AXIS D8204-E PoE++ Switch

ユーザーマニュアル

目次

本マニュアルについて 3
略語 3
ソリューションの概要 4
使用に当たって 5
ブラウザーから本製品へのアクセス 5
本製品のWebページについて理解する 5
本製品の内蔵ヘルプについて理解する 6
設定例 7
アクセスVLANの設定 7
MACアドレスに基づいてIPアドレスを予約する 8
ネットワーク冗長性を実現するスイッチ間の冗長リンクの作成 8
VAPIXを使用したポートのPoEのオン/オフの切り替え 9
MACsecの設定 9
静的CAK 9
動的CAK 10
1Gbps SFPモジュールの接続 12
システムのメンテナンス 13
本製品の再起動 13
工場出荷時の設定にリセットします。 13
デバイスソフトウェアをアップグレードする 14
代替ソフトウェア画像に戻す 14
仕様 15
製品概要 15
トラブルシューティング 16
サイバーセキュリティ 17
脆弱性の管理 17
セキュリティ通知 17
安全な製品ライフサイクル管理 17

本マニュアルについて

注

本製品は、ネットワーク装置の運用および保守を担当するネットワーク管理者が使用することを目的としています。一般的なスイッチ機能、セキュリティ、インターネットプロトコル (IP)、および SNMP (Simple Network Management Protocol) に関する基本的な知識があることを前提としています。

このユーザーマニュアルは、以下の方法に関する情報を提供します。

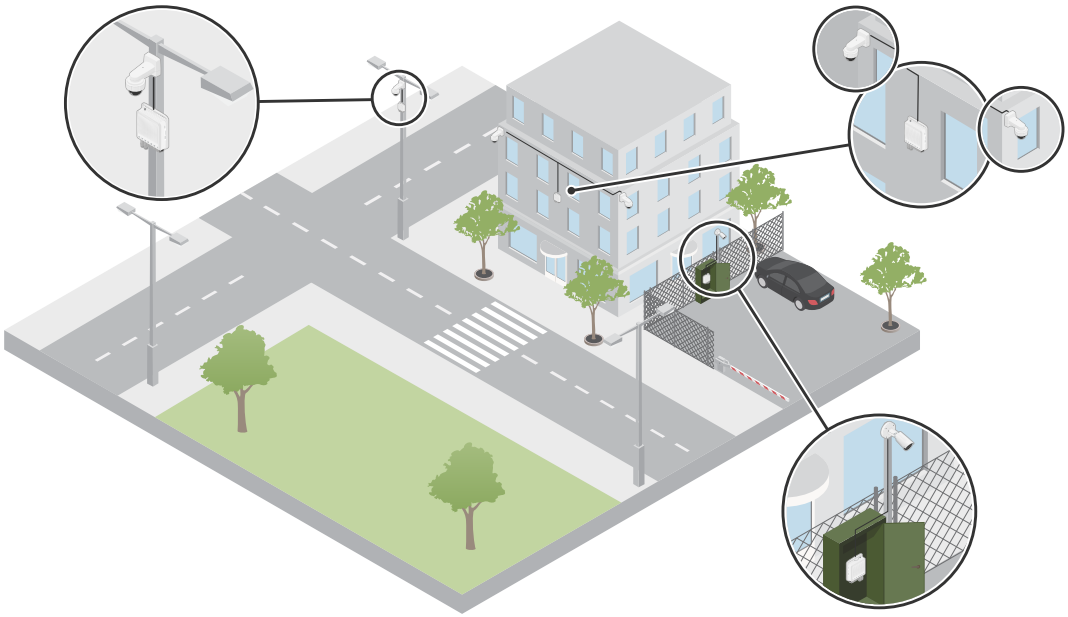
- 本製品にアクセスする
- 選択した設定例の設定
- 本製品のメンテナンスの実施

本製品の機能とその設定については、本製品の状況に応じた内蔵のヘルプで詳しく説明しています。

略語

略語	説明
MACsec	Media Access Control Security
802.1X	ネットワークアクセスコントロール
802.1AE	MACsecと同様
CAK	Connectivity Association Key
CKN	Connectivity Key Name
DHCP	Dynamic Host Configuration Protocol
OpenSSL	Open-Source Software Library
PoE	Power over Ethernet
RADIUS	リモート認証ダイヤルインユーザーサービス
SFP	ファイバーインターフェース、小型フォームファクタープラグ
SFP+	Enhanced Small Form-factor Plug
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TLS	トランスポート層セキュリティ
VLAN	仮想ローカルエリアネットワーク

ソリューションの概要



Axisエッジデバイスは構内に設置され、イーサーネットを介してAxisスイッチに接続されます。これらのスイッチは光ファイバーで接続されています。

使用に当たって

ブラウザーから本製品へのアクセス

注

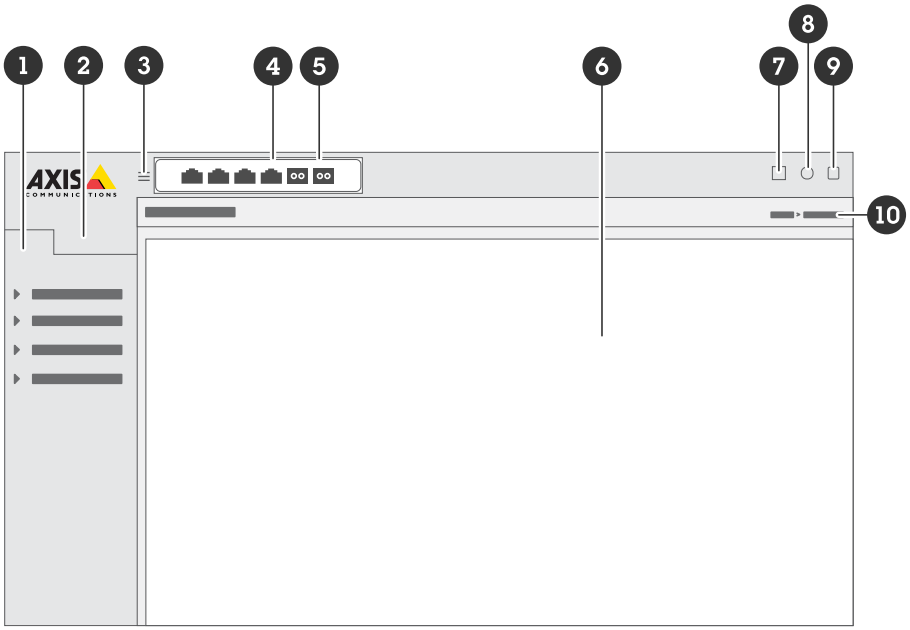
- インストールガイドの指示に従って、デバイスのインストール、接続、給電を行います。
- このセクションの手順をしたがうと、製品のWebページが表示され、製品の設定および管理ができます。

1. AXIS IP UtilityまたはAXIS Device Managerを使用して、ネットワーク上の本装置を探します。デバイスの検出方法の詳細については、*axis.com/support*を参照してください。
2. 製品ラベルに記載されているのユーザー名およびパスワードを入力します。デフォルトのユーザー名はrootです。
3. セットアップウィザードの手順に従って以下を行います。

– パスワードの変更 (セキュリティ上の理由から推奨)
– DHCPを使用して、または手動でIPアドレスを設定する
– 日付と時刻情報を設定する
– システム情報を設定する

4. [Save (保存)] をクリックします。
5. 新しいパスワードを使用して再ログインします。

本製品のWebページについて理解する



1 基本的な機能
2 高度な機能
3 トグルボタン - メニューの非表示/表示
4 RJ45ポートステータスインジケーター
5 SFPポートステータス LED
6 基本的な機能/高度な機能を提供するコンテンツエリア
7 保存ボタン - 設定がスタートアップ設定ファイルに保存されます
8 ヘルプボタン - 状況に応じた内蔵のヘルプにアクセスします
9 ログアウトボタン
10 メニューパス

本製品の内蔵ヘルプについて理解する

本製品には状況に応じた内蔵のヘルプが用意されています。このヘルプでは、本製品の基本的な機能および高度な機能やその設定に関する詳細情報を提供しています。特定のビューのヘルプコンテンツにアクセスするには、

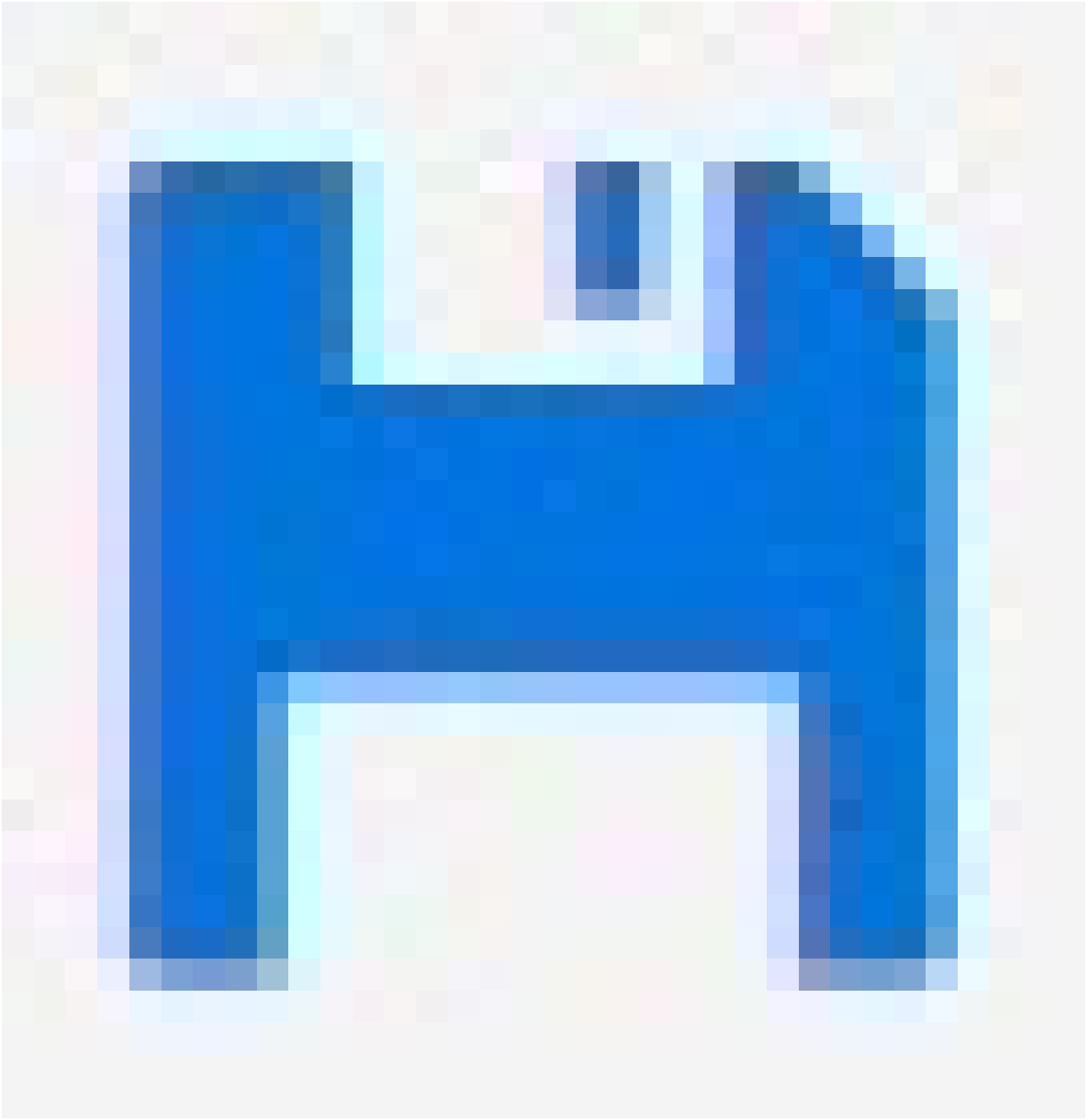


をクリックします。ヘルプコンテンツには、内蔵のの用語集で詳しく説明されている、クリック可能な用語や頭字語も含まれています。

設定例

注

スイッチの設定を構成または更新したら、必ず



をクリックして、更新をスタートアップ設定ファイルに保存してください。

スタートアップ設定ファイルは、スイッチを再起動またはリブートしても残りますが、スイッチを工場出荷時の設定にリセットした後は残りません。

アクセスVLANの設定

通常、VLANは大規模なネットワークで複数のブロードキャストドメインを作成するために使用されますが、ネットワークトラフィックを分離するためにも使用できます。たとえば、ビデオトラフィックは1つのVLANの一部であり、他のネットワークトラフィックは別のVLANの一部である場合があります。

1. [Advanced (詳細設定)] > [VLANs] > [Configuration (設定)] に移動します。
2. [Global VLAN Configuration (グローバルVLAN設定)] の [Allowed Access VLANs (許可されたアクセスVLAN)] のフィールドに、作成する VLAN ID を入力します。たとえば、1、10

～13、200、300と入力すると以下のVLAN IDが作成されます。1、10、11、12、13、200および300です。

3. 特定のポートを **[Port VLAN Configuration (ポートVLAN設定)]** で作成したVLAN IDに割り当てるには、そのIDを **[Port VLAN]** のフィールドに入力します。
4. **[Save (保存)]** をクリックします。

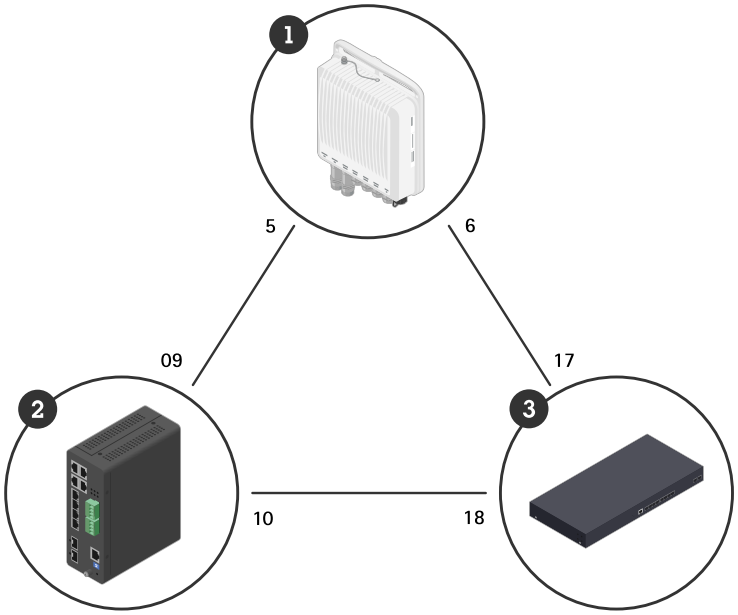
MACアドレスに基づいてIPアドレスを予約する

1. **[Advanced (詳細設定)]** > **[DHCP]** > **[Server (サーバー)]** > **[Configuration (設定)]** > **[Pool (プール)]** の順に移動します。
2. **[Add New Pool (新しいプールの追加)]** をクリックします。
3. プールの名前を入力し、**[Save (保存)]** をクリックします。名前にはスペースを使用できません。
4. プールの設定にアクセスするには、追加した名前をクリックします。
5. **[Type (タイプ)]** ドロップダウンメニューで **[Host (ホスト)]** を選択します。
6. その他の必要な設定、**[IP (IP)]** アドレス、**[Subnet Mask (サブネットマスク)]** および **[Default Router (デフォルトルーター)]** などを入力します。
7. **[Client Identifier (クライアント識別子)]** ドロップダウンメニューで **[MAC (MAC)]** を選択します。
8. **ハードウェアアドレス**フィールドに、装置のMACアドレスを入力します。
9. **[Save (保存)]** をクリックします。

ネットワーク冗長性を実現するスイッチ間の冗長リンクの作成

ネットワーク冗長性が必要な場合は、スパニングツリー設定を使用してスイッチ間に冗長リンクを作成できます。

例:
この例では、スイッチAXIS D8204-E (1)、AXIS D8208-R (2)、およびAXIS T8516 (3)が冗長リンクで接続されており、追加のVLANは設定されていません。スイッチ間のアップリンクに障害が発生すると、冗長リンクがアクティブになり、ネットワーク接続が提供されます。



Device name (装置名):	モデル名	CISTポート
スイッチ - 1	AXIS D8204-E	5、6
スイッチ - 02	AXIS D8208-R	9, 10
スイッチ - 3	AXIS T8516	17, 18

各スイッチのWebページに冗長リンクを作成するには:

1. [Advanced (詳細設定)] > [Spanning Tree (スパニングツリー)] > [Configuration (設定)] > [Bridge Settings (ブリッジの設定)] に移動します。
2. [Protocol Version (プロトコルバージョン)] ドロップダウンメニューの [Basic Settings (基本設定)] で、[RSTP] を選択し、[Save (保存)] をクリック します。
3. [Advanced (詳細設定)] > [Spanning Tree (スパニングツリー)] > [Configuration (設定)] > [CIST Port (CISTポート)] に移動します。
4. [CIST Normal Port Configuration (CIST標準ポート設定)] で、次のようにスイッチのポートで [STP Enabled (STP有効)] が選択されているのを確認します。

– スイッチ – 1:ポート5および6
– スイッチ – 2:ポート9および10
– スイッチ – 3:ポート17および18

5. [Save (保存)] をクリックします。

注

特定のポートがプライマリ通信リンクとして使用されているのを確認するには、[CIST Normal Port Configuration (CIST標準ポート設定)] の下に、そのポートの [Path Cost (パスコスト)] を入力します 。指定しない場合、スイッチはポートを自動的に選択します。たとえば、プライマリ通信リンクとしてポート17を使用する場合は、[Path Cost (パスコスト)] 値10からポート6、[Path Cost (パスコスト)] 値50からポート18を入力します。

VAPIXを使用したポートのPoEのオン/オフの切り替え

VAPIXで以下のコマンドを使用して、特定のポートのPoEのオン/オフを切り替えることができます。

- PoEをオンに切り替える:
  `http://[IP address of the switch]/axis-cgi/nvr/poe/setportmode.cgi?port=[number of the port on the switch]&enabled=yes&schemaversion=1`
- PoEをオフに切り替える:
  `http://[IP address of the switch]/axis-cgi/nvr/poe/setportmode.cgi?port=[number of the port on the switch]&enabled=no&schemaversion=1`

MACsecの設定

MACsecの設定により、MACsec対応の2つのデバイス間に安全な接続が確立され、デバイス間の通信の機密性が確保され、認証が行われ、リプレイ攻撃からの保護が確保されます。

静的CAK

Connectivity Association Key (CAK) とは、デバイス間の安全な通信を保証する暗号鍵です。128ビットの鍵の場合は16進数で32文字、256ビットの鍵の場合は16進数で64文字でなければなりません。

Connectivity Key Name (CKN) は、デバイス間で安全なMACsec接続を確立するために鍵を識別し、許可されたデバイスのみが安全な通信に参加できるようにします。CKNは16進数で2〜64文字の範

囲で、文字数は偶数でなければなりません。CKNは使用するCAKを特定し、MACsec通信を確立するために、CAKとCKNがリンクの両側で一致する必要があります。

CAKとCKNは、手動でも生成することも、OpenSSLを使用して生成することもできます。

OpenSSL を使用して CAK および CKN を生成する

1. OpenSSLがインストールされているコンピューターで、コマンドプロンプトを開きます。
2. CAKを生成する:
   - openssl rand -hex 16と入力します。
   - Enterキーを押します。
3. CKNを生成する:
   - openssl rand -hex 8と入力します。
   - Enterキーを押します。
4. CAKとCKNを保存します。これらは後で必要になります。

AXIS OS デバイスの設定

1. デバイスのwebインターフェースで、**[System (システム)]** > **[Security (セキュリティ)]** > **[Network access control and encryption (ネットワークアクセスコントロールおよび暗号化)]** に移動します。
2. **[Authentication method (認証方式)]** に **[IEEE 802.1AE MACsec (Static CAK/Pre-Shared Key)]** を選択します。
3. **[Key agreement connectivity association key name (鍵合意Connectivity Association Key名)]** にCKNを入力します。
4. **[Key agreement connectivity association key name (鍵合意Connectivity Association Key名)]** にCAKを入力します。
5. **[Save (保存)]** をクリックします。

スイッチの設定を

1. スイッチのwebインターフェースで、**[Advanced (詳細設定)]** > **[Security (セキュリティ)]** > **[MACsec]** > **[Configuration (設定)]** > **[Policies (ポリシー)]** に移動します。
2. **[Add Policy (ポリシーの追加)]** をクリックします。
3. ポリシーの名前を入力します。
4. **[Enable (有効にする)]** を選択し、生成したCAKとCKNを入力します。
5. **[Save (保存)]** をクリックします。
6. **[Advanced (詳細設定)]** >**[Security (セキュリティ)]** >**[MACsec]** >**[Configuration (設定)]** >**[Interfaces (インターフェース)]** に移動します。
   - デバイスに接続されている **[Interfaces (インターフェース)]** に、ドロップダウンリストから新規のポリシーを選択します。
   - **[Save (保存)]** をクリックします。

接続の確認

1. スイッチのwebインターフェースで、**[System (システム)]** > **[Security (セキュリティ)]** > **[MACsec]** > **[Status (ステータス)]** > **[Status (ステータス)]** に移動します。
2. **[State (状態)]** のステータスインジケーターが緑色になっていることを確認します。

動的CAK

CAKは、IEEE 802.1Xおよび認証サーバーを使用する認証および鍵管理プロセスを通じて生成されます。これにより、鍵を動的に生成・管理できるため、長期鍵を手動で設定する必要がありません。

注

- ネットワーク上でRADIUSサーバーが設定されており、アクセスできることを確認してください。
- RADIUSサーバーに*Axisデバイス IDのCA証明書*をインストールします。

接続デバイスの設定

1. デバイスのwebインターフェースで、**[System (システム)]** > **[Security (セキュリティ)]** > **[Network access control and encryption (ネットワークアクセスコントロールおよび暗号化)]** に移動します。
2. **[Authentication method (認証方式)]** に **[IEEE 802.1X EAP-TLS / IEEE 802.1AE MACsec (Dynamic CAK)]** を選択します。
3. **[Client certificate (クライアント証明書)]** については、RADIUSサーバーが信頼するAxisデバイスID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。
4. **[CA certificates (CA証明書)]** は、証明書が選択されていない場合、接続しているネットワークに関係なくデバイスが自己認証します。
5. **[EAP ID]** にクライアント証明書に関連付けられたユーザーIDを入力します。EAP ID は、選択したクライアント証明書の [Common Name (CN)(共通名)] のフィールドと一致する必要があります。
6. **[EAPOL Version (EAPOL バージョン)]** リストから、ネットワークスイッチが使用するバージョンを選択します。
7. **[Use IEEE 802.1x (IEEE 802.1xを使用する)]** をオンにしてIEEE 802.1xプロトコルを使用します。
8. **[Save (保存)]** をクリックします。

スイッチで802.1Xを設定する

1. スイッチのwebインターフェースで、**[Advanced (詳細設定)]** > **[Security (セキュリティ)]** > **[Radius]** > **[Configuration (設定)]** に移動します。
2. **[Add new server (新規サーバーの追加)]** をクリックし、ホスト名とパスワードを入力します。
3. **[Save (保存)]** をクリックします。
4. **[Advanced (詳細設定)]** > **[Spanning Tree (スパニングツリー)]** > **[Configuration (設定)]** > **[CIST Ports (CISTポート)]** に移動します。
5. お使いのデバイスが接続されているポートの**[STP Enabled (STP有効)]** のチェックボックスのチェックを外します。
6. **[Save (保存)]** をクリックします。
7. **[Advanced (詳細設定)]** > **[Security (セキュリティ)]** > **[802.1X]** > **[Configuration (設定)]** に移動します。
8. **[Mode (モード)]** のリストから **[Enabled (有効)]** を選択します。
9. 該当するポートの **[Admin state (管理状態)]** を **[Port-based 802.1X (ポートベースの802.1X)]** に設定します。
10. **[Save (保存)]** をクリックします。

802.1x接続の確認

1. デバイスのwebインターフェースで **[System (システム)]** > **[Security (セキュリティ)]** に移動します。
2. **[802.1X Authorized (802.1X認証済み)]** のステータスインジケーターが緑色になっていることを確認します。

スイッチでMACsecを設定する

1. スイッチのwebインターフェースで、[Advanced (詳細設定)] > [Security (セキュリティ)] > [MACsec] > [Configuration (設定)] > [Policies (ポリシー)] に移動します。
2. [Add policy (ポリシーの追加)] をクリックし、ポリシーの名前を入力します。
3. [Save (保存)] をクリックします。
4. [Advanced (詳細設定)] >[Security (セキュリティ)] >[MACsec] >[Configuration (設定)] >[Interfaces (インターフェース)] に移動します。
5. デバイスに接続されているインターフェースに、リストから新規作成したポリシーを選択します。
6. [Save (保存)] をクリックします。

MACsec接続の確認

1. [System (システム)] > [Security (セキュリティ)] > [MACsec] > [Status (ステータス)] > [Status (ステータス)] に移動します。
2. [State (状態)] のステータスインジケーターが緑色になっていることを確認します。

注

接続状態が保留中のままの場合は、デバイスを再起動します。

1Gbps SFPモジュールの接続

1. [Advanced (詳細設定)] > [Ports (ポート)] > [Configuration (設定)] に移動します。
2. モジュールを接続したポート (5または6) で、[Configured (設定済み)] を1 Gbps FDXに設定します。

注

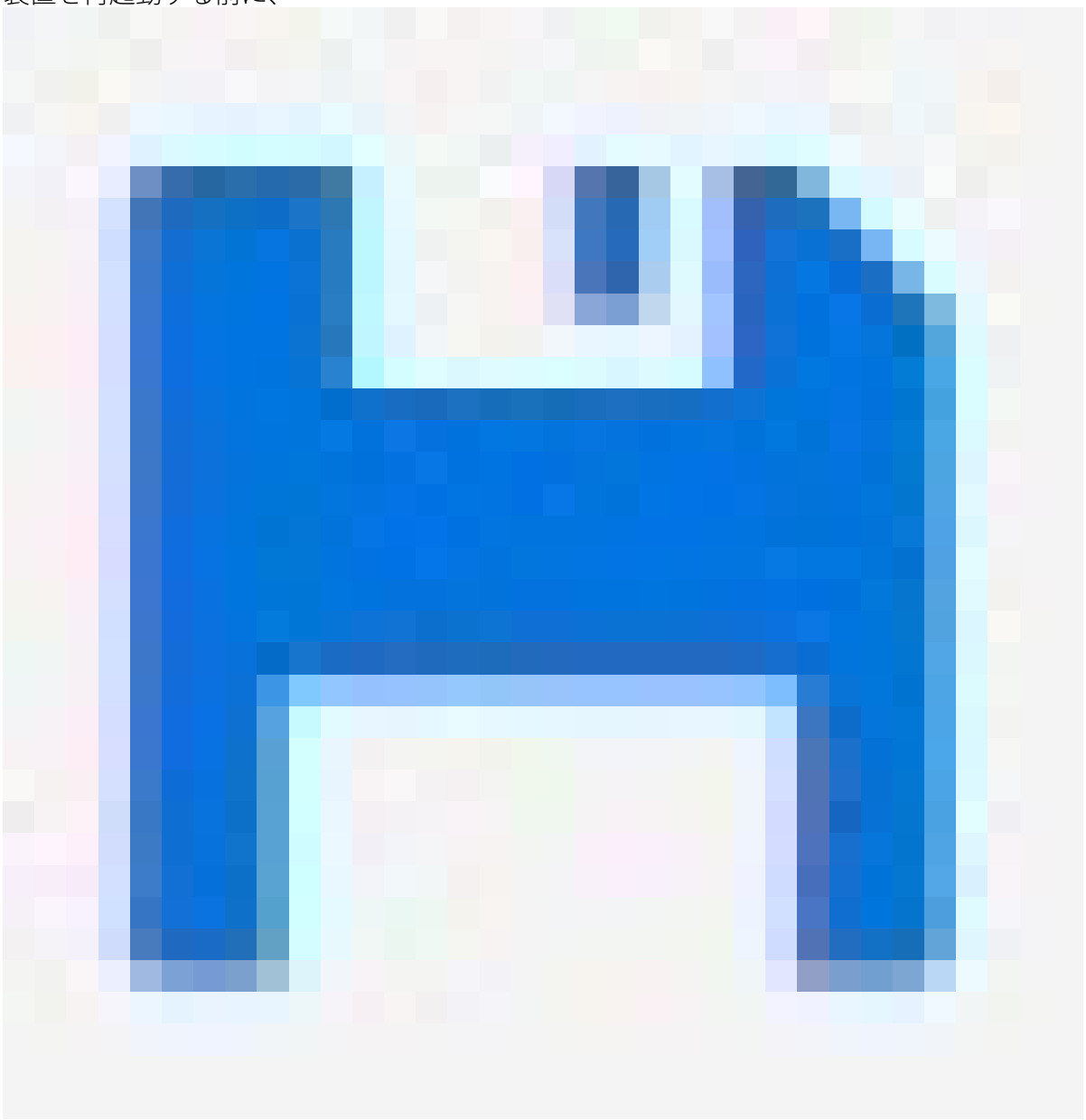
ポートをAuto (自動) に設定すると、SFPとSFP+の両方が動作するようになります。

システムのメンテナンス

本製品の再起動

注

- 再起動中は、製品を経由するトラフィックに影響があります。
- 装置を再起動する前に、



をクリックして、設定をスタートアップ設定ファイルに保存します。

1. [Advanced (詳細設定)] > [Maintenance (メンテナンス)] > [Restart Device (デバイスの再起動)] に移動します。
2. [Yes (はい)] をクリックします。再起動後、本製品は正常に起動します。

工場出荷時の設定にリセットします。

重要

保存された設定は、工場出荷時の状態にリストアされます。

1. [Advanced (詳細設定)] > [Maintenance (メンテナンス)] > [Factory Defaults (工場出荷時の設定)] に移動します。

2. [Yes (はい)] をクリックします。

パスワードを忘れた場合は、以下の手順にしたがって工場出荷時の設定にリセットします。

1. 電源を含むすべての接続をスイッチから切り離します。
2. RJ45ケーブルをポート1とポート2の間に接続します。
3. 電源ケーブルを接続し、スイッチの電源を入れます。
4. 5分後にRJ45ケーブルを取り外します。電源ケーブルは接続したままにしておいてください。
5. ユニットをコンピューターに接続します。IPアドレスがデフォルトのIPアドレスである192.168.0.254に戻るはずです。
6. [Advanced (詳細設定)] > [Maintenance (メンテナンス)] > [Factory Defaults (工場出荷時の設定)] に移動します。
7. [Yes (はい)] をクリックします。

デバイスソフトウェアをアップグレードする

重要

ソフトウェアのアップグレードには最大10分かかります。この間に装置を再起動したり、電源を切ったりしないでください。

注

アップグレード中は、製品を経由するトラフィックに影響があります。

1. [Advanced (詳細設定)] > [Maintenance (メンテナンス)] > [Device Software (デバイスソフトウェア)] > [Software Upgrade (ソフトウェアアップグレード)] に移動します。
2. 指定した場所からソフトウェアファイルを選択するには、[Select file... (ファイルを選択)] をクリックします。
3. [アップグレード] をクリックします。

ソフトウェアのアップグレード後、本製品は正常に再起動します。

代替ソフトウェア画像に戻す

本製品のアクティブ (プライマリ) ソフトウェア画像の代わりに代替 (バックアップ) ソフトウェア画像の使用を選択できます。[Advanced (詳細設定)] > [Maintenance (メンテナンス)] > [Device Software (デバイスソフトウェア)] > [Software Selection (ソフトウェアの選択)] の順に選択すると、両方の画像の情報の表が表示されます。

注

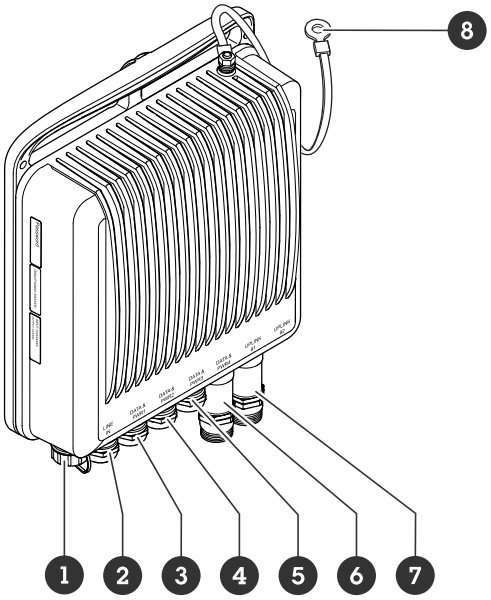
- アクティブな画像がすでに代替画像として設定されている場合、[Active Image (アクティブな画像)] の表のみが表示され、[Activate Alternate Image (代替画像をアクティブ化する)] ボタンは無効になります。
- 代替画像がすでにアクティブ画像として設定されている場合 (手動またはプライマリ画像が破損した場合)、新しいソフトウェア画像が本製品にアップロードされると、新しい画像がアクティブ画像として自動的に設定されます。
- 古いバージョンのソフトウェアでは、ソフトウェアのバージョンと日付の情報が空になる場合があります。これは正常です。

代替画像をアクティブ画像として設定するには:

1. [Advanced (詳細設定)] > [Maintenance (メンテナンス)] > [Device Software (デバイスソフトウェア)] > [Software Selection (ソフトウェアの選択)] の順に移動します。
2. [Activate Alternate Image (代替画像をアクティブ化する)] をクリックします。

仕様

製品概要



1　電源コネクターポート
2　– 5.RJ45 PoEポート
6　– 7.SFPスロット
8　アースケーブル

トラブルシューティング

デバイスへのアクセスの問題

ブラウザからデバイスにアクセスする際、ログインできない

HTTPSが有効になっている場合、ログインを試行す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ます。場合によっては、ブラウザ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。

root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。手順については、*工場出荷時の設定にリセットします。, on page 13*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。

さらにサポートが必要な場合は、*axis.com/support*または*Axis ネットワークスイッチ設定ガイド*を参照してください。

サイバーセキュリティ

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

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

脆弱性の管理

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

セキュリティ通知

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

安全な製品ライフサイクル管理

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

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

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

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

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

T10231182_ja

2026-11 (M1.17)

© 2025 – 2026 Axis Communications AB