

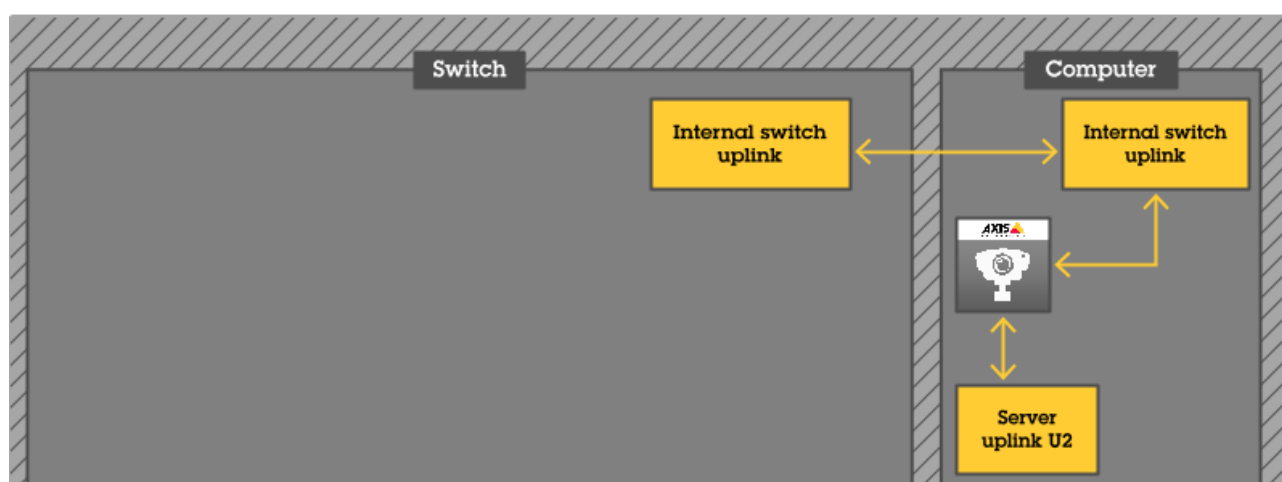
AXIS Camera Station S2108 Appliance

デバイスについて

AXIS Camera Station S2108 Applianceは、PoEスイッチを内蔵したオールインワン録画ソリューションです。最大4K解像度までのカメラに対応し、信頼性の高い高解像度監視を実現するように設計されています。迅速かつ簡単にインストールできるように、このアプライアンスにはAXIS Camera Stationビデオ管理ソフトウェアが事前に構成されてプリロードされています。ライセンスおよび必要なすべてのシステムソフトウェアも含まれています。AXIS Camera Stationの直感的なユーザーインターフェースにより、ユーザーは広範に及ぶAxisの映像監視カメラや他のIP製品を最大限に活用することができます。オペレーティングシステムはソリッドステートドライブ (SSD) に格納され、5年間のハードウェア保証が付属します。このアプライアンスは、信頼性の高い監視ソリューションを提供します。

AXIS Camera Station S2108 Applianceは、次の2つの部分で構成されます。

- **スイッチ:** Power over Ethernet (PoE) スイッチを内蔵しています。
- **コンピューター:** ビデオ管理ソフトウェアAXIS Camera Stationなど、監視ソリューションの作成に必要なすべてのソフトウェアがプリロードされています。

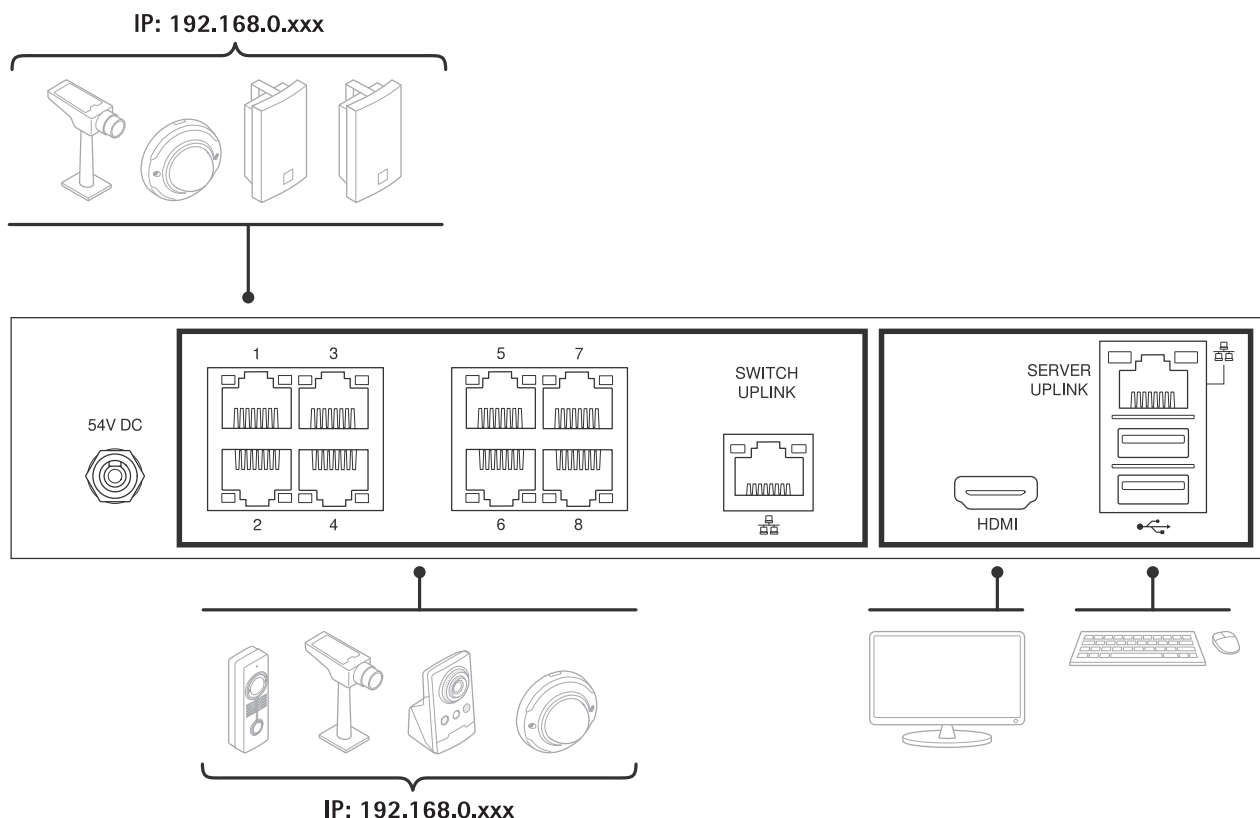


- スイッチとコンピューターは2つの別々の部品です。
- スイッチとコンピューターは、内部アップリンクコネクタ経由で通信します。1つはスイッチの電源基板にあり、もう1つはコンピュータのマザーボードにあります。
- サーバーアップリンクは、既存のネットワークに接続できる外部ネットワークインターフェースです。
- サーバーアップリンクに接続された装置は、スイッチに直接接続された装置と通信できません。
- サーバーアップリンクに接続された装置は、スイッチに接続された装置とAXIS Camera Stationを介して通信できます。

設定例

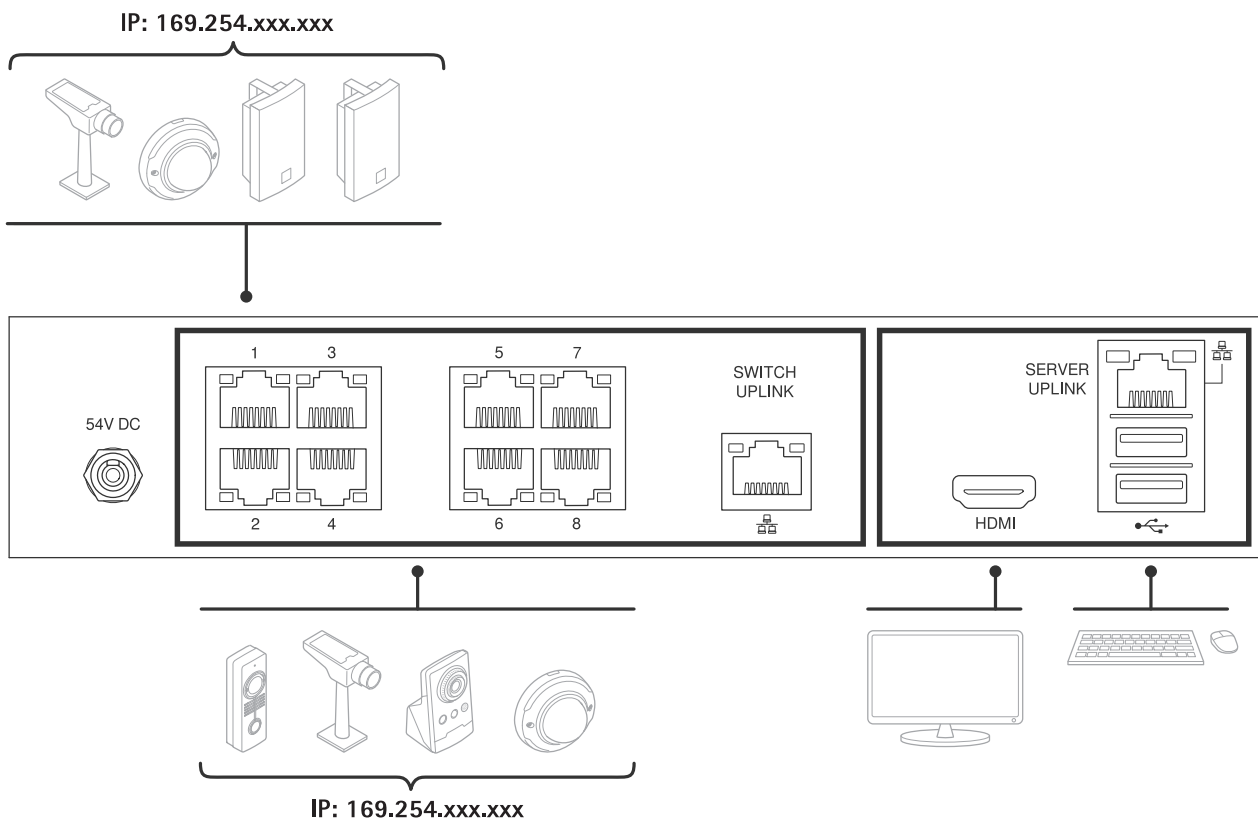
各装置に静的アドレスを割り当てる

各装置とAXIS S2108 Applianceに静的なIPアドレスを割り当てることで、独立したネットワークを作成できます。このネットワークは、ネットワーク間でパラメーターが一致しない限り、別の外部ネットワークと相互接続することはできません。コンピュータは、サーバーアップリンクポートを介して、引き続きインターネットに接続できます。PoE給電ポートに装置を接続するとすぐに、装置はリンクローカルアドレスを取得し、AXIS S2108アプライアンスに一致する固定IPセットを必要とします。



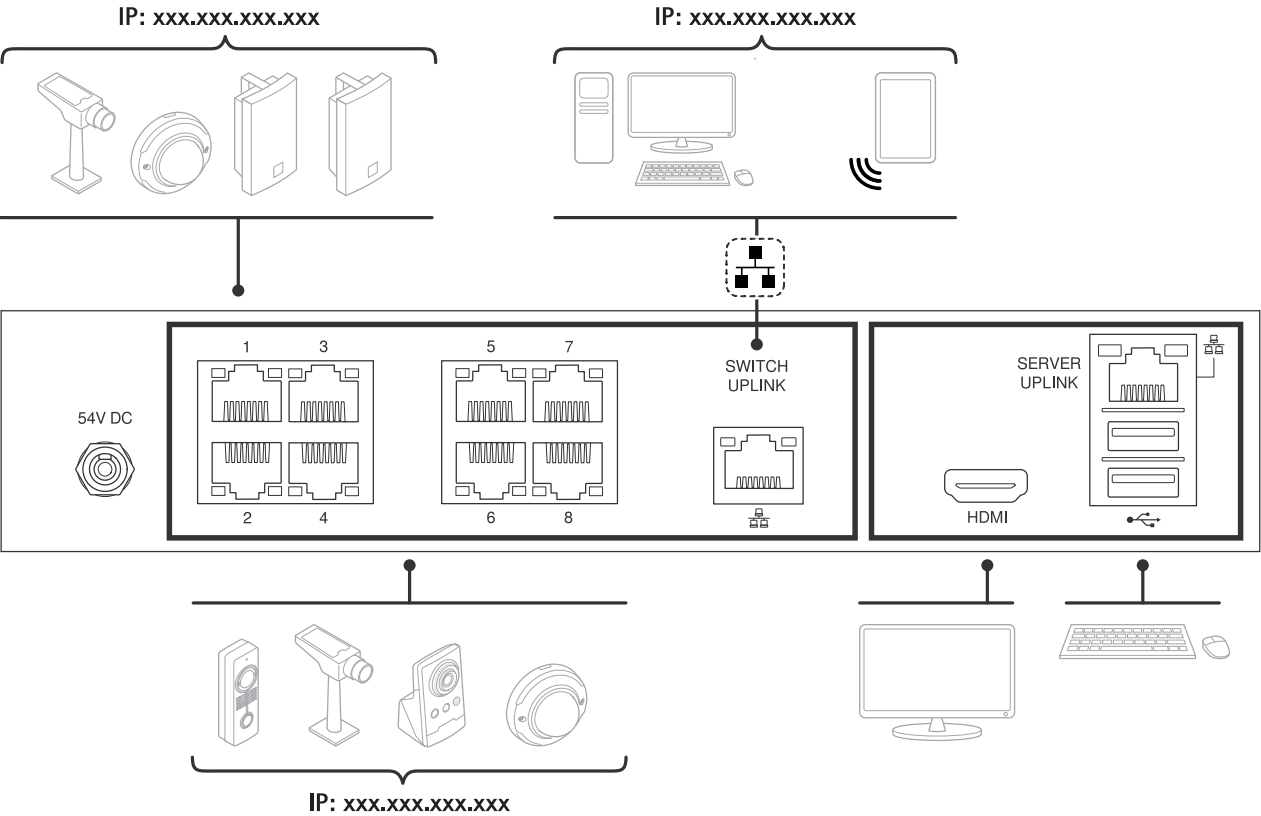
ローカルアドレスを使用する

各装置とAXIS S2108 Applianceでリンクローカルアドレスを使用して、独立したネットワークを作成できます。このネットワークは、他の外部ネットワークと相互接続することはできません。コンピュータは、サーバーアップリンクポートを介して、引き続きインターネットに接続できます。PoE給電ポートに装置を接続するとすぐに、装置はリンクローカルアドレスを取得し、AXIS S2108 ApplianceのAXIS Camera Stationから見つけれられるようになります。



別のネットワークからDHCPサーバーを使用する

既存のネットワークとDHCPサーバーをスイッチのアップリンクに接続することで、AXIS S2108 Applianceと接続された装置が相互に通信できるようになります。これにより、接続されたすべての装置にDHCPサーバーからIPアドレスが付与されるようになります。インターネット接続がそのネットワークで可能であれば、AXIS S2108 Applianceでも可能になります。それ以外の場合、コンピュータは独自に、サーバーアップリンクポートを介して、引き続きインターネットに接続できます。PoE給電ポートに装置を接続すると、DHCPサーバーがアクティブであれば、装置はDHCPアドレスを取得します。



使用に当たって

AXIS Camera Station録画サーバーを設定する標準的なワークフローは次のとおりです。

1. デバイスをインストールする
2. Windows®の初期設定:装置を設置した後、いくつかの手順に従って、地域、言語、キーボードレイアウト、管理者アカウントとそのパスワードを設定します。
3. Axisレコーダーの初期設定:Windowsの初期設定の後、AXIS Recorder Toolboxが開き、コンピューター名、日付と時刻、ネットワークなど、基本的かつ必要な設定を行う手順が表示されます。Axisレコーダーの初期設定, on page 15を参照してください。
4. Windows®を構成します。以下をお勧めします。
 - Windows®を最新バージョンに更新します。を参照してください。
 - 標準ユーザーアカウントを作成します。ユーザーアカウントの作成, on page 22を参照してください。
5. AXIS Camera Stationを最新バージョンに更新します。
 - システムがオンラインの場合：AXIS Recorder Toolboxアプリを開いて、**[Update AXIS Camera Station (AXIS Camera Stationの更新)]** をクリックします。
 - システムがオフラインの場合：axis.com に移動し、最新バージョンをダウンロードしてください。
6. AXIS Camera Stationクライアントを起動します。
7. AXIS Camera Stationサーバーへの接続
8. AXIS Camera Stationの設定, on page 17

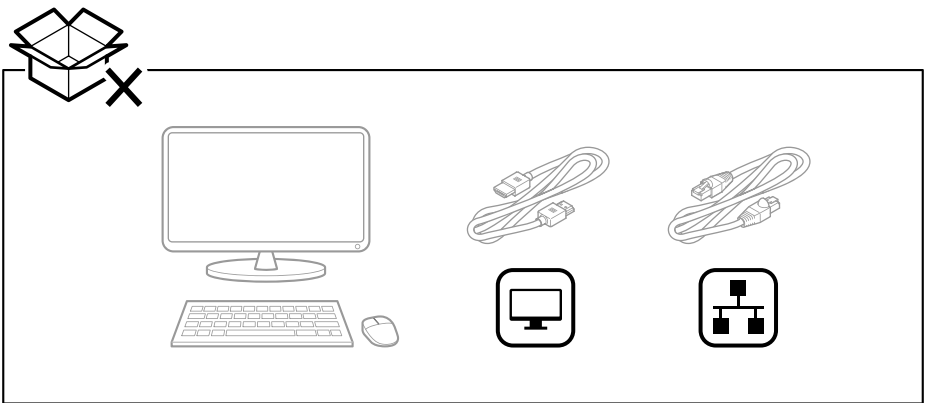
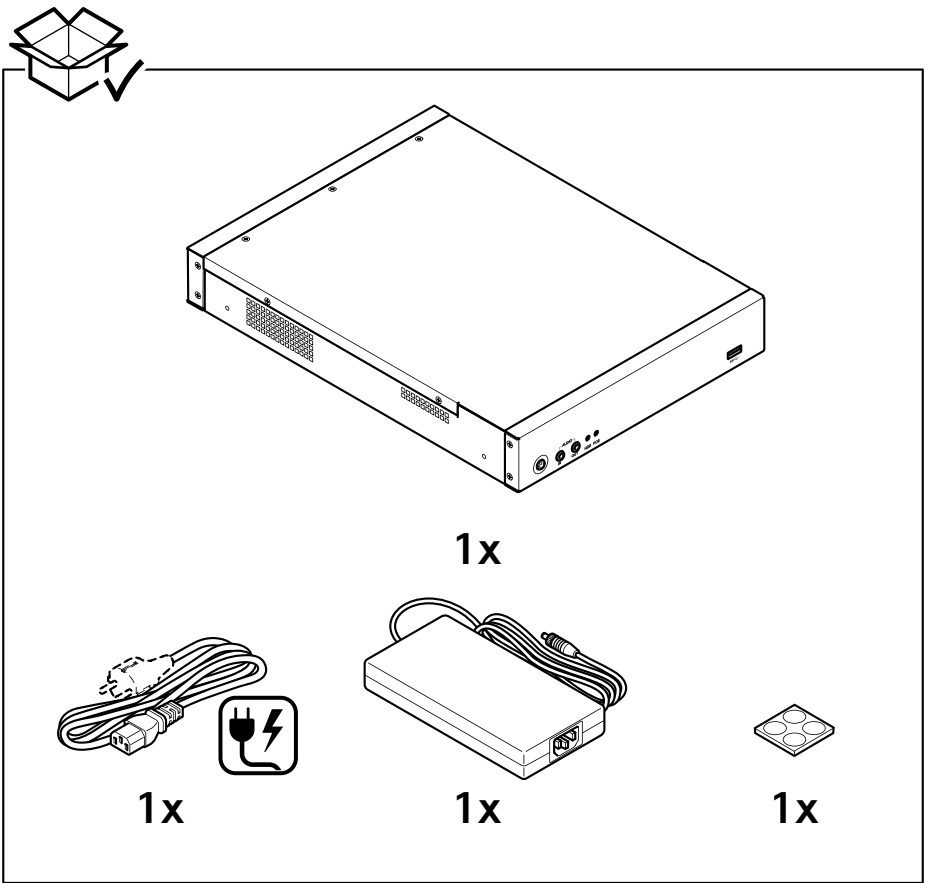
デバイスをインストールする

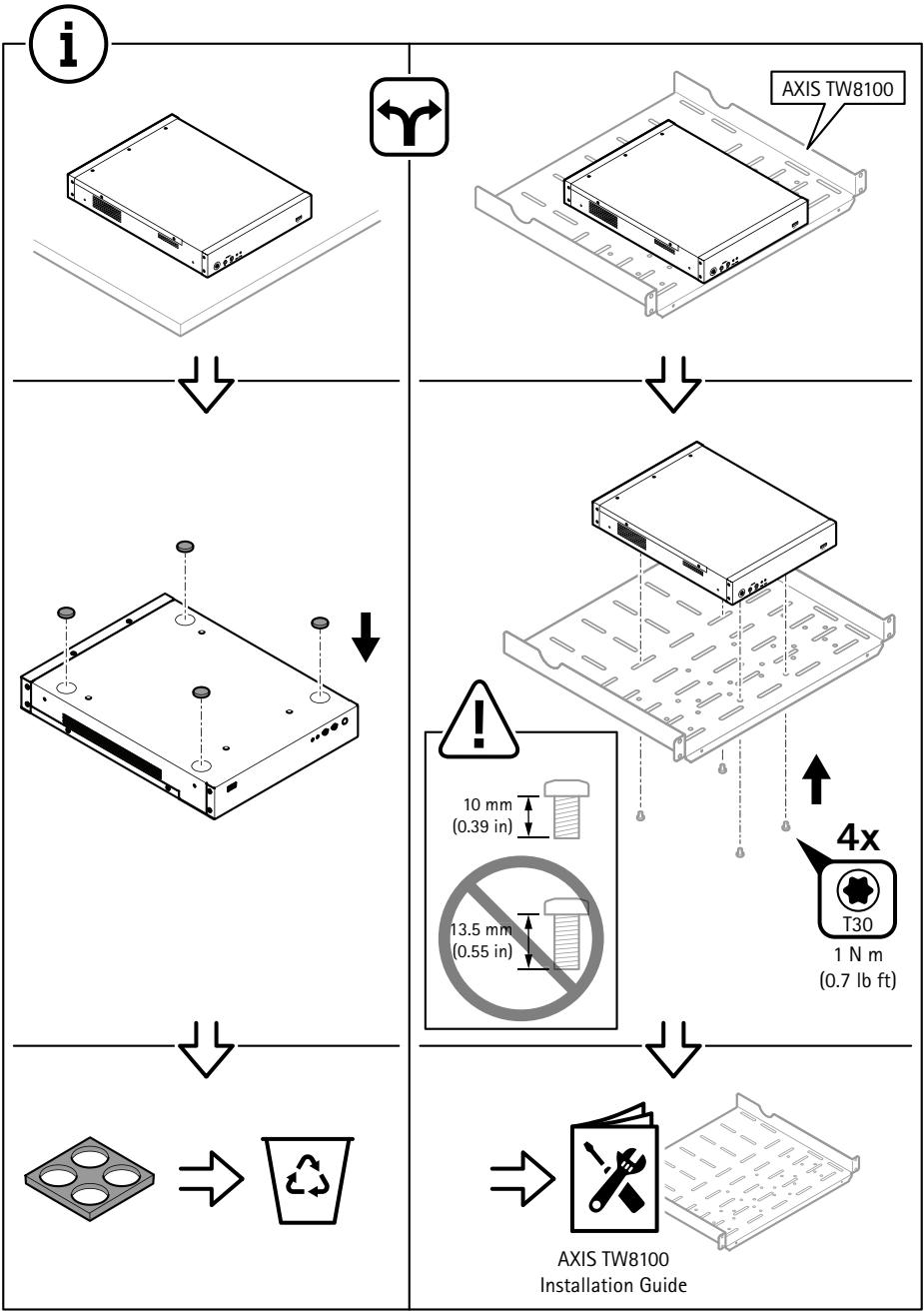
インストール前

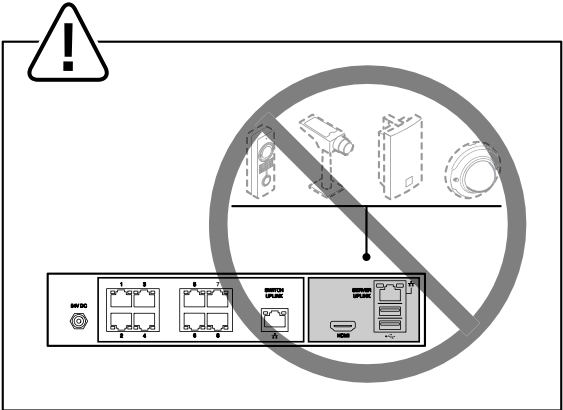
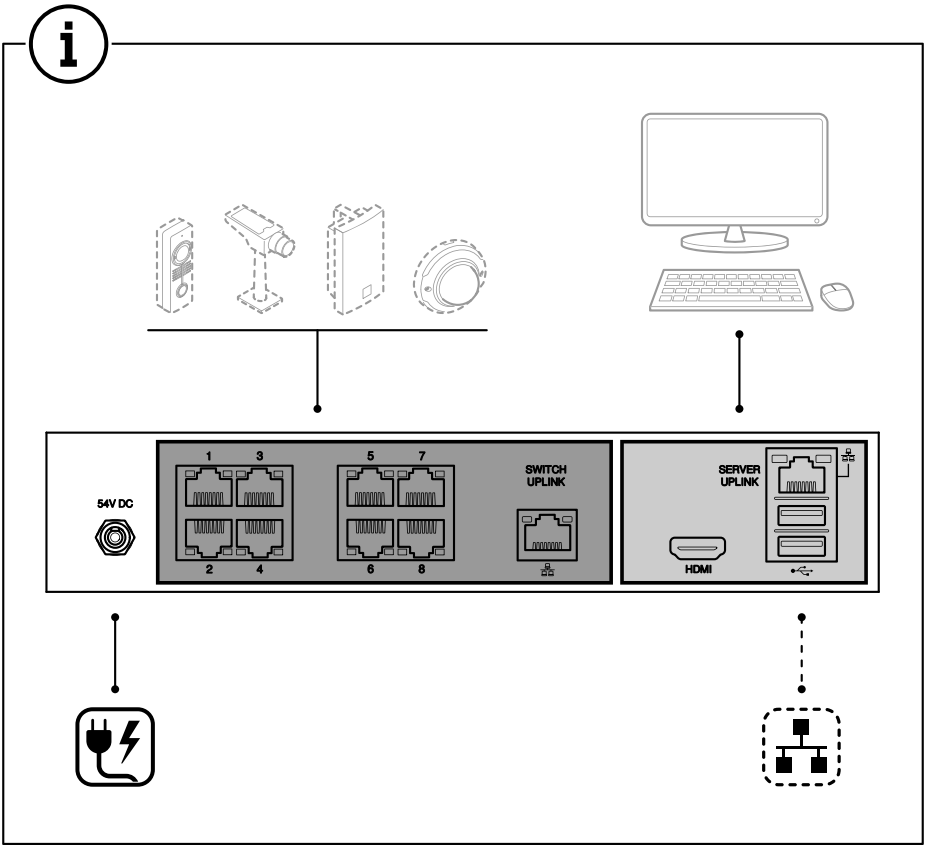
- 設置に使用する追加のアクセサリ (モニター、マウス、キーボード、ネットワークケーブル) を準備します。
- 異なるユーザーアカウントの使用方法を理解してください。

次の表に、Axisシステムのインストール、設定、操作に使用できるユーザーアカウントを示します。

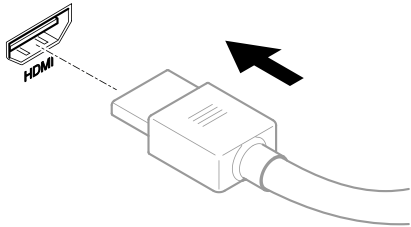
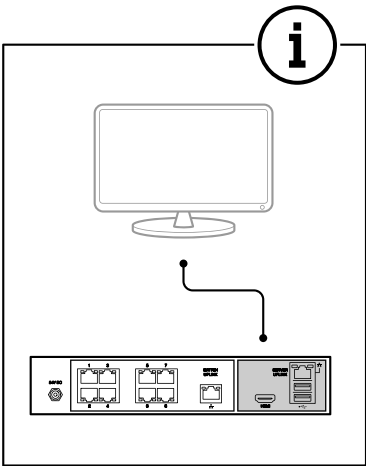
ユーザーアカウント	説明	注
MyAxis	最新のソフトウェアのダウンロード、ライセンスシステムへのアクセス、Axisセキュアリモートアクセス、システムの健全性監視に使用。	<i>my.axis.com</i> から登録。
Windows®		
Windows® 管理者	Windows® の管理者権限。AXIS Camera Stationの管理者として使用しないことをお勧めします。	Windows® の初期設定中に作成されます。
AXIS Camera Station管理者権限を持つWindows® ユーザー	AXIS Camera Stationの管理者権限が付与されたWindows® ユーザー。システムインテグレーターまたはシステム管理者が設定またはトラブルシューティングに使用。	Windows® の設定で作成されます。
AXIS Camera Stationのオペレーター権限または閲覧者権限を持つWindows® ユーザー	AXIS Camera Stationのオペレーター権限または閲覧者権限が付与されたWindows® ユーザー。	Windows® の設定で作成されます。
デバイス		
装置管理者	管理者がビデオ管理システムから、またはデバイスのWebページからカメラにアクセスするために使用。	装置のWebページから、または装置をAXIS Camera Stationに追加したときに作成されます。



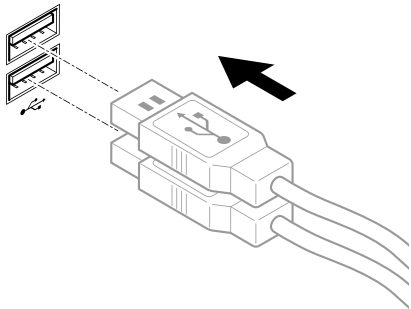
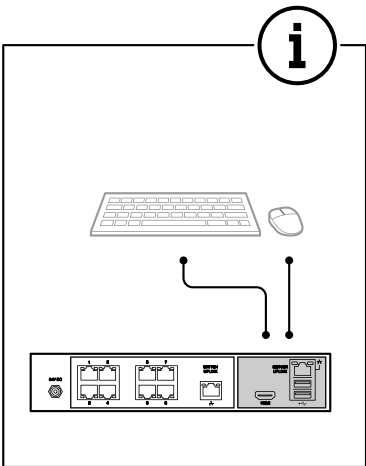




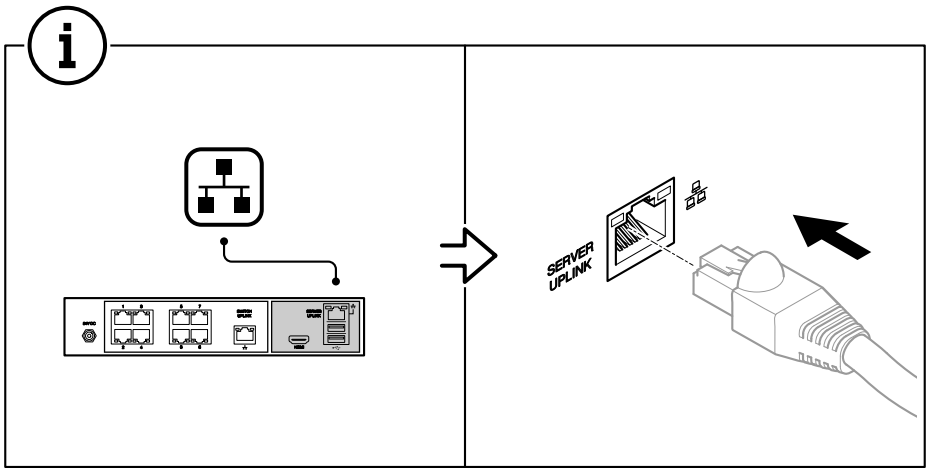
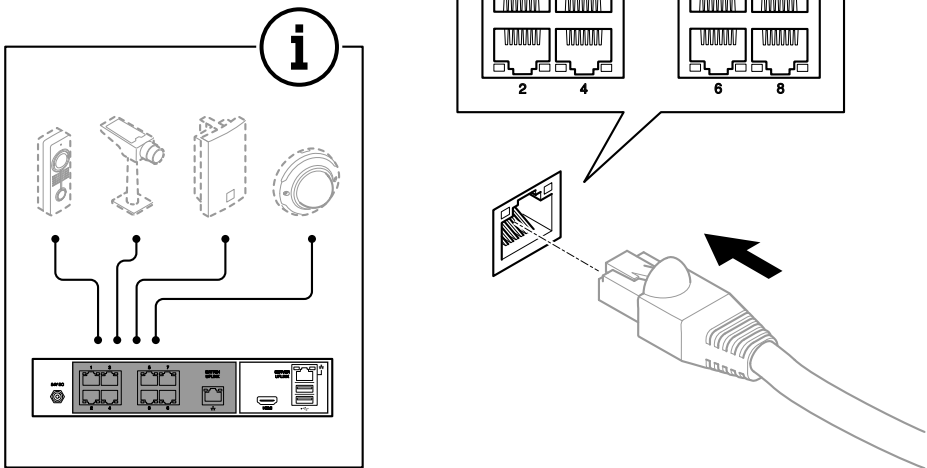
1.1



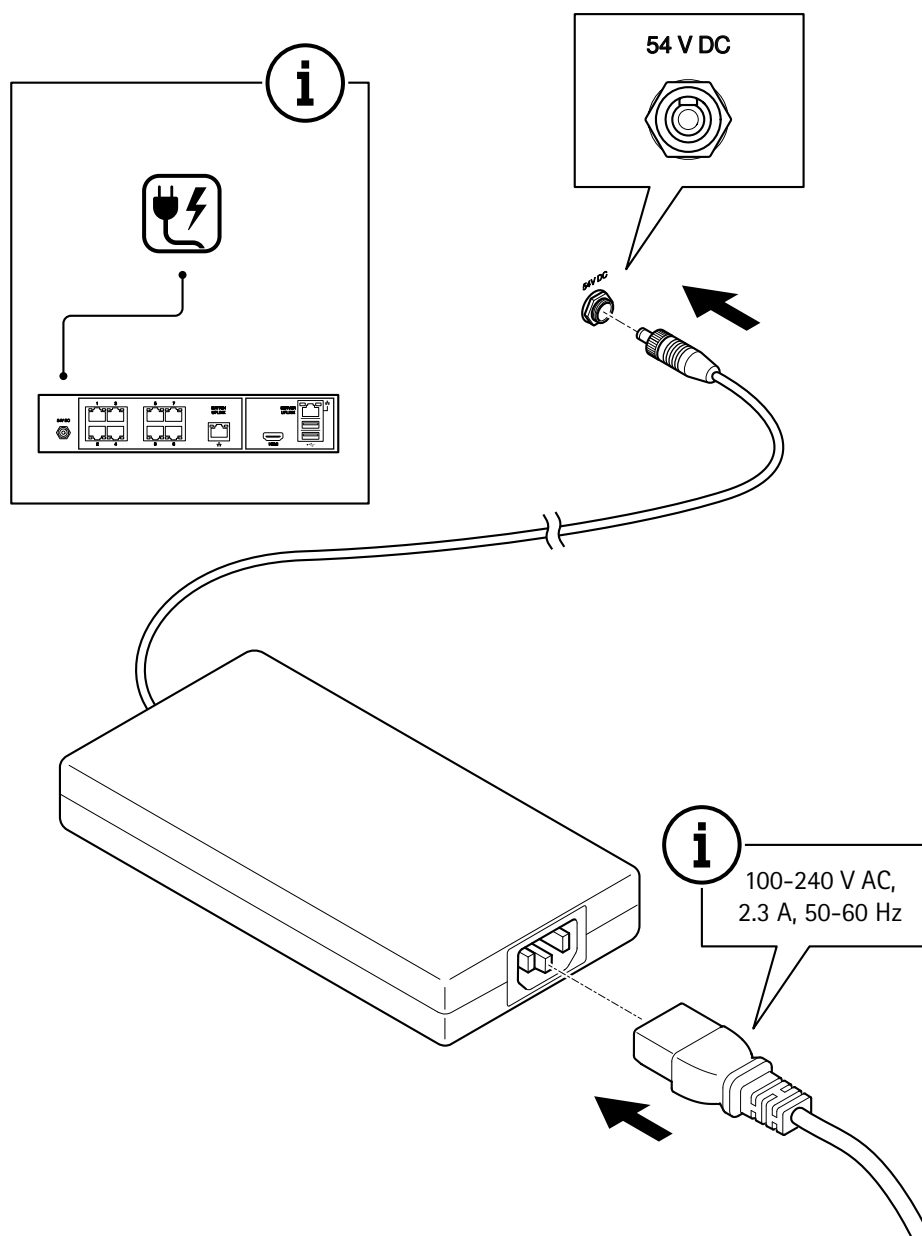
1.2



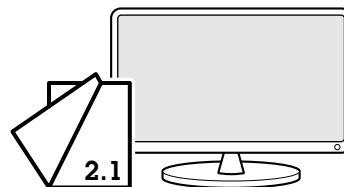
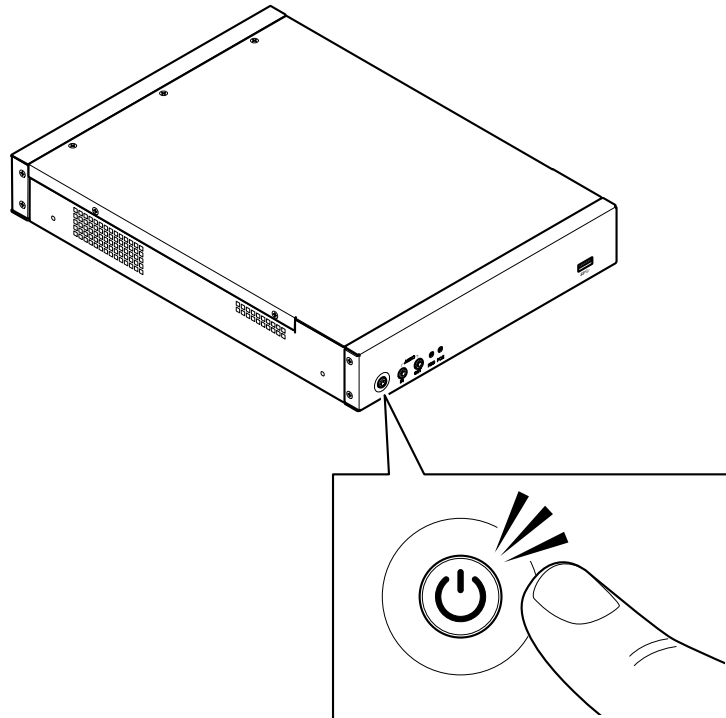
1.3



1.4



1.5



デバイスを構成する

Axisレコーダーの初期設定

Windows®の設定が完了すると、AXIS Recorder Toolboxが自動的に開き、初回設定のセットアップアシスタントの説明が表示されます。このセットアップアシスタントで、AXIS Recorder Toolboxで装置を管理する前に、いくつかの基本的で必要な設定を行います。

1. [Light (ライト)] または [Dark (ダーク)] テーマを選択し、[Next (次へ)] をクリックします (ご使用の製品で選択できる場合)。
2. 必要に応じコンピューター名を変更し、[Next (次へ)] をクリックします。
3. [Date and time (日付と時刻)] で以下の設定を行い、[Next (次へ)] をクリックします。
 - タイムゾーンを選択します。
 - NTPサーバを設定するには、[NTP server (NTP サーバー)] を選択し、NTPサーバーのアドレスを入力します。
 - 手動で設定するには、[Manual (手動)] を選択し、日付と時刻を選択します。
4. [Network settings (ネットワーク設定)] で以下の設定を行い、[Next (次へ)] をクリックします。
 - [Use automatic IP settings (DHCP) (自動IP設定 (DHCP) を使用する)] と [Use automatic DNS settings (自動DNS設定を使用する)] は、デフォルトでオンになっています。
 - デバイスがDHCPサーバーを使用してネットワークに接続されている場合は、割り当てられたIPアドレス、サブネットマスク、ゲートウェイ、および優先DNSが自動的に表示されます。
 - デバイスがネットワークに接続されていないか、利用可能なDHCPサーバーがない場合は、ネットワークの要件に応じて、IPアドレス、サブネットマスク、ゲートウェイ、および優先DNSを手動で入力します。
5. **Finish (終了)** をクリックします。コンピューター名を変更した場合、AXIS Recorder Toolboxからデバイスの再起動を求めるメッセージが表示されます。

サーバーにログインする

AXIS Camera Stationクライアントを使用すると、同じコンピューターやネットワーク上にインストールされている1つまたは複数のサーバーに接続することができます。AXIS Camera Stationサーバーには、異なる方法で接続できます。

最後に使用したサーバー - 前のセッションで使用したサーバーに接続します。

このコンピューター - クライアントと同じコンピューターにインストールされているサーバーに接続します。

リモートサーバー - リモートサーバーとの接続, on page 16を参照してください。

Axis secure remote access - AXISセキュアリモートアクセスにサインイン, on page 16を参照してください。

注

初めてサーバーに接続する際に、クライアントではサーバー証明書IDが確認されます。正しいサーバーに接続していることを確認するには、AXIS Camera Station Service Controlに表示されている証明書IDを手動で確認します。

Server list (サーバーリスト)	サーバーリストからサーバーに接続するには、 [Server list (サーバーリスト)] ドロップダウンメニューからサーバーを選択します。サーバーリストを作成または編集するには、  をクリックします。
Import server list (サーバーリストのインポート)	AXIS Camera Stationからエクスポートされたサーバーリストファイルをインポートするには、右下の [Import server list (サーバーリストをインポート)] をクリックして、.mslファイルを参照します。
Delete saved passwords (保存したパスワードの削除)	接続済みのすべてのサーバーで保存されたユーザー名とパスワードを削除するには、 [Delete saved passwords (保存したパスワードを削除)] をクリックします。
Change client proxy settings (クライアントのプロキシ設定を変更)	サーバーに接続するには、クライアントのプロキシ設定を変更する必要がある場合があります。 Change client proxy settings (クライアントプロキシ設定の変更)] をクリックします。

リモートサーバーとの接続

1. [リモートサーバー] を選択します。
2. [Remote server (リモートサーバー)] ドロップダウンリストからサーバーを選択するか、IPアドレスまたはDNSアドレスを入力します。サーバーが表示されていない場合は、 をクリックして使用可能なすべてのリモートサーバーのリストを更新します。サーバーがデフォルトのポート番号 (55754) とは異なるポートでクライアントを受け入れるよう設定されている場合は、IPアドレスの後にポート番号 (192.168.0.5:46001など) を入力します。
3. 以下のいずれかの操作を行います。
 - 現在のWindows® ユーザーとしてログインするには、**[Log in as current user (現在のユーザーでログイン)]** を選択します。
 - **[Log in as current user (現在のユーザーでログイン)]** のチェックマークを外し、**[Log in (ログイン)]** をクリックします。別の認証情報を使用してログインする場合は、**[Other user (その他のユーザー)]** を選択して別のユーザー名とパスワードを入力します。

AXISセキュアリモートアクセスにサインイン

重要

セキュリティおよび機能性の向上を目的として、**Axis Secure Remote Access (v1)** を **Axis Secure Remote Access v2** へアップグレードします。現行バージョンは2025年12月1日をもって提供終了となる予定のため、それまでにAxis Secure Remote Access v2へのアップグレードを強くお勧めします。

お使いの AXIS Camera Station S2108 Applianceシステムへの影響：

- 2025年12月1日以降、**Axis Secure Remote Access (v1)**を使用してシステムにリモートアクセスすることはできなくなります。
- **Axis Secure Remote Access v2**を使用するには、AXIS Camera Station Proバージョン6.8にアップグレードする必要があります。このアップグレードは、2026年3月1日まで、AXIS Camera Station 5をご利用中のすべてのユーザーに無料で提供されます。

注

- Axis Secure Remote Accessを使用してサーバーに接続しようとする、サーバーはクライアントを自動的にアップグレードできません。
 - プロキシサーバーがネットワークデバイスと AXIS Camera Station S2108 Applianceサーバーの間にある場合、AXIS Secure Remote Accessを使用してサーバーにアクセスするには、AXIS Camera Station S2108 Applianceサーバー上のWindowsでプロキシ設定を行う必要があります。
1. [AXISセキュアリモートアクセスにサインイン] リンクをクリックします。
 2. MyAxisアカウントの認証情報を入力します。
 3. [Sign in (サインイン)] をクリックします。
 4. [Grant (許可)] をクリックします。

AXIS Camera Stationの設定

このチュートリアルでは、システムを立ち上げて実行するための基本的な手順について説明します。

開始する前に、以下をご確認ください。

- インストール内容に応じてネットワークを設定します。ネットワーク設定, on page 19を参照してください。
- 必要な場合は、サーバーポートを設定します。サーバーポートの設定, on page 20を参照してください。
- セキュリティ上の問題を考慮します。セキュリティに関する考慮事項を参照してください。

必要な設定を行った後で、AXIS Camera Stationによる作業を開始することができます。

1. ビデオ管理システムを起動する, on page 17
2. デバイスの追加, on page 17
3. 録画方法の設定, on page 18
4. ライブビデオを表示する, on page 18
5. 録画の表示, on page 18
6. ブックマークの追加, on page 18
7. 録画のエクスポート, on page 18
8. AXIS File Playerでの録画の再生と検証, on page 18

ビデオ管理システムを起動する

AXIS Camera Stationのクライアントアイコンをダブルクリックすると、AXIS Camera Stationクライアントが起動します。クライアントの初回起動時には、同じコンピューターにインストールされたAXIS Camera Stationサーバーに自動的にログインします。

複数のAXIS Camera Stationサーバーに異なる方法で接続できます。

デバイスの追加

AXIS Camera Stationを初めて起動すると、デバイスの追加ページが開きます。AXIS Camera Stationにより、ネットワークで接続されているデバイスが検索され、検出されたデバイスのリストが表示されます。

1. 追加するカメラをリストから選択します。カメラが見つからない場合は、[Manual search (手動検索)] をクリックします。
2. [追加] をクリックします。

3. [クイック設定] または [Site Designer設定] を選択します。[Next (次へ)] をクリックします。
4. デフォルト設定を使用し、録画方法が [None (なし)] に設定されていることを確認します。[インストール] をクリックします。

録画方法の設定

1. [設定] - [録画とイベント] - [録画方法] を選択します。
2. カメラを選択します。
3. [Motion detection (動体検知)] または [Continuous (連続)] をオンにします。
4. [適用] をクリックします。

ライブビデオを表示する

1. [Live view (ライブビュー)] タブを開きます。
2. ライブビデオを表示するカメラを選択します。

録画の表示

1. [Recordings (録画)] タブを開きます。
2. 録画を表示するカメラを選択します。

ブックマークの追加

1. 録画に移動します。
2. タイムラインで、ズームインとズームアウトを行い、マーカーが目的の位置になるようにタイムラインを動かします。
3.  をクリックします。
4. ブックマークの名前と説明を入力します。キーワードを使用すると、ブックマークがつけやすくなります。
5. 録画をロックするには、[録画削除を防止] を選択します。

注

録画のロックを解除するには、[Prevent recording deletion (録画削除を防止)] をクリアするか、ブックマークを削除します。

6. [OK] をクリックして、ブックマークを保存します。

録画のエクスポート

1. [Recordings (録画)] タブを開きます。
2. 録画をエクスポートするカメラを選択します。
3.  をクリックすると、選択マーカーが表示されます。
4. マーカーをドラッグして、エクスポートする録画を含めます。
5.  をクリックして、[Export (エクスポート)] タブを開きます。
6. [Export... (エクスポート)] をクリックします。

AXIS File Playerでの録画の再生と検証

1. エクスポートした録画を含むフォルダーに移動します。

2. AXIS File Playerをダブルクリックします。
3.  をクリックすると、録画のノートが表示されます。
4. デジタル署名を検証するには、次のようにします。
 - 4.1. [Tools > Verify digital signature (ツール > デジタル署名の検証)] に移動します。
 - 4.2. [Validate with password (パスワードで検証)] を選択し、パスワードを入力します。
 - 4.3. [Verify (検証)] をクリックして検証結果を確認します。

注

- デジタル署名は署名付きビデオとは異なります。署名付きビデオは、そのビデオが録画されたカメラを特定できるため、改ざんされていないことを確認できます。詳細については、署名付きビデオとカメラのユーザーマニュアルを参照してください。
- 保存されたファイルがAXIS Camera Stationデータベースと接続していない場合 (インデックスされていないファイル)、AXIS File Playerで再生できるように変換する必要があります。ファイルの変換については、Axisテクニカルサポートにお問い合わせください。

ネットワーク設定

AXIS Camera Stationクライアント、AXIS Camera Stationサーバー、接続されたネットワーク装置が異なるネットワークにある場合は、AXIS Camera Stationを使用する前にプロキシまたはファイアウォールの設定が必要になる可能性があります。

クライアントのプロキシ設定

プロキシサーバーによってクライアントとサーバーが分離されている場合は、クライアントのプロキシ設定を編集します。

1. AXIS Camera Stationクライアントを開きます。
2. [Change client proxy settings (クライアントのプロキシ設定を変更)] をクリックします。
3. クライアントのプロキシ設定を変更します。
4. [OK] をクリックします。

サーバーのプロキシ設定

プロキシサーバーによってネットワーク装置とサーバーが分離されている場合は、サーバーのプロキシ設定を編集します。

1. AXIS Camera Station Service Controlを開きます。
2. [Modify settings (設定の変更)] を選択します。
3. [Proxy settings (プロキシの設定)] セクションで、デフォルトのシステムアカウントのインターネットオプションを使用するか、[Use manual proxy settings (手動でプロキシを設定する)] を選択します。
4. [保存] をクリックします。

NATとファイアウォール

クライアントとサーバーがNATやファイアウォールなどで隔てられている場合は、NATやファイアウォールを設定して、AXIS Camera Station Service Controlで指定されているHTTPポート、TCPポート、ストリーミングポートがファイアウォールやNATを通過できるようにします。NATまたはファイアウォールの設定手順については、ネットワーク管理者に問い合わせてください。

サーバーポートの設定

AXIS Camera Stationサーバーでは、ポート55752 (HTTP)、55754 (TCP)、55756 (モバイル通信)、および55757 (モバイルストリーミング) がサーバーとクライアントの間の通信に使用されます。必要な場合、これらのポートはAXIS Camera Station Service Controlで変更できます。

セキュリティに関する考慮事項

カメラおよび録画への不正アクセスを防ぐには:

- すべてのネットワーク装置 (カメラ、ビデオエンコーダ、補助装置) で強力なパスワードを使用します。
- AXIS Camera Station S2108 Applianceサーバー、カメラ、ビデオエンコーダ、補助デバイスをオフィスネットワークから分離された安全なネットワークにインストールします。AXIS Camera Station S2108 Applianceクライアントは、インターネットアクセスのあるネットワークなど別のネットワーク上のコンピューターにインストールすることができます。
- すべてのユーザーが強力なパスワードを使用していることを確認してください。

システムをオンラインでライセンスする

AXIS Camera Stationクライアントとサーバーの両方にインターネット接続が必要です。

1. **[設定] - [ライセンス] - [管理]** を選択します。
2. **[Manage licenses online (オンラインでライセンスを管理)]** がオンになっていることを確認します。
3. My Axisアカウントでサインインします。
4. ライセンスキーが自動的に生成され、**[License keys (ライセンスキー)]** で表示されます。
5. ライセンスキーを別途購入した場合は、**[Add license key (ライセンスキーの追加)]** でライセンスキーを入力します。
6. **[追加]** をクリックします。
7. AXIS Camera Stationクライアントで、**[Configuration (設定)] > [Licenses (ライセンス)] > [Keys (キー)]** に移動して、ライセンスキーが表示されていることを確認します。

システムをオフラインでライセンスする

1. **[設定] - [ライセンス] - [管理]** を選択します。
2. **[Manage licenses online (オンラインでライセンスを管理する)]** をオフにします。
3. **[システムファイルのエクスポート]** をクリックします。
4. システムファイルをUSBフラッシュドライブに保存します。
5. My Axisアカウントでサインインします。
6. **[Upload system file (システムファイルをアップロード)]** をクリックして、システムファイルをUSBフラッシュドライブからアップロードします。
7. ライセンスキーが自動的に生成され、**[License keys (ライセンスキー)]** に表示されます。
8. ライセンスキーを別途購入した場合は、**[Add license key (ライセンスキーの追加)]** でライセンスキーを入力します。
9. **[追加]** をクリックします。
10. **[License keys (ライセンスキー)]** で、**[Download license file (ライセンスファイルのダウンロード)]** をクリックして、USBフラッシュドライブにファイルを保存します。
11. AXIS Camera Stationクライアントで、**[Configuration (設定)] > [Licenses (ライセンス)] > [Management (管理)]** に移動します。

12. **[Import license file (ライセンスファイルのインポート)]** をクリックし、USBフラッシュドライブのライセンスファイルを選択します。
13. **[Configuration (設定)] > [Licenses (ライセンス)] > [Keys (キー)]** に移動して、ライセンスキーが表示されていることを確認します。

ローカル Windows® ユーザーアカウントの管理

ユーザーアカウントの作成

個人データと情報のセキュリティを強化するために、ローカルアカウントごとにパスワードを追加することをお勧めします。

重要

ローカルアカウントのパスワードを作成したら、そのパスワードを忘れないでください。ローカルアカウントのパスワードを紛失したパスワードを回復する方法はありません。

1. [Settings (設定)] > [アカウント] > [Other people (他のユーザー)] > [Add someone else to this PC (このPCに他のユーザーを追加)] の順に移動します。
2. [I don't have this person's sign-in information (このユーザーのサインイン情報を持っていない)] をクリックします。
3. [Add a user without a Microsoft account (Microsoftアカウントを持たないユーザーを追加する)] をクリックします。
4. ユーザー名、パスワード、およびパスワードのヒントを入力します。
5. [Next (次へ)] をクリックし、指示に従います。

管理者アカウントを作成する

1. [Settings (設定)] > [Accounts (アカウント)] > [Other people (その他のユーザー)] に移動します。
2. 変更するアカウントに移動し、[Change account type (アカウントの種類の変更)] をクリックします。
3. [Account type (アカウントの種類)] に移動し、[Administrator (管理者)] を選択します。
4. [OK] をクリックします。
5. デバイスを再起動し、新しい管理者アカウントでログインします。

ローカルユーザーグループを作成する

1. [Computer Management (コンピューター管理)] に移動します。
2. [Local Users and Groups (ローカルユーザーとグループ)] > [Group (グループ)] の順に移動します。
3. [Group (グループ)] を右クリックし、[New Group (新しいグループ)] を選択します。
4. グループ名と説明を入力します。
5. グループメンバーの追加:
 - 5.1. [追加] をクリックします。
 - 5.2. [詳細設定] をクリックします。
 - 5.3. グループに追加するユーザー アカウントを見つけて、[OK] をクリックします。
 - 5.4. もう一度 [OK] をクリックします。
6. [Create (作成)] をクリックします。

ユーザーアカウントを削除します。

重要

アカウントを削除すると、ログイン画面からユーザーアカウントが削除されます。また、ユーザーアカウントに保存されているすべてのファイル、設定、およびプログラムデータも削除します。

1. [Settings (設定)] > [Accounts (アカウント)] > [Other people (その他のユーザー)] に移動します。
2. 削除するアカウントに移動し、[Remove (削除)] をクリックします。

ユーザーアカウントのパスワードを変更する

1. 管理者アカウントでログインします。
2. [User Accounts (ユーザーアカウント)] > [User Accounts (ユーザーアカウント)] > [Manage another account in sequence (別のアカウントを順番に管理する)] の順に移動します。
デバイス上のすべてのユーザーアカウントの一覧が表示されます。
3. パスワードを変更するユーザーアカウントを選択します。
4. [Change the password (パスワードの変更)] をクリックします。
5. 新しいパスワードを入力し、[Change password (パスワードの変更)] をクリックします。

ユーザーアカウントのパスワードリセットディスクを作成する

USBフラッシュドライブにパスワードリセットディスクを作成することをお勧めします。このディスクを使用して、パスワードをリセットできます。パスワードリセットディスクがないと、パスワードをリセットできません。

注

Windows® 10以降を使用している場合は、パスワードを忘れたときのために、ローカルアカウントにセキュリティの質問を追加できるため、パスワードリセットディスクを作成する必要はありません。これを行うには、[Start (スタート)] ボタンをクリックし、[Settings (設定)] > [Sign-in options (サインインオプション)] > [Update your security questions (セキュリティに関する質問の更新)] の順にクリックします。

1. ローカルユーザーアカウントを使用してデバイスにログインします。接続されているアカウントのパスワードリセットディスクを作成することはできません。
2. 空のUSBフラッシュドライブを装置に接続します。
3. [Windows® 検索フィールドから、[Create a password reset disk (パスワード リセット ディスクの作成)] に進みます。
4. パスワードディスクの作成ウィザードで、[Next (次へ)] をクリックします。
5. USBフラッシュドライブを選択し、[Next (次へ)] をクリックします。
6. 現在のパスワードを入力し、[Next (次へ)] をクリックします。
7. 画面の指示に従います。
8. USBフラッシュドライブを取り外し、安全な場所に保管してください。パスワードを何度変更しても、新しいディスクを作成する必要はありません。

AXIS Camera Stationのユーザーアカウントの管理

ユーザー権限

[Configuration (設定)] > [Security (セキュリティ)] > [User permissions (ユーザー権限)] に移動して、AXIS Camera Station S2108 Applianceのユーザーとグループを確認します。

注

AXIS Camera Station S2108 Applianceサーバーを実行しているコンピューターの管理者は、自動的に AXIS Camera Station S2108 Applianceの管理者権限が付与されます。管理者グループの権限を変更したり、削除したりすることはできません。

ユーザーまたはグループを追加する前に、それらがローカルコンピューターに登録されているか、Windows® Active Directoryのユーザーアカウントを持っていることを確認してください。ユーザーまたはグループを追加するには、「ユーザーまたはグループの追加」を参照してください。

ユーザーがグループに所属している場合、そのユーザーには、個人またはグループに割り当てられる最も高いロール権限が付与されます。たとえば、カメラXへのアクセス権を持つユーザーが、カメラYおよびZへのアクセス権を持つグループにも所属している場合、そのユーザーは3台のカメラすべてへのアクセス権を持ちます。

	エントリが1人のユーザーであることを示します。
	エントリがグループであることを示します。
名称	ローカルコンピューターまたはActive Directoryに表示されるユーザー名。
ドメイン	ユーザーまたはグループが属するドメイン。
役割	ユーザーまたはグループに割り当てられるアクセスロール。表示される値:管理者、オペレーター、閲覧者。
詳細	ローカルコンピューターまたはActive Directoryに表示されるユーザーの詳細情報。
サーバー	ユーザーまたはグループが属するサーバー。

ユーザーまたはグループの追加

Microsoft Windows® とActive Directoryのユーザーとグループは AXIS Camera Station S2108 Applianceにアクセスできます。ユーザーを AXIS Camera Station S2108 Applianceに追加するには、ユーザーまたはグループをWindows® に追加する必要があります。

Windows® 10および11でユーザーを追加するには：

- Windowsキー + X を押し、[Computer Management (コンピューターの管理)] を選択します。
- [Computer Management (コンピューターの管理)] ウィンドウで、[Local Users and Groups (ローカルユーザーとグループ)] > [Users (ユーザー)]の順に移動します。
- [Users (ユーザー)] を右クリックし、[New user (新しいユーザー)] を選択します。
- ポップアップダイアログで、新規ユーザーの詳細を入力し、[User must change password at next login (ユーザーは次回ログイン時にパスワードの変更が必要)] をクリアします。
- [Create (作成)] をクリックします。

Active Directoryドメインをご使用の場合は、ネットワーク管理者にお問い合わせください。

ユーザーまたはグループの追加

1. [Configuration > Security > User permissions (設定 > セキュリティ > ユーザー権限)] に移動します。
2. [追加] をクリックします。利用可能なユーザーとグループがリストに表示されます。
3. [Scope (対象)] で、ユーザーとグループを検索する場所を選択します。
4. [Show (表示)] で、ユーザーまたはグループを表示するかどうかを選択します。ユーザーまたはグループの数が多すぎる場合、検索結果が表示されないことがあります。フィルターを使用して検索結果を絞り込みます。
5. ユーザーまたはグループを選択し、[追加] をクリックします。

対象	
サーバー	ローカルコンピューター上のユーザーまたはグループを検索する場合に選択します。
ドメイン	Active Directoryのユーザーまたはグループを検索する場合に選択します。
選択したサーバー	複数の AXIS Camera Station S2108 Appliance サーバーに接続している場合は、サーバーを選択して、そのサーバー上のユーザーまたはグループを検索します。

ユーザーまたはグループの設定

1. リストからユーザーまたはグループを選択します。
2. [Role (権限)] で、[Administrator (管理者)]、[Operator (オペレーター)]、または [Viewer (閲覧者)] を選択します。
3. [Operator (オペレーター)] または [Viewer (閲覧者)] を選択した場合は、ユーザーまたはグループの権限を設定することができます。ユーザーまたはグループの権限を参照してください。
4. Save (保存) をクリックします。

ユーザーまたはグループの削除

1. ユーザーまたはグループを選択します。
2. [削除] をクリックします。
3. ポップアップダイアログで [OK] をクリックするとユーザーまたはグループが削除されます。

ユーザーまたはグループの権限

ユーザーまたはグループに割り当てられるロールは3種類です。ユーザーまたはグループの権限の定義方法については、ユーザーまたはグループの追加を参照してください。

管理者 - すべてのカメラのビューのライブおよび録画ビデオへのアクセス、すべてのI/Oポートへのアクセスなど、システム全体へのフルアクセス。このロールは、システム設定にアクセスする必要があります。

オペレーター - カメラ、ビュー、I/Oポートを選択して、ライブおよび録画ビデオにアクセスします。オペレーターは AXIS Camera Station S2108 Applianceのすべての機能 (システムの設定を除く) へのフルアクセスが許可されます。

ビューワー - 選択したカメラ、I/Oポート、ビューのライブビデオにアクセスします。録画ビデオへのアクセスやシステムの設定を行うことはできません。

カメラ

[Operator (オペレーター)] または [Viewer (閲覧者)] の権限を持つユーザーまたはグループは、次のアクセス権を利用できます。

アクセス	カメラおよびすべてのカメラ機能へのアクセスを許可します。
ビデオ	このカメラからのライブ映像へのアクセスを許可します。
音声を聞く	カメラから受話するアクセスを許可します。
音声送話	カメラに送話するアクセスを許可します。
Manual Recording (手動録画)	手動で録画を開始・停止することができます。
Mechanical PTZ (メカニカルPTZ)	メカニカルPTZコントロールへのアクセスを許可します。メカニカルPTZ機能を備えたカメラでのみ利用できます。
PTZ優先度	PTZ優先度を設定します。数値が小さいほど、優先度が高いことを意味します。優先度を割り当てない場合は [0] に設定されます。優先度が最も高いのは管理者です。優先度の高い権限を持つユーザーがPTZカメラを操作する場合、デフォルトでは、他のユーザーは同じカメラを10秒間操作することができません。メカニカルPTZ機能を備えたカメラで、 [Mechanical PTZ (メカニカルPTZ)] が選択されているときのみ使用できます。

ビュー

[Operator (オペレーター)] または [Viewer (閲覧者)] の権限を持つユーザーまたはグループは、次のアクセス権を利用できます。複数のビューを選択し、アクセス権を設定することができます。

アクセス	AXIS Camera Station S2108 Applianceのビューへのアクセスを許可します。
編集	AXIS Camera Station S2108 Applianceでビューを編集することができます。

I/O

[Operator (オペレーター)] または [Viewer (閲覧者)] の権限を持つユーザーまたはグループは、次のアクセス権を利用できます。

アクセス	I/Oポートへのフルアクセス権を許可します。
読む	I/Oポートの状態を変更することなく、その状態を表示することができます。
Write (書き込み)	I/Oポートの状態を変更することができます。

システム

リスト内でグレー表示されているアクセス権限は設定できません。チェックマークは、そのユーザーまたはグループがこの権限を持っていることを意味します。

[Operator (オペレーター)] 権限を持つユーザーまたはグループは次のアクセス権を利用できます。[Take snapshots (スナップショットを撮る)] は [Viewer (閲覧者)] 権限でも利用できます。

スナップショットを撮る	ライブビューおよび録画モードでスナップショットを撮影できます。
録画のエクスポート	録画のエクスポートを許可します。
事故レポートの生成	事故レポートの生成を許可します。
Prevent access to recordings older than (これより古い録画へのアクセスを防止)	指定した分数よりも古い録画へのアクセスを防止します。ユーザーはこれらの録画を検索しても見つけることができません。
アラーム、タスク、ログへのアクセス	アラーム通知を受け取り、[Alarms and tasks (アラームとタスク)] バーと [Logs (ログ)] タブへのアクセスを許可します。
Access data search (データ検索へのアクセス)	イベント発生時の状況を追跡するためのデータ検索を許可します。
イベントにカテゴリーを追加する	録画 タブでイベントにカテゴリーを追加できるようにします。
イベントからカテゴリーを削除する	録画タブでイベントからカテゴリーを削除できるようにします。

アクセスコントロール

[Operator (オペレーター)] 権限を持つユーザーまたはグループは次のアクセス権を利用できます。[Access Management (アクセス管理)] は [Viewer (閲覧者)] 権限でも利用できます。

アクセスコントロールの設定	ドアとゾーン、識別プロファイル、カードフォーマットとPIN、暗号化通信、マルチサーバーを設定することができます。
アクセス管理	アクセス管理およびActive Directory設定にアクセスすることができます。

Viewer (閲覧者) のロールを持つユーザーまたはグループは、次のアクセス権を利用できます。

システムのヘルスマニタリング

[Operator (オペレーター)] 権限を持つユーザーまたはグループは次のアクセス権を利用できます。[>システムの健全性監視へのアクセス] は [Viewer (閲覧者)] 権限でも利用できます。

システムの健全性監視の設定	システムの健全性監視を設定することができます。
システムの健全性監視へのアクセス	システムの健全性監視にアクセスすることができます。

デバイスを管理する

セキュアブートの証明書を更新する

Microsoftは2011年に発行されたセキュアブート証明書の提供を2026年6月に終了し、新しい2023年の証明書に切り替えます。レコーダーを安全に保つため、有効期限までに2023年の証明書をインストールしてください。

2023年の証明書のインストールには、Windows 10 LTSC (Long-Term Servicing Channel) または Windows 11 LTSCが必要です。使用しているデバイスが保証期間内であるにもかかわらず、LTSCバージョンではなくWindows 10 SAC (Semi-Annual Channel) が動作している場合は、Axis Technical Supportにお問い合わせください。BIOSの更新や証明書の変更を行う前に、LTSCバージョンにアップグレード可能かどうかをお知らせします。

注

2026年6月以降、2023年の証明書を持たないデバイスは、引き続き通常通り動作しますが、Windows Boot Managerの更新や新たな脆弱性に対する失効リストなど、初期ブートプロセスに対する新しいセキュリティ保護は提供されません。

証明書のステータスを確認する

以下の方法で、2023年の証明書がインストールされており、Windowsのブートローダーが更新されていることを確認します。

方法1:

1. [Registry Editor (レジストリエディタ)] を開きます。
2. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicingに移動します。
3. UEFICA2023Statusの値を確認します。値が「Updated (更新済み)」となっている場合、2023年の証明書がインストールされています。

ab (Default)	REG_SZ	(value not set)
ab BucketHash	REG_SZ	5a3041a8e6c7476f988f369de06e65e224df7d53cf7f9...
ab ConfidenceLevel	REG_SZ	No Data Observed - Action Required
oi ConfidenceUpdateType	REG_DWORD	0x00000000 (0)
oi LastParsedBucketDataVersion	REG_DWORD	0x0000000c (12)
ab UEFICA2023Status	REG_SZ	Updated
oi WindowsUEFICA2023Capable	REG_DWORD	0x00000002 (2)

方法2:

1. [Windows Security (Windowsセキュリティ)] を開きます。
2. [Device security (デバイスセキュリティ)] に移動します。
3. [Secure boot (セキュアブート)] で、ステータスメッセージを確認します。証明書が最新の場合、カードに“Secure Boot is on and all required certificate updates have been applied. No further certificate changes are needed”(セキュアブートがオンになっており、必要なすべての証明書の更新が適用されました。これ以上の証明書の変更は必要ありません) と表示されます。

Secure boot

Secure Boot is on and all required certificate updates have been applied.
No further certificate changes are needed.

注

Windowsセキュリティは、デバイスに2026年4月14日付けの累積更新プログラム以降がインストールされている場合のみ、証明書のステータスを表示します。証明書のステータスに関するメッセージが表示されない場合は、最新のWindows更新プログラムをインストールするか、代わりに方法1をお試しください。

推奨されるアクション

BIOSアップデートにより、2023年の証明書がファームウェアに永続的に保存されます。これが最も信頼性の高い方法であるため、Windows Updateを通じてすでに証明書をインストール済みの場合もこの方法をお勧めします。

重要

Windows Updateを通じて証明書をインストールしただけでは、その後、BIOSのセキュアブートキーを工場出荷時の設定にリセットすると、証明書が失われ、セキュアブートがオンになっている状態ではデバイスが起動しなくなります。セキュアブートキーをリセットする前に、BIOSを更新して証明書を永続化してください。

BIOSを通じて証明書を更新する

使用しているモデルに対応するBIOSバージョン、またはそれ以降のバージョンをインストールしてください。これらは、Axis.comの製品ページからダウンロードできます。

モデル	BIOSの最低バージョン
AXIS S2208	TBC
AXIS S2212	TBC
AXIS S2216	TBC
AXIS S2224	TBC
AXIS S2108	Z218-004
AXIS S2208 Mk II	Z670-005
AXIS S2212 Mk II	Z671-005
AXIS S2216 Mk II	Z672-005
AXIS S2224 Mk II	Z673-005

Windows Updateを通じて証明書を更新する

使用しているモデルでBIOSアップデートがまだ提供されていない場合は、代わりにWindows Updateを通じて2023年の証明書を入手することができます。

重要

この方法でインストールされた証明書は、ファームウェアではなく、現在のセキュアブートデータベースに保存されます。BIOSのセキュアブートキーを工場出荷時の設定にリセットすると、証明書が失われ、セキュアブートがオンになっている状態ではデバイスが起動できなくなる可能性があります。この方法をすでに使用している場合も、モデルのBIOSアップデートが利用可能になり次第、インストールしてください。

以下のパスに従って使用します。

1. 使用しているデバイスがWindows 10 LTSCまたは Windows 11 LTSCを実行していることを確認します。
2. 2026年4月14日以降にリリースされたすべてのWindows更新プログラムをインストールします。

3. [Windows Security (Windowsセキュリティ)] > [Device security (デバイスセキュリティ)] > [Secure Boot (セキュアブート)] に移動して、証明書のステータスを確認します。
4. 最新の更新プログラムをインストールしても証明書が更新されない場合は、レジストリ値 **UEFICA2023Status**を確認します。使用しているデバイスで自動アップデートができない場合は、BIOSを更新するか、Axis Technical Supportにお問い合わせください。

重要

使用環境のすべてのリカバリメディア、ブート環境、およびドライバーが2023年の証明書によって署名されていることを確認するまでは、2011年の証明書を手動で取り消さないでください。その前に2011年の証明書を取り消すと、セキュアブートがオンになっている状態でデバイスを起動できなくなります。

現在のBIOSのバージョンを確認する

現在のBIOSを確認するには:

1. デバイスの電源を入れ、Axisロゴが表示されるまでDELキーを繰り返し押します。
2. [Main (メイン)] の最初の項目として、バージョン番号が表示されます。

BIOSを更新する

BIOSファイルのダウンロードページに掲載されているBIOSガイドに記載されている手順に従ってください。

Windows®を更新します

Windows®は定期的に更新プログラムをチェックします。更新プログラムが利用可能になると、デバイスは自動的に更新プログラムをダウンロードしますが、インストールは手動で行う必要があります。

注

スケジュールされたシステムの再起動中に録画が中断されます。

更新プログラムを手動で確認するには、次の手順を実行します。

1. [Settings (設定)] > [Windows Update (Windows更新プログラム)] に移動します。
2. [Check for updates (クリックして更新)] をクリックします。

Windows®の更新プログラムの設定を構成する

必要に応じて、Windows®の更新プログラムを実行する方法とタイミングを変更できます。

注

スケジュールされたシステムの再起動中に、進行中のすべての録画が停止します。

1. 実行アプリを開きます。
 - [Windows System (Windowsシステム)] > [Run (実行)] に移動するか、
2. 「gpedit.msc」と入力して、[OK] をクリックします。Local Group Policy Editor (ローカルグループポリシーエディター) が開きます。
3. [Computer Configuration (コンピューターの構成)] > [Administrative Templates (管理用テンプレート)] > [Windows Components (Windowsコンポーネント)] > [Windows Update (Windows更新プログラム)] の順に移動します。
4. 必要に応じて設定を構成します (例を参照)。

例:

ユーザーの操作なしで更新プログラムを自動的にダウンロードしてインストールし、必要に応じて営業時間外に装置を再起動するには、次の設定を使用します。

1. [Always automatically restart at the scheduled time (常にスケジュールされた時刻に自動的に再起動する)] を開き、次のいずれかを選択します。
 - 1.1. オン
 - 1.2. 再起動タイマーにより、ユーザーには作業を保存する15分間の時間的猶予があります。
 - 1.3. [OK] をクリックします。
2. [Configure Automatic Updates (自動更新の構成)] を開き、次の項目を選択します。
 - 2.1. オン
 - 2.2. Configure Automatic updates (自動更新を構成する):自動ダウンロードとインストールのスケジュール設定
 - 2.3. Schedule Install day (インストール日のスケジュール):毎週日曜日
 - 2.4. Schedule Install time (インストール時刻のスケジュール): 00:00
 - 2.5. [OK] をクリックします。
3. [Allow Automatic Updates immediate installation (自動更新を直ちにインストールする)] を開き、次を選択します。
 - 3.1. オン
 - 3.2. [OK] をクリックします。

電力管理

このスイッチの総電源容量は105 Wです。これは、接続されているすべての装置に出力される最大電力です。

ほとんどの場合、接続された装置は要求電力よりも少ない電力を消費します。電力使用量を最適化するために、PoEコントローラーは、接続された装置が最大125 Wまで要求できるようにすると同時に、実際の電力使用量を105 Wに制限します。

たとえば、スイッチが8台のPoE Class 3装置に電力を供給するとします。

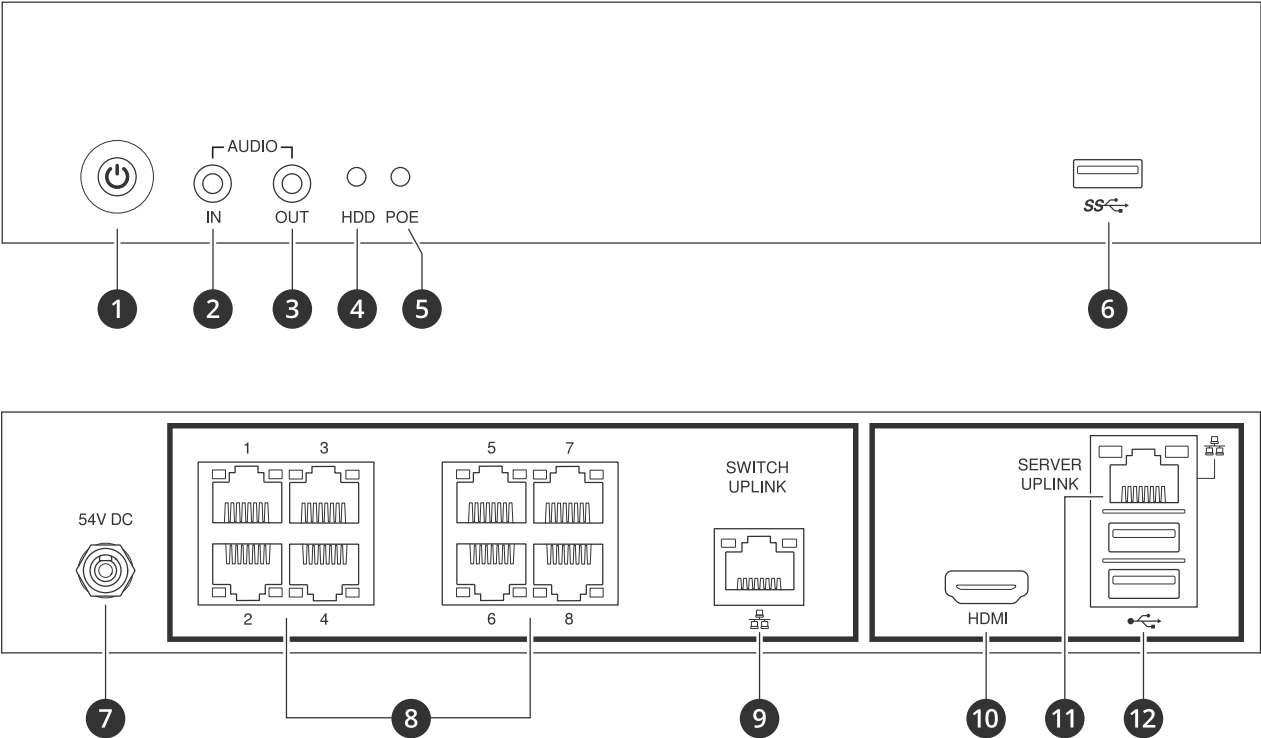
- 1台のPoE Class 3装置は15.4 Wの電力を要求します。
- 8台のPoE Class 3装置は $(8 \times 15.4) = 123.2$ Wの電力を要求します。これは、PoEコントローラーで許容される125 Wの制限内です。
- 1台のPoE Class 3装置は通常10～12 Wの電力を消費します。
- 8台のPoE Class 3装置は通常80～96 Wの電力を消費します。これは、総電源容量の105 Wの制限内です。

▲ 警告

- 接続された装置が125 Wを超える電力を要求した場合:
 - 最後に接続された装置は起動しません。
 - 最後に接続された装置を取り外すか、他の装置を取り外すことで十分なPoE電源容量を確保するまで、PoE過負荷LEDは赤色に点灯します。
- 接続されている装置が実際に105 Wを超える電力を消費している場合:
 - 最後に電源を入れた装置がシャットダウンされ、再起動を試みます。
 - PoE過負荷LEDは点灯しません。

製品概要

前面と背面



- 1 電源ボタン/電源LED
- 2 音声入力
- 3 音声出力
- 4 ハードドライブアクティビティLED
- 5 PoEポートのステータスLED
- 6 USB 3.0ポート
- 7 電源コネクタ
- 8 PoEポート
- 9 RJ45スイッチアップリンクポート
- 10 HDMIポート
- 11 RJ45サーバーアップリンクポート
- 12 USB 2.0ポート

仕様

フロントLED

LEDインジケーター	カラー	説明
電源	緑	サーバー上
ハードドライブ	黄点滅	ハードドライブのアクティビティ
	赤点滅	考えられるハードドライブの障害
PoE過負荷	赤	PoE電源容量超過
	オフ	OK

リアLED

ネットワークの速度とアクティビティ	カラー	説明
右LED	オレンジ	10/100 Mbit/秒
	緑 ¹	1000 Mbit/秒
左LED	緑点滅	ネットワーク状態

1. これはスイッチアップリンクとサーバーアップリンクに対してのみ有効です。

トラブルシューティング

システムリカバリの実行

デバイスで完全なシステム障害が発生した場合は、回復イメージを使用してWindows® システムを再作成する必要があります。AXIS Network Video Recorder Recovery Kitをダウンロードするには、Axisの技術サポートに連絡し、お使いの装置のシリアル番号を知らせてください。

注

AXIS Network Video Recorder Recovery Kitには、以下の2つのバージョンがあります。

- **sb11** — 2011年の証明書を使用しているデバイス向けです。
- **sb23** — 2023年の証明書に移行したデバイス向けです。

Recovery Kitをダウンロードする前に、証明書のステータスを確認し、それに応じたバージョンを選択してください。間違ったバージョンを選択すると、インストール後に起動できず、正しい画像で最初からやり直す必要があります。これによってデバイスが損傷することはありません。

デバイスにすでに2023年の証明書がインストールされている場合、2011年の証明書を手動で失効していない限り、sb11バージョンは引き続き安全に使用できます。失効すると、sb23のみが機能します。

システムを再作成するには:

1. AXIS Network Video Recorder Recovery KitとAXIS Network Video Recorder Recovery: ISO to USB Toolをダウンロードします。
2. USBドライブをコンピューターに挿入します。
 - 16 GBのUSBドライブを使用します。
 - USBドライブがフォーマットされ、既存のデータはすべて消去されます。
3. AXIS Network Video Recorder Recovery: ISO to USB Toolを実行し、画面の指示に従います。USBドライブへのデータの書き込みには約10～15分かかります。
4. AXIS Network Video Recorder Recovery: ISO to USB Toolが完了したら、USBドライブを取り出してデバイスに接続します。
5. デバイスを起動します。
6. Axisのスプラッシュ画面が表示されたら、F12キーを押します。
7. **[UEFI: USB Drive (UEFI : USBドライブ)]** をクリックします。
8. USBドライブに移動し、enterキーを押します。システムがAXIS Network Video Recorder Recovery Kitで起動します。
9. **[Reinstall Operating System (オペレーティングシステムの再インストール)]** をクリックします。
リカバリが完了するまでに約10～15分かかります。詳細な手順については、回復キットのダウンロードを参照してください。

AXIS Camera Stationのトラブルシューティング

AXIS Camera Stationのトラブルシューティング方法については、*AXIS Camera Station*のユーザーズマニュアルを参照してください。

さらに支援が必要ですか？

参考リンク

- [AXIS Camera Station ユーザーズマニュアル](#)
- [AXIS セキュアリモートアクセスにサインイン](#)
- [AXIS Camera Station のウイルス対策許可リストに含める内容](#)

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。

T10181903_ja

2026-07 (M7.2)

© 2022 – 2026 Axis Communications AB