AXIS A4612 Network Bluetooth® Reader

ユーザーマニュアル

目次

インストール....3
....3
使用に当たって....4
ネットワーク上のデバイスを検索する....4
ブラウザーサポート....4
装置のwebインターフェースを開く....4
デバイスを構成する....5
IPアドレスの設定....5
デバイスソフトウェアをアップグレードする....5
CA証明書とユーザー証明書のアップロード....5
webインターフェース....7
....7
ダッシュボード....7
....7
モジュール....7
13.56 MHzカードリーダー....7
Bluetooth....8
I/O....8
アクティブ出力....8
リレー....8
カスタマイズ....8
システム....9
システムダッシュボード....9
ネットワーク接続....9
日付と時刻....11
証明書....11
診断....12
メンテナンス....14
仕様....15
製品概要....15
シグナリングLED....15
ボタン....16
コントロールボタン....16
静電容量式タッチボタン....16
ケーブル....16
外部電源....16
ネットワーク コネクター....16
電源の優先順位....16
アクティブ出力....17
中継ケーブル....17
入力ケーブル....17
装置を清掃する....18
トラブルシューティング....19
工場出荷時の設定にリセットする....19
デバイスの現在のソフトウェアバージョンを確認する....19
ソフトウェアのアップグレード....19
技術的な問題と解決策....20
パフォーマンスに関する一般的な検討事項....21
サポートに問い合わせる....21
商標の帰属....22

インストール

以下のビデオで、AXIS A46 Network Reader Seriesの設置方法の例をご覧ください。

すべての設置シナリオに対応した完全な手順および安全に関する重要な情報については、設置ガイドを参照してください。

- AXIS A4610: *axis.com/products/axis-a4610/support*
- AXIS A4612: *axis.com/products/axis-a4612/support*



使用に当たって

ネットワーク上のデバイスを検索する

Windows®で検索したAxisデバイスにIPアドレスの割り当てを行うには、AXIS IP Utilityを使用します。アプリケーションは無料で、*axis.com/support*からダウンロードできます。

注

AXIS IP Utilityが動作しているコンピューターが、Axisデバイスと同じネットワークセグメント(物理サブネット) 上にあることが必要です。

1. Axisデバイスに電源とネットワークを接続します。
2. AXIS IP Utilityを起動します。ネットワークで使用できるすべてのデバイスが、自動的にリストに表示されます。
3. ブラウザーからデバイスにアクセスするには、リスト内で名前をダブルクリックします。

ブラウザーサポート

以下のブラウザーでデバイスを使用できます。

	Chrome™	Firefox®	Edge™	Safari®
Windows®	✓	✓	✓	
macOS®	✓	✓	✓	✓
Linux®	✓	✓	✓	
その他のオペレーティングシステム	✓	✓	✓	

✓: 推奨:

*: 制限付きでサポート

装置のwebインターフェースを開く

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には、AXIS IP Utilityを使用して、ネットワーク上で装置を見つけます。
2. デフォルトユーザー名とパスワードを入力します。
   - バージョン3.1より前のデバイスソフトウェア: `admin`および`pass`
   - デバイスソフトウェア3.1以降: `root`および`pass`

初めてデバイスにアクセスする際には、パスワードとデバイス名の変更を促すメッセージが表示されます。*webインターフェース, on page 7*を参照してください。

装置のwebインターフェースにあるすべてのコントロールとオプションの説明については、*webインターフェース, on page 7*を参照してください。

デバイスを構成する

このデバイスは、追加設定なしで標準のリーダーとして機能します。このセクションには、ハードウェアの設置完了後に、製品を稼働させるために設置担当者が行う必要のあるすべての重要な設定に関する説明が記載されています。

IPアドレスの設定

装置 はLANに接続されています。有効なIPアドレスを割り当てるか、LAN DHCPサーバーからIPアドレスを取得する必要があります。WebインターフェースでIPアドレスとDHCPを設定します。

IPアドレスを手動で設定するには：

1. [System (システム)] > [Network connection (ネットワーク接続)] > [Basic configuration (基本設定)] の順に移動します。
2. [IP address settings (IPアドレス設定)] で、[Use DHCP Server (DHCPサーバーの使用)] をオンにすると、LAN DHCPサーバーからIPアドレスが自動的に取得されいます。
3. IPアドレス、サブネットマスク、デフォルトゲートウェイを入力します。
4. 手動DNS設定を使用するには、[Always use manual DNS settings (常に手動DNS設定を使用する)] をオンにします。
5. プライマリDNSとセカンダリDNSを入力します。
6. ホスト名とベンダークラス識別子を入力して、デバイスを識別します。
7. [Required port mode (必要なポートモード)] のオプションを選択します。

現在のIPアドレスを確認するには：

注

- 装置を再起動しても設定は変わりません。

1. デバイスを開き、コントロールボタンを約15秒間長押しし、背面LEDインジケーターが同時に赤と緑に変わり、短いビープ音が1回鳴るまで待ちます。
2. コントロール ボタンを離すと、スピーカーを通じて装置から現在のIPアドレスが伝えられます。

デバイスソフトウェアをアップグレードする

デバイスに初めてログインする際に、デバイスのソフトウェアをアップグレードすることをお勧めします。*axis.com/support*で、装置の最新バージョンをダウンロードします。新規バージョンをアップロードするには、以下の手順を実行します。

1. [System (システム)] > [Maintenance (メンテナンス)] の順に移動します。
2. [Firmware upload (ファームウェアアップロード)] をクリックし、ダウンロードしたソフトウェアバージョンを選択します。
3. [Upload (アップロード)] をクリックします。

注

アップロード後に装置が再起動して、アップグレードが完了します。

CA証明書とユーザー証明書のアップロード

注

- 証明書IDは40文字以下で、小文字、大文字、数字、「_」、「-」のみを含めます。
- 2048ビットより長いRSA秘密鍵が割り当てられている証明書が拒否された場合は、以下のメッセージが表示されます。
- ECC (楕円曲線暗号) に基づく証明書の場合は、secp256r1 (prime256v1およびNIST P-256とも呼ばれる) とsecp384r1 (NIST P-384とも呼ばれる) 曲線のみを使用します。

CA証明書をアップロードするには：

1. [System (システム)] > [Certificates (証明書)] > [CA Certificates (CA証明書)] の順に移動します。
2. ＋ [Upload (アップロード)] をクリックします。
3. **証明書ID**を入力します。
4. [Select file (ファイルの選択)] をクリックして、CA証明書をアップロードします。
5. [Upload (アップロード)] をクリックします。

ユーザー証明書をアップロードするには：

1. [System (システム)] > [Certificates (証明書)] > [User Certificates (ユーザー証明書)] の順に移動します。
2. ＋ [Upload (アップロード)] をクリックして、証明書または秘密鍵をアップロードします。
3. **証明書ID**を入力します。
4. [Select file (ファイルの選択)] をクリックして、ユーザー証明書と秘密鍵をアップロードします。
5. 秘密鍵をアップロードする場合は、**デフォルトの鍵のパスワード**があれば、それを入力します。
6. [Upload (アップロード)] をクリックします。

注

ドアコントローラーのWebインターフェースでリーダーを接続する必要があります。ドアコントローラーのユーザーマニュアルを参照してください。

webインターフェース

注

このセクションで説明する機能と設定のサポートは、装置によって異なります。このアイコン は、機能または設定が一部の装置でのみ使用できることを示しています。

装置の新規通知にアクセスします。

ユーザーメニューは以下を含みます。

- Device time (デバイスの時刻):装置の現在の時刻。
- Change language (言語の変更)：言語を変更します。
- Change password (パスワードの変更):装置へのログインに必要なパスワードを変更します。
- ヘルプ:製品のヘルプにアクセスします。
- 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製品情報が表示されます。
- ログアウト:現在のアカウントからログアウトします。

ダッシュボード

コンテキストメニューは以下を含みます。

- Rename device (装置名の変更)：装置名を変更します。

Locate (位置特定)：リーダーを特定するための音声を再生します。

Serial number (シリアル番号):装置のシリアル番号。

Firmware version (ファームウェアバージョン)：現在装置で動作しているソフトウェアのバージョン。

MAC address (MACアドレス)：装置固有の識別子番号。

Uptime (アップタイム)：装置が動作している時間の長さが表示されます。

Hardware version (ハードウェアバージョン)：現在装置で動作しているハードウェアのバージョン。

Power source (電源)：現在の電源。

Modules (モジュール)：→ をクリックしてカードおよびリーダーのモジュール情報を表示・更新します。

モジュール

13.56 MHzカードリーダー

Module name (モジュール名)：入出力仕様のモジュール名を入力します。

使用可能なカードタイプ：カードリーダーが受け付けるカードのタイプをドロップダウンリストから選択します。

Bluetooth

⋮ コンテキストメニューは以下を含みます。

- **Module information (モジュール情報)**：Bluetoothリーダー名、モジュールタイプ、ボードタイプ、アセンブリバージョン、アプリケーションバージョン、ブートローダバージョンが表示されます。
- **Locate (位置特定)**：クリックすると、接続されているモジュールが検索されます。

Module name (モジュール名)：入出力仕様のモジュール名を入力します。

信号強度:携帯電話とのBluetoothモジュール通信の距離を選択します。

認証方法の起動：携帯電話の認証方法を1つまたは複数選択します。

- **Tap in app (アプリでタップ)**：これを選択すると、ユーザーが携帯電話で実行されているアプリケーションアイコンをタップした際に認証が有効になります。
- **装置との対話**：これを選択すると、ユーザーが静電容量式タッチ ボタンをタッチした際に認証が有効になります。*製品概要, on page 15*を参照してください。

注

Bluetooth信号の強度は、短距離では最大3 m、長距離では最大10 mまで設定可能です。この範囲は携帯電話の機種や設置環境によって異なります。

I/O

アクティブ出力

Logical state (論理状態):ドアの状態を示します。論理状態は、システムがドア開要求を受信していないときはオフ、ドア開要求を受信するとオンになります。

Output state (出力状態):物理的出力の実際の状態を示します。通常モードのとき、出力状態は論理状態と同じになります。反転モードとセキュリティモードのときは、論理状態と出力状態が反転します。

モード:ドロップダウンメニューからモードを選択します。

- [**Normal (通常)**] :出力は常時オフ状態ですが、ドア開要求があるとオンになります。
- **Security (セキュリティ)**:このモードでは、出力は接続リレーと接続します。このモードでは、出力は常時オン状態です。ドア開閉要求があると、出力ワイヤーを通じてコードがセキュリティリレーに送信されます。リレーがコードが正しいかどうかを確認します。
- **Inverted (反転)**:出力は常時オン状態ですが、ドア開要求があるとオフになります。

Test (テスト):クリックして、I/Oのアクティブ出力が動作しているか確認します。

リレー

Relay state (リレー状態):物理的なリレーの状態を示します。

Test (テスト):クリックしてリレーが作動しているか確認します。

カスタマイズ

信号音量

信号音量とは、アクセスコントロールシステムで通信が行われる際に装置から発生する音のレベルを指しています。例として、カードの読み取り時やアクセスの許可時に装置から発生するビープ音などが挙げられます。

キービープ音量：音量を設定します。

警告音音量：装置の動作状態が切り替わった際に発生する警告や信号の音量を設定します。例として、電源が入った際やケーブルが接続された際に発生する音の音量が上げられます。

輝度

Signaling LEDs intensity (信号LEDの強度)：LEDの輝度を設定します。

Backlight enabled (逆光の有効化) :オンにすると、逆光が有効になります。

Intensity (強度)：逆光の強さを設定します。

システム

システムダッシュボード

Download diagnostic package (診断パッケージをダウンロード):クリックすると、診断パッケージをファイルとしてダウンロードすることができます。

Network connection (ネットワーク接続):→ をクリックしてネットワーク設定を編集します。

- Network overview (ネットワークオーバービュー):現在デバイスに設定されているネットワーク設定が表示されます。

日付と時刻：装置の現在の日付と時刻が表示されます。→ をクリックして日付と時刻を編集します。

Maintenance (メンテナンス):デバイスの現在のソフトウェアバージョンを表示します。→ をクリックするとメンテナンスWebページに移動します。

- Download backup (バックアップのダウンロード)：装置の設定ファイルをコンピューターにダウンロードする場合にクリックします。
- Restore configuration (設定のリストア)：クリックすると、設定ファイルをアップロードして、ダイアログでインポート設定を選択することができます。

ネットワーク接続

ローカルネットワーク

イーサーネットケーブルで装置をローカルエリアネットワークに接続することができます。

IPアドレス設定

Use DHCP server (DHCPサーバーの使用)：オンにすると、LAN DHCPサーバーからIPアドレスが自動的に取得されます。ほとんどのネットワークでは、自動DNS (DHCP) をお勧めします。

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、固定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。

Network mask (ネットワークマスク)：ネットワークマスクを入力して、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。

Default gateway (デフォルトゲートウェイ)：デフォルトゲートウェイのアドレスを入力します。これにより、オフLAN機器との通信が可能となります。

Current IP address settings (現在のIPアドレス設定)：現在装置に設定されているIPアドレスが表示されます。

DNS設定

Always use manual DNS settings (常に手動DNS設定を使用する)：DNS設定を手動で行う場合にオンにします。

Primary DNS (プライマリDNS)：ドメイン名をIPアドレスに変換するプライマリDNSサーバーのアドレスを入力します。工場出荷時設定にリセットした後は、プライマリDNS値が「8.8.8.8」となります。

セカンダリDNS：プライマリDNS にアクセスできない場合に代わりに機能するセカンダリDNSサーバーのアドレスを入力します。工場出荷時設定にリセットした後は、セカンダリDNS値が「8.8.4.4」となります。

Current DNS settings (現在のDNS設定)：現在装置に設定されているDNS設定が表示されます。

高度な設定

ホスト名:IPネットワークIDを入力します。使用できる文字は、A～Z、a～z、0～9、-、_です。

ベンダークラス識別子：DHCPオプション60の文字列として、ベンダー クラス識別子を入力します。

Required port mode (必要なポートモード)：優先するネットワークインターフェースのポートモードを選択します：自動または半二重 - 10 mbps。100 Mbpsのトラフィックにおいて使用しているネットワークケーブルの信頼性が低い場合は、より低い10 Mbpsのビット レートが必要になる場合があります。

現在のポートの状態：現在のネットワークインターフェースのポートの状態 (半二重または全二重 - 10 mbpsまたは100 mbps) が表示されます。

Webサーバー

内蔵Webサーバーにアクセスできる標準的なWebブラウザで装置を設定することができます。HTTPSプロトコルにより、装置とブラウザ間の安全な通信が実現します。

HTTP port (HTTPポート):使用するHTTPポートを入力します。

HTTPS port (HTTPSポート):使用するHTTPSポートを入力します。

Minimum allowed TLS version (許可される最小TLSバージョン)：装置の接続に必要な最も低いTLSバージョンを選択します。

HTTPS ユーザー証明書：HTTPサーバーのユーザー証明書と秘密鍵を選択します。選択されていないと、装置で自己署名証明書が使用されます。

Enable remote access (リモートアクセスの有効化)：オンにすると、オフLAN IPアドレスからインターコムWebサーバーへのリモートアクセスが有効になります。

ファイアウォール

ファイアウォールはお使いのデバイスを保護し、許可されたユーザーのみがネットワークにアクセスできるようにします。

Disabled (無効):トグルを使用して、ファイアウォールを有効または無効にします。

日付と時刻

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。

時刻同期の設定

Automatic time from NTP or internet (NTPまたはインターネットの自動時刻)：トグルスイッチを使用して、NTPサーバーまたはインターネットとの時刻同期を有効または無効にします。

NTPサーバーアドレス：同期させるNTPサーバーアドレスを入力します。

Synchronize with browser (ブラウザとの同期)：クリックすると、装置の時刻がコンピューターの時刻と同期されます。

タイムゾーン:

手動選択：装置のタイムゾーンを選択します。

カスタムルール：手動でタイムゾーンを入力します。

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。 お使いのデバイスでは、以下の証明書と秘密鍵の形式がサポートされています。

- PEM
- CER
- PFX
- DER

CA certificates (CA証明書)：CA証明書を使用して、ピア証明書を認証することができます。装置からネットワークへの接続時に、認証サーバーのIDが検証されます。

重要

デバイスを工場出荷時の設定にリセットすると、すべての証明書が削除されます。

CA certificates (CA証明書):装置のID検証に使用される証明書を選択します。

＋ Upload (アップロード)：CA証明書をアップロードして、証明書IDを入力します。

Search (検索)：証明書IDを入力し、CA証明書のリストからそれを見つけます。

：クリックすると、装置から証明書が削除されます。

：クリックすると、証明書情報が表示されます。

ユーザー証明書：ユーザー証明書により、ユーザーのIDが検証されます。自己署名または認証局 (CA) 発行の証明書のどちらでも可能です。自己署名証明書により、CA発行証明書の取得前に使用できる限定的な保護が得られます。

ユーザー証明書：本人確認に使用される証明書と秘密鍵を選択します。

＋ Upload (アップロード)：クリックして、ユーザー証明書と秘密鍵をアップロードします。鍵のパスワードがある場合は、それを入力します。

Search (検索)：証明書IDを入力し、ユーザー証明書のリストからそれを見つけます。

：クリックすると、装置から証明書が削除されます。

：クリックすると、証明書情報が表示されます。

診断

診断ログにより、報告された問題を特定して解決することができます。診断機能を使用して、診断ログをキャプチャーします。これは後からダウンロードすること、また技術サポートに利用することができます。

Ping：IPアドレスにテストデータを送信するには：

- [Ping] をクリックします。
- IPアドレスまたはURLを入力します。
- [Ping] をクリックします。

Close (閉じる)：クリックすると、ダイアログが閉じます。

診断パッケージ

診断パッケージは、ネットワークパケットとsyslogメッセージの対象エリアが含まれているZIPファイルです。装置、設定、ネットワークトラフィック、クラッシュログ、メモリ統計に関する情報が含まれています。また、ネットワークパケット数と装置でキャプチャーされたsyslogメッセージのサイズが表示されます。

キャプチャーの再起動：クリックすると、パケットキャプチャーが再起動します。

Download (ダウンロード):クリックすると、診断パッケージをファイルとしてダウンロードすることができます。

装置でのネットワークパケットキャプチャー

Download (ダウンロード):クリックすると、キャプチャーされたネットワークパケットをダウンロードすることができます。

開始:クリックすると、ネットワークの受信パケットと送信パケットのキャプチャーが開始します。

注

開始 (start) をクリックすると、以前にキャプチャーされたパケットは削除されます。

Stop (停止):クリックすると、ネットワークの受信パケットと送信パケットのキャプチャーが停止します。

Syslogのキャプチャー：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。

⋮ コンテキストメニューは以下を含みます。

- Delete captured messages (キャプチャーされたメッセージの削除)：クリックすると、syslogメッセージが削除されます。

Download (ダウンロード):クリックすると、syslogメッセージがダウンロードされます。

開始:クリックすると、データのキャプチャーが開始します。

Stop (停止):クリックすると、データのキャプチャーが停止します。

ネットワークパケットキャプチャーのダウンロード

これにより、装置ネットワークインターフェースの送受信パケットをキャプチャーし、コンピューターにダウンロードすることができます。

開始:クリックすると、データのキャプチャーが開始します。

キャプチャー時間：キャプチャーを実行する時間を設定します。

Stop (停止):クリックすると、データのキャプチャーが停止します。

リモートサーバーへのsyslogの送信：トグルを使用して、syslogを有効化または無効化します。これにより、syslogメッセージをsyslogサーバーに送信して、記録のの保存と録画の分析を行うことができます。

サーバーアドレス:syslogアプリケーションが実行されているサーバーのIPアドレスまたはMACアドレスを入力します。

重大度レベル：トリガー時に送信するメッセージの重大度を選択します。

メンテナンス

Reset to default (デフォルトにリセットする):クリックすると、装置が工場出荷時の設定にリセットされます。

- [Keep network settings and certificates (ネットワーク設定と証明書を維持する)] を選択して、ネットワークと証明書について行った設定を維持します。
- [Reset everything (すべてリセットする)] を選択すると、すべてのデバイス設定がリセットされます。
- Reset (リセット):クリックすると、リセットされます。

装置の再起動：クリックして、装置を再起動します。

Download backup (バックアップのダウンロード)：装置の設定ファイルをコンピューターにダウンロードする場合にクリックします。

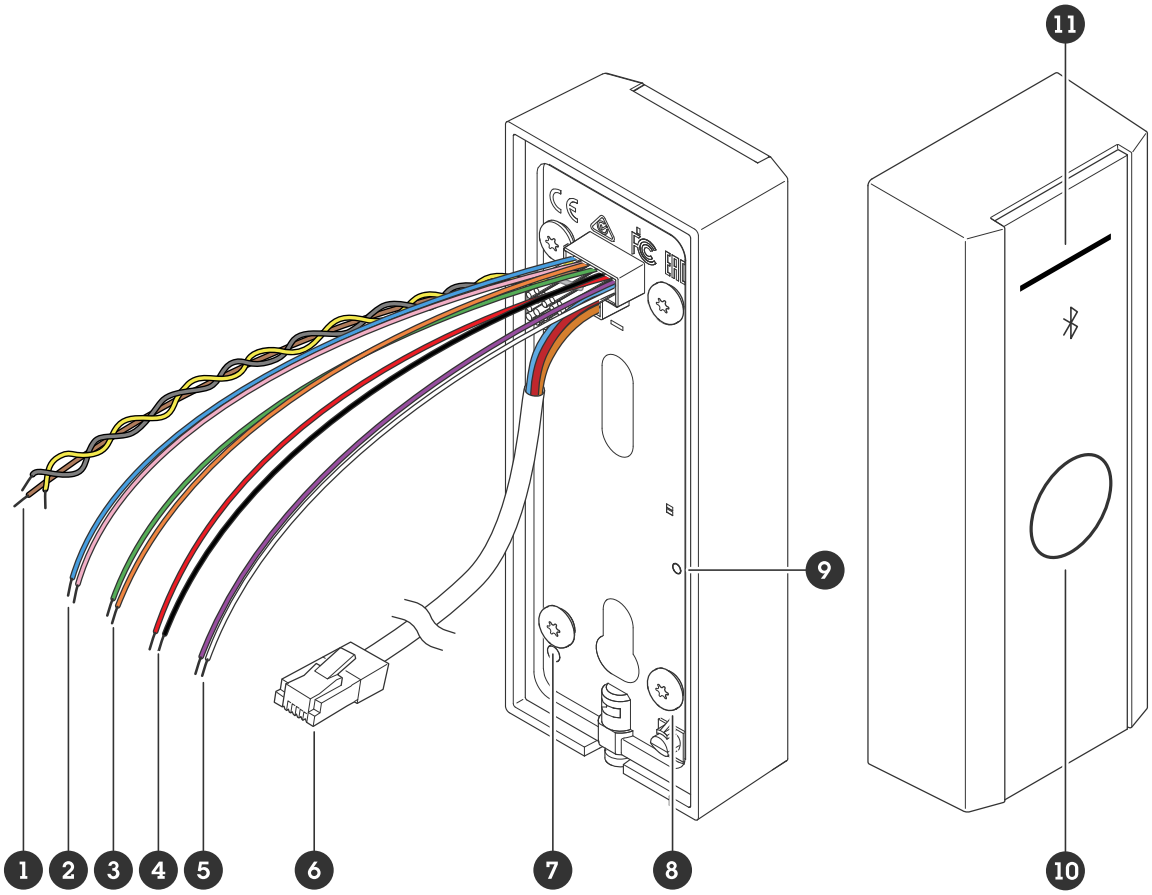
Restore configuration (設定のリストア)：クリックすると、設定ファイルをアップロードして、ダイアログでインポート設定を選択することができます。

ファームウェア：デバイスで現在実行されているソフトウェアバージョンの概要、デバイスで使用可能な最小ソフトウェアバージョン、ブートローダーバージョン、ソフトウェアのビルドタイプ、日時が表示されます。

Firmware upload (ファームウェアのアップロード)：クリックすると、ソフトウェアファイルをアップロードして、装置ソフトウェアをアップグレードすることができます。

仕様

製品概要



1 中継ケーブル
2 入力ケーブル 1
3 入力ケーブル 2
4 外部電源
5 アクティブ出力
6 ネットワークコネクタ (PoE)
7 コントロールボタン
8 タンパースイッチ
9 背面LEDインジケーター
10 静電容量式タッチボタン
11 リーダーインジケーターストライプ

シグナリングLED

ステータスLED	説明
白	デバイスを特定します。
緑	有効な認証です。
赤	カード待機中は常時点灯します。認証が無効な場合は点滅します。

注

バックライトと輝度レベルの設定方法については、*カスタマイズ, on page 8*を参照してください。

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。

- 現在のIPアドレスの確認。ボタンを約15秒間長押しし、背面LEDインジケーターが同時に赤と緑に変わり、短いビープ音が1回鳴るまで待ちます。
- 製品を工場出荷時の設定にリセットする。*工場出荷時の設定にリセットする, on page 19*を参照してください。
- デバイスの再起動。ボタンを1秒未満押すと、装置が再起動します。
- 静的IPアドレス (192.168.1.100) への切り替え。
  - ボタンを約15秒間長押しし、デバイスの背面にあるLEDインジケーターが同時に赤と緑に点灯し、ビープ音が鳴るまで待ちます。
  - 赤色のLEDが消えてビープ音が2回鳴ったら、ボタンをを離します。
- DHCPサーバーへの切り替え：
  - ボタンを15秒間長押しし、背面LEDインジケーターが同時に赤と緑に変わり、短いビープ音が1回鳴るまで待ちます。
  - 赤色のLEDが消えてビープ音が2回聞こえるまで、ボタンを3秒間押し続けます。
  - 緑色のLEDが消えて、赤色のLEDが再び点灯し、ビープ音が3回鳴ったら、ボタンを離します。

静電容量式タッチボタン

静電容量式タッチボタンにより、Bluetooth認証による入退室要求が可能となります。ユーザーはボタンを押すことで認証を有効化することができます。装置のWebページでこのボタンを設定する必要があります。*Bluetooth, on page 8*を参照してください。

ケーブル

外部電源

デバイスには外部電源に接続するためのケーブルが付いています。

機能	カラー	仕様
DC +	赤	12 V DC、最大12.0 W
DC -	黒	ケーブル (長さ): 350 mm

ネットワーク コネクター

Power over Ethernet (PoE) 対応RJ45イーサネットコネクター

電源の優先順位

本装置は、PoEまたはDC入力から電源を供給できます。を参照してください。

⚠ 警告

ユニットは、外部電源とPoEを同時に使用することはできません。複数の電源を併用すると、デバイスが損傷する恐れがあります。

- PoEとDCの両方が接続されている場合は、DCが電源として使用されます。
- PoEとDCの両方が接続されており、現在はDCが電源を供給しています。DCが失われると、装置ではPoE経由で給電が行われます。
- 起動時にPoEが使用されている場合、装置の起動後にDCが接続されても、電源供給にDCが使用されます。

アクティブ出力

アクティブ出力ケーブルは、セキュリティリレーまたは電気錠への接続に使用されます。

注

セキュリティ強化のため、リーダーとロックの間に *[2N Security Relay (2Nセキュリティリレー)]* を追加します。

機能	カラー	仕様
DC +	白	電源に応じて9.8～13.8 V DC、最大600 mA。 PoE: 11.6 V DC: 電源電圧 -0.4 V ケーブル (長さ): 350 mm
DC -	バイオレット	

中継ケーブル

アクセスロックやセンサーを管理するための中継ケーブル。

機能	カラー	注	仕様
NO	黄	通常、フェイルセキュアロックのために開いている。	最大1 A 30 V DC ケーブル (長さ): 350 mm
COM	灰色	コモン	
NC	茶	通常、フェイルセーフロックのために閉じている。	

入力ケーブル

入力ケーブルを使用することで、装置のコントロールパネルと入力装置間の良好な通信が可能となり、外部入力デバイスに接続することができます。この装置には、入力1と入力2の2つの入力コネクターが備わっています。これにより、ドアポジションセンサーとREXボタンを接続することができます。

ケーブル	カラー	仕様
入力1+	ピンク	0～30 V DC
入力1-	青	
入力2+	オレンジ	
入力2-	緑	

装置を清掃する

注

- 強力な化学薬品は装置を損傷する可能性があります。窓ガラス用洗剤やアセトンなどの化学薬品を使用して装置をクリーニングしないでください。
- シミの原因となるため、直射日光や高温下での清掃は避けてください。

1. 圧縮空気を使用すると、装置からほこりやごみを取り除くことができます。
2. 必要に応じて、ぬるま湯に浸した柔らかいマイクロファイバーの布で装置を清掃してください。
3. シミを防ぐために、きれいな非研磨性の布で装置から水分を拭き取ってください。

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

注

- 工場出荷時の設定にリセットすると、すべての設定が工場出荷時のデフォルト値に戻ります。

1. 装置を開きます。
2. ボタンを約24秒間長押しして、背面LEDインジケーターが赤、緑に変わってオフになるまで待ちます。

注

異なる間隔で、1回目、2回目、3回目、4回目のビープ音が聞こえます。

3. 4回目のビープ音が鳴ったら、コントロールボタンを離します。これでプロセスが完了し、製品が工場出荷時の設定にリセットます。
4. 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、パスワードの設定、および製品へのアクセスを行います。
   *axis.com/support*のサポートページに、インストールおよび管理ソフトウェアツールが用意されています。

装置の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。[System (システム)] > [Maintenance (メンテナンス)] > [Reset to default (デフォルトにリセットする)] に移動します。

デバイスの現在のソフトウェアバージョンを確認する

デバイスのソフトウェアによってデバイスの機能が決まります。問題のトラブルシューティングを行う際は、まず現在のソフトウェアバージョンを確認することをお勧めします。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。

現在のソフトウェアバージョンは、以下の2つの方法で確認できます。

- 以下の手順に従ってデバイスのwebインターフェースに移動します。
  - [Dashboard (ダッシュボード)] に移動します。
  - [Firmware (ファームウェア)] に移動します。*メンテナンス, on page 14*を参照してください。

ソフトウェアのアップグレード

重要

- 事前設定済みの設定とカスタム設定は、装置のソフトウェアのアップグレード時に保存されます (その機能が新しいファームウェアバージョンで利用できる場合)。ただし、この動作をAxis Communications ABが保証しているわけではありません。
- アップグレードプロセス中は、装置を電源に接続したままにしてください。

注

最新のソフトウェアバージョンでデバイス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。アップグレードする前に、AXIS OSと共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。最新のソフトウェアバージョンとリリースノートについては、*axis.com/support/device-software*にアクセスしてください。

1. ソフト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。これらのファイルは*axis.com/support/device-software*から無料で入手できます。
2. デバイスページにログインします。
3. [System (システム)] > [Maintenance (メンテナンス)] の順に移動して、[Firmware upload (ファームウェアのアップロード)] をクリックします。

4. ソフトウェアファイルを選択して、[Upload (アップロード)] をクリックします。

アップグレードが完了すると、製品は自動的に再起動します。

技術的な問題と解決策

IPアドレスの設定で問題が発生する

- デバイス用のIPアドレスと、デバイスへのアクセスに使用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アドレスを設定することはできません。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場合:
  1. デバイスをネットワークから切断します。
  2. コマンドウィンドウまたはDOSウィンドウで、`ping`コマンドとデバイスのIPアドレスを入力します。
  3. `Reply from <IP address>: 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そのIPアドレスがすでに使われている可能性があります。ネットワーク管理者から新しいIPアドレスを取得し、デバイスを再度インストールしてください。
  4. `Request timed out`が表示された場合は、Axisデバイスでそ 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、デバイスを再度インストールしてください。

デバイスへのアクセスの問題

ログインできない

HTTPSが有効になっているときは、ログインを試みるときに正しいプロトコル (HTTPまたはHTTPS) を使用していることを確認してください。場合によっては、ブラウザーのアドレスフィールドに手動で`http`または`https`を入力する必要があります。

アカウントのパスワードを忘れた場合は、デバイスを工場出荷時の設定にリセットする必要があります。*工場出荷時の設定にリセットする, on page 19*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を使用してデバイスのネットワーク上の場所を特定してください。デバイス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) を使用してデバイスを識別します。

証明書警告 `NET::ERR_CERT_AUTHORITY_INVALID`

証明書の警告は、OS装置の標準的な手順です。[Advanced (詳細設定)] をクリックしてから、[Proceed to *IP address* (unsafe) (*IP アドレス*に進む (危険))] をクリックし、装置のログインWebページにアクセスします。以下のようないくつかのオプションがあります。

- 別のブラウザまたは装置を使用する。
- 証明書の警告ページの任意の場所をクリックして、「thisisunsafe」と入力する。

Webページにアクセスしたら、[System (システム)] > [Maintenance (メンテナンス)] > [Firmware upload (ファームウェアのアップロード)] の順に移動して、最新の装置ソフトウェアに更新します。

このページで解決策が見つからない場合は、*axis.com/support*のトラブルシューティングセクションに記載されている方法を試してみてください。

パフォーマンスに関する一般的な検討事項

考慮すべき最も重要な要因:

- 貧弱なインフラによるネットワークの使用率が高いと帯域幅に影響します。

サポートに問い合わせる

さらにサポートが必要な場合は、*axis.com/support*にアクセスしてください。

商標の帰属

Bluetooth®マークとロゴは、Bluetooth SIG, Inc.が所有する登録商標です。Axis Communications ABは、ライセンスに基づいてこのマークを使用しています。その他の商標および商品名は、それぞれの所有者の商標です。

T10207283_ja

2026-05 (M4.2)

© 2024 – 2026 Axis Communications AB