

AXIS A1601 Network Door Controller

ユーザーマニュアル

AXIS A1601 Network Door Controller

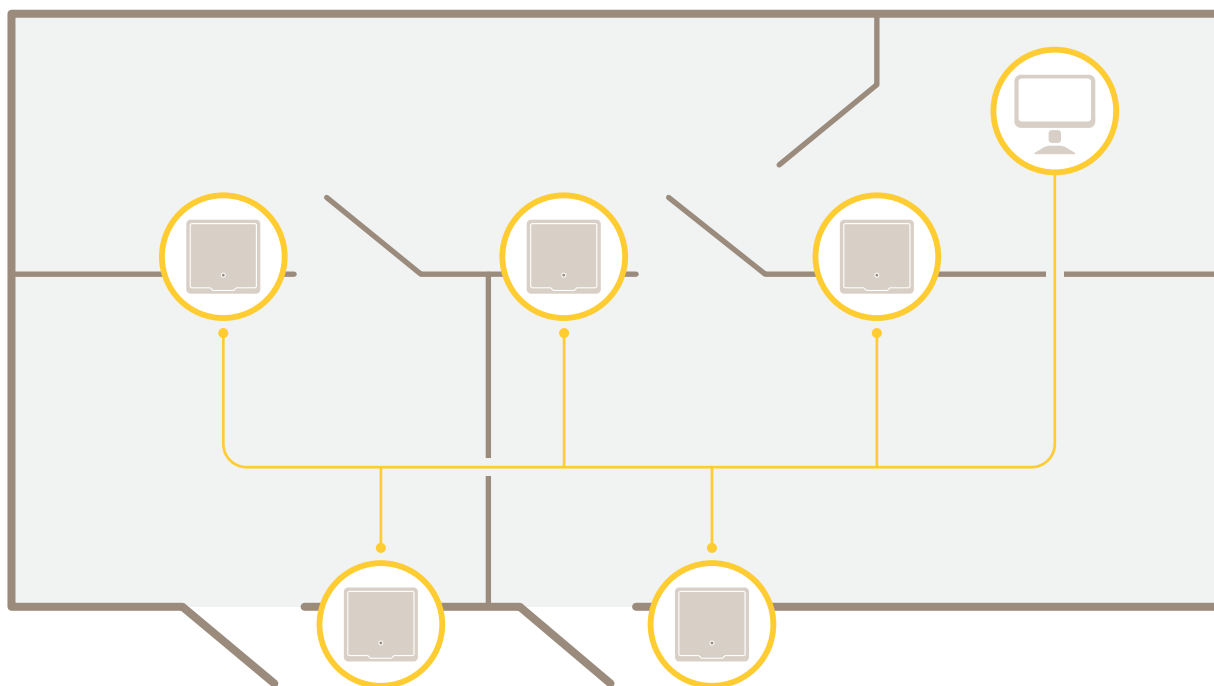
目次

| | |
|-----------------------|----|
| ソリューションの概要 | 3 |
| 製品の概要 | 5 |
| ネットワーク上のデバイスを検索する | 7 |
| 装置へのアクセス | 7 |
| インターネットから本製品にアクセスする方法 | 7 |
| 安全なパスワード | 7 |
| [Overview (概要)] ページ | 8 |
| システムの設定 | 9 |
| 設定 - 段階的な手順 | 9 |
| 言語の選択 | 9 |
| 日付と時刻の設定 | 9 |
| ネットワークの設定 | 10 |
| ハードウェアの設定 | 10 |
| ハードウェアの接続の確認 | 17 |
| カードおよびフォーマットの設定 | 18 |
| サービスの設定 | 20 |
| メンテナンス手順 | 21 |
| イベントの設定 | 23 |
| イベントログの表示 | 23 |
| イベントのログ設定 | 23 |
| アクションルールの設定方法 | 23 |
| リーダーからのフィードバック | 26 |
| システムオプション | 27 |
| セキュリティ | 27 |
| ネットワーク | 29 |
| ポートとデバイス | 34 |
| 保守 | 34 |
| サポート | 35 |
| 詳細設定 | 36 |
| トラブルシューティング | 37 |
| 工場出荷時の設定にリセットする | 37 |
| 現在のファームウェアの確認方法 | 37 |
| ファームウェアのアップグレード方法 | 37 |
| 現象、考えられる原因、対策 | 38 |
| 仕様 | 40 |
| LEDインジケータ | 40 |
| ボタン | 40 |
| コネクタ | 40 |
| 安全情報 | 47 |
| 危険レベル | 47 |
| その他のメッセージレベル | 47 |
| 装置インターフェース | 48 |
| ステータス | 48 |
| アクセスコントロール | 49 |
| システム | 49 |
| 保守 | 59 |

AXIS A1601 Network Door Controller

ソリューションの概要

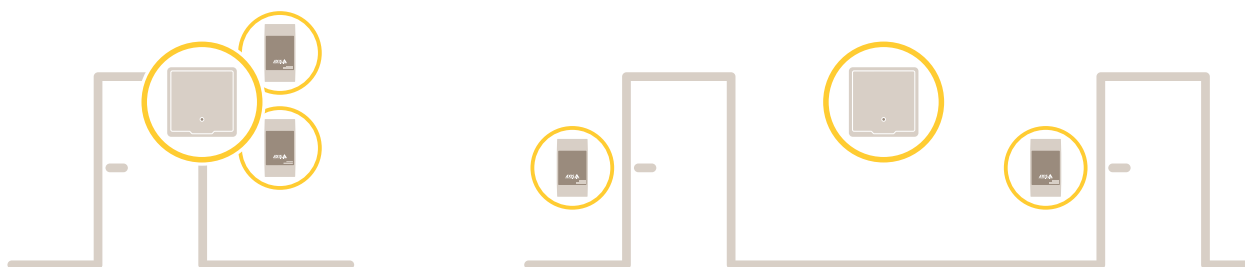
ソリューションの概要



ネットワークドアコントローラーは、既存のIPネットワークに容易に接続して給電することができ、特殊な配線は必要ありません。

AXIS A1601 Network Door Controller

ソリューションの概要

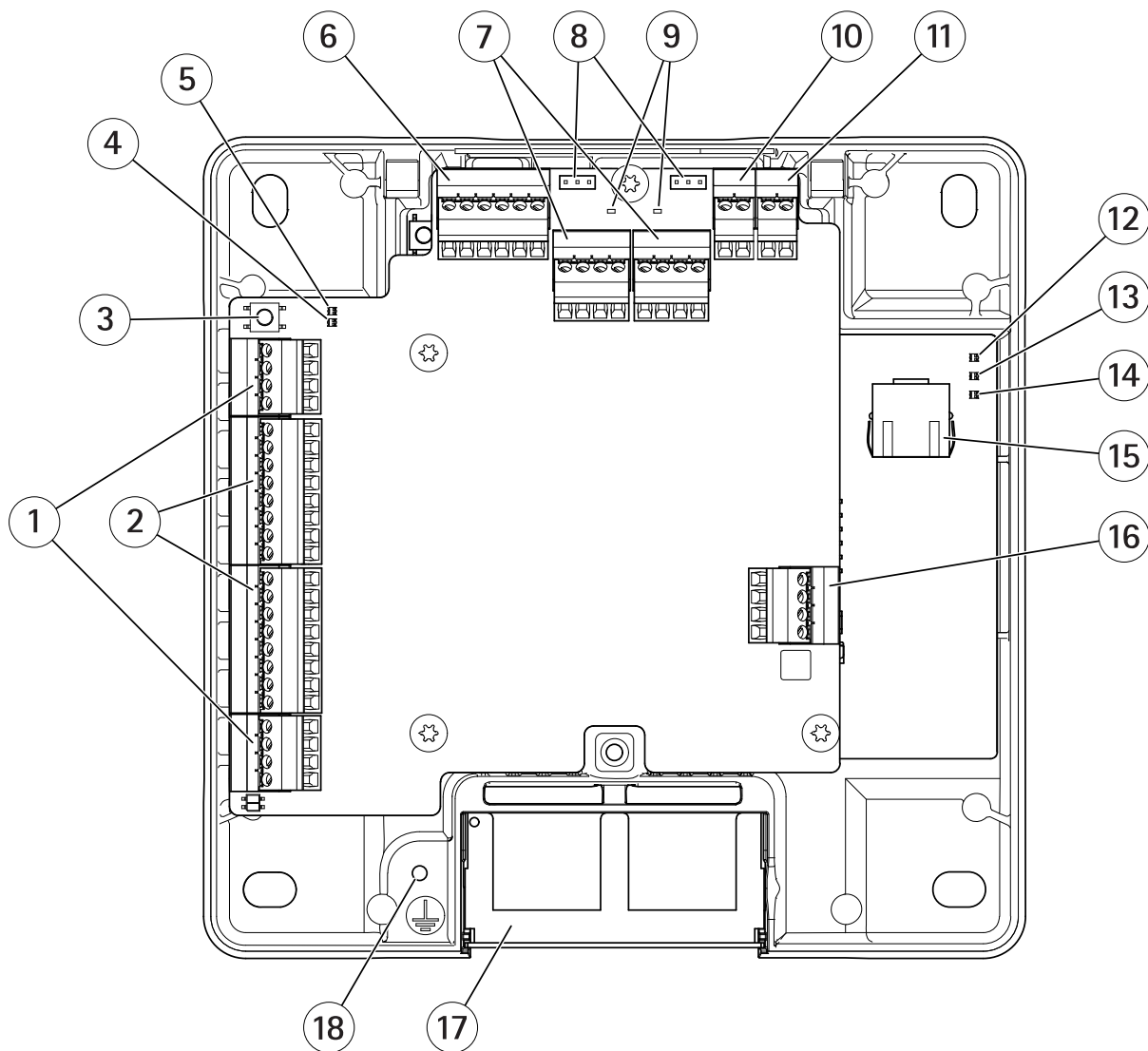


各ネットワークドアコントローラーは、ドアの近くに容易に取り付けることができるインテリジェントデバイスです。最大2つのリーダーに給電したり制御したりできます。

AXIS A1601 Network Door Controller

製品の概要

製品の概要



- 1 43ページドアコネクタ (×2)
- 2 41ページリーダーコネクタ (×2)
- 3 40ページコントロールボタン
- 4 リーダー過電流LED
- 5 リレー過電流LED
- 6 44ページ補助コネクタ
- 7 43ページリレーコネクタ (×2)
- 8 リレージャンパー (×2)
- 9 リレーLED (×2)
- 10 46ページバックアップバッテリー入力コネクタ
- 11 45ページ電源コネクタ
- 12 電源LED
- 13 ステータスLED

AXIS A1601 Network Door Controller

製品の概要

- 14 ネットワークLED
- 15 41ページネットワークコネクタ
- 16 45ページ外部コネクタ
- 17 リバーシブルケーブルカバー
- 18 アース位置

AXIS A1601 Network Door Controller

ネットワーク上のデバイスを検索する

ネットワーク上のデバイスを検索する

Windows®でAxisデバイスを探してIPアドレスの割り当てを行う方法については、AXIS IP UtilityまたはAXIS Device Managerを使用してください。いずれのアプリケーションも無料で、axis.com/supportからダウンロードできます。

IPアドレスの検索や割り当てを行う方法の詳細については、*IPアドレスの割り当てとデバイスへのアクセス方法を参照してください。*

装置へのアクセス

1. ブラウザーを開き、Axis装置のIPアドレスまたはホスト名を入力します。
本製品のIPアドレスが不明な場合は、AXIS IP UtilityまたはAXIS Device Managerを使用して、ネットワーク上で装置を見つけます。
2. ユーザー名とパスワードを入力します。初めて装置にアクセスする場合は、rootパスワードを設定する必要があります。を参照してください。
3. ブラウザーで装置のWebページが開きます。スタートページは概要ページと呼ばれています。

インターネットから本製品にアクセスする方法

プライベートネットワーク (LAN) 上の製品は、ネットワークルーターを使用することにより、インターネットへの接続を共有できます。これは、プライベートネットワークからインターネットにネットワークトラフィックを転送することによって行われます。

ほとんどのルーターは、パブリックネットワーク (インターネット) からプライベートネットワーク (LAN) へのアクセスを阻止するようあらかじめ設定されています。

イントラネット (LAN) 上にあるAxis製品を、NAT (ネットワークアドレス変換) ルーターの外側 (WAN側) から利用できるようにする場合は、**NATトラバーサル**をオンにします。NATトラバーサルを正しく設定すると、NATルーターの外部HTTPポートに着信するすべてのHTTPトラフィックが本製品に転送されます。

NATトラバーサル機能をオンにする方法

- [[**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定)**]] の順に選択します。
- **[Enable (有効にする)]** をクリックします。
- NATルーターを手動で設定して、インターネットからのアクセスを許可します。

注

- この場合、ルーターとは、NATルーター、ネットワークルーター、インターネットゲートウェイ、ブロードバンドルーター、ブロードバンド共有デバイスなどのネットワークルーティングデバイス、またはファイアウォールなどのソフトウェアを指します。
- NATトラバーサルを機能させるには、ルーターがNATトラバーサルに対応している必要があります。また、UPnP®にも対応している必要があります。

安全なパスワード

重要

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

AXIS A1601 Network Door Controller

ネットワーク上のデバイスを検索する

デバイスのパスワードは主にデータおよびサービスを保護します。Axisデバイスは、さまざまなタイプのインストールで使用される可能性があることから、パスワードポリシーを強制しません。

データを保護するために、次のことを強く推奨します。

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

rootパスワードの設定方法

Axis製品にアクセスするには、デフォルトの管理者ユーザー「**root**」のパスワードを設定する必要があります。このパスワードは、**[Configure Root Password (rootパスワードの設定)]** ダイアログで設定できます。このダイアログは、製品への初回アクセス時に表示されます。

ネットワークの傍受を防ぐには、暗号化されたHTTPS接続でrootパスワードを設定できますが、これにはHTTPS証明書が必要です。HTTPS (Hypertext Transfer Protocol over SSL) は、Webブラウザとサーバー間のトラフィックを暗号化するために使用されるプロトコルです。HTTPS証明書は、暗号化された情報交換を保証します。[27ページHTTPS](#)を参照してください。

デフォルトの管理者ユーザー名は、常に「**root**」であり、削除できません。rootのパスワードを忘れた場合は、製品を工場出荷時の設定にリセットする必要があります。[37ページ工場出荷時の設定にリセットする](#)を参照してください。

パスワードを設定するには、ダイアログでパスワードを直接入力します。

[Overview (概要)] ページ

本製品のWebページでは [\[Overview \(概要\)\]](#) ページに、ドアコントローラーの名前、MACアドレス、IPアドレス、およびファームウェアのバージョン情報が表示されます。また、このページでネットワーク上のコントローラーを識別することもできます。

本製品に最初にアクセスすると、[\[Overview \(概要\)\]](#) ページでは、ハードウェアの設定、日付と時刻の設定、ネットワーク設定を行うよう求められます。システムの設定の詳細については、[9ページ設定 - 段階的な手順](#)を参照してください。

本製品の他のWebページから [\[Overview \(概要\)\]](#) ページに戻るには、メニューバーの **[Overview (概要)]** をクリックします。

AXIS A1601 Network Door Controller

システムの設定

システムの設定

本製品の設定ページを開くには、概要ページの右上隅の **[Setup (設定)]** をクリックします。

Axis製品は、管理者が設定できます。ユーザーや管理者の詳細については、27ページを参照してください。

設定 – 段階的な手順

アクセスコントロールシステムの使用を開始する前に、以下の設定手順を完了する必要があります。


1. 英語が母国語でない場合でも、異なる言語で本製品のWebページを利用することができます。9ページ **言語の選択** を参照してください。
2. 日付と時刻を設定します。9ページを参照してください。
3. ネットワークを設定します。10ページを参照してください。
4. ドアコントローラーとリーダー、ロック、退出要求 (REX) 装置などの接続されたデバイスを設定します。10ページ **ハードウェアの設定** を参照してください。
5. ハードウェアの接続を確認します。17ページを参照してください。
6. カードおよびフォーマットを設定します。18ページを参照してください。

推奨メンテナンスの詳細については、21ページ **メンテナンス手順** を参照してください。

言語の選択

本製品のWebページのデフォルトの言語は英語ですが、本製品のファームウェアに含まれるどの言語にも切り替えることができます。利用可能な最新のファームウェアの詳細については、www.axis.comを参照してください。

いずれかの製品のWebページ上で言語を切り替えることができます。

言語を切り替えるには、言語のドロップダウンリスト  をクリックして言語を選択します。製品のすべてのWebページおよびヘルプページが選択した言語で表示されます。

注

- 言語を切り替えると、日付形式も選択した言語で一般に使用される形式に変更されます。データのフィールドに正しい形式が表示されます。
- 本製品を工場出荷時の設定へのリセットを行うと、製品のWebページの表示は再び英語になります。
- 本製品を復元または再起動したり、ファームウェアをアップグレードしたりすると、製品のWebページは引き続き、選択した言語を使用します。

日付と時刻の設定

本製品の日付と時刻を設定するには、**[Setup > Date & Time (設定 > 日付と時刻)]** に移動します。

日付と時刻は以下のいずれかの方法で設定できます。

- Network Time Protocol (NTP) サーバーから日付と時刻を取得します。10ページを参照してください。
- 手動で日付と時刻を設定します。10ページを参照してください。
- コンピューターから日付と時刻を取得します。10ページを参照してください。

[Current controller time (コントローラーの現在時刻)] ドアコントローラーの現在の日付と時刻 (24時間形式) が表示されます。

AXIS A1601 Network Door Controller

システムの設定

[System Options (システムオプション)] ページでも同じ日付と時刻のオプションを利用できます。[] [Setup > Additional Controller Configuration > System Options > Date & Time (設定 > 追加のコントローラー設定 > システムオプション > 日付と時刻)] に移動します。

Network Time Protocol (NTP) サーバーから日付と時刻を取得する

1. [Setup > Date & Time (設定 > 日付と時刻)] に移動します。
2. ドロップダウンリストから [Timezone (タイムゾーン)] を選択します。
3. 夏時間を使用する地域では、[Adjust for daylight saving (夏時間の調整を行う)] を選択します。
4. [Synchronize with NTP (NTPと同期する)] を選択します。
5. デフォルトのDHCPアドレスを選択するか、NTPサーバーのアドレスを入力します。
6. [Save (保存)] をクリックします。

NTPサーバーと同期すると、NTPサーバーからデータが送信されるため、日付と時刻が継続的に更新されます。NTP設定に関する詳細については、31ページNTP設定を参照してください。

NTPサーバーとしてホスト名を使用する場合は、DNSサーバーの設定を行う必要があります。30ページDNS設定を参照してください。

日付と時刻を手動で設定する

1. [Setup > Date & Time (設定 > 日付と時刻)] に移動します。
2. 夏時間を使用する地域では、[Adjust for daylight saving (夏時間の調整を行う)] を選択します。
3. [Set date & time manually (日付と時刻を手動で合わせる)] を選択します。
4. 希望する日付と時刻を入力します。
5. [Save (保存)] をクリックします。

日付と時刻の手動による設定では、日付と時刻が1回設定されますが、自動的に更新されません。これは、外部NTPサーバーとの接続が確立されていないために、日付または時刻を更新する必要がある場合は、変更を手動で行う必要があることを意味します。

コンピューターから日付と時刻を取得する

1. [Setup > Date & Time (設定 > 日付と時刻)] に移動します。
2. 夏時間を使用する地域では、[Adjust for daylight saving (夏時間の調整を行う)] を選択します。
3. [Set date & time manually (日付と時刻を手動で合わせる)] を選択します。
4. [Sync now and save (今すぐ同期して保存)] をクリックします。

コンピューターの時刻を使用する場合、日付と時刻は、コンピューターの時刻と1回同期されますが、その後自動的に更新されません。これは、システムの管理に使用するコンピューターで日付や時刻を変更した場合は、再び同期する必要があることを意味します。

ネットワークの設定

ネットワークの基本設定を行うには、[Setup > Network Settings (設定 > ネットワーク設定)] または [Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 基本設定)] に移動します。

ネットワーク設定の詳細については、29ページネットワークを参照してください。

AXIS A1601 Network Door Controller

システムの設定

ハードウェアの設定

ハードウェア設定を完了する前に、リーダーやロックなどのデバイスをAxis製品に接続することはできます。しかし、ハードウェア設定を完了してからの方がデバイスの接続が簡単になります。設定が完了すると、ハードウェアピン配置図が利用可能になるからです。ハードウェアピン配置図は、デバイスをピンに接続する方法のガイドで、メンテナンスの参照表として使用できます。メンテナンスの手順については、21ページを参照してください。

ハードウェアを初めて設定する場合は、以下のいずれかの方法を選択してください。

- ハードウェア設定ファイルをインポートします。11ページを参照してください。
- 新しいハードウェア設定を作成します。12ページを参照してください。

注

製品のハードウェアがまだ設定されていない場合や、設定が削除されている場合は、概要ページの通知パネルで **[Hardware Configuration (ハードウェア設定)]** が利用可能になります。

ハードウェア設定ファイルをインポートする方法

ハードウェア設定ファイルをインポートすることで、Axis製品のハードウェア設定を素早く完了できます。

ある製品からファイルをエクスポートし、それを別の製品にインポートすることで、何度も同じ手順を繰り返さなくても同じハードウェア設定の複数のコピーを作成できます。エクスポートしたファイルをバックアップとして保存し、それらを使用して以前のハードウェア設定を復元することもできます。詳細については、11ページハードウェア設定ファイルをエクスポートする方法を参照してください。

ハードウェア設定ファイルをインポートするには:

1. **[Setup > Hardware Configuration (設定 > ハードウェア設定)]** に移動します。
2. **[Import hardware configuration (ハードウェア設定のインポート)]** をクリックします。ハードウェア設定が既に存在する場合は、**[Reset and import hardware configuration (ハードウェア設定のリセットとインポート)]** をクリックします。
3. 表示されるファイルブラウザダイアログで、コンピューター上のハードウェア設定ファイル (*.json) を見つけて選択します。
4. **[OK]** をクリックします。

ハードウェア設定ファイルをエクスポートする方法

Axis製品のハードウェア設定をエクスポートすることで、同じハードウェア設定の複数のコピーを作成することができます。エクスポートしたファイルをバックアップとして保存し、それらを使用して以前のハードウェア設定を復元することもできます。

注

フロアのハードウェア設定は、エクスポートできません。

ワイヤレスロックの設定は、ハードウェアの構成のエクスポートには含まれません。

ハードウェア設定ファイルをエクスポートするには:

1. **[Setup > Hardware Configuration (設定 > ハードウェア設定)]** に移動します。
2. **[Export hardware configuration (ハードウェア設定のエクスポート)]** をクリックします。
3. ブラウザーの種類によっては、エクスポートを完了するためにダイアログを経由する必要があります。
特に指定がない限り、エクスポートされたファイル (*.json) はデフォルトのダウンロードフォルダーに保存されます。Webブラウザのユーザー設定で、ダウンロードフォルダーを選択できます。

AXIS A1601 Network Door Controller

システムの設定

新しいハードウェア設定の作成

要件に応じた手順に従います。

- 12ページ周辺機器なしで新しいハードウェア設定を作成する方法
- 15ページワイヤレスロックの新しいハードウェア設定を作成する方法
- 16ページエレベーター制御システム (AXIS A9188) を含む新しいハードウェア設定を作成する方法

周辺機器なしで新しいハードウェア設定を作成する方法

1. [Setup > Hardware Configuration (設定 > ハードウェア設定)] に移動し、[Start new hardware configuration (新しいハードウェア設定の開始)] をクリックします。
2. Axis製品の名前を入力します。
3. 接続されたドアの数を選択し、[Next (次へ)] をクリックします。
4. 要件に従ってドアモニター (ドアポジションセンサー) とロックを設定し、[Next (次へ)] をクリックします。利用可能なオプションの詳細については、12ページドアモニターとロックの設定方法を参照してください。
5. 使用するリーダーとREXデバイスを設定し、[Finish (完了)] をクリックします。利用可能なオプションの詳細については、14ページリーダーとREX装置の設定方法を参照してください。
6. [Close (閉じる)] をクリックするか、リンクをクリックしてハードウェアピン配置図を表示します。

ドアモニターとロックの設定方法

新しいハードウェア設定でドアのオプションを選択している場合、ドアモニターとロックを設定することができます。

1. ドアモニターを使用する場合は、[Door monitor (ドアモニター)] を選択してから、ドアモニターの回路の接続方法に適したオプションを選択します。
2. ドアの開放直後にドアロックがすぐにロックされるようにするには、[Cancel access time once door is opened (ドアが開放されるとアクセス時間をキャンセル)] を選択します。
再ロックを遅らせる場合は、[Relock time (再ロックの時間)] で遅延時間をミリ秒で設定します。
3. ドアのモニター時間のオプションを指定します。ドアモニターを使用しない場合は、ロック時間のオプションを指定します。
4. ロック回路の接続方法に適したオプションを選択します。
5. ロックモニターを使用する場合は、[Lock monitor (ロックモニター)] を選択してから、ロックモニターの回路の接続方法に適したオプションを選択します。
6. リーダー、REX装置、およびドアモニターの入力接続を監視する場合は、[Enable supervised inputs (状態監視を有効にする)] を選択します。
詳細については、15ページ監視入力の使用方法を参照してください。

注

- ほとんどのロック、ドアモニター、およびリーダーのオプションは、リセットしたり新しいハードウェア設定を開始したりしなくても、変更することができます。[Setup > Hardware Reconfiguration (設定 > ハードウェアの再設定)] に移動します。
- ドアコントローラーごとに1つのロックモニターを接続できます。したがって、ダブルロックドアを使用する場合、いずれかのロックのみにロックモニターを設定できます。2つのドアを同じドアコントローラーに接続する場合は、ロックモニターを使用できません。

AXIS A1601 Network Door Controller

システムの設定

ドアモニターと時間のオプションについて

以下のドアモニターのオプションが利用できます。

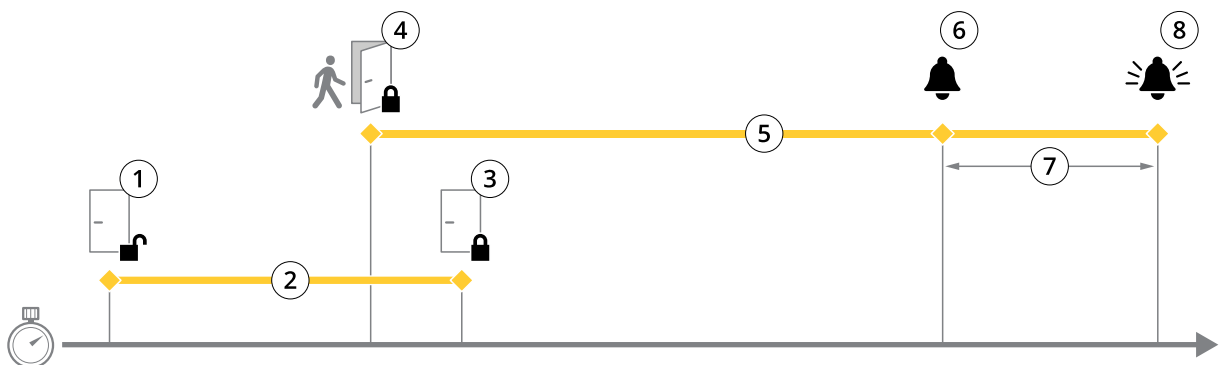
- **[Door monitor (ドアモニター)]** – デフォルトで選択されています。ドアにはそれぞれ個別にモニターが備えられていて、ドアがこじ開けられたり、長時間開放された場合などに信号を送信します。ドアモニターを使用しない場合は選択を解除します。
 - **[Open circuit = Closed door (開路 = ドアを閉じる)]** – ドアモニターの回路がNO (ノーマルオープン) の場合に選択します。回路が閉じると、ドアモニターはドアが開いている信号を発信します。回路が開くと、ドアモニターはドアが閉じている信号を発信します。
 - **[Open circuit = Open door (開路 = ドアを開放)]** – ドアモニターの回路がNC (ノーマルクローズ) の場合に選択します。回路が開くと、ドアモニターはドアが開いている信号を発信します。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発信します。
- **[Cancel access time once door is opened (ドアが開放されるとアクセス時間をキャンセル)]** – 共連れの発生を防ぐために選択します。ドアモニターでドアが開放されていることが通知されると直ちにドアがロックされます。

以下のドアの時間のオプションは常時利用できます。

- **[Access time (アクセス時間)]** – 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。ドアが開放されるか設定時間に到達するまでは、ドアはロック解除されたままになります。ドアが閉じられると、アクセス時間が過ぎたかどうかに関わらず、ロックされます。
- **[Long access time (長いアクセス時間)]** – 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。長いアクセス時間は、すでに設定されているアクセス時間を上書きして、長いアクセス時間を選択したユーザーに対して有効になります。

[Door monitor (ドアモニター)] を選択すると、以下のドアの時間のオプションが利用可能になります。

- **[Open too long time (長時間のドア開放)]** – ドアを開放したままにできる秒数を設定します。設定時間に到達した時点でドアがまだ開放されていると、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、開放が長すぎるイベントでトリガーするアクションを設定してください。
- **[Pre-alarm time (プリアラーム時間)]** – プリアラームとは、長時間のドア開放になる前にトリガーされる警告信号です。アクションルールの設定方法に応じて、閉じるべきドアから入ろうとしている人物を管理者に通知および警告することで、長時間ドア開放アラームがトリガーされるのを防ぎます。長時間ドア開放アラームのトリガー前に、システムがプリアラームの警告信号を発信する秒数を設定します。プリアラームを無効にするには、プリアラーム時間を0に設定します。



- 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 プリアラームの生成

AXIS A1601 Network Door Controller

システムの設定

- 7 プリアラーム時間
- 8 長時間のドア開放アラームの生成

アクションルールの設定方法については、23ページアクションルールの設定方法を参照してください。

ロックのオプションについて

以下のロック回路オプションがあります。

- **[Relay (リレー)]** – ドアコントローラーあたり1ロックでのみ使用できます。ドアコントローラーに2つのドアを接続している場合、リレーを使用できるのは、2つ目のドアのロックのみです。
- **[None (なし)]** – Lock 2でのみ利用できます。ロックを1つのみ使用する場合に選択します。

以下のロックモニターのオプションは、シングルドアの設定で利用できます。

- **[Lock monitor (ロックモニター)]** – 選択するとロックモニターのコントロールを利用できます。次に監視するロックを選択します。ロックモニターはダブルロックのドアでのみ使用することができ、2つのドアがドアコントローラーに接続されている場合は使用できません。
 - **[Open circuit = Locked (開路 = ロック)]** – ロックモニター回路をNC(ノーマルクローズ)にする場合に選択します。回路が閉じると、ロックモニターはドアのロックが解除されたとの信号を発信します。回路が開くと、ロックモニターはドアがロックされたとの信号を発信します。
 - **[Open circuit = Unlocked (開路 = ロック解除)]** – ロックモニター回路をNO(ノーマルオープン)にする場合に選択します。回路が開くと、ロックモニターはドアのロックが解除されたとの信号を発信します。回路が閉じると、ロックモニターはドアのがロックされたとの信号を発信します。

リーダーとREX装置の設定方法

新しいハードウェア設定でドアモニターとロックを設定している場合、リーダーと退出要求 (REX) 装置を設定できます。

1. リーダーを使用する場合は、チェックボックスを選択してから、リーダーの通信プロトコルに適したオプションを選択します。
2. ボタン、センサー、またはプッシュバーなどのREX装置を使用する場合は、チェックボックスを選択してから、REX装置の回路の接続方法に適したオプションを選択します。

REX信号がドアの開放に影響しない(メカニカルハンドルまたはプッシュバー付きドアなど) 場合は、**[REX does not unlock door (REXでドアをロック解除しない)]** を選択します。

3. ドアコントローラーに複数のリーダーまたはREX装置を接続している場合は、それぞれのリーダーまたはREX装置の設定が修正されるまで上記の2つの手順を再度行ってください。

リーダーおよびREX装置のオプションについて

以下のリーダーのオプションがあります。

- **[Wiegand]** – Wiegandプロトコルを使用するリーダーを選択します。次にリーダーでサポートされているLEDコントロールを選択します。シングルLEDコントロールを備えたリーダーは通常、赤と緑の間で切り替えます。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。これは、それぞれのLEDが個別に制御されることを意味します。両方のLEDがオンの場合、ライトはオレンジ色になります。リーダーがサポートするLEDコントロールについては、メーカーの情報を参照してください。
- **[OSDP, RS485 half duplex (OSDP、RS485半二重)]** – 半二重をサポートするRS485リーダーを選択します。リーダーがサポートするプロトコルについては、メーカーの情報を参照してください。

以下のREX装置のオプションがあります。

- **[Active low (アクティブ低)]** – REX装置による閉回路をアクティブにする場合に選択します。

AXIS A1601 Network Door Controller

システムの設定

- [Active high (アクティブ高)] – REX装置による開回路をアクティブにする場合に選択します。
- [REX does not unlock door (REXでドアをロック解除しない)] – REX信号がドアの開放に影響しない(メカニカルハンドルまたはプッシュバー付きドアなど)場合に選択します。ユーザーがアクセス時間内にドアを開いていれば、ドアのこじ開けのアラームはトリガーされません。ユーザーがREX装置をアクティブ化するとドアが自動的にロック解除される場合は選択解除します。

注

ほとんどのロック、ドアモニター、およびリーダーのオプションは、リセットしたり新しいハードウェア設定を開始したりしなくても、変更することができます。[Setup > Hardware Reconfiguration (設定 > ハードウェアの再設定)]に移動します。

監視入力の使用法

監視入力は、ドアコントローラーとドアモニターとの間の接続ステータスを報告します。接続が中断されると、イベントが有効になります。

監視入力を使用するには:

1. 使用するすべての監視入力に終端抵抗器を設置します。42ページの接続図を参照してください。
2. [Setup > Hardware Reconfiguration (設定 > ハードウェアの再設定)]に移動し、[Enable supervised inputs (監視入力を有効にする)]を選択します。ハードウェアの設定中に監視入力を有効にすることもできます。

状態監視の互換性について

次の機能は、状態監視をサポートしています。

- ドアモニター。43ページドアコネクタを参照してください。

ワイヤレスロックの新しいハードウェア設定を作成する方法

1. [Setup > Hardware Configuration (設定 > ハードウェア設定)]に移動し、[Start new hardware configuration (新しいハードウェア設定の開始)]をクリックします。
2. Axis製品の名前を入力します。
3. 周辺機器のリストで、ワイヤレスゲートウェイのメーカーを選択します。
4. 有線のドアを接続する場合は、[1 Door (1 ドア)]チェックボックスをオンにし、[Next (次へ)]をクリックします。ドアが含まれない場合は、[Finish (完了)]をクリックします。
5. ロックのメーカーに応じて、以下の箇条書きのいずれかに従って進んでください。
 - **ASSA Aperio**: リンクをクリックしてハードウェアピン配置図を表示するか、[Close (閉じる)]をクリックし、[Setup > Hardware Reconfiguration (設定 > ハードウェアの再設定)]に移動して設定を完了します。15ページAssa Aperio™のドアとデバイスの追加を参照してください。
 - **SmartIntego**: リンクをクリックしてハードウェアピン配置図を表示するか、[Click here to select wireless gateway and configure doors (ここをクリックしてワイヤレスゲートウェイを選択し、ドアを設定する)]をクリックして設定を完了します。21ページSmartIntegoの設定方法を参照してください。

Assa Aperio™のドアとデバイスの追加

ワイヤレスドアをシステムに追加する前に、Aperio PAP (Aperioプログラミングアプリケーションツール)を使用し、接続されたAssa Aperioコミュニケーションハブとドアをペアリングする必要があります。

ワイヤレスドアを追加するには:

1. [Setup (設定)] > [Hardware Reconfiguration (ハードウェアの再設定)]を選択します。

AXIS A1601 Network Door Controller

システムの設定

2. [Wireless Doors and Devices (ワイヤレスドアおよびデバイス)] で、[Add door (ドアの追加)] をクリックします。
3. [Door name (ドア名)] フィールドに、わかりやすい名前を入力します。
4. [Lock (ロック)] の [ID] フィールドに、追加するデバイスの6文字のアドレスを入力します。デバイスのアドレスは、製品のラベルに印刷されています。
5. 必要に応じて、[Door position sensor (ドアポジションセンサー)] で、[Built in door position sensor (内蔵ドアポジションセンサー)] または [External door position sensor (外部ドアポジションセンサー)] を選択します。

注

外部ドアポジションセンサー (DPS) を使用する場合は、Aperioロックデバイスを設定する前に、デバイスがドアハンドルの状態検知に対応していることを確認してください。

6. 必要に応じて、[Door position sensor (ドアポジションセンサー)] の [ID] フィールドに、追加するデバイスの6文字のアドレスを入力します。デバイスのアドレスは、製品のラベルに印刷されています。
7. [Add (追加)] をクリックします。

エレベーター制御システム (AXIS A9188) を含む新しいハードウェア設定を作成する方法

重要

ハードウェア設定を作成する前に、AXIS A9188 Network I/O Relay Moduleでユーザーを追加する必要があります。A9188のWebインターフェース > [Preferences > Additional device configuration > Basic setup > Users > Add > User setup (環境設定 > 追加のデバイス設定 > 基本設定 > ユーザー > 追加 > ユーザーの設定)] に移動します。

注

それぞれのAxis Network Door Controllerで、最大2つのAXIS 9188 Network I/O Relay Modulesを設定できます。

1. ドアコントローラーのWebページで、[Setup > Hardware Configuration (設定 > ハードウェア設定)] に移動し、[Start new hardware configuration (新しいハードウェア設定の開始)] をクリックします。
2. Axis製品の名前を入力します。
3. 周辺機器のリストで、[Elevator control (エレベーターコントロール)] を選択してAXIS A9188 Network I/O Relay Moduleを含め、[Next (次へ)] をクリックします。
4. 接続されたリーダーの名前を入力します。
5. 使用するリーダープロトコルを選択し、[Finish (完了)] をクリックします。
6. [Network Peripherals (ネットワーク周辺機器)] をクリックして設定を完了するか (16ページネットワーク周辺機器の追加および設定の方法参照)、リンクをクリックしてハードウェアピン配置図を表示します。

ネットワーク周辺機器の追加および設定の方法

重要

- ネットワーク周辺機器を設定する前に、AXIS A9188 Network I/O Relay Moduleでユーザーを追加する必要があります。AXIS A9188のWebインターフェース > [Preferences > Additional device configuration > Basic setup > Users > Add > User setup (環境設定 > 追加のデバイス設定 > 基本設定 > ユーザー > 追加 > ユーザーの設定)] に移動します。
 - 別のAXIS A1001 Network Door Controllerをネットワーク周辺機器として追加しないでください。
1. デバイスを追加するには [Setup > Network Peripherals (設定 > ネットワーク周辺機器)] に移動します。
 2. [Discovered devices (検知されたデバイス)] でデバイスを見つけます。

AXIS A1601 Network Door Controller

システムの設定

3. [Add this device (このデバイスを追加)] をクリックします。
4. デバイスの名前を入力します。
5. AXIS A9188のユーザー名とパスワードを入力します。
6. [Add (追加)] をクリックします。

注

[Manually add device (デバイスを手動で追加)] ダイアログにMACアドレスまたはIPアドレスを入力すると、ネットワーク周辺機器を手動で追加できます。

重要

スケジュールを削除する場合は、まずそのスケジュールがネットワークI/Oリレー モジュールで使用されていないことを確認してください。

ネットワーク周辺機器にI/Oおよびリレーを設定する方法

重要

ネットワーク周辺機器を設定する前に、AXIS A9188 Network I/O Relay Moduleでユーザーを追加する必要があります。AXIS A9188のWebインターフェース > [Preferences > Additional device configuration > Basic setup > Users > Add > User setup (環境設定 > 追加のデバイス設定 > 基本設定 > ユーザー > 追加 > ユーザーの設定)] に移動します。

1. [Setup > Network Peripherals (設定 > ネットワーク周辺機器)] に移動し、[Added devices (追加するデバイス)] 行をクリックします。
2. フロアとして設定するI/Oとリレーを選択します。
3. [Set as floor (フロアとして設定)] をクリックし、名前を入力します。
4. [Add (追加)] をクリックします。

ハードウェアの接続の確認

ハードウェアの設置と設定が完了すると、ドアコントローラーの有効期限内はいつでも、接続されたドアのモニター、ネットワークのI/Oリレーモジュール、ロック、リーダーの機能を確認することができます。

設定を確認し、検証コントロールにアクセスするには [Setup > Hardware Connection Verification (設定 > ハードウェア接続の確認)] に移動します。

ドアの制御の検証

- **ドアの状態** – ドアモニター、ドアのアラームおよびロックの現在の状態を確認します。[Get current state (現在の状態を取得)] をクリックします。
- **ロック** – ロックを手動でトリガーします。プライマリロックとセカンダリロックがある場合は両方に適用されます。[Lock (ロック)] または [Unlock (ロックを解除)] をクリックします。
- **ロック** – アクセス権を付与するロックを手動でトリガーします。プライマリロックにのみ適用されます。[Access (アクセス権)] をクリックします。
- **リーダー: フィードバック** – さまざまなコマンドについて、音声やLED信号などのリーダーからのフィードバックを確認します。コマンドを選択し、[Test (テスト)] をクリックします。利用可能なフィードバックの種類は、リーダーによって異なります。詳細については、26ページリーダーからのフィードバックを参照してください。メーカーの指示も参照してください。
- **リーダー: いたずら** – 前回のいたずらに関する情報を取得します。リーダーがインストールされている場合、最初に試行されたいたずらが登録されます。[Get last tampering (前回のいたずらに関する情報を取得)] をクリックします。

AXIS A1601 Network Door Controller

システムの設定

- ・ **リーダー: カードの読み取り** – 前回のカード読み取りに関する情報、または、リーダーによって許可された他のユーザートークンの種類に関する情報を取得します。[**Get last credential (前回の認証情報を取得)**] をクリックします。
- ・ **REX** – 前回、押された退出要求 (REX) 装置に関する情報を取得します。[**Get last REX (前回のREXに関する情報を取得)**] をクリックします。

フロアのコントロール検証

- ・ **フロアの状態** – フロアアクセスの現在の状態を確認します。[**Get current state (現在の状態を取得)**] をクリックします。
- ・ **フロアのロックとフロアのロック解除** – フロアアクセスを手動でトリガーします。プライマリロックとセカンダリロックがある場合は両方に適用されます。[**Lock (ロック)**] または [**Unlock (ロックを解除)**] をクリックします。
- ・ **フロアアクセス** – 一時的なフロアアクセスを手動で許可します。プライマリロックにのみ適用されます。[**Access (アクセス権)**] をクリックします。
- ・ **エレベーターリーダー: フィードバック** – さまざまなコマンドについて、音声やLED信号などのリーダーからのフィードバックを確認します。コマンドを選択し、[**Test (テスト)**] をクリックします。利用可能なフィードバックの種類は、リーダーによって異なります。詳細については、26ページリーダーからのフィードバックを参照してください。メーカーの指示も参照してください。
- ・ **エレベーターリーダー: いたずら** – 前回のいたずらに関する情報を取得します。リーダーがインストールされている場合、最初に試行されたいたずらが登録されます。[**Get last tampering (前回のいたずらに関する情報を取得)**] をクリックします。
- ・ **エレベーターリーダー: カードの読み取り** – 前回のカード読み取りに関する情報、または、リーダーによって許可された他のユーザートークンの種類に関する情報を取得します。[**Get last credential (前回の認証情報を取得)**] をクリックします。
- ・ **REX** – 前回、押された退出要求 (REX) 装置に関する情報を取得します。[**Get last REX (前回のREXに関する情報を取得)**] をクリックします。

カードおよびフォーマットの設定

ドアコントローラーには一般に使用されている定義済みのカードフォーマットがいくつかあり、そのまま使用することも、必要に応じて変更することもできます。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。各カードフォーマットには、カードに保存される情報の体系化の方法を規定する、さまざまなルールセットやフィールドマップがあります。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。リーダーがサポートするカードフォーマットの詳細については、メーカーの指示を参照してください。

カードフォーマットを有効にするには:

1. [Setup > Configure cards and formats (設定 > カードとフォーマットの設定)] に移動します。
2. 接続するリーダーが使用するカードフォーマットに一致する1つ以上のカードフォーマットを選択します。

カードフォーマットを新規作成するには:

1. [Setup > Configure cards and formats (設定 > カードとフォーマットの設定)] 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. Add card format (カードフォーマットの追加) ダイアログで、カードフォーマットの名前、説明、およびビット長を入力します。19ページカードフォーマットの説明を参照してください。
4. [Add field map (フィールドマップの追加)] をクリックして必要な情報をフィールドに入力します。19ページフィールドマップを参照してください。
5. 複数のフィールドマップを追加するには、上記の手順を繰り返します。

AXIS A1601 Network Door Controller

システムの設定

[Card formats (カードフォーマット)] リストのアイテムを展開してカードフォーマットの説明とフィールドマップを表示するには、▶ をクリックします。

カードフォーマットを編集するには、✎ をクリックし、カードフォーマットの説明とフィールドマップを必要に応じて変更します。その後、[Save (保存)] をクリックします。

[Edit card format (カードフォーマットの編集)] ダイアログまたは [Add card format (カードフォーマットの追加)] ダイアログでフィールドマップを削除するには、⊖ をクリックします。

カードフォーマットを削除するには、⊖ をクリックします。

重要

- 最低1つ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。詳細については、10ページハードウェアの設定および14ページリーダーとREX装置の設定方法を参照してください。
- 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、「Format A」と「Format B」という2つの32ビットカードフォーマットを定義して「Format A」を有効にしている場合は、先に「Format A」を無効にしない限り、「Format B」を有効にすることはできません。
- 有効にしているカードフォーマットがない場合は、[Card raw only (カード保存未加工データのみ)] および [Card raw and PIN (カード保存未加工データとPIN)] の識別タイプを使用してカードを識別し、さらにユーザーにアクセス権を付与することができます。ただし、リーダーのメーカーまたはリーダーの設定によって異なるカード保存未加工データが生成される場合があるため、この方法はお勧めできません。

カードフォーマットの説明

- [Name (名前)] (必須) - 分かりやすい名前を入力します。
- [Description (説明)] - 必要に応じて追加情報を入力します。この情報は、[Edit card format (カードフォーマットの編集)] ダイアログおよび [Add card format (カードフォーマットの追加)] ダイアログにのみ表示されます。
- [Bit length (ビット長)] (必須) - カードフォーマットのビット長を入力します。1~1000000000の数値にする必要があります。

フィールドマップ

- [Name (名前)] (必須) - フィールドマップ名をスペースなしで入力します。例: OddParity。
一般的なフィールドマップの例は、次のとおりです。
 - [Parity (パリティ)] - エラー検知にパリティビットを使用します。通常、パリティビットはバイナリコード文字列の先頭または末尾に追加され、ビット数が奇数と偶数のどちらであるかを示します。
 - [EvenParity] - 偶数パリティビットは文字列に偶数のビット数があることを確認します。値1を持つビットがカウントされます。カウントがすでに偶数の場合、パリティビット値は0に設定されます。カウントが奇数の場合は、カウントの合計が偶数の数になるように、偶数のパリティビット値は1に設定されます。
 - [OddParity] - 奇数パリティビットは文字列に奇数のビット数があることを確認します。値1を持つビットがカウントされます。カウントがすでに奇数の場合、この奇数のパリティビット値は0に設定されます。カウントが偶数の場合は、カウントの合計が奇数の数になるように、偶数のパリティビット値は1に設定されます。
 - [FacilityCode] - トークンが順序付きエンドユーザーの認証情報バッチと一致することを確認するために設備コードが使用される場合があります。従来、使用されていたアクセスコントロールシステムは、検証の精度が低く、合致するサイトコードでエンコードされていた認証情報バッチで、すべての従業員の入場を許可していました。本製品で設備コードを検証するには、大文字と小文字を区別する、このフィールドマップの名前が必須です。

AXIS A1601 Network Door Controller

システムの設定

- [CardNr] - カード番号またはユーザーIDは、アクセスコントロールシステムの検証で最も一般に使用されている情報です。本製品でカード番号を検証するには、大文字と小文字を区別する、このフィールドマップの名前が必須です。
- [CardNrHex] - 本製品でカード番号のバイナリデータは小文字の16進数にエンコードされています。これは主に、リーダーから予想したカード番号を取得できない場合のトラブルシューティング目的で使用されます。
- [Range (範囲)] (必須) - フィールドマップのビット範囲を入力します。例: 1、2~17、18~33、および34。
- [Encoding (エンコード方式)] (必須) - 各フィールドマップのエンコード方式を選択します。
 - [BinLE2Int] - バイナリデータをリトルエンディアン方式のビット並び順で整数としてエンコードします。整数とは、小数点以下を含めない整数にする必要があることを意味します。リトルエンディアン方式のビット並び順とは、最初のビットが最小(下位)であることを意味します。
 - [BinBE2Int] - バイナリデータをビッグエンディアン方式のビット並び順で整数としてエンコードします。整数とは、小数点以下を含めない整数にする必要があることを意味します。ビッグエンディアン方式のビット並び順とは、最初のビットが最大(上位)であることを意味します。
 - [BinLE2Hex] - バイナリデータをリトルエンディアン方式のビット並び順で小文字の16進数としてエンコードします。16進数システムは、ベース16の番号システムとも呼ばれ、次の16種類の固有の記号で構成されます。数字0~9および文字a~f。リトルエンディアン方式のビット並び順とは、最初のビットが最小(下位)であることを意味します。
 - [BinBE2Hex] - バイナリデータをビッグエンディアン方式のビット並び順で小文字の16進数としてエンコードします。16進数システムは、ベース16の番号システムとも呼ばれ、次の16種類の固有の記号で構成されます。数字0~9および文字a~f。ビッグエンディアン方式のビット並び順とは、最初のビットが最大(上位)であることを意味します。
 - [BinLEIBO2Int] - バイナリデータはBinLE2Intと同様にエンコードされますが、フィールドマップを使用してエンコードする前に、カード未加工データが逆のバイト順で複数バイトシーケンスに読み出されます。
 - [BinBEIBO2Int] - バイナリデータはBinBE2Intと同様にエンコードされますが、フィールドマップを使用してエンコードする前に、カード未加工データが逆のバイト順で複数バイトシーケンスに読み出されます。

ご使用のカードフォーマットでどのフィールドマップが使用されているかについては、メーカーの指示を参照してください。

サービスの設定

[Setup (設定)] ページの [Configure Services (サービスの設定)] を使用して、ドアコントローラーで使用できる外部サービスの設定にアクセスします。

SmartIntego

SmartIntegoは、ドアコントローラーで処理できるドアの数を増やすワイヤレスソリューションです。

SmartIntegoの必要条件

SmartIntegoの設定を進める前に、以下の必要条件を満たす必要があります。

- csvファイルを作成する必要があります。このcsvファイルには、SmartIntegoソリューションで使用されるGatewayNodeとドアに関する情報が含まれます。このファイルは、SimonsVossパートナーによって提供されるスタンドアロンソフトウェアで作成されます。
- SmartIntegoのハードウェア設定が行われました。15ページワイヤレスロックの新しいハードウェア設定を作成する方法を参照してください。

AXIS A1601 Network Door Controller

システムの設定

注

- SmartIntego設定ツールは、バージョン2.1.6452.23485、ビルド2.1.6452.23485 (2017年8月31日午後1:02:50)以降である必要があります。
- Advanced Encryption Standard (AES) はSmartIntegoに対応していないため、SmartIntego設定ツールで無効にする必要があります。

SmartIntegoの設定方法

注

- 示された必要条件を満たしていることを確認します。
 - バッテリーの状態がさらにわかりやすくなるように、[Setup (設定)] > [Configure event and alarms logs (イベントとアラームのログ設定)] の順に選択し、アラームとして [Door — Battery alarm (ドア — バッテリーアラーム)] または [IdPoint — Battery alarm (IdPoint — バッテリーアラーム)] を追加します。
 - ドアモニターの設定はインポートされたCSVファイルに入っています。通常の設置では、この設定を変更する必要はありません。
1. [Browse... (参照...)] をクリックし、CSVファイルを選択して、[Upload file (ファイルのアップロード)] をクリックします。
 2. GatewayNodeを選択し、[Next (次へ)] をクリックします。
 3. 新しい設定のプレビューが表示されます。必要に応じて、ドアモニターを無効にします。
 4. [Configure (設定)] をクリックします。
 5. 設定に含まれるドアの概要が表示されます。[Settings (設定)] をクリックして、各ドアを個別に設定します。

SmartIntegoの再設定方法

1. 一番上のメニューで [Setup (設定)] をクリックします。
2. [Configure Services (サービスの設定)] > [Settings (設定)] をクリックします。
3. [Re-configure (再設定)] をクリックします。
4. [Browse... (参照...)] をクリックし、CSVファイルを選択して、[Upload file (ファイルのアップロード)] をクリックします。
5. GatewayNodeを選択し、[Next (次へ)] をクリックします。
6. 新しい設定のプレビューが表示されます。必要に応じて、ドアモニターを無効にします。

注

ドアモニターの設定はインポートされたCSVファイルに入っています。通常の設置では、この設定を変更する必要はありません。

7. [Configure (設定)] をクリックします。
8. 設定に含まれるドアの概要が表示されます。[Settings (設定)] をクリックして、各ドアを個別に設定します。

メンテナンス手順

アクセスコントロールシステムのスムーズな動作を保つために、ドアコントローラーや接続されたデバイスを含めて、アクセスコントロールシステムを定期的にメンテナンスすることをお勧めします。

少なくとも年に一度はメンテナンスを行ってください。提案するメンテナンス手順には以下の手順が含まれますが、これらに限定されません。

AXIS A1601 Network Door Controller

システムの設定

- ドアコントローラーと外部デバイスの間がすべてしっかりと接続されていることを確認します。
- すべてのハードウェアの接続を確認します。17ページドアの制御の検証を参照してください。
- 接続された外部デバイスも含めて、システムが正常に機能することを確認します。
 - カードを通し、リーダー、ドア、およびロックをテストします。
 - システムにREX装置、センサー、またはその他のデバイスが含まれる場合は、それらもテストします。
 - アクティブになったら、いたずら警告をテストします。

上記のいずれかの手順で不良が示されたり、予想通りの動作にならなかったりした場合は、以下の操作を行います。

- 適切な機器を使用してワイヤーの信号をテストし、ワイヤーまたはケーブルが何らかの損傷を受けていないかチェックします。
 - 損傷を受けたか不良が示されたケーブルおよびワイヤーをすべて交換します。
 - ケーブルとワイヤーを交換したら、すべてのハードウェアの接続をもう一度確認します。17ページドアの制御の検証を参照してください。
- ドアコントローラーが予想どおりに動作しない場合は、詳細について37ページ、トラブルシューティングと34ページ保守を参照してください。

AXIS A1601 Network Door Controller

イベントの設定

イベントの設定

ユーザーによるカードの読み取りやREX装置のアクティブ化など、システムでイベントが発生すると、イベントログにイベントが記録されます。

- イベントログを表示します。23ページを参照してください。
- イベントログをエクスポートします。を参照してください。
- イベントのログ設定を行います。23ページイベントのログ設定を参照してください。

イベントログの表示

記録されたイベントを表示するには、[Event Log (イベントログ)] に移動します。

イベントログのアイテムを展開して、イベントの詳細を表示するには、▶ をクリックします。

イベントログにフィルターを適用すると、特定のイベントを検索しやすくなります。リストにフィルターを適用するには、1つまたは複数のイベントログフィルターを選択して、[Apply filters (フィルターを適用)] をクリックします。詳細については、23ページイベントログのフィルターを参照してください。

管理者として、いくつかのイベントが他よりも重要になる場合があります。したがって、記録すべきイベントを選択することができます。詳細については、23ページイベントログのオプションを参照してください。

イベントログのフィルター

以下のフィルターから1つまたはいくつかを選択すると、イベントログの範囲を絞り込むことができます。

- User (ユーザー) – 選択したユーザーに関連するイベントでフィルター処理します。
- Door & floor (ドア&フロア) – 特定のドアまたはフロアに関連するイベントでフィルター処理します。
- Topic (トピック) – イベントタイプでフィルター処理します。
- Date and time (日付と時刻) – イベントログを日付と時刻の範囲でフィルター処理します。

イベントのログ設定

[Configure event log (イベントのログ設定)] ページでは、どのイベントをログに記録するかを定義できます。

イベントログのオプション

イベントログに含めるイベントを定義するには、[Setup > Configure Event Logs (設定 > イベントのログ設定)] に移動します。

イベントのログ作成には次のオプションが利用できます。

- [No logging (ログ作成なし)] – イベントのログ作成を無効にします。イベントは、イベントログに登録されることも、ログが作成されることもありません。
- [Log for all sources (すべてのソースでログを作成)] – イベントのログ作成が有効になります。イベントがイベントログに登録され、ログが作成されます。

AXIS A1601 Network Door Controller

イベントの設定

アクションルールの設定方法

イベントページでは、さまざまなイベントが発生したときに本製品がアクションを実行するように設定できます。いつどのようにアクションをトリガーするかを定義した一連の条件をアクションルールと呼びます。複数の条件が定義されている場合、すべての条件が満たされたときにアクションがトリガーされます。

利用可能なトリガーおよびアクションの詳細については、本製品に内蔵されているヘルプを参照してください。

この例では、ドアがこじ開けられたときに、出力ポートを有効にするアクションルールを設定する方法を示します。

1. [Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (設定 > 追加のコントローラー設定 > システムオプション > ポートとデバイス > I/Oポート)] に移動します。
2. 目的の [I/Oポートタイプ] ドロップダウンリストから [出力] を選択し、[名前] を入力します。
3. I/Oポートの [標準状態] を選択し、[保存] をクリックします。
4. [Events > Action Rules (イベント > アクションルール)] に移動し、[Add (追加)] をクリックします。
5. [トリガー] ドロップダウンリストから [ドア] を選択します。
6. ドロップダウンリストから [ドアアラーム] を選択します。
7. ドロップダウンリストから希望するドアアラームを選択します。
8. ドロップダウンリストから [ドアのこじ開け] を選択します。
9. 必要に応じて、[スケジュール] と [追加条件] を選択します。以下を参照してください。
10. [アクション] の [タイプ] ドロップダウンリストから [出力ポート] を選択します。
11. [ポート] ドロップダウンリストから目的の出力ポートを選択します。
12. 状態を [アクティブ] に設定します。
13. アクションの [継続時間] を入力し、[指定時間経過後に反対の状態に移行] を選択します。ここで、アクションの継続時間を入力します。
14. [OK] をクリックします。

アクションルールで複数のトリガーを使用するには、[追加の条件] を選択し、[追加] をクリックして、トリガーを追加します。追加の条件を使用している場合、すべての条件が満たされたときにアクションがトリガーされます。

アクションが繰り返しトリガーされるのを防ぐには、[最小待ち時間] を設定します。アクションが再びアクティブになるまでトリガーを無視する時間を時間、分、秒の形式で入力します。

詳細については、本製品に内蔵されているヘルプを参照してください。

送信先を追加する方法

本製品は、イベントやアラームメッセージを送信することができます。本製品が通知メッセージを送信するには、少なくとも1件以上の送信先を定義する必要があります。利用可能なオプションについては、を参照してください。

送信先を追加するには：

1. [Setup > Additional Controller Configuration > Events > Recipients (設定 > 追加のコントローラー設定 > イベント > 送信先)] に移動し、[Add (追加)] をクリックします。
2. わかりやすい名前を入力します。
3. 送信先の [Type (タイプ)] を選択します。
4. 送信先のタイプに必要な情報を入力します。

AXIS A1601 Network Door Controller

イベントの設定

5. [Test (テスト)] をクリックして、送信先への接続をテストします。
6. [OK] をクリックします。

電子メールの送信先を設定する方法

電子メールの送信先は、電子メールプロバイダーのリストから選択したり、企業の電子メールサーバーなどのSMTPサーバー、ポート、認証方法を指定して設定することができます。

注

一部の電子メールプロバイダーは、大量の添付ファイルの受信や表示を防止したり、スケジュールにしたがって送信された電子メールなどの受信を防止するセキュリティフィルターを備えています。電子メールプロバイダーのセキュリティポリシーを確認して、メールの送信の問題が発生したり、電子メールアカウントがロックされたりしないようにしてください。

プロバイダーのリストからメール送信先を設定します。

1. [Events > Recipients (イベント > 送信先)] に移動し、[Add (追加)] をクリックします。
2. [名前] を入力して、[タイプ] リストから [電子メール] を選択します。
3. メール送信先のアドレスを [送信先] フィールドに入力します。複数のアドレスを指定する場合は、カンマで区切ります。
4. [プロバイダー] リストから電子メールプロバイダーを選択します。
5. 電子メールアカウントのユーザーIDとパスワードを入力します。
6. [テスト] をクリックして、テストメールを送信します。

たとえば、企業メールサーバーを使用しているメール送信先を設定するには、上記の手順で、[プロバイダー] ではなく [ユーザー定義] を選択します。送信元として表示するメールアドレスを、[送信元] フィールドに入力します。[詳細設定] を選択し、SMTPサーバーのアドレス、ポート、認証方法を指定します。必要に応じて、[暗号の使用] を選択し、暗号化された接続を使用してメールを送信します。サーバー証明書の検証には、Axis製品で利用できる証明書を使用できます。証明書をアップロードする方法については、28ページ *証明書* を参照してください。

スケジュールを作成する方法

スケジュールはアクションルールのトリガーとして、または追加条件として使用できます。既定のスケジュールのどれかを使用するか、または以下のように新しいスケジュールを作成します。

新しいスケジュールを作成するには:

1. [Setup > Additional Controller Configuration > Events > Schedules (設定 > 追加のコントローラー設定 > イベント > スケジュール)] に移動し、[Add (追加)] をクリックします。
2. 分かりやすい名前をつけ、日、週、月、または年のスケジュールを入力します。
3. [OK] をクリックします。

アクションルールでスケジュールを使用するには、[Action Rule Setup] (アクションルール設定) ページの [Schedule (スケジュール)] ドロップダウンリストからスケジュールを選択します。

繰り返しの設定方法

繰り返しは、たとえば5分ごとまたは1時間ごとにアクションルールを繰り返すトリガーする場合に使用します。

繰り返しを設定するには:

1. [Setup > Additional Controller Configuration > Events > Recurrences (設定 > 追加のコントローラー設定 > イベント > 繰り返し)] に移動し、[Add (追加)] をクリックします。

AXIS A1601 Network Door Controller

イベントの設定

2. わかりやすい名前と繰り返しのパターンを入力します。
3. [OK] をクリックします。

アクションルールで繰り返しの設定を使用するには、まずアクションルール設定ページの[トリガー]ドロップダウンリストから[時刻]を選択し、2番目のドロップダウンリストで[繰り返し]を選択します。

繰り返しを変更または削除するには、[繰り返しリスト]から[繰り返し]を選択し、[変更]または[削除]をクリックします。

リーダーからのフィードバック

リーダーはLEDやブザーを使用してフィードバックメッセージをユーザー(ドアにアクセスしようとしている人物)に送信します。ドアコントローラーは数種類のフィードバックメッセージをトリガーでき、いくつかはドアコントローラーに事前定義され、ほとんどのリーダーでサポートされています。

リーダーにはいくつかのLED動作がありますが、通常は、照明が赤、緑、オレンジの各色でさまざまに連続して点灯または点滅します。

また、さまざまな長さのブザー信号を繰り返す1ピッチのブープ音でメッセージを送信することもあります。

次表に、リーダーからのフィードバックをトリガーするドアコントローラーに事前定義されているイベントと、そのイベントの代表的なフィードバック信号を示します。AXISリーダーのフィードバック信号は、AXISリーダーに付属のインストールガイドに記載されています。

| イベント | Wiegand デュアルLED | Wiegand シングルLED | OSDP | ブザーのパターン | 状態 |
|-------------------------|-----------------|-----------------|---------|----------|--------|
| Idle (待機中) ¹ | Off (オフ) | 赤 | 赤 | サイレント | 通常 |
| RequirePIN (PINが必要) | 赤/緑: 点滅 | 赤/緑: 点滅 | 赤/緑: 点滅 | 短いブザー音2回 | PINが必要 |
| AccessGranted | 緑 | 緑 | 緑 | ブープ | アクセス許可 |
| AccessDenied | 赤 | 赤 | 赤 | ブープ | アクセス拒否 |

1. ドアが閉じられ、ロックされた場合に Idle (待機中) の状態になります。

上記以外のフィードバックメッセージは、アクセス管理システムなどのクライアントが、本機能をサポートし、必要な信号を発信することができるリーダーを使って、VAPIX®アプリケーションプログラミングインターフェースを使用して設定する必要があります。詳細については、アクセス管理システム開発者およびリーダーのメーカーによって提供されたユーザー情報を参照してください。

AXIS A1601 Network Door Controller

システムオプション

システムオプション

セキュリティ

ユーザー

ユーザーアクセスコントロールは、デフォルトで有効になっていて、[Setup > Additional Controller Configuration > System Options > Security > Users (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > ユーザー)]で設定できます。管理者は、ユーザー名とパスワードを付与して、ユーザーを設定できます。

ユーザーリストには、権限のあるユーザーとユーザーグループ(アクセスレベル)が表示されます。

- **管理者**には、すべての設定に対する無制限のアクセス権があります。管理者は他のユーザーを追加、変更、削除できます。

注

[**暗号化および非暗号化**] オプションを選択すると、Webサーバーがパスワードを暗号化します。暗号化および非暗号化は、新しい製品または工場出荷時の設定にリセットされた製品のデフォルトオプションです。

[**HTTP/RTSP パスワードの設定**] で、許可するパスワードのタイプを選択します。暗号化に対応していないクライアントが閲覧する場合や、最近ファームウェアをアップグレードしたばかりで、既存のクライアントは暗号化に対応しているが、再ログインして設定を行わないと暗号化機能を使用できない場合は、非暗号化パスワードの使用を許可する必要があります。

ONVIF

ONVIFは、インターフェースの標準化を促進して、IPベースの物理的なセキュリティ製品を効果的に相互運用することを目指している、オープンな業界フォーラムです。

ユーザーを作成すると、ONVIF通信が自動的に有効になります。製品とのすべてのONVIF通信には、ユーザー名とパスワードを使用します。詳細については、www.onvif.orgを参照してください。

IPアドレスフィルター

IPアドレスフィルタリングは、[[Setup > Additional Controller Configuration > System Options > Security > IP Address Filter (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > IPアドレスフィルター)]]で有効にします。IPアドレスフィルタリングが有効になると、リスト内のIPアドレスからの本製品へのアクセスは許可または拒否されます。リストから[許可]または[拒否]を選択し、[適用]をクリックして、IPアドレスフィルタリングを有効にします。

管理者は、最大256のIPアドレスをリストに追加できます(1つのエントリーに複数のIPアドレスを含めることができます)。

HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer、またはHTTP over SSL) は暗号化されたブラウジングを可能にするWebプロトコルです。ユーザーやクライアントがHTTPSを使用して、適切なデバイスがアクセスしているかを検証することもできます。HTTPSが提供するセキュリティレベルは、ほとんどの商用情報の交換に十分適合していると考えられています。

Axis製品は、管理者のログイン時にHTTPSが必要かどうかを設定できます。

HTTPSを使用するには、まずHTTPS証明書をインストールする必要があります。証明書をインストールして管理するには、[[Setup > Additional Controller Configuration > System Options > Security > Certificates (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > 証明書)]]に移動します。28ページ *証明書* を参照してください。

Axis製品でHTTPSを有効にするには、以下の操作を行います。

AXIS A1601 Network Door Controller

システムオプション

1. [Setup > Additional Controller Configuration > System Options > Security > HTTPS (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > HTTPS)] に移動します。
2. インストール済み証明書のリストからHTTPS証明書を選択します。
3. 必要に応じて、[暗号] をクリックして、SSLで使用する暗号化アルゴリズムを選択します。
4. [HTTPS接続ポリシー] をユーザーグループごとに設定します。
5. [保存] をクリックすると、設定が有効になります。

希望するプロトコルを使用してAxis製品にアクセスするには、ブラウザのアドレスフィールドに、HTTPSプロトコルの場合は「https://」、HTTPプロトコルの場合は「http://」を入力します。

HTTPSポートは[System Options > Network > TCP/IP > Advanced (システムオプション > ネットワーク > TCP/IP > 詳細設定)] ページで変更できます。

IEEE 802.1X

IEEE 802.1XはポートベースのNetwork Admission Control用の標準規格であり、有線およびワイヤレスのネットワークデバイスを安全に認証します。IEEE 802.1Xは、EAP (Extensible Authentication Protocol) に基づいています。

IEEE 802.1Xで保護されているネットワークにアクセスするには、デバイスは認証される必要があります。認証を実行するのは認証サーバーで、一般的には、FreeRADIUS、Microsoft Internet Authentication ServerなどのRADIUSサーバーです。

Axisの実装においては、Axis製品と認証サーバーは、EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) を使用するデジタル証明書で自己証明を行います。証明書は、**認証局 (CA)** が発行します。以下の証明書が必要です。

- 認証サーバーを認証するCA証明書。
- CAが署名した、Axis製品を認証するクライアント証明書

証明書を作成し、インストールするには、[[Setup > Additional Controller Configuration > System Options > Security > Certificates (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > 証明書)]] に移動します。28ページ証明書を参照してください。

Axis製品がIEEE 802.1Xで保護されているネットワークにアクセスするのを許可するには、以下の手順を実行します。

1. [Setup > Additional Controller Configuration > System Options > Security > IEEE 802.1X (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > IEEE 802.1X)] に移動します。
2. インストールされている証明リストから[CA証明書]と[クライアント証明書]を選択します。
3. [設定] からEAPOLバージョンを選択して、クライアント証明書に関連付けられているEAPのIDを入力します。
4. チェックボックスにチェックを入れて、IEEE 802.1Xを有効にし、[保存] をクリックします。

注

認証を正しく行うには、Axis製品の日付と時刻をNTPサーバーと同期させる必要があります。を参照してください。

証明書

証明書は、ネットワーク上のデバイスの認証に使用されます。一般的なアプリケーションには、暗号化されたWebブラウジング (HTTPS)、IEEE 802.1Xによるネットワーク保護、電子メールなどによるメッセージの通知などがあります。本製品では、以下の2種類の証明書を使用できます。

サーバー/クライアント証明書 - 本製品を認証します。**サーバー/クライアント証明書**は、自己署名証明書と認証局 (CA) 発行の証明書のどちらでも使用できます。自己署名証明書による保護には制限がありますが、認証局発行の証明書を取得するまで利用できます。

AXIS A1601 Network Door Controller

システムオプション

CA証明書 - ピア証明書 (たとえば、本製品がIEEE 802.1Xで保護されたネットワークに接続している場合の認証サーバーの証明書など) を認証します。本製品には、CA証明書が何種類かプリインストールされています。

注

- 製品が工場出荷時の値にリセットされると、プリインストールされたCA証明書以外のすべての証明書が削除されます。
- 製品が工場出荷時の値にリセットされると、プリインストールされたCA証明書以外のすべての証明書が削除されます。

自己署名証明書の作成方法

1. [[Setup > Additional Controller Configuration > System Options > Security > Certificates (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > 証明書)] に移動します。
2. [自己署名証明書の作成] をクリックして、必要な情報を入力します。

CA署名済み証明書を作成し、インストールする方法

1. 自己署名証明書を作成するには、を参照してください。
2. [[Setup > Additional Controller Configuration > System Options > Security > Certificates (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > 証明書)] に移動します。
3. [証明書の署名要求の作成] をクリックして、必要な情報を入力します。
4. PEM形式の証明書請求をコピーして、希望するCAに送信します。
5. 署名付き証明書を受け取ったら、[証明書のインストール] をクリックして、証明書をアップロードします。

追加のCA証明書をインストールする方法

1. [[Setup > Additional Controller Configuration > System Options > Security > Certificates (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > 証明書)] に移動します。
2. 証明書をアップロードするには、[証明書のインストール] をクリックして、証明書をアップロードします。

ネットワーク

TCP/IPの基本設定

Axis製品は、IP version 4 (IPv4) とIP version 6 (IPv6) をサポートします。

Axis製品は、以下の方法でIPアドレスを取得できます。

- **動的IPアドレス** - [Obtain IP address via DHCP (DHCPを使用してIPアドレスを取得する)] がデフォルトで選択されています。これは、Axis製品が Dynamic Host Configuration Protocol (DHCP) 経由で自動的にIPアドレスを取得するように設定されていることを意味します。
ネットワーク管理者は、DHCPを使用することでIPアドレスの一元管理と自動割り当てができます。
- **静的IPアドレス** - 静的IPアドレスを使用するには、[Use the following IP address (次のIPアドレスを使用する)] を選択し、IPアドレス、サブネットマスクおよびデフォルトのルーターを指定します。その後、[Save (保存)] をクリックします。

DHCPは、動的IPアドレス通知を使用しているか、DHCPでDNSサーバーを更新可能な場合 (これによって名前 (ホスト名) でAxis製品にアクセスできます) にのみ有効にしてください。

AXIS A1601 Network Door Controller

システムオプション

DHCPを有効にして本製品にアクセスできなくなった場合は、AXIS IP Utilityを実行し、ネットワークで接続されているAxis製品を検索するか、本製品を工場出荷時の設定にリセットしてからインストールをやり直す必要があります。工場出荷時の値にリセットする方法については、37ページを参照してください。

AXIS Video Hosting System (AVHS)

AVHSをAVHSサービスと共に使用すると、インターネットを介して、コントローラー管理やログにどこからでも簡単、安全にアクセスできます。近くのAVHSサービスプロバイダーを見つけるには、www.axis.com/hostingを参照してください。

AVHSの設定は、[[**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 基本設定)**]]で行います。AVHSサービスへの接続はデフォルトで有効になっています。無効にするには、**[Enable AVHS (AVHSを有効にする)]** ボックスをオフにします。

[One-click enabled (ワンクリックを有効にする)] - 製品のコントロールボタン (5 ページ、[製品の概要](#)を参照) を約3秒間押し続けて、インターネットを介してAVHSサービスに接続します。登録後は、**[Always (常時)]** が有効になり、本製品はAVHSサービスに接続し続けます。ボタンを押してから24時間以内に本製品を登録しなかった場合、本製品とAVHSサービスの接続が切断されます。

[Always (常時)] - 本製品は、インターネットを介したAVHSサービスへの接続を継続的に試行します。本製品は、いったん登録されると、AVHSサービスに接続し続けます。本製品がすでにインストール済みで、ワンクリックインストールを使用する必要がない場合、このオプションを使用することができます。

注

AVHSサポートは、サービスプロバイダーからのサブスクリプションの可用性に依存します。

AXIS Internet Dynamic DNS Service

AXIS Internet Dynamic DNS Serviceは、ホスト名を割り当てて、本製品へのアクセスを容易にします。詳細については、www.axiscam.netを参照してください。

本製品をAXIS Internet Dynamic DNS Serviceに登録するには、[[**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 基本設定)**]] に移動します。**[Services (サービス)]** でAXIS Internet Dynamic DNS Serviceの**[Settings (設定)]** ボタンをクリックします (インターネットへのアクセスが必要)。製品に関してAXIS Internet Dynamic DNS Serviceに現在登録されているドメイン名は、いつでも削除することができます。

注

AXIS Internet Dynamic DNS ServiceにはIPv4が必要です。

TCP/IPの詳細設定

DNS設定

DNS (Domain Name Service) は、ホスト名からIPアドレスへの変換を行います。DNS設定は、[[**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定)**]]で行います。

DHCPサーバーから提供されるDNS設定を使用するには、**[Obtain DNS server address via DHCP (DHCPを使用してDNSサーバーアドレスを取得する)]** を選択します。

手動設定を行うには、**[Use the following DNS server address (次のDNSサーバーアドレスを使用する)]** を選択して、次のように指定します。

ドメイン名 - Axis製品が使用するホスト名を検索するドメインを入力します。セミコロンで区切って、複数のドメイン名を指定することができます。ホスト名には、完全修飾ドメイン名の最初の部分を使用します。たとえば、完全修飾ドメイン名がmyserver.mycompany.comの場合、myserverがホスト名です (mycompany.comはドメイン名)。

AXIS A1601 Network Door Controller

システムオプション

Primary/Secondary DNS server (プライマリ/セカンダリDNSサーバー)- プライマリDNSサーバーとセカンダリDNSサーバーのIPアドレスを入力します。セカンダリDNSサーバーは、プライマリDNSサーバーが使用できない場合に使用されます。セカンダリDNSサーバーの指定は省略可能です。

NTP設定

NTP (Network Time Protocol) は、ネットワーク上の機器の時刻を同期するために使用します。NTP設定は、[[**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定)**]]で行います。

DHCPサーバーから提供されるNTP設定を使用するには、[[**Obtain NTP server address via DHCP (DHCPを使用してNTPサーバーアドレスを取得する)**]]を選択します。

手動で設定を行うには、[[**Use the following NTP server address (次のNTPサーバーアドレスを使用する)**]]を選択して、NTPサーバーのホスト名またはIPアドレスを入力します。

ホスト名の設定

IPアドレスの代わりにホスト名を使用して本製品にアクセスすることができます。通常、ホスト名は割り当てられたDNS名と同じです。ホスト名は[[**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細)**]]、[]で設定します。

IPv4で実行されているDHCPサーバーによって提供されるホスト名を使用するには、[[**Obtain host name via IPv4 DHCP (IPv4のDHCPを使用してホスト名を取得)**]]を選択します。

ホスト名を手動で設定するには、[[**Use the host name (ホスト名を使用する)**]]を選択します。

[[**Enable dynamic DNS updates (DNSの動的更新を有効にする)**]]を選択すると、Axis製品のIPアドレスが変わるたびに、ローカルのDNSサーバーが動的に更新されます。詳細については、オンラインヘルプを参照してください。

リンクローカルIPv4アドレス

[[**Link-Local IPv4 Address (リンクローカルIPv4アドレス)**]]は、デフォルトで有効であり、本製品に追加のIPアドレスを割り当てます。この追加のIPアドレスは、ローカルネットワーク上の同じセグメントにある他のホストから本製品にアクセスするために使用されます。本製品は、リンクローカルIPアドレスと、静的IPアドレスまたはDHCPによって提供されるIPアドレスの両方を同時に持つことができます。

この機能は、[[**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定)**]]で無効にできます。

HTTP

本製品で使用するHTTPポートは、[[**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定)**]]で変更できます。デフォルト設定の80に加えて、1024~65535の範囲のポートを使用できます。

HTTPS

本製品で使用するHTTPSポートは、[[**Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定)**]]で変更できます。デフォルト設定の443に加えて、1024~65535の範囲のポートを使用できます。

HTTPSを有効にするには、[[**Setup > Additional Controller Configuration > System Options > Security > HTTPS (設定 > 追加のコントローラー設定 > システムオプション > セキュリティ > HTTPS)**]]に移動します。詳細については、27ページ**HTTPS**を参照してください。

AXIS A1601 Network Door Controller

システムオプション

IPv4用NATトラバーサル (ポートマッピング)

プライベートネットワーク (LAN) 上のデバイスは、ネットワークルーターを使用することにより、インターネットへの接続を共有できます。これは、プライベートネットワークから「外部」(つまり、インターネット)へネットワークトラフィックを転送することによって行われます。ほとんどのネットワークルーターが、パブリックネットワーク (インターネット) からプライベートネットワーク (LAN) へのアクセスを阻止するようあらかじめ設定されており、プライベートネットワーク (LAN) のセキュリティは高いものになっています。

NATトラバーサルは、イントラネット (LAN) 上にある本製品を、NATルーターの外側 (WAN) から利用できるようにしたい場合に使用します。NATトラバーサルを正しく設定すると、NATルーターの外部HTTPポートに着信するすべてのHTTPトラフィックが本製品に転送されます。

NATトラバーサルは、[\[\[Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced \(設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定\)\]\]](#) で設定します。

注

- NATトラバーサルを機能させるには、ルーターがNATトラバーサルに対応している必要があります。また、UPnP[®]にも対応している必要があります。
- この場合、ルーターとは、NATルーター、ネットワークルーター、インターネットゲートウェイ、ブロードバンドルーター、ブロードバンド共有デバイスなどのネットワークルーティングデバイス、またはファイアウォールなどのソフトウェアを指します。

有効化/無効化 - 有効にすると、本製品はUPnPを使用してネットワーク上のNATルーターにポートマッピングを設定します。本製品でUPnPを有効にする必要があります ([\[\[Setup > Additional Controller Configuration > System Options > Network > UPnP \(設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > UPnP\)\]\]](#) を参照してください)。

Use manually selected NAT router (手動で選択したNATルーターを使用する) - このオプションを選択すると、手動でNATルーターを選択して、フィールドにルーターのIPアドレスを入力できます。ルーターを指定しなかった場合、本製品がネットワーク上でNATルーターを自動的に検索します。複数のルーターが検出された場合は、デフォルトのルーターが選択されます。

Alternative HTTP port (代替HTTPポート) - このオプションを選択すると、外部HTTPポートを手動で定義できます。1024~65535の範囲でポートを入力してください。ポートフィールドが空白の場合や、デフォルトの設定 (0) が表示されている場合、NATトラバーサルを有効にしたときにポート番号が自動的に選択されます。

注

- NATトラバーサルが無効になっている場合でも、代替のHTTPポートを使用したり、アクティブにすることができます。これは、NATルーターがUPnPをサポートしておらず、NATルーターでポート転送を手動設定する必要がある場合に便利です。
- すでに使用されているポートを手動で入力しようとすると、別の使用可能なポートが自動的に選択されます。
- ポートが自動的に選択されると、このフィールドに表示されます。この選択を変更するには、新しいポート番号を入力して、**[Save (保存)]** をクリックします。

FTP

本製品でFTPサーバーを実行することにより、新しいファームウェア、ユーザーアプリケーションなどのアップロードができるようになります。FTPサーバーは、[\[\[Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced \(設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定\)\]\]](#) で無効にできます。

RTSP

本製品でRTSPサーバーが動作している場合、接続先のクライアントからイベントストリームを開始できます。RTSPポート番号は [\[Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced \(設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 詳細設定\)\]](#) で変更できます。デフォルトポートは554です。

AXIS A1601 Network Door Controller

システムオプション

注

RTSPサーバーが無効になっている場合、イベントストリームは使用できません。

SOCKS

SOCKSは、ネットワークプロキシプロトコルです。SOCKSサーバーを使用してファイアウォールやプロキシサーバーの外側のネットワークにアクセスするようにAxis製品を設定できます。この機能は、ファイアウォールの内側のローカルネットワーク上のAxis製品からローカルネットワークの外側（インターネットなど）に通知やアラームを送信したり、アップロードなどを行う必要がある場合に役立ちます。

SOCKSは、[[Setup > Additional Controller Configuration > System Options > Network > SOCKS (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > SOCKS)]] で設定します。詳細については、オンラインヘルプを参照してください。

QoS (Quality of Service)

QoS (Quality of Service) は、ネットワーク上の特定のトラフィックに対してそのサービスの品質を保証します。QoSに対応したネットワークでは、トラフィックに優先順位を付け、アプリケーションで使用できる帯域幅を制御することができるので、ネットワークの信頼性が高まります。

QoS は、[Setup > Additional Controller Configuration > System Options > Network > QoS (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > QoS)] で設定できます。Axis製品では、DSCP (Differentiated Services Codepoint) 値を使用して、イベント/アラームトラフィックおよび管理トラフィックにマークを付けることができます。

SNMP

SNMP (Simple Network Management Protocol) を使用すると、離れた場所からネットワーク装置を管理できます。SNMPコミュニティは、SNMPを実行しているネットワーク装置と管理ステーションのグループです。各グループは、コミュニティ名で識別されます。

本製品でSNMPを有効にするには、[[Setup > Additional Controller Configuration > System Options > Network > SNMP (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > SNMP)]] ページに移動します。

必要なセキュリティのレベルに応じて、使用するSNMPのバージョンを選択してください。

トラップは、本製品によって重要なイベントやステータスの変化に関して管理システムにメッセージを送るために使用されます。[Enable traps (トラップを有効にする)] をチェックして、トラップメッセージの送信先IPアドレスとメッセージを受け取る [Trap community (トラップコミュニティ)] を入力します。

注

HTTPSを有効にした場合は、SNMP v1とSNMP v2cは無効にしてください。

[Traps for SNMP v1/v2 (SNMP v1/v2トラップ)] は、重要なイベントやステータスの変化に関して管理システムにメッセージを送るために本製品によって使用されます。[Enable traps (トラップを有効にする)] をチェックして、トラップメッセージの送信先IPアドレスとメッセージを受け取る [Trap community (トラップコミュニティ)] を入力します。

本製品では、以下のトラップを使用することができます。

- ・ コールドスタート
- ・ ウォームスタート
- ・ リンクアップ
- ・ 認証失敗

SNMP v3は、暗号化と安全なパスワードを提供します。SNMP v3でトラップを使用するには、SNMP v3管理アプリケーションが必要です。

AXIS A1601 Network Door Controller

システムオプション

SNMP v3を使用するには、HTTPSを有効にする必要があります(27ページHTTPSを参照してください)。SNMP v3を有効にするには、ボックスにチェックマークを入れ、初期ユーザーパスワードを指定してください。

注

初期パスワードは1回しか設定できません。パスワードを忘れた場合は、本製品を工場出荷時の設定にリセットする必要があります。37ページ工場出荷時の設定にリセットするを参照してください。

UPnP

本製品は、UPnP®に対応しています。UPnPはデフォルトで有効になっているため、本製品は、このプロトコルをサポートしているオペレーティングシステムとクライアントによって自動的に検出されます。

UPnPは、[[Setup > Additional Controller Configuration > System Options > Network > UPnP (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > UPnP)]]で無効にできます。

Bonjour

Axis製品は、Bonjourに対応しています。Bonjourはデフォルトで有効になっているため、本製品は、このプロトコルをサポートしているオペレーティングシステムとクライアントによって自動的に検出されます。

Bonjourは、[[Setup > Additional Controller Configuration > System Options > Network > Bonjour (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > Bonjour)]]で無効にできます。

ポートとデバイス

I/Oポート

補助コネクタは、外部装置との接続に使用する、設定可能な入出力ポートを4つ備えています。

外部コネクタは、外部装置との接続に使用する、設定可能な入出力ポートを2つ備えています。

I/Oポートは、[Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (設定 > 追加のコントローラー設定 > システムオプション > ポートとデバイス > I/Oポート)]で設定できます。ポートの方向([入力]または[出力])を選択します。ポートには分かりやすい名前を付けることができ、ポートの[Normal states (標準状態)]は、[Open circuit (開路)]または[Grounded circuit (接地回路)]に設定できます。

ポートの状態

[System Options > Ports & Devices > Port Status (システムオプション > ポートとデバイス > ポートの状態)]ページのリストには、本製品の入出力ポートの状態が表示されます。

保守

Axis製品は保守機能を備えています。これらは、[[Setup > Additional Controller Configuration > System Options > Maintenance (設定 > 追加のコントローラー設定 > システムオプション > メンテナンス)]]で使用できます。

Axis製品が予想どおりに動作しない場合は、[再起動]をクリックして、Axis製品を正しく再起動します。この場合、現在の設定には影響がありません。

注

再起動により、サーバーレポートのすべてのエントリーが消去されます。

[再起動]をクリックすると、設定の大半が工場出荷時のデフォルト値にリセットされます。以下の設定はリセットされません。

- ・ ブートプロトコル (DHCPまたは静的)
- ・ 静的IPアドレス

AXIS A1601 Network Door Controller

システムオプション

- デフォルトルーター
- サブネットマスク
- システム時刻
- IEEE 802.1X設定

[デフォルト]をクリックすると、IPアドレスなど、すべての設定が工場出荷時の値にリセットされます。このボタンは慎重に使用する必要があります。Axis製品は、コントロールボタンを使用してリセットすることもできます。37ページ工場出荷時の設定にリセットするを参照してください。

ファームウェアのアップグレードについては、37ページファームウェアのアップグレード方法を参照してください。

サポート

サポートの概要

[[Setup > Additional Controller Configuration > System Options > Support > Support Overview (設定 > 追加のコントローラー設定 > システムオプション > サポート > サポートの概要)]] ページには、トラブルシューティングに関する情報や技術支援が必要な場合の連絡先情報があります。

37ページ、トラブルシューティングも参照してください。

システムの概要

Axis製品の状態および設定の概要を確認するには、[Setup > Additional Controller Configuration > System Options > Support > System Overview (設定 > 追加のコントローラー設定 > システムオプション > サポート > システムの概要)]に移動します。ここでは、ファームウェアバージョン、IPアドレス、ネットワークとセキュリティの設定、イベントの設定、最近のログの内容などの情報が表示されます。

Logs & Reports (ログとレポート)

[[Setup > Additional Controller Configuration > System Options > Support > Logs & Reports (設定 > 追加のコントローラー設定 > システムオプション > サポート > ログとレポート)]] ページでは、システム分析やトラブルシューティングに役立つログとレポートが生成されます。Axisの技術サポートに連絡する場合は、質問と共にサーバーレポートをお送りください。

System Log (システムログ) - システムイベントに関する情報を表示します。

Access Log (アクセスログ) - 製品へのアクセスに失敗したすべてのログをリストします。本製品への接続をすべて表示するように設定することもできます (下記参照)。

View Server Report (サーバーレポートを表示) - 製品ステータスに関する情報をポップアップウィンドウに表示します。アクセスログは自動的にサーバーレポートに含まれます。

Download Server Report (サーバーレポートをダウンロード) - UTF-8テキスト形式の完全なサーバーレポートを含んだ.zipファイルを生成します。製品のライブビューのスナップショットを含めるには、[Include snapshot from Live View (ライブビューからスナップショットを撮影してレポートに含める)]を選択してください。Axisのサポートに連絡する際には、必ず、.zipファイルを添えて問い合わせを行ってください。

Parameter List (パラメーターリスト) - 本製品のパラメーターと現在の設定を表示します。トラブルシューティングを行う場合やAxisのサポートに問い合わせを行う場合に役立ちます。

Connection List (接続リスト) - メディアストリームに現在アクセスしているすべてのクライアントを表示します。

Crash Report (クラッシュレポート) - デバッグ情報を含むアーカイブを生成します。レポートの生成には数分かかります。

AXIS A1601 Network Door Controller

システムオプション

システムログとアクセスログのログレベルは、[[Setup > Additional Controller Configuration > System Options > Support > Logs & Reports > Configuration (設定 > 追加のコントローラー設定 > システムオプション > サポート > ログとレポート > 構成)] で設定します。アクセスログは、本製品への接続をすべて表示するように設定することもできます ([Critical, Warnings & Info (致命的、警告、情報)] を選択します)。

詳細設定

スクリプト処理

上級ユーザーは、スクリプト処理を使用して、スクリプトをカスタマイズし、使用することができます。

注意

使い方を誤ると、予期せぬ動作が発生したり、Axis製品にアクセスできなくなる場合があります。

Axisでは、どのような結果になるかを理解するまで、この機能を使用しないことを強くお勧めします。Axisは、スクリプトのカスタマイズによって発生した問題についてはサポートを行いませんのでご注意ください。

スクリプトエディターを開くには、[[Setup > Additional Controller Configuration > System Options > Advanced > Scripting (設定 > 追加のコントローラー設定 > システムオプション > 詳細設定 > スクリプト処理)] に移動します。スクリプトが問題を引き起こす場合は、Axis製品を工場出荷時の設定にリセットしてください(37ページ参照)。

詳細については、www.axis.com/developerを参照してください。

ファイルのアップロード

ファイル (Webページや画像) をAxis製品にアップロードし、カスタム設定として使用することができます。ファイルをアップロードするには、[[Setup > Additional Controller Configuration > System Options > Advanced > File Upload (設定 > 追加のコントローラー設定 > システムオプション > 詳細設定 > ファイルのアップロード)] に移動します。

アップロードしたファイルには、<http://<IPアドレス>/local/<ユーザー>/<ファイル名>> を介してアクセスします。<ユーザー>には、アップロードしたファイル用に選択したユーザーグループ (管理者) を指定します。

AXIS A1601 Network Door Controller

トラブルシューティング

トラブルシューティング

工場出荷時の設定にリセットする

重要

工場出荷時の設定へのリセットは慎重に行ってください。工場出荷時の設定へのリセットを行うと、IPアドレスを含むすべての設定が工場出荷時の値にリセットされます。

本製品を工場出荷時の設定にリセットするには、以下の手順を実行します。

1. 本製品の電源を切ります。
2. コントロールボタンを押した状態で電源を再接続します。5 ページ、製品の概要を参照してください。
3. ステータスLEDインジケーターが再びオレンジ色に変わるまで、コントロールボタンを押し続けます (25秒間)。
4. コントロールボタンを離します。プロセスが完了すると、ステータスLEDインジケーターが緑色に変わります。これで本製品は工場出荷時の設定にリセットされました。ネットワーク上に利用可能なDHCPサーバーがない場合、デフォルトのIPアドレスは192.168.0.90になります。
5. インストールおよび管理ソフトウェアツールを使用して、IPアドレスの割り当て、パスワードの設定、製品へのアクセスを行います。

Webインターフェースを使用して、各種パラメーターを工場出荷時の設定に戻すこともできます。Setup > Additional Controller Configuration > Setup > System Options > Maintenance (設定 > 追加のコントローラー設定 > 設定 > システムオプション > メンテナンス) を選択し、Default (デフォルト) をクリックします。

現在のファームウェアの確認方法

ファームウェアは、ネットワークデバイスの機能を決定するソフトウェアです。問題のトラブルシューティングを行う際には、まず、現在のファームウェアバージョンを確認してください。最新バージョンには、特定の問題の修正が含まれていることがあります。

Axis製品の現在のファームウェアバージョンは、概要ページに表示されます。

ファームウェアのアップグレード方法

重要

- ユーザーが正しくアップグレードしなかったことに起因する修理については、販売店は費用を請求する権利を保有します。
- あらかじめ設定済みの設定とカスタム設定は、(その機能が新しいファームウェアで利用できる場合)、ファームウェアのアップグレード時に保存されます。ただし、この動作をAxisが保証しているわけではありません。
- 以前のバージョンのファームウェアをインストールする場合は、その後、Axis製品を工場出荷時設定にリストアする必要があります。

AXIS A1601 Network Door Controller

トラブルシューティング

注

- アップグレードのプロセスが完了すると、Axis製品は自動的に再起動します。Axis製品のアップグレード後に手動で再起動する場合、アップグレードが失敗した疑いがある場合でも、5分間待ってください。
 - データベースのユーザーやグループ、証明書、その他のデータのアップデートは、ファームウェアのアップグレード後に行われるため、最初の起動が完了するまで数分かかることがあります。必要な時間はデータの量によって異なります。
 - 最新のファームウェアをダウンロードして製品をアップグレードすると、製品に最新機能が追加されます。ファームウェアを更新する前に、ファームウェアとともに提供されるアップグレード手順とリリースノートを必ずお読みください。
- 最新のファームウェアファイルをコンピューターにダウンロードします。ファームウェアファイルはAxisサポートページ (www.axis.com/support) から無料で入手できます。
 - 製品のWebページで、**[Setup > Additional Controller Configuration > System Options > Maintenance (設定 > 追加のコントローラー設定 > システムオプション > メンテナンス)]** に移動します。
 - [Upgrade Server (サーバーのアップグレード)]** で、**[Choose file (ファイルの選択)]** をクリックして、コンピューター上のファイルを指定します。
 - Axis製品をアップグレード後、工場出荷時の設定に自動的にリストアする場合は、**[Default (デフォルト)]** チェックボックスをオンにします。
 - [Upgrade (アップグレード)]** をクリックします。
 - Axis製品がアップグレードされて再起動するまで、約5分間待ちます。そのあと、Webブラウザのキャッシュをクリアします。
 - 製品にアクセスします。

現象、考えられる原因、対策

ファームウェアのアップグレードで問題が発生する

| | |
|-------------------|--|
| ファームウェアのアップグレード失敗 | ファームウェアのアップグレードに失敗した場合、製品は以前のファームウェアを再度読み込みます。ファームウェアのファイルを確認して、もう一度試してください。 |
|-------------------|--|

IPアドレスの設定で問題が発生する

| | |
|-----------------------|--|
| ARP/Pingを使用している | 再インストールを行います。Axis製品の電源投入後、2分以内にIPアドレスを設定する必要があります。Pingの長さは408に設定します。手順については、 axis.com の『インストールガイド』を参照してください。 |
| Axis製品が別のサブネット上にある | Axis製品のIPアドレスとAxis製品にアクセスするコンピューターのIPアドレスが異なるサブネットにある場合は、IPアドレスを設定できません。ネットワーク管理者に連絡して、適切なIPアドレスを取得してください。 |
| IPアドレスが別のデバイスで使用されている | Axis製品をネットワークから切断します。Pingコマンドを実行します(コマンドウィンドウまたはDOSウィンドウで、pingコマンドと本装置のIPアドレスを入力します)。 <ul style="list-style-type: none">もし、「Reply from <Axis製品のIPアドレス>: bytes=32; time=10...」という応答を受取った場合は、ネットワーク上の別のデバイスでIPアドレスがすでに使用中の可能性があります。ネットワーク管理者から新しいIPアドレスを取得し、Axis製品を再度インストールしてください。 |

AXIS A1601 Network Door Controller

トラブルシューティング

- もし、「Request timed out」が表示された場合は、Axis製品でそのIPアドレスを使用できます。この場合は、すべてのケーブル配線をチェックし、Axis製品を再度インストールしてください。

同じサブネット上の別のデバイスとIPアドレスが競合している可能性がある
DHCPサーバーによって動的アドレスが設定される前は、Axis製品の静的IPアドレスが使用されます。つまり、デフォルトの静的IPアドレスが別のデバイスでも使用されていると、Axis製品のアクセスに問題が発生する可能性があります。

ブラウザーからAxis製品にアクセスできない

| | |
|-----------------------|---|
| ログインできない | HTTPSが有効な場合は、正しいプロトコル (HTTPまたはHTTPS) を使用してログインしてください。ブラウザーのアドレスフィールドに、手動で「http」または「https」と入力する必要がある場合があります。 rootユーザーのパスワードを忘れた場合は、製品を工場出荷時の設定にリセットする必要があります。37ページ工場出荷時の設定にリセットするを参照してください。 |
| DHCPによってIPアドレスが変更された | DHCPサーバーから取得したIPアドレスは動的なアドレスであり、変更されることがあります。IPアドレスが変更された場合は、AXIS IP UtilityまたはAXIS Device Managerを使用してAxis製品のネットワーク上の場所を特定してください。Axis製品のモデルまたはシリアル番号、あるいはDNS名 (設定されている場合) を使用して製品を識別します。 必要に応じて、静的IPアドレスを手動で割り当てることができます。手順については、製品ページ (axis.com) にある『IPアドレスを割り当ててデバイスにアクセスする方法』のドキュメントを参照してください。 |
| IEEE 802.1X使用時の証明書エラー | 認証を正しく行うには、Axis製品の日付と時刻をNTPサーバーと同期させる必要があります。を参照してください。 |

Axis製品にローカルにアクセスできるが、外部からアクセスできない

| | |
|---------------|---|
| ルーターの設定 | Axis製品への着信データトラフィックを許可するようにルーターを設定するには、NATトラバーサル機能を有効にします。この機能を有効にすると、Axis製品へのアクセスを許可するようにルーターが自動設定されます。32ページIPv4用NATトラバーサル (ポートマッピング) を参照してください。ルーターはUPnP®に対応している必要があります。 |
| ファイアウォールによる保護 | インターネットのファイアウォールについて、ネットワーク管理者に確認してください。 |
| デフォルトルーターが必要 | ルーターを設定する必要があるかどうか、[Setup > Network Settings (設定 > ネットワーク設定)] または [Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (設定 > 追加のコントローラー設定 > システムオプション > ネットワーク > TCP/IP > 基本設定)] で確認してください。 |

AXIS A1601 Network Door Controller

仕様

仕様

ULのマークが付いたテキストは、UL 293またはUL 294インストールでのみ有効です。

LEDインジケータ

| LED | カラー | 説明 |
|---------|------|---|
| ネットワーク | 緑 | 100 Mbit/sネットワークに接続している場合、点灯します。ネットワークパケットを送受信した場合、点滅します。 |
| | オレンジ | 10 Mbit/sネットワークに接続している場合、点灯します。ネットワークパケットを送受信した場合、点滅します。 |
| | 消灯 | ネットワーク接続なし。 |
| 状態 | 緑 | 正常動作であれば緑色に点灯します。 |
| | オレンジ | 起動時、設定の復元時に点灯します。 |
| | 赤 | アップグレードに失敗した場合に、ゆっくりと点滅。 |
| 電源 | 緑 | 正常動作。 |
| | オレンジ | ファームウェアアップグレード中は緑とオレンジの交互点滅。 |
| リレー過電流 | 赤 | 短絡または過電流が検知された場合に点灯します。 |
| | 消灯 | 正常動作。 |
| リーダー過電流 | 赤 | 短絡または過電流が検知された場合に点灯します。 |
| | 消灯 | 正常動作。 |
| リレー | 緑 | リレーが有効です。 ¹ |
| | 消灯 | リレーが無効です。 |

1. COMがNOに接続するとリレーが有効になります。

注

- ステータスLEDは、イベントの発生時に点滅させることができます。
- ステータスLEDを点滅させ、本製品を識別できるように設定することができます。[**Setup > Additional Controller Configuration > System Options > Maintenance (設定 > 追加のコントローラー設定 > システムオプション > メンテナンス)**]に移動します。

ボタン

コントロールボタン

コントロールボタンは、以下の用途で使用します。

- 製品を工場出荷時の設定にリセットする。37ページ工場出荷時の設定にリセットするを参照してください。

AXIS A1601 Network Door Controller

仕様

コネクタ

ネットワークコネクタ

RJ45イーサネットコネクタ、Power over Ethernet Plus (PoE+) 対応。

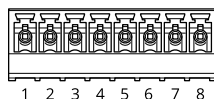
UL: Power over Ethernet (PoE) は、44~57 V DC、15.4 W / 30 Wを提供できる、UL 294認定Power over Ethernet IEEE 802.3af/802.3at Type 1 Class 3、またはPower over Ethernet Plus (PoE+) IEEE 802.3at Type 2 Class 4有限電源インジェクタによって供給される必要があります。Power over Ethernet (PoE) は、AXIS T8133 Midspan 30 W 1-portが搭載されたULによって評価されています。

リーダーコネクタ

リーダーとの通信用のRS485およびWiegandの両プロトコルに対応する8ピンターミナルブロック×2。

指定の電源出力値は、2つのリーダーポート間で共有されます。つまり、ドアコントローラーに接続されるすべてのリーダー向けに12 V DC、486 mAが供給されます。

製品のWebページで使用するプロトコルを選択します。



RS485 の設定

| 機能 | ピン | 注 | 仕様 |
|----------------|-----|---|--------------------------------|
| DCグラウンド (GND) | 1 | | 0 V DC |
| DC出力 (+12 V) | 2 | リーダーに電力を供給します。 | 両方のリーダーに合わせて12 V DC、最大486 mA |
| RX/TX | 3-4 | 全二重: RX。半二重: RX/TX。 | |
| TX | 5-6 | 全二重: TX。 | |
| 設定可能 (入力または出力) | 7-8 | デジタル入力 — 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。 | 0~30 V DC (最大) |
| | | デジタル出力 - リレーなど、誘導負荷とともに使用する場合は、過渡電圧から保護するために、ダイオードを負荷と並列に接続します。 | 0~30 V DC (最大)、オープンドレイン、100 mA |

重要

- ・ コントローラーからリーダーに電力を供給する場合、適格なケーブル長は最大200 mです。
- ・ コントローラーからリーダーに電力を供給しない場合に、以下のケーブル要件を満たす場合、リーダーデータ用の適格なケーブル長は最大1000 mです。シールド付きツイストペア (1組)、AWG 24、120 Ωインピーダンス。

Wiegand の設定

AXIS A1601 Network Door Controller

仕様

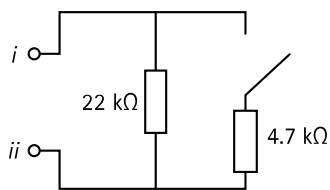
| 機能 | ピン | 注 | 仕様 |
|----------------|-----|---|--------------------------------|
| DCグラウンド (GND) | 1 | | 0 V DC |
| DC出力 (+12 V) | 2 | リーダーに電力を供給します。 | 両方のリーダーに合わせて12 V DC、最大486 mA |
| D0 | 3 | | |
| D1 | 4 | | |
| O | 5-6 | デジタル出力、オープンドレイン | |
| 設定可能 (入力または出力) | 7-8 | デジタル入力 - 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。 | 0~30 V DC (最大) |
| | | デジタル出力 - リレーなど、誘導負荷とともに使用する場合は、過渡電圧から保護するために、ダイオードを負荷と並列に接続します。 | 0~30 V DC (最大)、オープンドレイン、100 mA |

重要

- ・ コントローラーからリーダーに電力を供給する場合、適格なケーブル長は最大150 mです。
- ・ コントローラーからリーダーに電力を供給しない場合に、以下のケーブル要件を満たす場合、リーダーデータ用の適格なケーブル長は最大150 mです。AWG 22。

状態監視入力

状態監視を使用するには、下図に従って終端抵抗器を設置します。



i 入力
ii 0 VDC (-)

UL: 状態監視入力は、盗難防止向けの用途としてULによって評価されませんでした。ドアモニターとREXのみが終端抵抗器を使用した監視をサポートします。

注

シールド付きツイストケーブルを使用することをお勧めします。シールドを0 V DCに接続します。

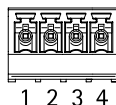
AXIS A1601 Network Door Controller

仕様

ドアコネクタ

ドア監視デバイス用4ピンターミナルブロック (×2) (デジタル入力)。

ドアモニターのみが終端抵抗器を使用した監視をサポートします。接続が中断されると、アラームがトリガーされます。監視入力を使用するには、終端抵抗器を設置します。状態監視入力の接続図を使用します。42ページを参照してください。



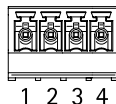
| 機能 | ピン | 備考 | 仕様 |
|---------|------|--|----------------|
| DCグラウンド | 1, 3 | | 0 V DC |
| 入力 | 2, 4 | ドアモニターとの通信用。 デジタル入力または監視入力 - それぞれピン1または3に接続し、動作させない場合はフロート状態 (未接続) のままにします。 | 0~30 V DC (最大) |

重要

以下のケーブル要件を満たす場合、ケーブルの長さは最大 30 m です。AWG 24。

リレーコネクタ

ロックやゲートのインターフェースをコントロールするなど利用可能なForm Cリレー用4ピンのターミナルブロック×2。



| 機能 | ピン | 備考 | 仕様 |
|---------------|----|--|--------------------------------------|
| DCグラウンド (GND) | 1 | | 0 V DC |
| NO | 2 | NO (ノーマルオープン)。 リレーデバイス接続用。NOとDCグラウンド間でフェイルセキュアロックを接続します。 ジャンパー未使用時、2つのリレーピンは他の残りの回路から直流的に分離されます。 | 最大電流 = 2 A (リレーごと) 最大電圧 = 30 V DC |
| COM | 3 | 共通 | |
| NC | 4 | NC (ノーマルクローズ)。 リレーデバイス接続用。NCとDCグラウンド間でフェイルセーフロックを接続します。 ジャンパー未使用時、2つのリレーピンは他の残りの回路から直流的に分離されます。 | |

リレー電源ジャンパー

リレー電源ジャンパーが取り付けられている場合、12 V DCまたは24 V DCをリレーCOMにピンに接続します。

AXIS A1601 Network Door Controller

仕様

これはGNDピンとNOピン間、もしくはGNDピンとNCピン間のロックに接続するために使用できます。

| 電源 | 12 V DCでの最大電力 ¹ | 24 V DCでの最大電力 ¹ |
|------|----------------------------|----------------------------|
| DC入力 | 1 600 mA | 800 mA |
| PoE | 800 mA | 400 mA |

1. 電力は2つのリレーとAUX I/O 12 V DCの間で共有されます。

注意

ロックに極性がない場合は、外部フライバックダイオードを追加することをお勧めします。

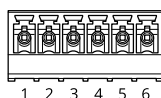
補助コネクタ

補助コネクタに外部装置を接続し、動体検知、イベントトリガー、アラーム通知などと組み合わせて使用することができます。補助コネクタは、0 V DC基準点と電力 (DC出力) に加えて、以下へのインターフェースを提供します。

デジタル入力 - オープンサーキットとクローズサーキットの切り替えが可能なデバイス (PIRセンサー、ドア/窓の接触、ガラス破損検知器など) を接続するための入力です。

デジタル出力 - リレーやLEDなどの外部デバイスを接続します。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースまたは製品のWebページから有効にすることができます。

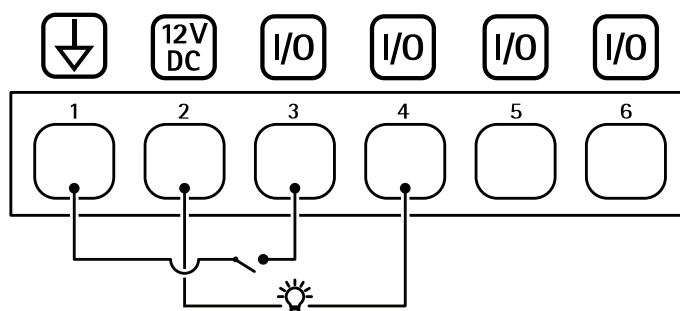
6ピンターミナルブロック



| 機能 | ピン | 備考 | 仕様 |
|----------------|-----|--|--------------------------------|
| DCアース | 1 | | 0 V DC |
| DC出力 | 2 | 補助装置の電源供給に使用できます。 注: このピンは、電源出力としてのみ使用できます。 | I/Oごとに12 V DC 最大負荷 = 50 mA |
| 設定可能 (入力または出力) | 3-6 | デジタル入力 - 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。 | 0~30 V DC (最大) |
| | | デジタル出力 - アクティブ時はピン1 (DCグラウンド) に内部で接続し、非アクティブ時はフロート状態 (未接続) になります。リレーなど、誘導負荷とともに使用する場合は、過渡電圧から保護するために、ダイオードを負荷と並列に接続します。内部12 V DC出力 (ピン2) が使用されている場合、各I/Oは12 V DC、50 mA (最大) の外部負荷に電源を供給できます。オープンドレイン接続を外部電源と組み合わせて使用する場合、I/Oは0~30 V DC、100 mAのDC給電を管理できます。 | 0~30 V DC (最大)、オープンドレイン、100 mA |

AXIS A1601 Network Door Controller

仕様

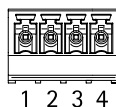


- 1 DCグランド
- 2 DC出力 12V
- 3 I/O (入力として設定)
- 4 I/O (出力として設定)
- 5 設定可能I/O
- 6 設定可能I/O

外部コネクタ

ガラスの破壊検知や火災検知などの外部デバイスで使用する4ピンターミナルブロックです。

UL: このコネクタは、盗難/火災警報用途向けとしてはULによって評価されていません。



| 機能 | ピン | 備考 | 仕様 |
|----------------|------|--|--------------------------------|
| DCグランド | 1, 3 | | 0 V DC |
| 設定可能 (入力または出力) | 2, 4 | デジタル入力 – 動作させるにはピン1または3に接続し、動作させない場合はフロート状態 (未接続) のままにします。 | 0~30 V DC (最大) |
| | | デジタル出力 – 動作させるにはピン1または3に接続し、動作させない場合はフロート状態 (未接続) のままにします。リレーなど、誘導負荷とともに使用する場合は、過渡電圧から保護するために、ダイオードを負荷と並列に接続します。 | 0~30 V DC (最大)、オープンドレイン、100 mA |

電源コネクタ

DC電源入力用2ピンターミナルブロック。定格出力が100 W以下または5 A以下の安全特別低電圧 (SELV) に準拠した有限電源 (LPS) を使用してください。



AXIS A1601 Network Door Controller

仕様

| 機能 | ピン | 備考 | 仕様 |
|------------|----|--|---------------------|
| 0 V DC (-) | 1 | | 0 V DC |
| DC入力 | 2 | Power over Ethernetを使用しないときのコントローラーへの電源供給用。 注: このピンは、電源入力としてのみ使用できます。 | 10.5~28 V DC、最大36 W |

UL: アプリケーションに応じて適切な定格で、UL 294、UL 293、またはUL 603の認定を受けた電源によって供給されるDC電源。

バックアップバッテリー入力コネクタ

内蔵チャージャー付きバッテリーを使用するバックアップソリューション用です。12 V DC入力。

UL: このコネクタはULによって評価されていません。

重要

バッテリーの入力を使用する場合、外部3 Aスローブローフューズを直列に接続する必要があります。



| 機能 | ピン | 備考 | 仕様 |
|------------|----|--|---------------------|
| 0 V DC (-) | 1 | | 0 V DC |
| バッテリーの入力 | 2 | 他の電源が利用できないときのドアコントローラーへの電力供給用です。 注: このピンはバッテリー電源入力としてのみ使用できます。UPSへの接続専用です。 | 11~13.7 V DC、最大36 W |

AXIS A1601 Network Door Controller

安全情報

安全情報

危険レベル

▲危険

回避しない場合、死亡または重傷につながる危険な状態を示します。

▲警告

回避しない場合、死亡または重傷につながるおそれのある危険な状態を示します。

▲注意

回避しない場合、軽傷または中程度の怪我につながるおそれのある危険な状態を示します。

注意

回避しない場合、器物の破損につながるおそれのある状態を示します。

その他のメッセージレベル

重要

製品を正しく機能させるために不可欠な重要情報を示します。

注

製品を最大限に活用するために役立つ有用な情報を示します。

AXIS A1601 Network Door Controller










装置インターフェース

装置インターフェース

本装置のインターフェースにアクセスするには、Webブラウザで装置のIPアドレスを入力します。

注

このセクションは、AXIS Camera Station Secure Entryファームウェアを使用したAXIS A1601 Network Door Controllerにのみ有効です。

-  メインメニューの表示/非表示を切り取ります。
-  製品のヘルプにアクセスします。
-  言語を変更します。
-  ライトテーマまたはダークテーマを設定します。
-  ユーザーメニューは以下を含みます。
 -  ログインしているユーザーに関する情報。
 -  **Change user (ユーザーの変更)**: 現在のユーザーをログアウトさせ、新しいユーザーにログインさせます。
 -  **Log out (ログアウト)**: 現在のユーザーをログアウトさせます。
-  コンテキストメニューは以下を含みます。
 - Analytics data (分析データ)**: 個人以外のブラウザデータの共有に同意します。
 - フィードバック**: フィードバックを共有して、ユーザーエクスペリエンスの向上に役立てます。
 - 法的情報**: Cookieおよびライセンスについての情報を表示します。
 - 詳細情報**: ファームウェアのバージョンとシリアル番号を含む装置情報を表示します。
 - Legacy device interface (従来の装置インターフェース)**: 装置インターフェースを従来の装置インターフェースに変更します。

ステータス

NTP sync (NTP同期)

装置がNTPサーバーと同期しているかどうかや、次の同期までの残り時間など、NTP同期情報を表示します。

NTP settings (NTP設定): クリックすると、NTPの設定を変更できる [Date and time (日付と時刻)] のページに移動します。

装置情報

ファームウェアのバージョンとシリアル番号を含む装置情報を表示します。

ファームウェアのアップグレード: クリックすると、[Maintenance (メンテナンス)] ページに移動し、ファームウェアのアップグレードができるようになります。

AXIS A1601 Network Door Controller

装置インターフェース

アクセスコントロール

アラーム

Device motion (デバイスの動き): ドアコントローラーのデバイスの動きが検知されたときに、システムでアラームをトリガーすることが、デフォルトで有効になっています。

ケーシング開放: ドアコントローラーのケーシングの開放が検知されたときに、システムでアラームをトリガーすることが、デフォルトで有効になっています。

外部からのいたずら: I/O 13に接続されています。オンにすると、外部からのいたずらが検知されたときにシステムでアラームがトリガーされます。たとえば、外部キャビネットが開閉されたときです。

状態監視: 状態監視をオンにし、終端抵抗器を設定します。

- 並列優先接続を使用するには、[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。
- 直列優先接続を使用するには、[Serial first connection (直列優先接続)] を選択し、[Resistor values (抵抗器の値)] ドロップダウンリストから抵抗器の値を選択します。

周辺機器

Upgrade readers (リーダーのアップグレード): クリックすると、リーダーが新しいファームウェアバージョンにアップグレードされます。オンラインでアップグレードできるのは、AXIS A4020-E Readerのみです。

システム

日付と時刻

時刻の形式は、Webブラウザの言語設定によって異なります。

注

装置の日付と時刻をNTPサーバーと同期することをお勧めします。

Synchronization (同期): 装置の日付と時刻を同期するオプションを選択します。

- **Automatic date and time (manual NTS KE servers) (日付と時刻の自動設定 (手動NTS KEサーバー)):** DHCPサーバーに接続された安全なNTPキー確立サーバーと同期します。
 - **Manual NTS KE servers (手動NTS KEサーバー):** 1台または2台のNTPサーバーのIPアドレスを入力します。2台のNTPサーバーを使用すると、両方からの入力に基づいて装置が同期し、時刻を調整します。
- **Automatic date and time (NTP servers using DHCP) (日付と時刻の自動設定 (DHCPを使用したNTPサーバー)):** DHCPサーバーに接続されたNTPサーバーと同期します。
 - **Fallback NTP servers (フォールバックNTPサーバー):** 1台または2台のフォールバックサーバーのIPアドレスを入力します。
- **Automatic date and time (manual NTP servers) (日付と時刻の自動設定 (手動NTPサーバー)):** 選択したNTPサーバーと同期します。
 - **Manual NTP servers (手動NTPサーバー):** 1台または2台のNTPサーバーのIPアドレスを入力します。2台のNTPサーバーを使用すると、両方からの入力に基づいて装置が同期し、時刻を調整します。
- **Custom date and time (日付と時刻のカスタム設定):** 日付と時刻を手動で設定する。[Get from system (システムから取得)] をクリックして、コンピューターまたはモバイル装置から日付と時刻の設定を1回取得します。

タイムゾーン: 使用するタイムゾーンを選択します。夏時間と標準時間に合わせて、時刻が自動的に調整されます。

AXIS A1601 Network Door Controller

装置インターフェース

注

システムは、すべての録画、ログ、およびシステム設定で日付と時刻の設定を使用します。

ネットワーク

IPv4

Assign IPv4 automatically (IPv4 自動割り当て): ネットワークルーターに自動的に装置にIPアドレスを割り当てさせる場合に選択します。ほとんどのネットワークでは、自動IP (DHCP) をお勧めします。

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

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

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

IPv6

Assign IPv6 automatically (IPv6 自動割り当て): IPv6をオンにし、ネットワークルーターに自動的に装置にIPアドレスを割り当てさせる場合に選択します。

Hostname (ホスト名)

Assign hostname automatically (ホスト名自動割り当て): ネットワークルーターに自動的に装置にホスト名を割り当てさせる場合に選択します。

Hostname (ホスト名): 装置にアクセスする別の方法として使用するホスト名を手動で入力します。ホスト名は、サーバーレポートとシステムログで使用されます。使用できる文字は、A～Z、a～z、0～9、-、_です。

DNS servers (DNSサーバー)

Assign DNS automatically (DNS 自動割り当て): ネットワークルーターに自動的に装置に検索ドメインとDNSサーバーアドレスを割り当てさせる場合に選択します。ほとんどのネットワークでは、自動DNS (DHCP) をお勧めします。

Search domains (検索ドメイン): 完全修飾でないホスト名を使用する場合は、[Add search domain (検索ドメインの追加)] をクリックし、装置が使用するホスト名を検索するドメインを入力します。

DNS servers (DNSサーバー): [Add DNS server (DNSサーバーを追加)] をクリックして、DNSサーバーのIPアドレスを入力します。このサーバーは、ホスト名からローカルネットワーク上のIPアドレスへの変換を行います。

HTTPおよびHTTPS

AXIS A1601 Network Door Controller

装置インターフェース

次によってアクセスを許可: ユーザーが [HTTP]、[HTTPS]、または [HTTP and HTTPS (HTTPおよびHTTPS)] プロトコルを介して装置に接続することを許可するかどうかを選択します。

HTTPSは、ユーザーからのページ要求とWebサーバーから返されたページの暗号化を提供するプロトコルです。暗号化された情報の交換は、サーバーの真正性(サーバーが本物であること)を保証するHTTPS証明書の使用により制御されます。

装置でHTTPSを使用するには、HTTPS証明書をインストールする必要があります。[System (システム) > Security (セキュリティ)] に移動し、証明書の作成とインストールを行います。

注

暗号化されたWebページをHTTPS経由で表示する場合、特に初めてページを要求するときに、パフォーマンスが低下することがあります。

HTTP port (HTTPポート): 使用するHTTPポートを入力します。ポート80または1024~65535の範囲の任意のポートを使用できます。管理者としてログインしている場合は、1~1023の範囲の任意のポートを入力することもできます。この範囲のポートを使用すると、警告が表示されます。

HTTPS port (HTTPSポート): 使用するHTTPSポートを入力します。ポート443または1024~65535の範囲の任意のポートを使用できます。管理者としてログインしている場合は、1~1023の範囲の任意のポートを入力することもできます。この範囲のポートを使用すると、警告が表示されます。

Certificate (証明書): 装置のHTTPSを有効にする証明書を選択します。

Friendly name (フレンドリ名)

Bonjour®: オンにしてネットワーク上で自動検出を可能にします。

Bonjour name (Bonjour名): ネットワークで表示されるフレンドリ名を入力します。デフォルト名は装置名とMACアドレスです。

Use UPnP® (UPnPを使用): オンにしてネットワーク上で自動検出を可能にします。

UPnP name (UPnP名): ネットワークで表示されるフレンドリ名を入力します。デフォルト名は装置名とMACアドレスです。

One-Click Cloud Connection (ワンクリッククラウド接続)

One-Click cloud connection (O3C) とO3Cサービスを共に使用すると、インターネットを介して、ライブビデオや録画ビデオにどこからでも簡単かつ安全にアクセスできます。詳細については、axis.com/end-to-end-solutions/hosted-servicesを参照してください。

Allow O3C (O3Cを許可):

- **One-click (ワンクリック):** デフォルトの設定です。インターネットを介してO3Cサービスに接続するには、装置のコントロールボタンを押し続けます。コントロールボタンを押してから24時間以内に装置をO3Cサービスに登録する必要があります。登録しない場合、装置はO3Cサービスから切断されます。装置を登録すると、[Always (常時)] が有効になり、装置はO3Cサービスに接続されたままになります。
- **Always (常時):** 装置は、インターネットを介してO3Cサービスへの接続を継続的に試行します。装置が登録されると、O3Cサービスに接続したままになります。装置のコントロールボタンに手が届かない場合は、このオプションを使用します。
- **No (なし):** O3Cサービスを無効にします。

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

Host (ホスト): プロキシサーバーのアドレスを入力します。

Port (ポート): アクセスに使用するポート番号を入力します。

AXIS A1601 Network Door Controller

装置インターフェース

Login (ログイン) と Password (パスワード): 必要な場合は、プロキシサーバーのユーザー名とパスワードを入力します。

Authentication method (認証方式)

- **Basic (ベーシック):** この方法は、HTTP用の最も互換性のある認証方式です。ユーザー名とパスワードを暗号化せずにサーバーに送信するため、**Digest (ダイジェスト)** 方式よりも安全性が低くなります。
- **Digest (ダイジェスト):** この認証方式は、常に暗号化されたパスワードをネットワークに送信するため、高いセキュリティレベルが得られます。
- **Auto (オート):** このオプションを使用すると、装置はサポートされている方法に応じて認証方法を選択できます。**Digest (ダイジェスト)** 方式が**Basic (ベーシック)** 方式より優先されます。

Owner authentication key (OAK) (所有者認証キー、OAK): [Get key (キーを取得)] をクリックして、所有者認証キーを取得します。これは、装置がファイアウォールやプロキシを介さずにインターネットに接続されている場合にのみ可能です。

SNMP

SNMP (Simple Network Management Protocol) を使用すると、離れた場所からネットワーク装置を管理できます。

SNMP: 使用するSNMPのバージョンを選択します。

- **v1 and v2c (v1およびv2c):**
 - **Read community (読み取りコミュニティ):** サポートされているSNMPオブジェクトすべてに読み取り専用のアクセスを行えるコミュニティ名を入力します。デフォルト値は **[public (パブリック)]** です。
 - **Write community (書き込みコミュニティ):** サポートされている(読み取り専用のものを除く)SNMPオブジェクトすべてに読み取りアクセス、書き込みアクセスの両方を行えるコミュニティ名を入力します。デフォルト値は **[write (書き込み)]** です。
 - **Activate traps (トラップの有効化):** オンにすると、トラップレポートが有効になります。装置はトラップを使用して、重要なイベントまたはステータス変更のメッセージを管理システムに送信します。装置インターフェースでは、SNMP v1およびv2cのトラップを設定できます。SNMP v3に変更するか、SNMPをオフにすると、トラップは自動的にオフになります。SNMP v3を使用する際は、SNMP v3管理アプリケーションでトラップを設定できます。
 - **Trap address (トラップアドレス):** 管理サーバーのIPアドレスまたはホスト名を入力します。
 - **Trap community (トラップコミュニティ):** 装置がトラップメッセージを管理システムに送信するときに使用するコミュニティを入力します。
 - **Traps (トラップ):**
 - **Cold start (コールドスタート):** 装置の起動時にトラップメッセージを送信します。
 - **Warm start (ウォームスタート):** SNMP設定が変更されたときに、トラップメッセージを送信します。
 - **Link up (リンクアップ):** リンクの状態が切断から接続に変わったときにトラップメッセージを送信します。
 - **Authentication failed (認証失敗):** 認証に失敗したときにトラップメッセージを送信します。

注

SNMP v1およびv2cトラップをオンにすると、すべてのAXIS Video MIBトラップが有効になります。詳細については、[AXIS OSポータル > SNMP](#)を参照してください。

- **v3:** SNMP v3は、暗号化と安全なパスワードを使用する、より安全性の高いバージョンです。SNMP v3を使用するには、HTTPSを有効化し、パスワードをHTTPSを介して送信することをお勧めします。これにより、権限のない人が暗号化されていないSNMP v1およびv2cトラップにアクセスすることも防止できます。SNMP v3を使用する際は、SNMP v3管理アプリケーションでトラップを設定できます。
 - **Password for the account "initial" (「initial」アカウントのパスワード):** 「initial」という名前のアカウントのSNMPパスワードを入力します。HTTPSを有効化せずにパスワードを送信できますが、推奨しません。SNMP v3のパスワードは1回しか設定できません。HTTPSが有効な場合にのみ設定することをお勧めします。パスワードの設定後は、パスワードフィールドが表示されなくなります。パスワードを設定し直すには、装置を工場出荷時の設定にリセットする必要があります。

AXIS A1601 Network Door Controller

装置インターフェース

Connected clients (接続されたクライアント)

装置に接続しているすべてのクライアントが一覧表示されます。

Update (更新): クリックすると、リストを更新できます。

セキュリティ

証明書

証明書は、ネットワーク上の装置の認証に使用されます。この装置は、次の2種類の証明書をサポートしています。

- **Client/server Certificates (クライアント/サーバー証明書)**

クライアント/サーバー証明書は装置のIDを認証します。自己署名証明書と認証局 (CA) 発行の証明書のどちらでも使用できます。自己署名証明書による保護は限られていますが、認証局発行の証明書を取得するまで利用できます。

- **CA証明書**

CA証明書はピア証明書の認証に使用されます。たとえば、装置をIEEE 802.1Xで保護されたネットワークに接続するときに、認証サーバーのIDを検証するために使用されます。装置には、いくつかのCA証明書がプリインストールされています。

以下の形式がサポートされています:

- 証明書形式: .PEM、.CER、.PFX
- 秘密鍵形式: PKCS#1、PKCS#12

重要

装置を工場出荷時の設定へのリセットを行うと、すべての証明書が削除されます。プリインストールされたCA証明書は、再インストールされます。



リスト内の証明書をフィルターします。



証明書の追加: クリックして証明書を追加します。



コンテキストメニューは以下を含みます。

- **Certificate information (証明書情報):** インストールされている証明書のプロパティを表示します。
- **Delete certificate (証明書の削除):** 証明書の削除。
- **Create certificate signing request (証明書の署名要求を作成する):** デジタルID証明書を申請するために登録機関に送信する証明書署名要求を作成します。

IEEE 802.1x

AXIS A1601 Network Door Controller

装置インターフェース

IEEE 802.1xはポートを使用したネットワークへの接続を制御するIEEEの標準規格で、有線およびワイヤレスのネットワーク装置を安全に認証します。IEEE 802.1xは、EAP (Extensible Authentication Protocol) に基づいています。

IEEE 802.1xで保護されているネットワークにアクセスするネットワーク装置は、自己の証明を行う必要があります。認証は認証サーバーによって行われます。認証サーバーは通常、FreeRADIUSやMicrosoft Internet Authentication ServerといったRADIUSサーバーです。

証明書

CA証明書なしで設定されている場合、サーバー証明書の検証は無効になり、装置は接続先のネットワークに関係なく自己の認証を試みます。

証明書を使用する場合、Axisの実装では、装置と認証サーバーは、EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) を使用してデジタル証明書で自己を認証します。

装置が証明書で保護されたネットワークにアクセスできるようにするには、署名されたクライアント証明書を装置にインストールする必要があります。

Client certificate (クライアント証明書): IEEE 802.1xを使用するクライアント証明書を選択します。認証サーバーは、この証明書を使用してクライアントの身元を確認します。

CA certificate (CA証明書): 認証サーバーの身元を確認するためのCA証明書を選択します。証明書が選択されていない場合、装置は、接続されているネットワークに関係なく自己を認証しようとします。

EAP identity (EAP 識別情報): クライアント証明書に関連付けられているユーザーIDを入力します。

EAPOL version (EAPOL のバージョン): ネットワークスイッチで使用されるEAPOLのバージョンを選択します。

Use IEEE 802.1x (IEEE 802.1x を使用): IEEE 802.1xプロトコルを使用する場合に選択します。

Prevent brute-force attacks (ブルートフォース攻撃を防ぐ)

Blocking (ブロック): オンにすると、ブルートフォース攻撃がブロックされます。ブルートフォース攻撃では、試行錯誤を繰り返す総当たり攻撃でログイン情報や暗号化キーを推測します。

Blocking period (ブロック期間): ブルートフォース攻撃をブロックする秒を入力します。

Blocking conditions (ブロックの条件): ブロックが開始されるまでに1秒間に許容される認証失敗の回数を入力します。ページレベルと装置レベルの両方で許容される失敗の数を設定できます。

IP address filter (IPアドレスフィルター)

Use filter (フィルターを使用する): 装置へのアクセスを許可するIPアドレスを絞り込む場合に選択します。

Policy (ポリシー): 特定のIPアドレスに対してアクセスを [Allow (許可)] するか [Deny (拒否)] するかを選択します。

Addresses (アドレス): 装置へのアクセスを許可するIP番号と拒否するIP番号を入力します。CIDR形式を使用できます。

カスタム署名されたファームウェア証明書

AXIS A1601 Network Door Controller

装置インターフェース

Axisのテストファームウェアまたは他のカスタムファームウェアを装置にインストールするには、カスタム署名付きファームウェア証明書が必要です。証明書は、ファームウェアが装置の所有者とAxisの両方によって承認されたと証明します。ファームウェアは、一意のシリアル番号とチップIDで識別される特定の装置でのみ実行できます。Axisが署名を行う鍵を保有しているため、カスタム署名付きファームウェア証明書はAxisのみが作成できます。

[Install (インストール)] をクリックして、証明書をインストールします。ファームウェアをインストールする前に、証明書をインストールする必要があります。

ユーザー

+ **Add user (ユーザーを追加):** クリックして、新規ユーザーを追加します。最大100人のユーザーを追加できます。

Username (ユーザー名): 一意のユーザー名を入力します。

New password (新しいパスワード): ユーザーのパスワードを入力します。パスワードの長は1~64文字である必要があります。印刷可能なASCII文字(コード32~126)のみを使用できます。これには、英数字、句読点、および一部の記号が含まれます。

Repeat password (パスワードの再入力): 同じパスワードを再び入力します。

Role (役割):

- **Administrator (管理者):** すべての設定へ全面的なアクセス権をもっています。管理者は他のユーザーを追加、更新、削除もできます。
- **Operator (オペレーター):** 次の操作を除く、すべての設定へのアクセス権があります。
 - すべての [System settings (システム設定)]。
 - アプリを追加しています。
- **ビューア:** 設定を変更するアクセス権を持っていません。



コンテキストメニューは以下を含みます。

Update user (ユーザーの更新): ユーザーのプロパティを編集します。

ユーザーの削除 (Delete user): ユーザーを削除します。rootユーザーは削除できません。

MQTT

MQTT (Message Queuing Telemetry Transport) はモノのインターネット (IoT) で使われる標準の通信プロトコルです。これはIoTの統合を簡素化するために設計されており、小さなコードフットプリントと最小限のネットワーク帯域幅でリモート装置を接続するために、さまざまな業界で使用されています。Axis装置のファームウェアに搭載されているMQTTクライアントは、装置で生成されたデータやイベントを、ビデオ管理システム (VMS) ではないシステムに統合することを容易にします。

装置をMQTTクライアントとして設定します。MQTT通信は、クライアントとブローカーという2つのエンティティに基づいています。クライアントは、メッセージの送受信を行うことができます。ブローカーは、クライアント間でメッセージをルーティングする役割を担います。

MQTTの詳細については、[AXIS OSポータル](#)を参照してください。

MQTT client (MQTTクライアント)

AXIS A1601 Network Door Controller

装置インターフェース

Connect (接続): MQTTクライアントのオン/オフを切り替えます。

Status (ステータス): MQTTクライアントの現在のステータスを表示します。

Broker (ブローカー)

Host (ホスト): MQTTサーバーのホスト名またはIPアドレスを入力します。

Protocol (プロトコル): 使用するプロトコルを選択します。

Port (ポート): ポート番号を入力します。

- 1883はMQTTオーバTCPのデフォルト値です。
- 8883はMQTTオーバSSLのデフォルト値です。
- 80はMQTTオーバWebSocketのデフォルト値です。
- 443はMQTTオーバWebSocket Secureのデフォルト値です。

Username (ユーザー名): クライアントがサーバーにアクセスするために使用するユーザー名を入力します。

Password (パスワード): ユーザー名のパスワードを入力します。

Client ID (クライアントID): クライアントIDを入力します。クライアントがサーバーに接続すると、クライアント識別子がサーバーに送信されます。

Clean session (クリーンセッション): 接続時と切断時の動作を制御します。選択した場合、接続時と切断時にステータス情報が破棄されます。

Keep alive interval (キープアライブの間隔): キープアライブの間隔を使用すると、クライアントは長時間のTCP/IPタイムアウトを待たなくても、サーバーが使用できなくなったことを検知できます。

Timeout (タイムアウト): 接続を終了する時間の間隔(秒)です。デフォルト値: 60

装置トピックの接頭辞: MQTTクライアントタブの接続メッセージやLWTメッセージ、MQTT公開タブの公開条件におけるトピックのデフォルト値で使用されます。

Reconnect automatically (自動再接続): 切断された場合に、クライアントを自動的に再接続するかどうかを指定します。

Connect message (接続メッセージ)

接続が確立されたときにメッセージを送信するかどうかを指定します。

Send message (メッセージの送信): オンにすると、メッセージを送信します。

Use default (デフォルトを使用): オフに設定すると、独自のデフォルトメッセージを入力できます。

Topic (トピック): デフォルトのメッセージのトピックを入力します。

Payload (ペイロード): デフォルトのメッセージの内容を入力します。

Retain (保持する): クライアントの状態をこのTopic (トピック)に保存する場合に選択します。

QoS: パケットフローのQoS layerを変更します。

最終意思およびテストメントメッセージ

最終意思テストメント(LWT)を使用すると、クライアントはブローカーへの接続時、認証情報と共にテストメントを提供します。後ほどいずれかの時点でクライアントが予期せず切断された場合(電源の停止など)、ブローカーから他のクライアントにメッセージを送信できます。このLWTメッセージは通常のメッセージと同じ形式で、同一のメカニズムを経由してルーティングされます。

Send message (メッセージの送信): オンにすると、メッセージを送信します。

Use default (デフォルトを使用): オフに設定すると、独自のデフォルトメッセージを入力できます。

Topic (トピック): デフォルトのメッセージのトピックを入力します。

AXIS A1601 Network Door Controller

装置インターフェース

Payload (ペイロード): デフォルトのメッセージの内容を入力します。

Retain (保持する): クライアントの状態をこのTopic (トピック)に保存する場合に選択します。

QoS: パケットフローのQoS layerを変更します。

MQTT publication (MQTT公開)

Use default topic prefix (デフォルトのトピックプレフィックスを使用): 選択すると、[MQTT client (MQTTクライアント)] タブの装置のトピックプレフィックスで定義されたデフォルトのトピックプレフィックスが使用されます。

Include topic name (トピック名を含める): 選択すると、条件を説明するトピックがMQTTトピックに含まれます。

Include topic namespaces (トピックの名前空間を含める): 選択すると、ONVIFトピックの名前空間がMQTTトピックに含まれます。

シリアル番号を含める: 選択すると、装置のシリアル番号が、MQTTペイロードに含まれます。

+ **条件の追加:** クリックして条件を追加します。

Retain (保持する): 保持して送信するMQTTメッセージを定義します。

- **None (なし):** すべてのメッセージを、保持されないものとして送信します。
- **Property (プロパティ):** ステートフルメッセージのみを保持として送信します。
- **All (すべて):** ステートフルメッセージとステートレスメッセージの両方を保持として送信します。

QoS: MQTT公開に適切なレベルを選択します。

MQTT サブスクリプション

+ **サブスクリプションの追加:** クリックして、新しいMQTTサブスクリプションを追加します。

サブスクリプションフィルター: 購読するMQTTトピックを入力します。

装置のトピックプレフィックスを使用: サブスクリプションフィルターを、MQTTトピックのプレフィックスとして追加します。

サブスクリプションの種類:

- **ステートレス:** 選択すると、エラーメッセージがステートレスメッセージに変換されます。
- **ステートフル:** 選択すると、エラーメッセージが条件に変換されます。ペイロードが状態として使用されます。

QoS: MQTTサブスクリプションに適切なレベルを選択します。

アクセサリ

I/O ports (I/Oポート)

AXIS A1601 Network Door Controller



装置インターフェース

デジタル入力を使用すると、開回路と閉回路の切り替えが可能な外部装置 (PIRセンサー、ドアまたは窓の接触、ガラス破損検知器など) を接続できます。

デジタル出力を使用して、リレーやLEDなどの外部装置を接続します。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースまたは装置インターフェースから有効化できます。

Port (ポート)

Name (名前): テキストを編集して、ポートの名前を変更します。


Direction (方向):  は、ポートが入力ポートであることを示します。  は、出力ポートであることを示します。ポートが設定可能な場合は、アイコンをクリックして入力と出力を切り替えることができます。

標準の状態:  の場合は開回路をクリックし、  の場合は閉回路をクリックします。

現在の状態: ポートの現在のステータスを表示します。入力または出力は、現在の状態が通常の状態とは異なる場合に有効化されます。装置の接続が切断されているか、DC 1Vを超える電圧がかかっている場合に、装置の入力は開回路になります。

注

再起動中、出力回路は開かれます。再起動が完了すると、回路は正常位置に戻ります。このページの設定を変更した場合、有効なトリガーに関係なく出力回路は正常位置に戻ります。

状態監視  : オンにすると、誰かがデジタルI/O装置への接続を改ざんした場合に、そのアクションを検出してトリガーできます。入力が開いているか閉じているかを検知するだけでなく、誰かが改ざんした場合 (つまり、切断または短絡) も検知することができます。接続を監視するには、外部I/Oループ内に追加のハードウェア (終端抵抗器) が必要です。

ログ

レポートとログ

Reports (レポート)

- **View the device server report (装置サーバーレポートを表示):** クリックして、製品ステータスに関する情報をポップアップウィンドウに表示します。アクセスログは自動的にサーバーレポートに含まれます。
- **Download the device server report (装置サーバーレポートをダウンロード):** クリックしてサーバーレポートをダウンロードします。これによって、UTF-8形式で作成された完全なサーバーレポートのテキストファイルと、現在のライブビュー画像のスナップショットを取めた.zipファイルが生成されます。サポートに連絡する際には、必ずサーバーレポート.zipファイルを含めてください。
- **Download the crash report (クラッシュレポートをダウンロード):** サーバーの状態に関する詳細情報が付随したアーカイブをクリックしてダウンロードします。クラッシュレポートには、サーバーレポートに記載されている情報と詳細なバグ情報が含まれます。レポートには、ネットワークトレースなどの機密情報が含まれている場合があります。レポートの生成には数分かかることがあります。

ログ

- **View the system log (システムログを表示):** 装置の起動、警告、重要なメッセージなど、システムイベントに関する情報をクリックして表示します。
- **View the access log (アクセスログを表示):** 誤ったログインパスワードの使用など、本装置への失敗したアクセスをすべてクリックして表示します。

ネットワークトレース

AXIS A1601 Network Door Controller

装置インターフェース

重要

ネットワークトレースファイルには、証明書やパスワードなどの機密情報が含まれている場合があります。

ネットワークトレースファイルはネットワーク上のアクティビティを録画するので、トラブルシューティングに役立ちます。秒または分でトレースの期間を選択し、[ダウンロード]をクリックします。

リモートシステムログ

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



Server(サーバー): クリックして新規サーバーを追加します。

Host (ホスト): サーバーのホスト名またはIPアドレスを入力します。

Format (形式): 使用するsyslogメッセージの形式を選択します。

- RFC 3164
- RFC 5424

Protocol (プロトコル): 使用するプロトコルとポートを選択します。

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

重大度: トリガー時に送信するメッセージを選択します。

CA証明書設定: 現在の設定を参照するか、証明書を追加します。

保守

Restart (再起動): 装置を再起動します。再起動しても、現在の設定には影響がありません。実行中のアプリケーションは自動的に再起動されます。

Restore (リストア): ほとんどの設定が工場出荷時の値に戻ります。その後、装置とアプリを再設定し、プリインストールしなかったアプリを再インストールし、イベントやPTZプリセットを再作成する必要があります。

重要

復元後に保存される設定は以下の場合のみです。

- ブートプロトコル (DHCPまたは静的)
- 静的なIPアドレス
- Default router (デフォルトルーター)
- Subnet mask (サブネットマスク)
- 802.1X settings (802.1Xの設定)
- O3C settings (O3Cの設定)

Factory default (工場出荷時設定): すべての設定を工場出荷時の値に戻します。その後、装置にアクセス可能なIPアドレスをリセットする必要があります。

AXIS A1601 Network Door Controller

装置インターフェース

注

検証済みのファームウェアのみを装置にインストールするために、すべてのAxisの装置ファームウェアにデジタル署名が付け加えられます。これによって、Axis装置の全体的なサイバーセキュリティの最低ラインがさらに上がります。詳細については、axis.comでホワイトペーパー「署名済みファームウェア、セキュアブート、およびプライベートキーのセキュリティ」を参照してください。

Firmware upgrade (ファームウェアのアップグレード): 新しいファームウェアバージョンにアップグレードします。新しいファームウェアには、機能の改善やバグの修正、まったく新しい機能が含まれています。常に最新のリリースを使用することをお勧めします。最新のリリースをダウンロードするには、axis.com/supportに移動します。

アップグレード時には、以下の3つのオプションから選択できます。

- **Standard upgrade (標準アップグレード):** 新しいファームウェアバージョンにアップグレードします。
- **Factory default (工場出荷時設定):** アップグレードすると、すべての設定が工場出荷時の値に戻ります。このオプションを選択すると、アップグレード後に以前のファームウェアバージョンに戻すことはできません。
- **Autorollback (オートロールバック):** 設定した時間内にアップグレードを行い、アップグレードを確認します。確認しない場合、装置は以前のファームウェアバージョンに戻されます。

Firmware rollback (ファームウェアのロールバック): 以前にインストールされたファームウェアバージョンに戻します。

