. AXIS Camera Station Proで、**[Configuration (設定)]** > **[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。

ワイヤレスロックの追加

AXIS Camera Station Pro Secure Entryは、ASSA ABLOY Aperio® のワイヤレスロックと通信ハブに対応しています。ワイヤレスロックは、ドアコントローラーのRS485コネクタに接続されたAperio通信ハブを介してシステムに接続します。16個のワイヤレスロックを1台のドアコントローラーに接続できます。



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

- 設定には、Axis ドアコントローラーでAXIS OSバージョン11.6.16.1以降が必要です。
 - 設定には、AXIS Door Controller Extensionの有効なライセンスが必要です。
 - Axis ドアコントローラーと AXIS Camera Station Pro Secure Entryサーバーの時刻を同期する必要があります。
 - 開始する前に、ASSA ABLOYがサポートするAperioアプリケーションを使用して、Aperio ロックとAperioハブをペアリングします。
 - RS485コネクタ1個につき、Aperioハブは1台のみ接続可能です。マルチドロップには対応していません。
 - ワイヤレスロックは、オフライン状態ではロック解除スケジュールに従いません。
1. ドアコントローラーにアクセスします。
 - 1.1. **[設定] - [デバイス] - [他のデバイス]** を選択します。
 - 1.2. Aperio通信ハブに接続されているドアコントローラーのwebインターフェースを開きます。
 2. AXIS Door Controller Extensionをオンにします。
 - 2.1. ドアコントローラーのwebインターフェースで、**[Apps (アプリ)]** に移動します。
 - 2.2. AXIS Door Controller Extensionのコンテキストメニュー  を開きます。
 - 2.3. **[Activate license with a key (キーによるライセンスのアクティブ化)]** をクリックし、ライセンスを選択します。
 - 2.4. **AXIS Door Controller Extension**をオンにします。
 3. 通信ハブを介してワイヤレスロックをドアコントローラーに接続します。
 - 3.1. ドアコントローラーのwebインターフェースで、**[Access control > Wireless locks (アクセスコントロール > ワイヤレスロック)]** に移動します。
 - 3.2. **[Connect communication hub (通信ハブを接続する)]** をクリックします。
 - 3.3. ハブの名前を入力し、**[Connect (接続)]** をクリックします。
 - 3.4. **[Connect wireless lock (ワイヤレスロックを接続)]** をクリックします。
 - 3.5. 追加するロックのアドレスと機能を選択し、**[Save (保存)]** をクリックします。
 4. ワイヤレスロック付きのドアを追加し、設定します。
 - 4.1. AXIS Camera Station Pro Secure Entryで、**Configuration > Access control > Doors and zones (設定 > アクセスコントロール > ドアとゾーン)** に移動します。
 - 4.2. **[Doors (ドア)]** で  **[Add (追加)]** をクリックします。
 - 4.3. **[Wireless door (ワイヤレスドア)]** を **[Door type (ドアタイプ)]** に選択し、Aperio 通信ハブに接続されているドアコントローラーを選択します。
 - 4.4. **[Next (次へ)]** をクリックします。
 - 4.5. **[Wireless lock (ワイヤレスロック)]** を選択します。
 - 4.6. ドアのA面とB面を定義し、センサーを追加します。詳細については、**ドアとゾーン**, on page 4を参照してください。
 - 4.7. **[Save (保存)]** をクリックします。

ワイヤレスロックを接続すると、ドアの概要でバッテリー残量とステータスを確認できます。

バッテリー残量	アクション
良好	なし
低	ロックは意図したとおりに作動しますが、バッテリー残量が限界に達する前にバッテリーを交換する必要があります。
重大	バッテリーを交換する。ロックが意図したとおりに動作しない可能性があります。

ロックステータス	アクション
オンライン	なし
ロックの詰まり	ロックの機械的な問題を解決してください。

ドア設定

ドアを編集するには:

1. [Configuration > Access control > Door and Zones (設定 > アクセスコントロール > 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。
4. [Door settings (ドア設定)] で設定を変更し、[Save (保存)] をクリックします。

アクセス時間 (秒)	アクセスが許可された後、ドアがロック解除された状態を維持する秒数を設定します。ドアは、たとえ時間が残っていても、閉まると再びロックされます。
Open-too-long time (sec) (長時間のドア開放 (秒))	ドアモニターを設定した場合のみ有効です。ドアが開いた状態を維持できる秒数を設定します。時間が切れた時点でドアがまだ開いている場合、ドアが開いている時間が長すぎることを知らせる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、このイベントが発生した際の処理を選択します。
長いアクセス時間 (秒)	この設定を有効にすると、カード所有者のアクセスが許可された後、ドアがロック解除された状態を維持する秒数を設定できます。これにより、標準のアクセス時間が上書きされます。
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た場合のみ有効です。 [Long access time (長時間アクセス時間)] が有効になっている場合、カード所持者に対してドアを開けた状態で維持できる秒数を設定します。標準の「長時間のドア開放」状態の時間を上書きします。
再ロックの遅延時間 (ms)	ドアが開いた後または閉まった後、ロック解除状態を維持する時間 (ミリ秒単位) 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。
ドアのこじ開け	ドアが強制的に開放された場合にシステムアラームを作動させるかどうかを選択します。ドア位置センサー (DPS) が必要です。
ドアが開いている時間が長すぎます	ドアが開いている時間が長すぎる場合にシステムアラームを作動させるかどうかを選択します。

ドアを削除するには:

1. [Configuration > Access control > Doors and zones > Doors (設定 > アクセスコントロール > ドアとゾーン > ドア)] を選択します。
2. リストからドアを選択します。
3. [ Remove (削除)] をクリックして確定します。

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 - ダブルスワイプすると、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、システムから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設定するか、既存のドアに適用することができます。

既存のドアに**2人ルール**を追加するには:

1. [Configuration (設定)] > [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、カードがスワイプされてから次のスワイプまで、またはその他の有効な認証情報が提供されてから次に提供されるまでの最大許容時間です。

既存のドアに**ダブルスワイプ**を追加するには:

1. [Configuration (設定)] > [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. [Access Management (アクセス管理)] タブを開きます。
 - 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、カードがスワイプされてから次のスワイプまで、またはその他の有効な認証情報が提供されてから次に提供されるまでの最大許容時間です。

ドア位置センサーの追加

ドア位置センサーは、ドアの物理的な状態を検知するスイッチです。ドアにドア位置センサーを追加し、その接続方法を設定することができます。

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 8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 15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ると、イベントをトリガーすることができます。

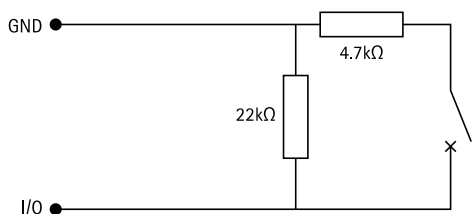
- ドアコントローラーとドアモニターの接続。ドア位置センサーの追加, on page 14を参照してください。
- Wiegandプロトコルを使用するドアコントローラーとリーダー間の接続。「リーダーの追加」, on page 17を参照してください。
- ドアコントローラーとREX装置間の接続。REX装置の追加, on page 18を参照してください。

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 K Ω parallel resistor and a 4.7 K Ω serial resistor (22 K Ω の並列抵抗器と4.7 K Ω 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。

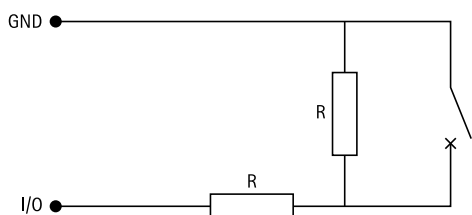
並列優先接続

抵抗器の値は 4.7 k Ω 及び 22 k Ω 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 k Ω の範囲内である必要があります。



緊急センサーを追加する

緊急入力を追加して、ドアをロックまたはロック解除するアクションを開始するように設定できます。回路の接続方法を設定することもできます。

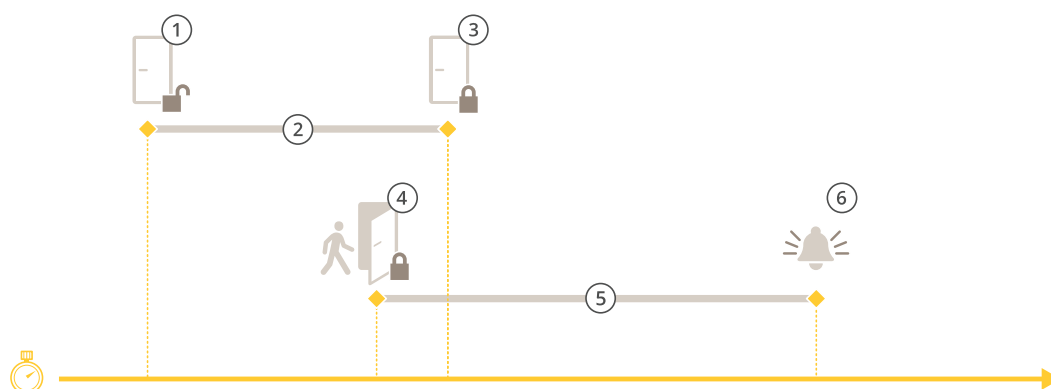
1. [Door configuration (ドアの設定)] ページに移動します。ドアを追加する手順については、on page 8を参照してください。
2. [Sensors (センサー)] で、**+** [Add (追加)] をクリックします。
3. [Emergency input (緊急入力)] を選択します。
4. [Emergency state (緊急状態)] で、回路接続を選択します。
5. デジタル入力新しい安定状態に移行するまで状態変化を無視するには、[Debounce time (ms) (デバウンス時間 (ミリ秒))] を設定します。

6. [Emergency action (緊急アクション)] で、ドアが緊急状態シグナルを受信したときにトリガーする緊急アクションを選択します。

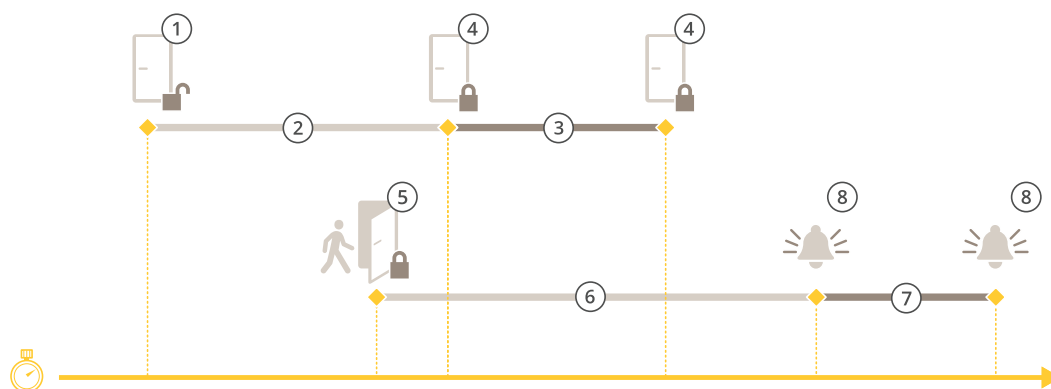
緊急状態	
回路が開いている	緊急入力回路はNC (Normally Closed) です。緊急入力、回路が開いたときに緊急状態信号を送信します。
回路が閉じている	緊急入力回路はNO (Normally Open) です。緊急入力、回路が閉じたときに緊急状態信号を送信します。

緊急アクション	
ドアロック解除	緊急状態信号を受信すると、ドアのロックが解除されます。
ドアのロック	緊急状態信号を受信すると、ドアがロックされます。

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 アクションなし - ロックはロックされたまま
- 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 アクションなし - ロックはロックされたまま
- 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

「リーダーの追加」

ドアコントローラーは、複数の有線リーダーに対応するように設定できます。ドアの片側または両側にリーダーを追加するか選択します。

カードフォーマットやPIN長のカスタム設定を適用した場合、**[Configuration (設定)] > [Access control (アクセスコントロール)] > [Doors and zones (ドアとゾーン)]** の**[Card formats (カードフォーマット)]** に表示されます。ドアとゾーン, on page 4を参照してください。

注

- ドアコントローラーに最大16台のBluetoothリーダーを追加することもできます。詳しくは、*Bluetoothリーダーの追加*, on page 19を参照してください。
 - AxisネットワークインターコムをIPリーダーとして使用する場合、システムはデバイスのWebページで設定されたPIN設定を使用します。
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 8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PIN長を使用する:
 - 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カードフォーマットを使用する:
 - 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システムの設定と異なる場合、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、この手順を繰り返します。

AXIS Barcode Readerの設置方法については、AXIS Barcode Readerの取り付け, on page 24を参照してください。

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。
IPリーダー	IPリーダーの場合は、[IP reader (IPリーダー)] を選択し、ドロップダウンメニューから装置を選択します。AxisネットワークインターコムをIPリーダーとして使用できます。

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	リーダーのタンパー入力を作動させる回路の状態を選択します。 • 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 15を参照してください。

REX装置の追加

ドアの片面または両面にREX (退出要求) 装置を追加できます。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 8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。利用可能なポートが1つしかない場合は、自動的にそのポートが選択されます。
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 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 15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信号を受信した際に、何のアクションも行わないようにする場合に選択します。

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。

IPリーダーを追加する

AXISネットワークインターコムやその他のIP対応デバイスをリーダーとして使用できます。ドアに割り当てる前に、AXIS Camera Station Proにデバイスを追加する必要があります。

注

開始する前に、IPリーダーの電源が入っており、AXIS Camera Station Proと同じネットワークに接続されていることを確認してください。

1. [Configuration (設定)] > [Devices (デバイス)] > [Add devices (デバイスの追加)] に移動します。
2. 検出されたデバイスのリストからIPリーダーを選択し、[Add (追加)] をクリックします。
3. プロンプトが表示されたら、デバイスの認証情報を入力します。

デバイスが追加されると、ドアに割り当てることができます。「リーダーの追加」, on page 17を参照してください。

Bluetoothリーダーの追加

AXIS A4612 Network Bluetooth Readerを使用して、Axis ドアコントローラーの有線ドアの接続範囲を拡張することができます。1つのドアコントローラーにつき、最大16のこのリーダーを割り当てることができます。各リーダーは、ドアロック、Request-to-Exit (REX)、Door Position Switch (DPS) を管理できます。

これらのリーダーを追加して使用する場合、追加のライセンスは必要ありません。

以下の手順に従って、AXIS A4612 Network Bluetooth Readerをドアに追加します。

1. AXIS A4612とドアコントローラーがペアリングされていることを確認します。AXIS Mobile CredentialアプリをBluetooth認証情報として使用する, on page 20を参照してください。
2. [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 8を参照してください。
3. ドアの片面で、**+** [Add (追加)] をクリックし、[Card reader (カードリーダー)] を選択します。
4. [IP reader (IPリーダー)] を選択し、ドロップダウンメニューからペアリングされたAXIS A4612を選択します。このリーダーを認証情報のペアリングに使用する場合は、ペアリング用にマークを付けます。[追加] をクリックします。
5. [Overview (オーバービュー)] タブで、識別プロファイルを変更します。ドアの片面のみにAXIS A4612を取り付け、反対の面にREXを使用する場合は、[Tap in app (アプリでタップ)] または[Touch reader (リーダーをタッチ)] のプロファイルを使用できます。

AXIS Mobile CredentialアプリをBluetooth認証情報として使用する

この例では、AXIS A4612 Bluetooth Readerをシステムに追加して、カード所持者がAXIS Mobile Credentialアプリを使用してドアを解錠できるようにする方法を示します。

1. Bluetoothリーダーを取り付け、ドアコントローラーに接続します。
2. ドアコントローラーのWebインターフェースでBluetoothリーダーを追加します。
 - 2.1. ドアコントローラーにアクセスし、[Peripherals (周辺機器)] > [Readers (リーダー)] に移動します。
 - 2.2. [Add reader (リーダーの追加)] をクリックします。
 - 2.3. [Add Bluetooth reader (Bluetoothリーダーの追加)] ダイアログに必要な情報を入力します。
 - 2.4. [追加] をクリックします。
3. AXIS Camera Station Pro Secure Entryで、ドアにBluetoothリーダーを追加します。
 - 3.1. [Configuration (設定)] > [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。
 - 3.2. Bluetoothリーダーを追加するドアを選択し、[Edit (編集)] をクリックします。
 - 3.3. Bluetoothリーダーが取り付けられているドアの側で **+** [Add (追加)] をクリックします。
 - 3.4. [Card reader (カードリーダー)] を選択します。
 - 3.5. [Add IP reader (IPリーダーの追加)] で、[IP reader (IPリーダー)] を選択します。
 - 3.6. [Select IP reader (IPリーダーの選択)] で、追加するBluetoothリーダーを選択します。
 - 3.7. [追加] をクリックします。
4. ペアリングするBluetoothリーダーを選択します。システム内の1台以上のBluetoothリーダーに対して、この手順を実行する必要があります。
 - 4.1. 先ほど追加したBluetoothリーダーを選択します。
 - 4.2. [Edit] (編集) をクリックします。
 - 4.3. [Edit bluetooth reader (Bluetoothリーダーの編集)] で、[Use this reader for pairing (ペアリングにこのリーダーを使用する)] を選択します。
 - 4.4. [適用] をクリックします。
5. [Tap in app (アプリでタップ)] または [Touch reader (リーダーにタッチ)] のいずれかの識別プロファイルを選択します。詳細については、識別プロファイル, on page 22を参照してください。

6. カード所持者にモバイル認証情報を追加します。認証情報の追加, on page 34を参照してください。
7. モバイル認証情報とペアリングリーダーをペアリングします。
 - 7.1. ペアリングが有効になったBluetoothリーダーにカード所持者の携帯電話を近づけます。
 - 7.2. カード所持者に送信された電子メールに記載されている手順に従います。

ゾーン

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):** このドアを通し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。概要については、**ドアとゾーンの例**, on page 7を参照してください。

1. [Configuration > Access control > Doors and zones > Zones (設定 > アクセスコントロール > ドアとゾーン > ゾーン)] を選択します。
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. [Configuration > Access control > Doors and zones > Zones (設定 > アクセスコントロール > ドアとゾーン > ゾーン)] を選択します。
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. [Configuration > Access control > Doors and zones > Zones (設定 > アクセスコントロール > ドアとゾーン > ゾーン)] を選択します。
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。ユーザーがその認証情報を再び使用するためには、いったん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設定するか、既存のゾーンに適用できます。既存のゾーンにセキュリティレベルを追加するには:

- [Configuration (設定)] > [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。
- セキュリティレベルを設定するゾーンを選択します。
- [Edit] (編集) をクリックします。
- [Security level (セキュリティレベル)] をクリックします。
- ゾーンに追加するセキュリティ機能をオンにします。
- [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1人目と同じ認証情報を使用して入場することを許可する場合に選択します。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1人目と同じ認証情報を使用して入場することを防ぐ場合に選択します。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を入力します。これにより、ユーザーがゾーンを離れるまでアンチパスバックが適用されます。[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です。

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せたものです。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。

注

動的QRをPINと共に使用する必要があります。

識別プロファイルを作成、編集、または削除するには、**[Configuration (設定)] > [Access control (アクセス管理)] > [Identification profiles (識別プロファイル)]** を選択します。

利用可能な識別プロファイル：

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。

QR - カード所持者は、ドアにアクセスするためにQR Code®をカメラに提示する必要があります。QR識別プロファイルは、静的QRと動的QRの両方に使用できます。

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。

アプリでタップ - カード所持者は、Bluetoothリーダーの範囲内に立っている状態で、AXIS Camera Stationモバイルアプリで認証情報をタップする必要があります。

リーダーにタッチ - カード所持者は、モバイル認証情報を設定した携帯電話をBluetoothリーダーにタッチする必要があります。

*QRコードは、日本およびその他の国々におけるデンソーウェーブ社の登録商標です。

識別プロファイルを作成する

1. **[Configuration (設定)] > [Access Control (アクセスコントロール)] > [Identification profiles (識別プロファイル)]** を選択します。
2. **+** **[Create identification profile (識別プロファイル)]** をクリックします。
3. 識別プロファイルの名前を入力します。
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. A面で、**+** **[Add (追加)]** をクリックし、識別タイプとスケジュールを選択します。
 - カード保有者に複数の識別タイプの使用を求めるには、同じ行で複数のタイプを選択します。
 - カード保有者がいずれかのタイプを使用できるようにするには、**+** **[Add (追加)]** を再度クリックして別の行を追加します。
6. B面で、**+** **[Add (追加)]** をクリックし、識別タイプとスケジュールを選択します。
7. **[OK]** をクリックします。



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。

識別プロファイルの設定

識別プロファイルを編集する

1. [Configuration (設定)] > [Access Control (アクセスコントロール)] > [Identification profiles (識別プロファイル)] を選択します。
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。

識別プロファイルを削除する

1. [Configuration (設定)] > [Access Control (アクセスコントロール)] > [Identification profiles (識別プロファイル)] を選択します。
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。

既定のカードフォーマットをリセットする

1. [Configuration (設定)] > [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)] を選択します。
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。

AXIS Barcode Reader

AXIS Barcode Readerは、Axisカメラにインストールできるアプリケーションです。AXISドアコントローラーは、外部周辺機器の認証キーを使用してアクセスを許可し、AXISバーコードリーダーおよびAXIS License Plate Verifierを認証します。AXIS Camera Station ProでAXIS License Plate Verifierを設定するワークフローの詳細については、を参照してください。

AXIS Barcode Readerの取り付け

1. axis.comからアプリケーションインストールをダウンロードします。

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

AXIS Barcode Readerの設定

1. QR識別プロフィールを変更する場合、[Configuration (設定)] > [Access control (アクセス管理)] > [Identification profiles (識別プロファイル)] に移動して  をクリックします。識別プロファイルを参照してください。
2. ドアを追加する手順については、[ドアの追加](#)を参照してください。
3. このドアの識別プロファイルとして [QR]を選択します。ドアの設定を参照してください。
4. 「バーコードのリーダーの追加。リーダーの追加を参照してください。
 - 4.1. ドアのどちらかの面で [Add reader (リーダーの追加)] をクリックします。
 - 4.2. [AXIS Barcode Reader (AXIS Barcode リーダー)]のドロップダウンリストから **リーダータイプ** を選択します。名前を入力し、[OK] をクリックします。

ドアコントローラーとの接続を作成します

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

カードフォーマットとPIN

カードフォーマットは、カードリーダーがカードからのデータをどのように解釈するかを定義するものです。あらかじめ定義されたカードフォーマットを使用・編集することができます。カスタムカードフォーマットを作成することも可能です。

[Configuration (設定)] > [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)] を選択します。このページには2つのタブがあります：

PIN設定 - PINの長さと言語を設定します。

カードの形式 - カード形式の表示、作成、編集、削除、および有効化を行います。

カードの形式

この表には、利用可能なすべてのカード形式と、以下の情報が記載されています。

使用中	その形式が有効かどうか。ビット長ごとに、一度に有効にできるフォーマットは1つだけです。
カード形式名	カードフォーマットの名称。
ビット長	カードフォーマットのビット長。
発生元	その書式がシステムのデフォルト書式であるか、あるいはユーザーが作成したカスタム書式であるか。

カード形式を追加する

1. [Configuration (設定)] > [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. **+** 追加をクリックします。
3. 名前と1～256の範囲でビット長を入力します。
4. 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。
5. 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。
6. 「カード番号」、「設備コード」、またはその両方をオンにします。カード形式では、少なくともいずれか一方を有効にする必要があります。
7. 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、指定した[Bit length (ビット長)] の範囲内である必要があります。
8. データフィールドのデータの出力形式を選択します。
 - 10進数:基数10の数体系。0～9の数字を使用します。
 - Hexadecimal (16進数):16進数:基数16の数体系:0～9の数字とa～fの文字を使用して表記されます。
9. ビット順を選択します。
 - リトルエンディアン:先頭ビットが最小、つまり最下位ビットになります。
 - ビッグエンディアン:先頭ビットが最大、つまり最上位ビットになります。
10. [OK]をクリックします。

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ビットのカード形式を2つ定義した場合、有効にできるのはいずれか一方のみです。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。
- 既定のカード形式は編集できますが、削除することはできません。既定のカード形式に加えた変更を元に戻すには、リセットアイコンを選択してデフォルト設定に戻します。作成したカード形式は削除できます。



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。

カードフォーマットの設定

カードフォーマットを編集する

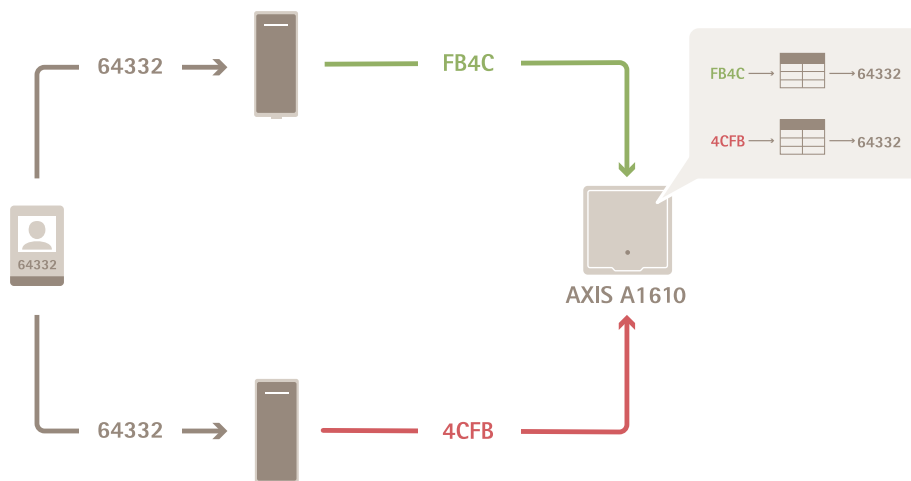
1. [Configuration (設定)] > [Access Control (アクセスコントロール)] > [Card formats and PIN (カードフォーマットとPIN)] を選択します。
2. カードフォーマットを選択して をクリックします。
3. 既定のカードフォーマットを編集する場合は、[Invert bit order (ビット順を反転する)] と [Invert byte order (バイト順を反転する)] のみを編集できます。
4. [OK]をクリックします。

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. [Configuration (設定)] > [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)] を選択します。
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。

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。

64332 = 1111 1011 0100 1100 → 0011 0010 1101 1111 = 13023
 → Read from left Read from right ←

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。

64 332 = 1111 1011 0100 1100 → 0100 1100 1111 1011 = 19707
 F B 4 C 4 C F B

26ビット標準のWiegandカードフォーマット

P FFFFFFF NNNNNNNNNNNNNNNNNN P
 ① ② ③ ④

- 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

PIN

PINの最小長と最大長を設定します。最小長と最大長に異なる値を設定する場合は、PINの入力が完了したことを示すPINの末尾文字を指定します。

- [Configuration (設定)] > [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。
- PINの最小長さと 最大長を入力します。
- 必要に応じて、PINの末尾文字を入力してください。
- [OK]をクリックします。

暗号化通信

OSDPセキュアチャンネル

AXIS Camera Station 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:

- [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。

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 Secure Channel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。
- AXIS Camera Station 5.47以降が必要です。
- 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かわらず、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55767です。ポート設定をカスタマイズするには、*General server settings* (サーバーの一般設定) を参照してください。
- サブサーバーをメインサーバーに接続すると、そのリーダーキーが置き換えられ、既存のBluetooth認証情報は無効になります。これを回避するには、サブサーバーではなくメインサーバー上でBluetooth認証情報を作成してください。

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 29](#)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 30](#)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 32](#)および「グループの追加」, [on page 36](#)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 32](#)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、[Configuration > Access control > Multi server (設定 > アクセスコントロール > 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、[Configuration > Access control > Multi server (設定 > アクセスコントロール > 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、[Configuration > Access control > Multi server (設定 > アクセスコントロール > 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 > Dashboard ((アクセス管理 > 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. [Configuration > Access control > Multi server (設定 > アクセスコントロール > 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:
 - [Configuration > Access control > Multi server (設定 > アクセスコントロール > 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。

Active Directory設定^{BETA}

注

Microsoft Windowsのユーザーアカウント、Active Directoryユーザーおよびグループは、AXIS Camera Station Pro Secure Entryにアクセスできます。Windowsでユーザーを追加する方法は、使用しているバージョンによって異なります。詳細については、support.microsoft.comにアクセスしてください。Active Directoryドメインネットワークを使用している場合は、ネットワーク管理者にお問い合わせください。

初めてActive Directory設定ページを開いたときに、AXIS Camera Station Pro Secure Entryでカード所有者にMicrosoft Active Directoryユーザーをインポートできます。Active Directoryユーザーをインポートする, on page 31を参照してください。

初期設定の後、Active Directory設定ページに次のオプションが表示されます。

- Active Directory内のグループに基づいてカード所有者グループを作成および管理します。
- Active Directoryとアクセス管理システム間のスケジュールされた同期を設定します。
- 手動で同期して、Active Directoryからインポートされたすべてのカード所有者を更新します。
- Active Directoryからのユーザーデータとカード所有者のプロパティ間のデータマッピングを管理します。

Active Directoryユーザーをインポートする

AXIS Camera Station Pro Secure Entryでカード所有者にActive Directoryユーザーをインポートするには:

1. **[Configuration (設定)] > [Access control (アクセスコントロール)] > [Active directory settings ^{BETA} (Active Directory設定 BETA)]**に移動します。
2. **[Set up import (インポートを設定する)]** をクリックします。
3. 画面に表示される手順に従ってこれら3つの主な手順を完了します。
 - 3.1. データマッピングのテンプレートとして使用するユーザーをActive Directoryから選択します。
 - 3.2. Active Directoryデータベースのユーザーデータをカード所有者のプロパティにマッピングします。
 - 3.3. アクセス管理システムで新しいカード所有者グループを作成し、インポートするActive Directoryグループを選択します。

インポートされたユーザーデータを変更することはできませんが、インポートされたカード所有者に認証情報を追加することはできます。認証情報の追加, on page 34を参照してください。

重要

Active Directoryでユーザーを無効にすると、AXIS Camera Station Proはそのカード所有者とすべての関連データ (履歴を含む) を完全に削除します。これは元に戻せません。カード所有者のデータを失わずにカード保持者のアクセスをブロックするには、Active Directoryでカード所有者を無効にするのではなく、AXIS Camera Station Proでカード所有者を停止してください。

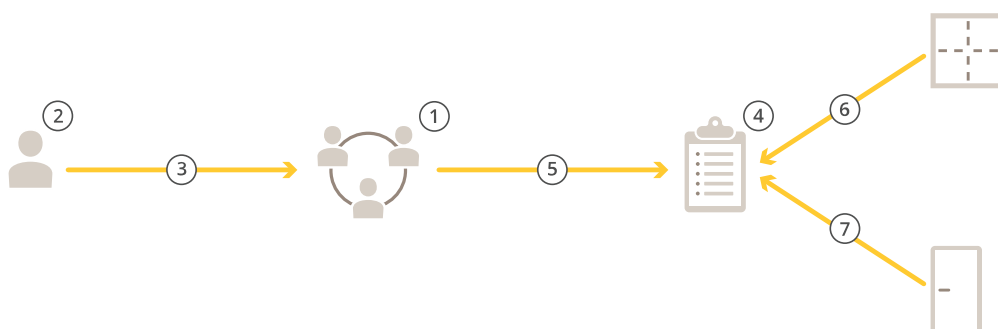
アクセス管理

[Access management (アクセス管理)] タブで、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を行います。

AXIS Camera Station Pro Secure EntryでAxisネットワークドアコントローラーを設定する手順の詳細については、「Axisネットワークドアコントローラーを設定する」を参照してください。

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。ワークフローの例:



1. 「グループの追加」, on page 36.
2. カード所持者の追加, on page 32.
3. カード所持者とグループの追加。
4. アクセスルールを追加します。 , on page 37.
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。本人を識別する認証情報を含むカード所有者を設定し、いつ、どのようにドアにアクセスできるのかを定義します。

また、Active Directoryデータベース内のユーザーをカード所持者としてマッピングすることもできます。Active Directory設定^{BETA}, on page 30を参照してください。

1. [Access Management (アクセス管理)] タブを開きます。
2. [Cardholder management (カード所持者監理)] > [Cardholders (カード所持者)] に移動し、**+** [Add (追加)] をクリックします。
3. カード所持者の姓名を入力します。必要に応じて、カード所持者に以下の詳細情報を追加します。
 - Email (電子メール) 欄に、カード所持者の電子メールアドレスを入力します。
 - Groups (グループ) から、カード所持者を追加したいグループを選択します。
 - Access rules (アクセスルール) で、そのカード所持者に適用したいアクセスルールを選択します。
4. 写真を追加するには、[Cardholder picture (カード所持者の写真)] をクリックし、以下のどちらかを選択します。

- Upload (アップロード)：デバイスから画像を追加します。
- Capture (キャプチャー)：カメラで直接写真を撮ります。

注

画像はJPG、PNG、GIF形式のいずれかである必要があります。画像は自動的に最大700×700ピクセルにリサイズされ、JPG形式に変換されます。

5. その他のオプションを設定するには、[Advanced (詳細)] をクリックします。
6. カード所有者に認証情報を追加します。認証情報の追加, on page 34を参照してください。
7. [Save (保存)] をクリックします。
8. バッジを印刷するには、1つ以上のカード所有者を選択し、[Print Badge ^{BETA} (バッジの印刷)] をクリックします。詳細については、^{BETA}バッジの印刷, on page 43を参照してください。

検索フィールドを使用して、カード所有者の名前または苗字で検索してください。ソースでフィルタリングするには、[Filter (フィルター)] をクリックして、[Local (ローカル)]、[Global (グローバル)]、[AD]、[Center (センター)]のいずれかを選択してください。

高度	
長いアクセス時間	ドアモニターが設置されている場合、カード所有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。
カード所有者の停止	カード所有者を停止する場合に選択します。これによって、そのカード所有者から一時的にすべてのアクセスが削除されます。
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、カード所有者は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これを使用できます。
閉鎖の対象外	カード所有者が閉鎖中に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)	カード所有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、カード所有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、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有者	サブサーバーでカード所有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有者にのみ使用できます。マルチサーバー ^{BETA} , on page 29を参照してください。



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。

カード所有者とグループの追加

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。

- QRコード認証情報, on page 34
- PIN認証情報, on page 34
- カード認証情報, on page 35
- ナンバープレートの認証情報, on page 35

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。

QRコード認証情報

注

QRコードを認証情報として使用するには、システムコントローラーとAXIS Barcode Readerを搭載したカメラの時刻が同期されている必要があります。両デバイスの時刻を同期させるため、同じ時刻ソースを使用することをお勧めします。

カード所持者にQRコ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、[QR-code (QRコード)] を選択します。
2. 認証情報の名前を入力します。
3. [Dynamic QR (動的QR)] はデフォルトで有効になっています。PIN認証情報と組み合わせて使用する必要があります。
4. 認証情報の開始日と終了日を設定します。
5. カード所持者を保存した後にQRコードを自動的に電子メールで送信するには、[Send QR code to cardholder when credential is saved (認証情報の保存時にカード所持者にQRコードを送信する)] を選択します。
6. [追加] をクリックします。

PIN認証情報

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. 必要に応じて、別のPINでサイレントアラームを作動させるには、**強制 PIN** を有効にし、強制PINを入力します。
4. 認証情報の**有効開始日**と **有効終了日**を設定します。
5. **[追加]** をクリックします。

モバイル認証情報

注

モバイル認証情報を受け取るには、カード保有者にメールアドレスが設定されている必要があります。

カード認証情報

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、システムですでに定義されてい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 readers (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。

注

2NデスクトップUSBカードリーダーを使用して、カードデータを取得できます。詳細については、「2NデスクトップUSBカードリーダーの設定」を参照してください。

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)]** をオン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。

ナンバープレートの認証情報

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

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 Camera Station Pro Secure Entryに追加します。デバイスの追加を参照してください。
2. 新しい装置のファーム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。ファームウェアのアップグレードを参照してください。
3. 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 8を参照してください。
 - 3.1. [Side A (側面A)] にリーダーを追加します。「リーダーの追加」, on page 17を参照してください。
 - 3.2. [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。
 - 3.3. 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。
 - 3.4. Okをクリックします。
4. 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。
5. AXIS License Plate Verifierを起動します。
6. AXIS License Plate Verifierを設定します。
 - 6.1. [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。
 - 6.2. [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。
 - 6.3. カメラのwebインターフェースからAXIS License Plate Verifierを開きます。
 - 6.4. セットアップウィザードをスキップします。
 - 6.5. [Settings (設定)] に移動します。
 - 6.6. [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。
 - 6.7. [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。
 - 6.8. [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。
 - 6.9. [Connect (接続)] をクリックします。
 - 6.10. [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。
 - 6.11. [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。
 - 6.12. 統合をオンにします。
7. アクセス権を付与するカード所有者を追加します。カード所持者の追加, on page 32を参照してください。
8. 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 34を参照してください。
9. 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 37を参照してください。
 - 9.1. スケジュールを追加します。
 - 9.2. 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。
 - 9.3. 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、カード所有者とそのアクセスルールをまとめて管理できます。

1. [ Access Management (アクセス管理)] タブを開きます。
2. [Cardholder management (カード所持者)] > [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)] を選択し、サブサーバーのカード所有者を表示・監視します。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。マルチサーバー^{BETA}, on page 29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. [Save (保存)] をクリックします。
7. グループ内のすべてのカード所有者のバッジを印刷するには、グループを選択し、[Print Badge ^{BETA} (バッジの印刷)] をクリックします。詳細については、*バッジ^{BETA}の印刷, on page 43*を参照してください。

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。

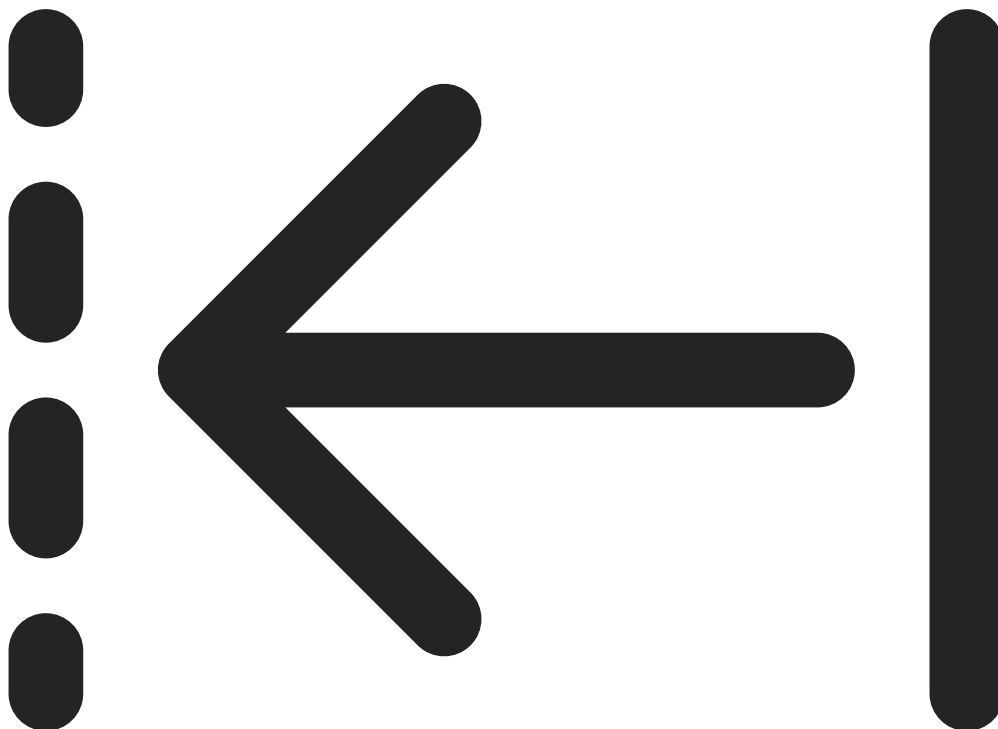
ドアとゾーン - アクセス権が適用される場所です。

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 Management (アクセス管理)] タブを開きます。
2. [Cardholder management (カード所持者の管理)] に移動します。

3. [Access rules (アクセスルール)]



で、**+** [Add (追加)] をクリックします。

4. アクセスルール名を入力し、[Next (次へ)] をクリックします。
5. カード所持者とグループを設定する:
 - 5.1. [Cardholders (カード所持者)] または [Groups (グループ)] で **+** [Add (追加)] をクリックします。
 - 5.2. 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。
 - 5.3. カード所持者やグループをアクセスルールに直接ドラッグ アンド ドロップして適用することもできます。ドラッグ操作を行うと、ドロップ可能なアクセスルールがハイライト表示されます。複数のカード所持者やグループを一度にドラッグすると、移動しようとしているものの数が表示されます。
6. ドアとゾーンを設定する:
 - 6.1. [Doors (ドア)] または [Zones (ゾーン)] で、**+** [Add (追加)] をクリックします。
 - 6.2. ドアまたはゾーンを選択し、[Add (追加)] をクリックします。
7. スケジュールを設定する:
 - 7.1. [Schedules (スケジュール)] で、**+** [Add (追加)] をクリックします。

7.2. 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。

8. [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。



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 Camera Station Pro Secure Entry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. [Access Management (アクセス管理)] タブを開きます。
2. [Reports (レポート)] > [System configuration (システム設定)] に移動します。
3. 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。

カード所持者の詳細レポート	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。
カード所持者のアクセスレポート	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レポート	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。
アクセスルールレポート	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。
ドアのアクセスレポート	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。
ゾーンのアクセスレポート	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。避難後に建物管理者が職員や来訪者の所在を把握するのに役立ちます。マスターポイントは、緊急時に担当者が報告する指定のリーダーです。システ

ムは、サイトにいる人とサイト外にいる人のレポートを生成します。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. [ Access Management (アクセス管理)] タブを開きます。
2. [Reports (レポート)] > [Cardholder activity (カード所持者の活動)] に移動します。
3.  [Add (追加)] をクリックし、[Roll call / Mustering (点呼/集合)] を選択します。
4. レポート名を入力します。
5. レポートに含めるゾーンを選択します。
6. レポートに含めるグループを選択します。
7. 集合レポートが必要な場合は、[Mustering point (集合場所)] とリーダーを選択します。
8. レポートのタイムフレームを選択します。
9. [Save (保存)] をクリックします。
10. 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。

インポートとエクスポート

カード所持者のインポート

このオプションは、CSVファイルからカード所持者、グループ、認証情報、写真をインポートします。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、以前に保存された設定を削除します。

また、Active Directoryデータベース内のユーザーをカード所持者としてマッピングすることもできます。Active Directory設定^{BETA}, on page 30を参照してください。

インポートオプション	
新規	既存のカード所有者を削除し、新しいカード所有者を追加します。
更新	既存のカード所持者を更新し、新しいカード所持者を追加します。
追加	既存のカード所持者を保持し、新しいカード所持者を追加します。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)] をクリックし、CSV ファイルを選択して、[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。これを使用して、重複する個人記録がインポートされるのを防ぎます。
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)] がオンになっています。

: 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 Camera Station Pro Secure Entry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、最後のインポートの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。

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。識別プロファイル, on page 22を参照してください。

QRまたはモバイル認証情報を送信するための電子メールテンプレートを編集するには:

1. [Access Management (アクセス管理)] タブで、[Settings (設定)] > [Email templates (電子メールテンプレート)] をクリックします。
2. テンプレートを編集し、[Update (更新)] をクリックします。

バッジのテンプレート BETA

バッジのテンプレートは、カード所持者の情報、写真、ロゴ、およびカスタムブランディングでカスタマイズできます。新規テンプレートの作成方法:

1. [Access management (アクセス管理)] > [Settings (設定)] > [Badge templates (バッジのテンプレート) ^{BETA}] に移動します。
2. [Create new template (テンプレートの新規作成)] をクリックします。
3. [Template name (テンプレート名)] のフィールドに名前を入力します。
4. デフォルトの印刷テンプレートとして使用するには、[Use as default template for printing (デフォルトの印刷テンプレートとして使用)] を選択します。
5. 以下の手順に従って、バッジのデザインをカスタマイズします。
 - 表面に表示するテキストフィールド (作成したカスタムフィールドも含む) を最大5つ選択します。印刷時には、入力済みのフィールドのみバッジに表示されます。
 - テキストのフォントとカラーを選択します。
 - 背景カラーまたは背景画像を追加します。

- 組織のロゴをアップロードします。
 - 裏面に背景カラーまたは背景画像のいずれかを追加します。
6. **[Save (保存)]** をクリックして変更を保存するか、**[Save as (名前を付けて保存)]** をクリックして新規テンプレートを作成します。

注

テンプレートはいったん作成すると編集できません。名前の変更のみ可能です。

バッジ^{BETA}の印刷

設定済みのバッジテンプレートを使用して、カード所持者のIDバッジを印刷できます。現在、カードのエンコーダ機能はサポートされていません。開始する前に:

- カード所持者が少なくとも1つのカード認証情報を保持していることを確認します。認証情報がないカード所持者のバッジを印刷することはできません。
- CR80カードサイズと厚手のカード用紙などの印刷材料に対応するプリンターが必要です。
- ブラウザの印刷設定を以下のように設定します。
 1. 用紙サイズをCR80またはカード寸法に合わせたカスタムサイズに設定します。
 2. 縦向きに設定します。
 3. 余白をオフにするか、最小に設定します。

重要

Secure Entryは、Windowsドライバーを搭載したプリンターに対応しています。HID Fargoプリンターシリーズは、正常に動作することが確認されています。プリンターのドライバーが必要な場合は、プリンターの供給元にお問い合わせください。

以下の手順に従って、バッジを印刷します。

1. **[Access management (アクセス管理)] > [Cardholder management (カード所持者の管理)] > [Cardholders (カード所持者)]** に移動します。
2. 1名または複数のカード所持者を選択します。
3. **[Print badge (バッジの印刷)]^{BETA}** をクリックします。
4. **[Select template (テンプレートの選択)]** をクリックし、**[Template (テンプレート)]** のドロップダウンメニューから使用するバッジテンプレートを選択します。
5. カード所持者が複数のカード認証情報を持っている場合、**[Card (カード)]** のドロップダウンメニューから1つ選択します。
6. **[Print (印刷)]** をクリックします。

注

お使いのプリンターが両面印刷に対応していない場合、まず表面のページをすべて印刷した後、カードの束を裏返してトレイに再びセットし、裏面のページを印刷してください。

T10231644_ja

2026-07 (M8.5)

© 2025 – 2026 Axis Communications AB