

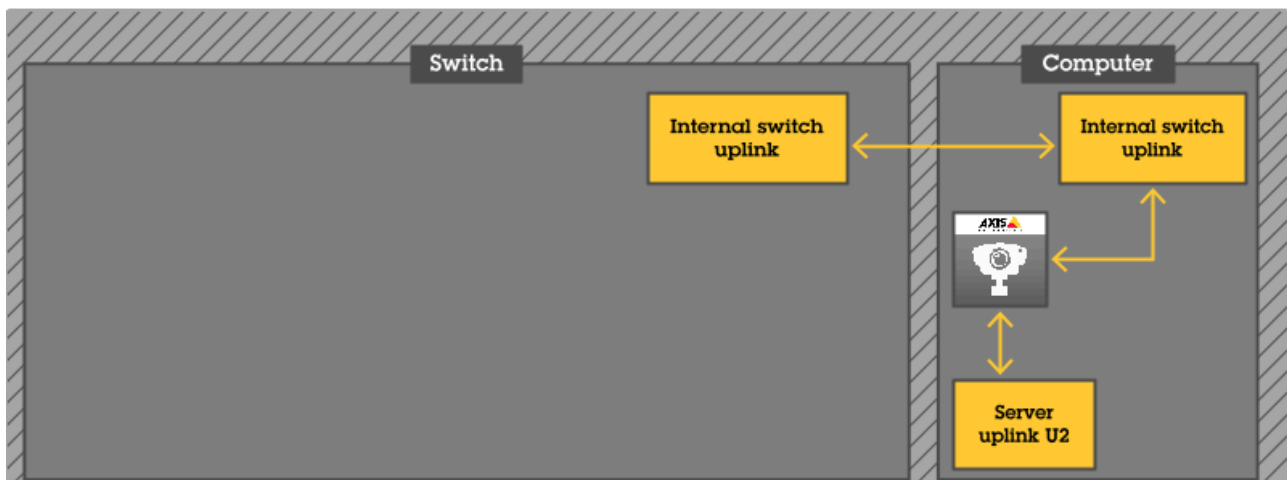
AXIS Camera Station S2108 Appliance

Über das Gerät

AXIS Camera Station S2108 Appliance ist eine All-in-One-Aufzeichnungslösung mit integriertem PoE-Switch und ist für eine zuverlässige Überwachung in hoher Auflösung mit Kameras bis zu 4K ausgelegt. Für eine schnelle und einfache Installation ist das Geräte vorkonfiguriert und mit der Videoverwaltungssoftware AXIS Camera Station einschließlich Lizenzen sowie der gesamten erforderlichen Systemsoftware vorinstalliert. AXIS Camera Station bietet eine intuitive Benutzeroberfläche, mit der Benutzer die breite Palette an Videoüberwachungskameras und anderen IP-Produkten von Axis optimal nutzen können. Das Gerät verfügt über ein Solid-State-Laufwerk (SSD), auf dem das Betriebssystem gespeichert ist, und bietet 5 Jahre Gewährleistung auf die Hardware. Es stellt eine zuverlässige Überwachungslösung dar.

AXIS Camera Station S2108 Appliance besteht aus zwei Teilen:

- **Switch:** Integrierter Power over Ethernet (PoE)-Switch.
- **Computer:** Wird mit der notwendigen Software ausgeliefert, die Sie zur Erstellung einer Überwachungslösung benötigen, einschließlich der Video Management Software AXIS Camera Station.

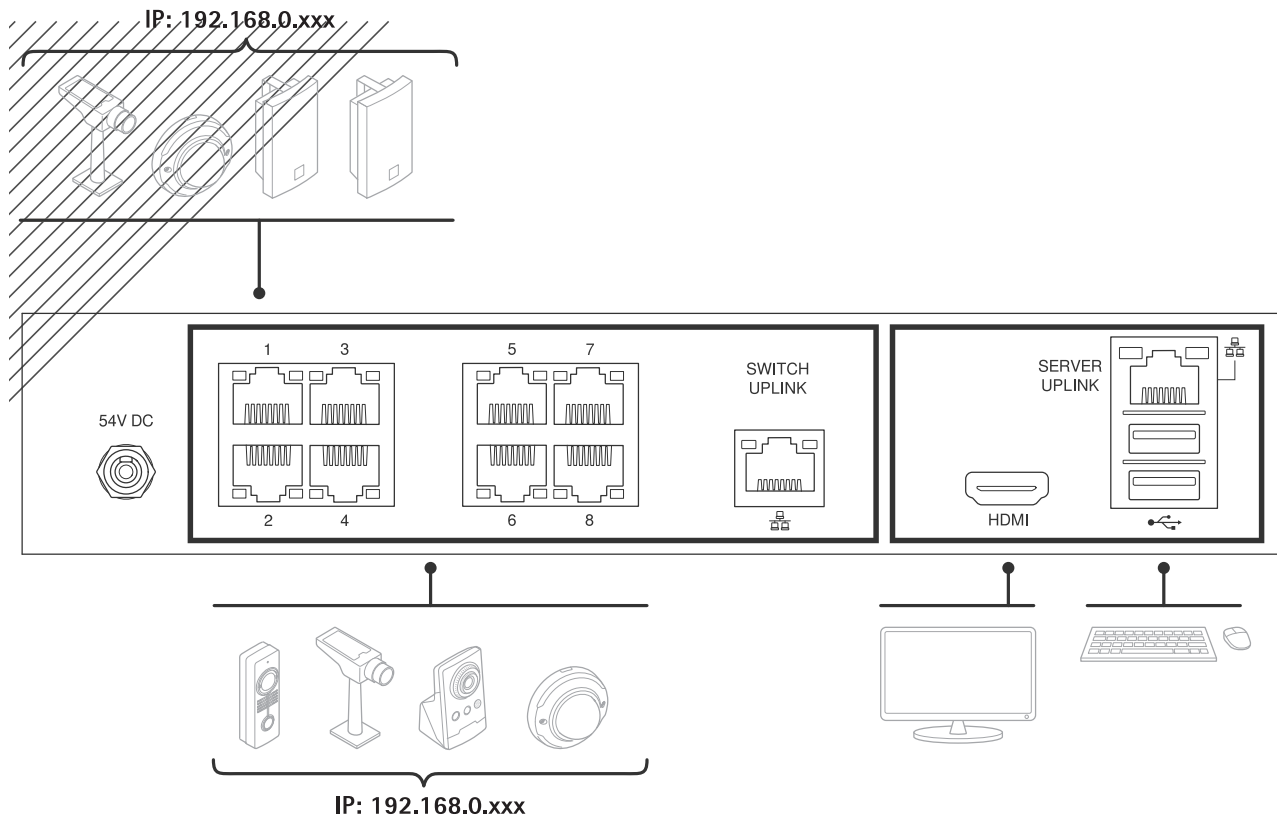


- Der Switch und der Computer sind zwei verschiedene Teile.
- Der Switch und der Computer kommunizieren über die internen Uplink-Anschlüsse: einer befindet sich auf der Netzplatine des Switches, der andere auf der Hauptplatine des Computers.
- Der Serveruplink ist eine externe Netzwerk-Schnittstelle, die eine Verbindung mit einem vorhandenen Netzwerk herstellen kann.
- Mit dem Serveruplink verbundene Geräte können nicht mit Geräten kommunizieren, die direkt mit dem Switch verbunden sind.
- Mit dem Serveruplink verbundene Geräte können über AXIS Camera Station mit Geräten kommunizieren, die mit dem Switch verbunden sind.

Setup-Beispiele

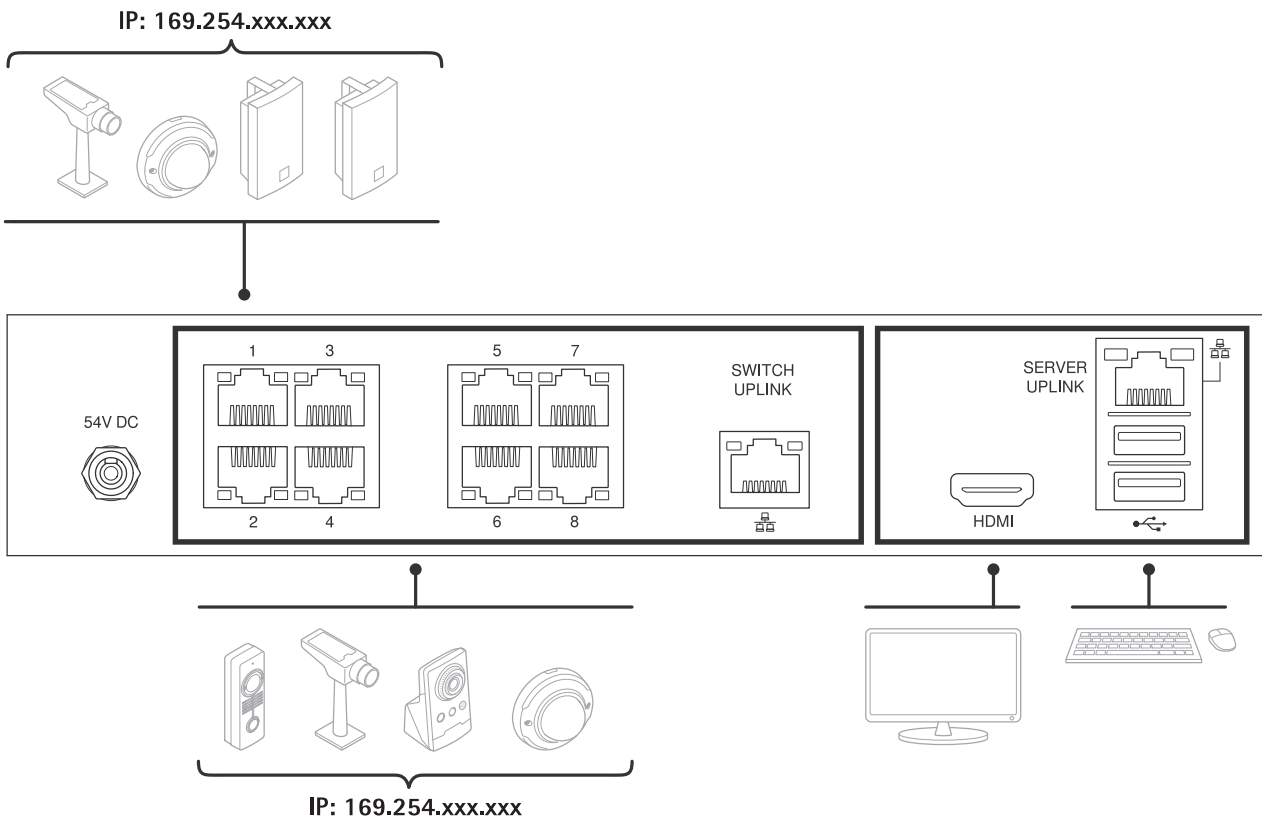
Jedem Gerät eine statische Adresse zuweisen

Sie können ein unabhängiges Netzwerk erstellen, indem Sie jedem Gerät und der AXIS S2108-Einheit statische IP-Adressen zuweisen. Dieses Netzwerk ist nur dann mit einem anderen externen Netzwerk verbunden, wenn die Parameter der beiden Netzwerke übereinstimmen. Über den Uplink-Port des Servers kann der Computer weiterhin eine Internetverbindung herstellen. Sobald die Geräte an die eingeschalteten PoE-Ports angeschlossen sind, wird die verbindungslokale Adresse angezeigt, und es wird ein fester IP-Satz benötigt, der mit der AXIS S2108-Einheit übereinstimmt.



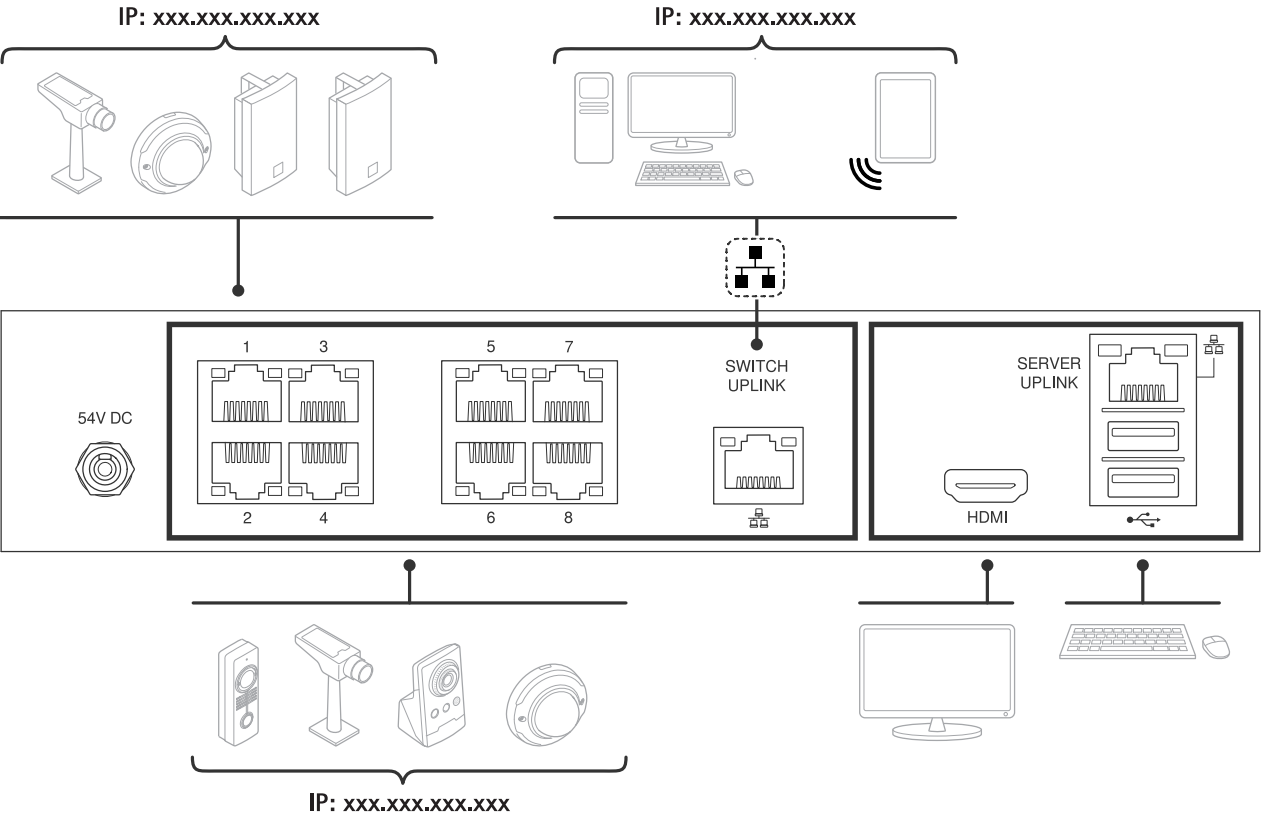
Lokale Adresse verwenden

Sie können ein unabhängiges Netzwerk erstellen, indem Sie auf jedem Gerät und der AXIS S2108-Einheit eine verbindungslokale Linkadresse verwenden. Dieses Netzwerk ist nicht mit einem anderen externen Netzwerk verbunden. Über den Uplink-Port des Servers kann der Computer weiterhin eine Internetverbindung herstellen. Sobald die Geräte an die eingeschalteten PoE-Ports angeschlossen sind, werden sie mit der verbindungslokalen Adresse verbunden und können von AXIS Camera Station auf dem AXIS S2108-Gerät gefunden werden.



Verwenden eines DHCP-Servers aus einem anderen Netzwerk

Sie können das AXIS S2108 mit den angeschlossenen Geräten verbinden, indem Sie ein bestehendes Netzwerk und einen DHCP-Server an den Switch-Uplink anschließen. Dadurch erhalten alle verbundenen Geräte eine IP-Adresse aus dem DHCP-Serverbereich. Wenn in diesem Netzwerk eine Internetverbindung vorhanden ist, ist sie auch für das AXIS S2108-Gerät verfügbar. Ansonsten kann der Computer weiterhin über den Uplink-Port des Servers eine Internetverbindung herstellen. Wenn die Geräte an die eingeschalteten PoE-Ports angeschlossen sind, wird ihnen die DHCP-Adresse zugewiesen, wenn der DHCP-Server aktiv ist.



Funktionsweise

Der Standardworkflow zum Konfigurieren eines AXIS Camera Station Recording Servers ist:

1. *Das Gerät installieren*
2. Erstes Windows®-Setup: Nach der Installation Ihres Geräts werden Sie durch einige Schritte geführt, um die Region, die Sprache, das Tastaturlayout, ein Administratorkonto und dessen Passwort einzurichten.
3. Erstes Setup des AXIS Recorders: Nach der Ersteinrichtung von Windows wird die AXIS Recorder Toolbox geöffnet, und Sie werden durch einige Schritte geführt, um grundlegende und notwendige Einstellungen vorzunehmen, z. B. Computername, Datum und Uhrzeit sowie Netzwerk. Siehe *Erstes Setup des Axis Recorders, on page 15*.
4. Windows® konfigurieren. Wir empfehlen:
 - Windows® auf die neuste Version aktualisieren. Siehe .
 - Ein Standardbenutzerkonto erstellen. Siehe *Ein Benutzerkonto erstellen, on page 21*.
5. AXIS Camera Station auf die neuste Version aktualisieren.
 - Wenn Ihr System online ist: Die AXIS Recorder Toolbox-App öffnen und auf **Update AXIS Camera Station** (AXIS Camera Station One aktualisieren) klicken.
 - Wenn Ihr System offline ist: *axis.com* aufrufen und die neueste Version herunterladen.
6. Starten Sie den AXIS Camera Station-Client.
7. *Verbindung zum Server der AXIS Camera Station herstellen*
8. *AXIS Camera Station konfigurieren, on page 17*

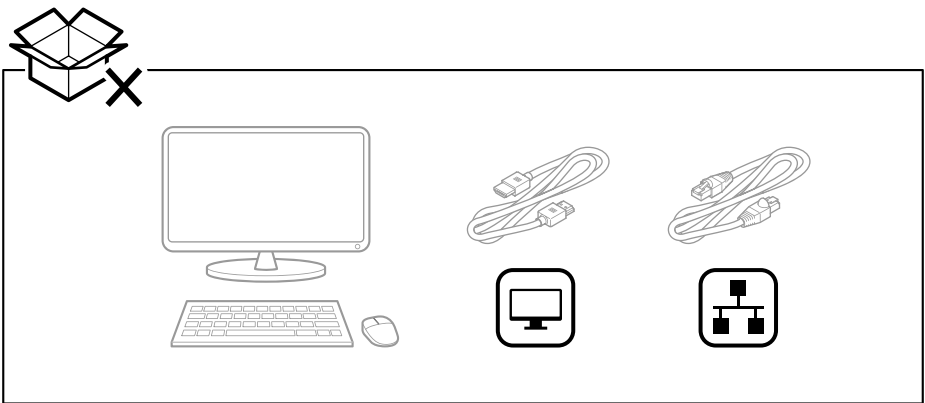
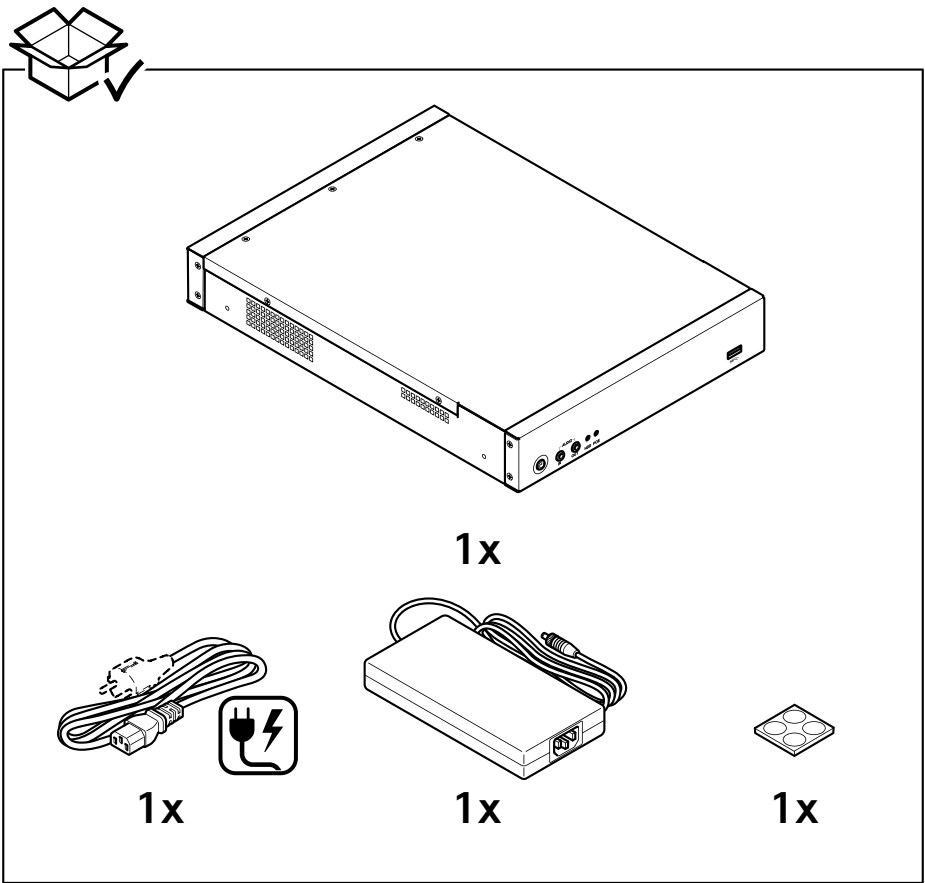
Das Gerät installieren

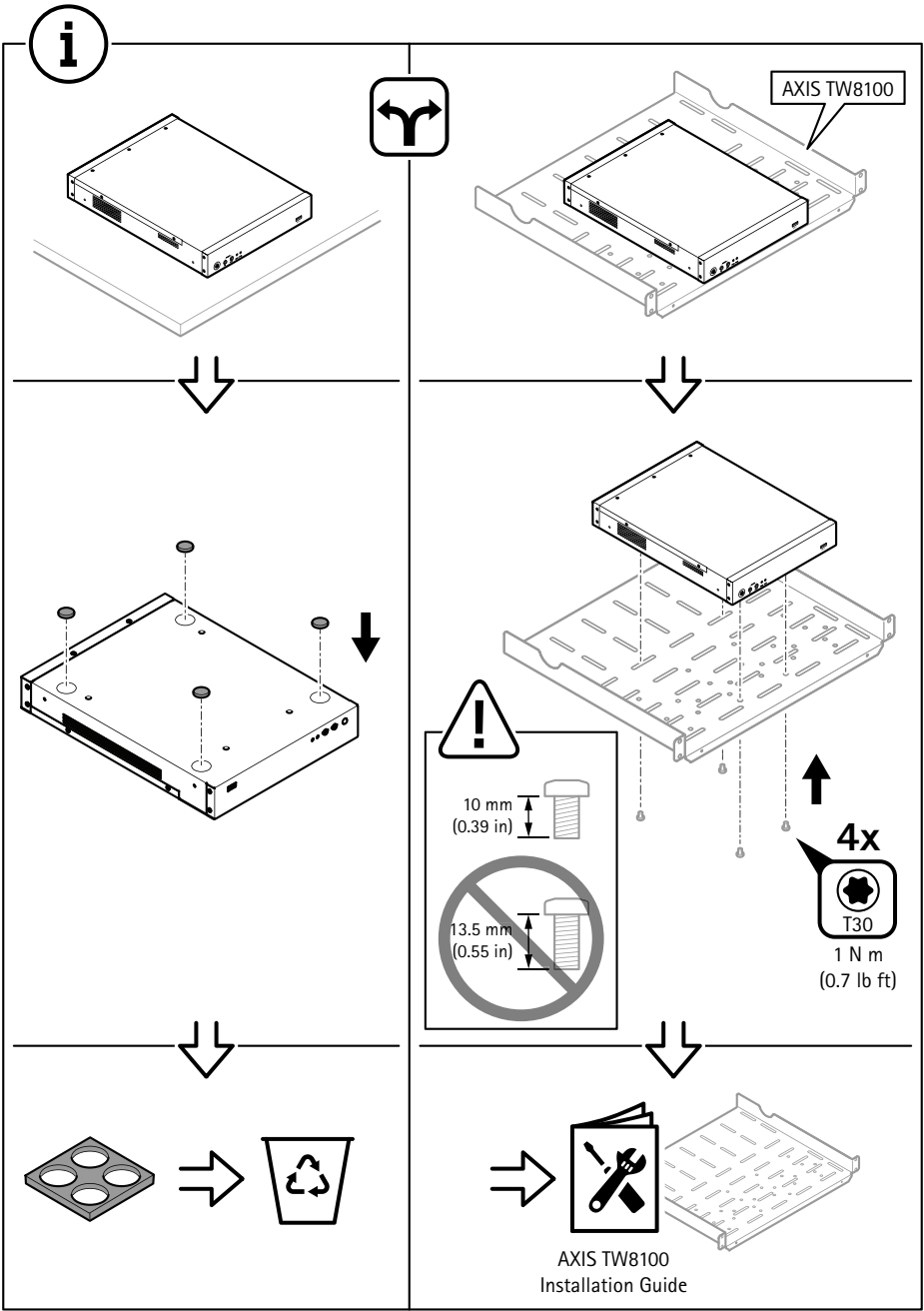
Vor der Installation

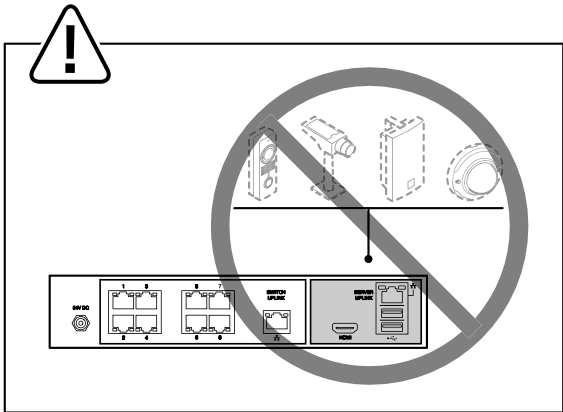
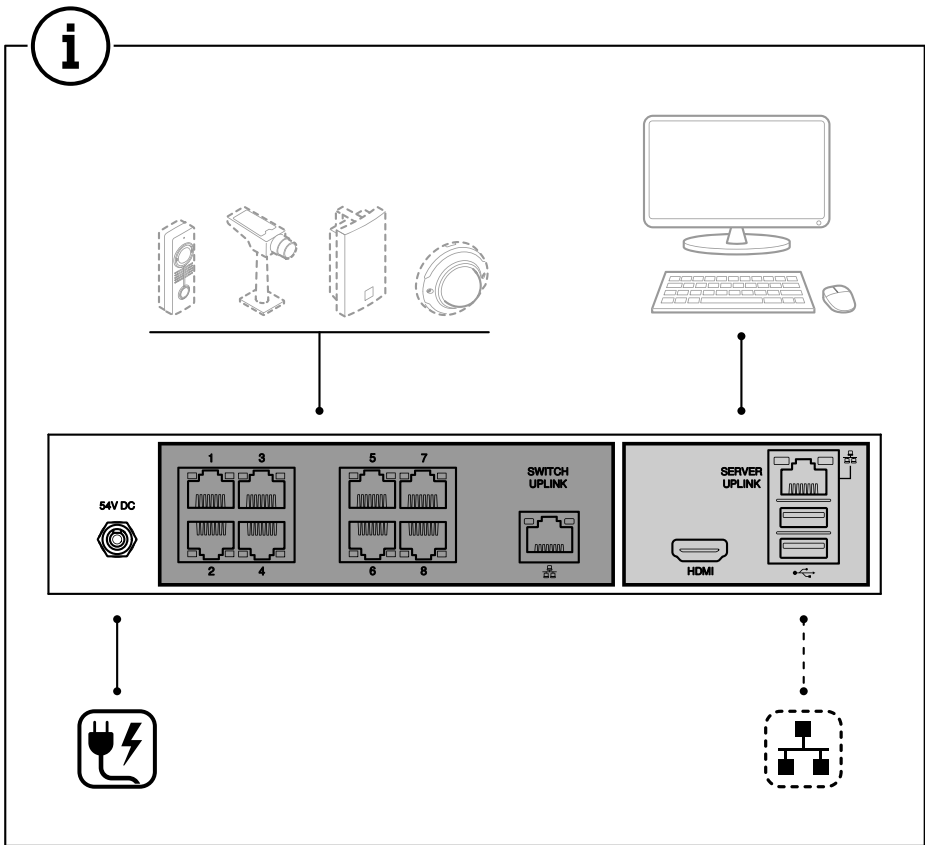
- Bereiten Sie weiteres Zubehör für die Installation vor: Monitor, Maus, Tastatur und Netzkabel.
- Die Verwendung verschiedener Benutzerkonten verstehen.

In der folgenden Tabelle sind die Benutzerkonten aufgeführt, die für die Installation, Konfiguration und den Betrieb Ihres AXIS Systems verwendet werden können.

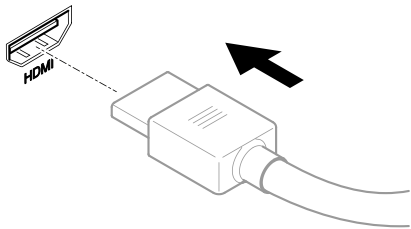
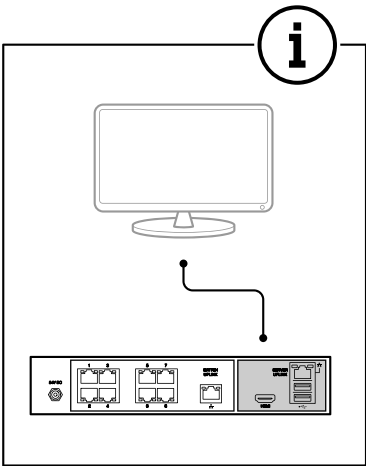
Benutzerkonto	Beschreibung	Hinweis
MyAxis	Wird verwendet, um die neueste Software herunterzuladen und auf das Lizenzsystem, AXIS Secure Remote Access und System Health Monitoring zuzugreifen.	Registriert von <i>my.axis.com</i> .
Windows®		
Windows®-Administrator	Administratorrechte in Windows®. Wir empfehlen Ihnen, dies nicht als AXIS Camera Station Administrator zu verwenden.	Erstellt während des ersten Windows®-Setups.
Windows®-Benutzer mit AXIS Camera Station Administratorrechten	Ein Windows®-Benutzer mit Administratorrechten in AXIS Camera Station, der von einem Systemintegrator oder Systemadministrator zur Konfiguration oder Fehlerbehebung verwendet werden kann.	In Windows®-Einstellungen erstellt.
Windows®-Benutzer mit Bediener- oder Betrachterrechten in AXIS Camera Station.	Ein Windows®-Benutzer mit Bediener- oder Betrachterrechten in AXIS Camera Station.	In Windows®-Einstellungen erstellt.
Gerät		
Geräteadministrator	Wird vom Administrator für den Zugriff auf die Kamera über das Video Management System oder die Webseite des Geräts verwendet.	Erstellt von der Gerätewebseite oder beim Hinzufügen des Geräts zur AXIS Camera Station.



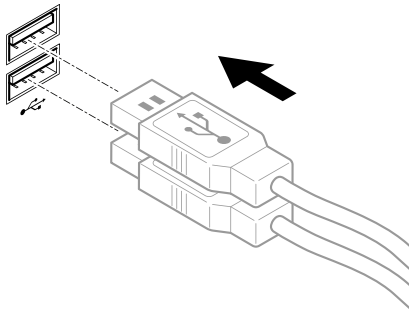
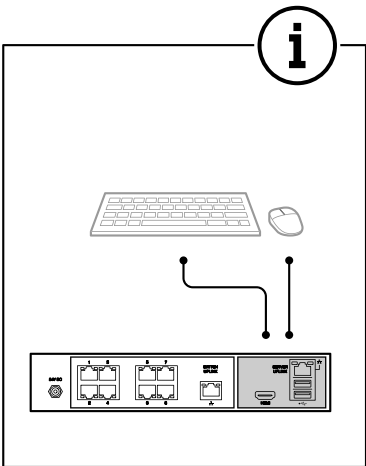




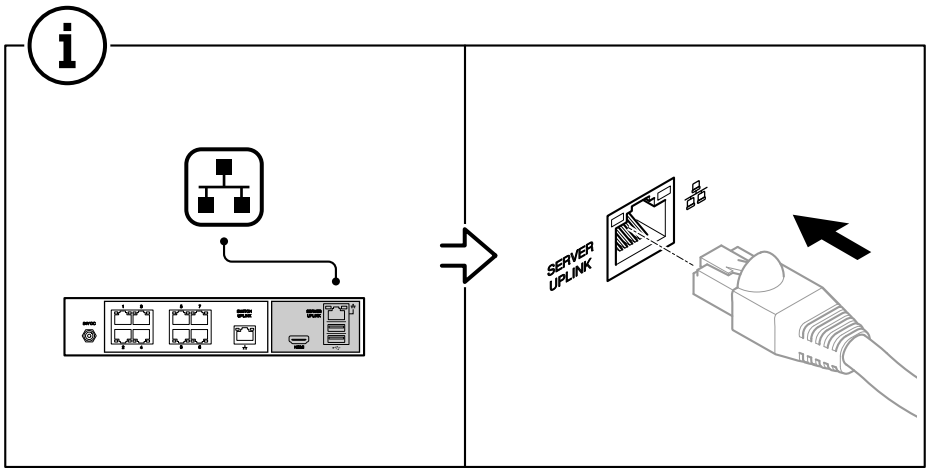
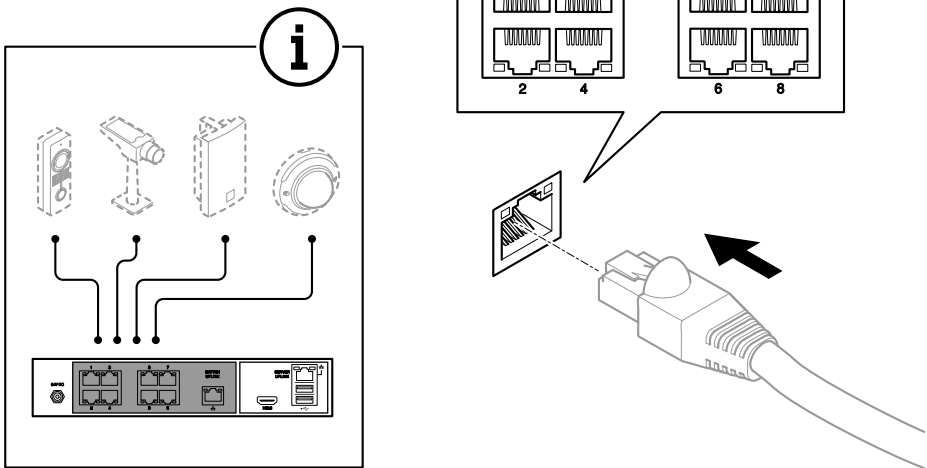
1.1



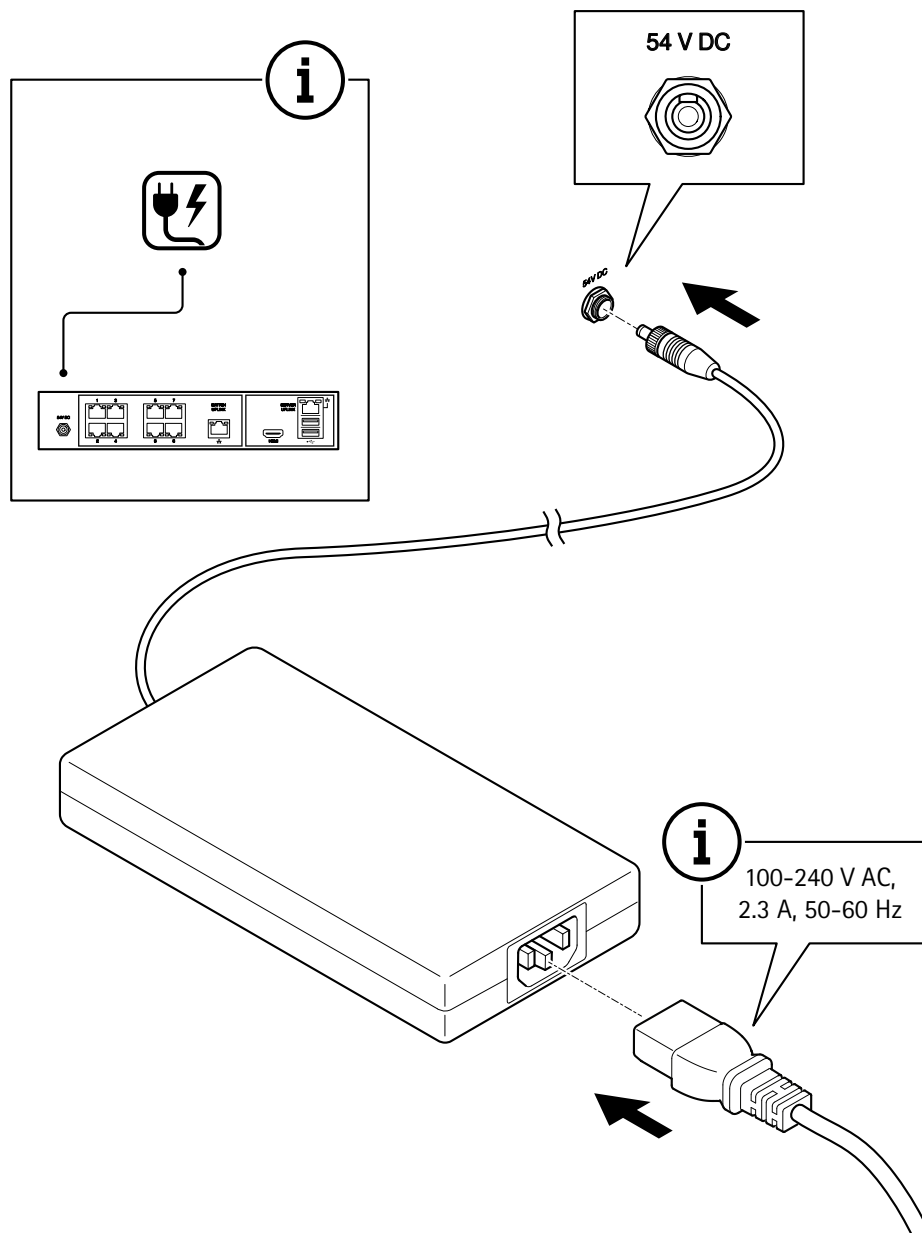
1.2



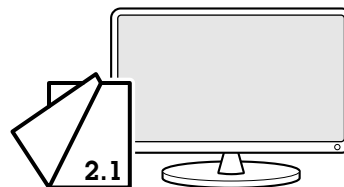
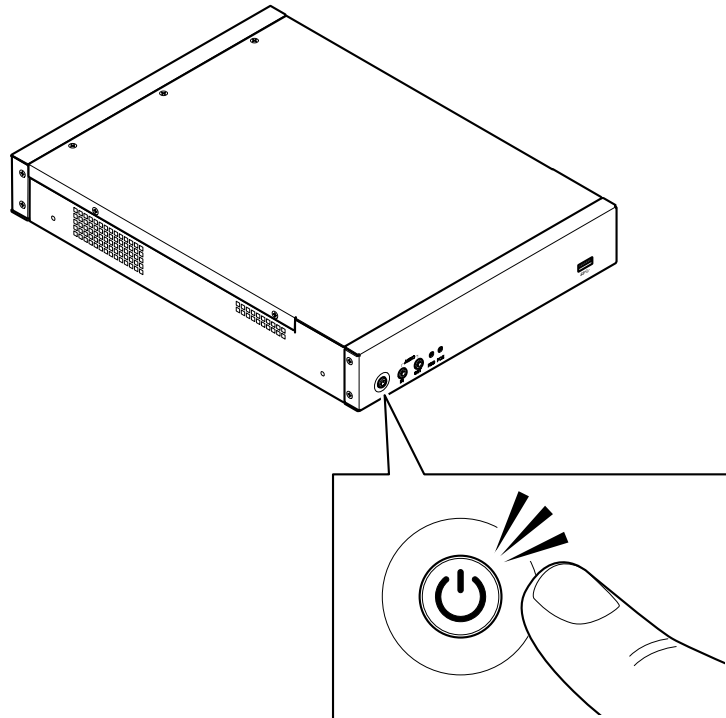
1.3



1.4



1.5



Ihr Gerät konfigurieren

Erstes Setup des Axis Recorders

Nach der Konfiguration von Windows® wird AXIS Recorder Toolbox automatisch geöffnet und Sie werden durch den Setup-Assistenten für die Erstkonfiguration geführt. Mit diesem Setup-Assistenten können Sie mehrere grundlegende und erforderliche Einstellungen konfigurieren, bevor Sie Ihr Gerät in AXIS Recorder Toolbox verwalten.

1. Wählen Sie als Erscheinungsbild **Light (Hell)** oder **Dark (Dunkel)**, und klicken Sie auf **Next (Weiter)**,, sofern Ihr Produkt diese Möglichkeit bietet.
2. Ändern Sie ggf. den Computernamen und klicken Sie auf **Weiter**.
3. Konfigurieren Sie unter **Date and time (Datum und Uhrzeit)** die folgenden Einstellungen und klicken Sie auf **Weiter**.
 - Wählen Sie eine Zeitzone.
 - **NTP server (NTP-Server)** auswählen, um einen NTP-Server einzurichten, und die NTP-Server-Adresse eingeben.
 - Wählen Sie zum manuellen Einstellen **Manual (Manuell)** aus und wählen Sie Datum und Uhrzeit aus.
4. Konfigurieren Sie unter **Network settings (Netzwerkeinstellungen)** die folgenden Einstellungen und klicken Sie auf **Weiter**.
 - **Automatische IP-Einstellungen (DHCP) verwenden** und **Automatische DNS-Einstellungen verwenden** sind standardmäßig aktiviert.
 - Wenn Ihr Gerät mit einem Netzwerk mit einem DHCP-Server verbunden ist, werden die zugewiesene IP-Adresse, Subnetzmaske, das Gateway und das bevorzugte DNS automatisch angezeigt.
 - Wenn Ihr Gerät nicht mit einem Netzwerk verbunden ist oder kein DHCP-Server verfügbar ist, geben Sie die IP-Adresse, die Subnetzmaske, das Gateway und das bevorzugte DNS je nach Netzwerkanforderungen ein.
5. Klicken Sie auf **Finish (Fertig)**. Wenn Sie den Computernamen geändert haben, werden Sie von AXIS Recorder Toolbox zum Neustart des Geräts aufgefordert.

Am Server anmelden

Mit dem AXIS Camera Station Client kann eine Verbindung zu einem mehreren Servern oder einem einzelnen Server, installiert auf dem lokalen Computer oder an einer anderen Stelle im Netzwerk, aufgebaut werden. Die Verbindung mit Servern von AXIS Camera Station ist auf verschiedene Weise möglich:

Zuletzt verwendete Server – Stellt eine Verbindung zu den Servern her, die in der vorherigen Sitzung verwendet wurden.

Dieser Computer – Stellt eine Verbindung zu dem Server her, der auf demselben Computer wie der Client installiert ist.

Remote-Server – Siehe *Mit einem Remote-Server verbinden, on page 16*.

AXIS Secure Remote Access – Siehe *Bei AXIS Secure Remote Access anmelden, on page 16*.

Hinweis

Beim ersten Verbindungsversuch mit einem Server prüft der Client die Serverzertifikat-ID. Um sicherzustellen, dass eine Verbindung mit dem richtigen Server hergestellt wird, die Zertifikat-ID manuell mit der in AXIS Camera Station Service Control angezeigten prüfen.

Server-Liste	Um eine Verbindung mit Servern aus einer Serverliste herzustellen, wählen Sie einen aus dem Drop-down Menü Server list (Serverliste) aus. Klicken Sie  , um Server-Listen zu bearbeiten.
Serverliste importieren	Es ist möglich, eine Server-Listendatei zu importieren, die aus der AXIS Camera Station exportiert wurde. Dafür klicken Sie Import server list (Server-Liste importieren) und suchen Sie nach einer .msl-Datei.
Gespeicherte Kennwörter löschen	Um die gespeicherten Benutzernamen und Kennwörter aller verbundenen Server zu löschen, klicken Sie auf Delete saved passwords (Gespeicherte Kennwörter löschen) .
Proxy-Einstellungen des Klienten ändern	Sie müssen möglicherweise die Client-Proxyeinstellungen ändern, um eine Verbindung mit einem Server herzustellen. Klicken Sie auf Change client proxy settings (Client-Proxyeinstellungen ändern) .

Mit einem Remote-Server verbinden

1. Remote-Server wählen.
2. Wählen Sie einen Server aus dem Auswahlmenü **Remote-Server** oder geben Sie die IP-Adresse oder DNS-Adresse in das Feld ein. Falls der Server nicht aufgeführt ist, klicken Sie auf , um die Liste aller verfügbaren Remote-Server zu aktualisieren. Wenn der Server so konfiguriert ist, dass er Clients auf einem anderen Port als dem Standardport 55754 zulässt, geben Sie die IP-Adresse gefolgt von der Portnummer ein, z. B.: 192.168.0.5:46001.
3. Einen der folgenden Schritte durchführen:
 - Wählen Sie **Log in as current user (Als aktueller Benutzer anmelden)**, um sich als der aktuelle Windows®-Benutzer anzumelden.
 - Leeren Sie das Feld **Als aktueller Benutzer anmelden** und klicken Sie auf **Anmelden**. Wählen Sie **Other user (Anderer Benutzer)** und geben Sie einen anderen Benutzernamen und Kennwort ein, um sich mit anderen Zugangsdaten anzumelden.

Bei AXIS Secure Remote Access anmelden

Wichtig

Um die Sicherheit und Funktionalität zu verbessern, führen wir ein Update von **Axis Secure Remote Access (v1)** auf **Axis Secure Remote Access v2** durch. Die aktuelle Version wird am 1. Dezember 2025 eingestellt, und wir empfehlen Ihnen dringend, vor diesem Zeitpunkt zu Axis Secure Remote Access v2 zu wechseln.

Was bedeutet das für Ihr AXIS Camera Station S2108 Appliance System?

- Nach dem 1. Dezember 2025 können Sie nicht mehr über **Axis Secure Remote Access (v1)** auf Ihr System zugreifen.
- Um **Axis Secure Remote Access v2** nutzen zu können, müssen Sie ein Upgrade auf AXIS Camera Station Pro Version 6.8 durchführen. Diese Aktualisierung ist derzeit für alle Benutzer von AXIS Camera Station 5 bis zum 1. März 2026 kostenlos.

Hinweis

- Beim Versuch, eine Verbindung über Axis Secure Remote Access mit einem Server herzustellen, kann der Server den Client nicht automatisch aktualisieren.
- Wenn sich der Proxy-Server zwischen dem Netzwerkgerät und dem AXIS Camera Station S2108 Appliance-Server befindet, müssen Sie die Proxy-Einstellungen in Windows auf dem AXIS Camera

Station S2108 Appliance-Server konfigurieren, um mit AXIS Secure Remote Access auf den Server zuzugreifen.

1. Klicken Sie den Link **Bei AXIS Secure Remote Access anmelden**.
2. Geben Sie die Anmeldedaten für Ihr MyAxis-Konto ein.
3. Klicken Sie auf **Anmelden**.
4. Klicken Sie auf **Gewähren**.

AXIS Camera Station konfigurieren

Dieses Tutorial führt Sie durch die ersten grundlegenden Schritte zum Einrichten und Starten Ihres Systems.

Vorbereitungen:

- Je nach Art Ihrer Installation das Netzwerk konfigurieren. Siehe *Netzwerkkonfiguration, on page 19*.
- Konfigurieren Sie bei Bedarf die Server-Ports. Siehe *Server-Port-Konfiguration, on page 19*.
- Berücksichtigen Sie dabei Sicherheitsbelange. Siehe *Hinweise zur Systemsicherheit*.

Nach Abschluss der erforderlichen Konfigurationsarbeiten können Sie mit der AXIS Camera Station arbeiten:

1. *Das Video Management System starten, on page 17*
2. *Geräte hinzufügen, on page 17*
3. *Konfigurieren des Aufzeichnungsverfahrens, on page 17*
4. *Live-Video ansehen, on page 18*
5. *Aufzeichnungen anzeigen, on page 18*
6. *Lesezeichen hinzufügen, on page 18*
7. *Aufzeichnungen exportieren, on page 18*
8. *Aufzeichnungen mit AXIS File Player wiedergeben und überprüfen, on page 18*

Das Video Management System starten

Um den AXIS Camera Station Client zu starten, klicken Sie mit einem Doppelklick auf das Symbol des Clients. Beim Erststart des Clients versucht dieser, sich bei dem auf demselben Computer installierten AXIS Camera Station Server anzumelden.

Die Verbindung mit mehreren Servern von AXIS Camera Station ist auf verschiedene Weise möglich.

Geräte hinzufügen

Die Seite Add devices (Geräte hinzufügen) wird beim ersten Start von AXIS Camera Station geöffnet. AXIS Camera Station durchsucht das Netzwerk nach verbundenen Geräten und zeigt eine Liste der gefundenen Geräte an.

1. Wählen Sie hinzuzufügende Kameras aus der Liste aus. Wenn Sie Ihre Kamera nicht finden können, klicken Sie auf **Manual search (Manuelle Suche)**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie entweder **Schnellkonfiguration** oder **Site Designer-Konfiguration**. Klicken Sie auf **Next (Weiter)**.
4. Die Standardeinstellungen verwenden und sicherstellen, dass das Aufzeichnungsverfahren auf **None (Keines)** gesetzt ist. **Install (Installieren)** anklicken.

Konfigurieren des Aufzeichnungsverfahrens

1. **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode aufrufen.**

2. Eine Kamera wählen
3. Aktivieren Sie **Motion detection (Bewegungserkennung)** oder **Continuous (Kontinuierlich)** oder beides.
4. Klicken Sie auf **Anwenden**.

Live-Video ansehen

1. Öffnen Sie eine Registerkarte **Live view (Live-Ansicht)**.
2. Wählen Sie eine Kamera aus, um ihr Live-Video anzusehen.

Aufzeichnungen anzeigen

1. Öffnen Sie eine Registerkarte **Recordings (Aufzeichnungen)**.
2. Wählen Sie die Kamera aus, von der Sie Aufzeichnungen ansehen möchten.

Lesezeichen hinzufügen

1. Zu Aufzeichnung wechseln.
2. Um die Zeitleistenmarkierung an die gewünschte Position zu setzen, zoomen Sie in die Zeitleiste und ziehen Sie daran.
3. Klicken Sie auf .
4. Einen Namen und eine Beschreibung für das Lesezeichen eingeben. Verwenden Sie Stichwörter, damit das Lesezeichen leicht zu finden ist.
5. Wählen Sie **Löschen von Aufzeichnungen verhindern**, um die Aufzeichnung zu sperren.

Hinweis

Um die Aufzeichnung zu entsperren, deaktivieren Sie **Prevent recording deletion (Löschung der Aufzeichnung verhindern)** oder löschen Sie das Lesezeichen.

6. Klicken Sie auf **OK**, um das Lesezeichen zu speichern.

Aufzeichnungen exportieren

1. Öffnen Sie eine Registerkarte **Recordings (Aufzeichnungen)**.
2. Wählen Sie die Kamera aus, von der Sie Aufzeichnungen exportieren möchten.
3. Um die Auswahlmarkierungen anzuzeigen,  anklicken.
4. Ziehen Sie die Markierungen, um die zu exportierenden Aufzeichnungen einzuschließen.
5. Klicken Sie auf , um die Registerkarte **Export** zu öffnen.
6. Klicken Sie auf **Export... (Exportieren...)**

Aufzeichnungen mit AXIS File Player wiedergeben und überprüfen

1. Wechseln Sie in den Ordner mit den exportierten Aufzeichnungen.
2. AXIS File Player doppelklicken.
3. Klicken Sie auf , um die Aufzeichnungshinweise anzeigen zu können.
4. Die digitale Signatur überprüfen:
 - 4.1. **Tools > Digitale Signatur überprüfen** aufrufen.
 - 4.2. Wählen Sie **Mit Kennwort validieren** und geben Sie Ihr Kennwort ein.
 - 4.3. Klicken Sie auf **Verify (Überprüfen)**, um die Überprüfungsergebnisse anzuzeigen.

Hinweis

- Eine digitale Signatur unterscheidet sich von signiertes Video. Mithilfe eines signierten Videos können Sie eine Aufzeichnung bis zu der Kamera zurückverfolgen, von der sie stammt, und so sicherstellen, dass sie nicht manipuliert wurde. Weitere Informationen dazu finden Sie unter *Signierte Videos* und in der Bedienungsanleitung der Kamera.
- Wenn gespeicherte Dateien keine Verbindung zu einer Datenbank der AXIS Camera Station haben (nicht indizierte Dateien), müssen Sie sie konvertieren, damit sie im AXIS File Player wiedergegeben werden können. Wenden Sie sich an den technischen Support von Axis, wenn Sie Hilfe bei der Konvertierung Ihrer Dateien benötigen.

Netzwerkconfiguration

Konfigurieren Sie vor Verwendung von AXIS Camera Station die Einstellungen für Proxyserver oder Firewall, wenn sich der AXIS Camera Station Client, AXIS Camera Station Server und die Netzwerk-Geräte in verschiedenen Netzwerken befinden.

Client-Proxyeinstellungen

Wenn der Client und der Server durch einen Proxyserver getrennt sind, müssen die Proxyeinstellungen des Clients angepasst werden.

1. Öffnen Sie AXIS Camera Station Client.
2. **Client-Proxyeinstellungen ändern** anklicken.
3. Ändern Sie die Proxyeinstellungen des Client.
4. Klicken Sie auf **OK**.

Proxyeinstellungen des Servers

Wenn die Netzwerk-Geräte und der Server durch einen Proxyserver getrennt sind, müssen die Proxyeinstellungen des Servers konfiguriert werden.

1. Die Dienststeuerung der AXIS Camera Station öffnen.
2. **Einstellungen ändern** wählen.
3. Im Abschnitt Proxyeinstellungen die Standardeinstellung **Option Internetkonto System** oder **Proxyeinstellungen manuell einrichten** wählen.
4. **Save (Speichern)** anklicken.

NAT und Firewall

Wenn Client und Server durch NAT, Firewall oder eine ähnliche Einrichtung getrennt sind, konfigurieren Sie diese so, dass die in AXIS Camera Station Service Control angegebenen Ports HTTP, TCP und Streaming nicht von NAT/Firewall blockiert werden. Wenden Sie sich an den Administrator des Netzwerks, um zu erfahren, wie sich NAT oder die Firewall konfigurieren lassen.

Server-Port-Konfiguration

AXIS Camera Station Server verwendet die Ports 55752 (HTTP), 55754 (TCP), 55756 (mobile Kommunikation) und 55757 (mobiles Streaming) für die Kommunikation zwischen dem Server und dem Client. Bei Bedarf können Sie die Ports über AXIS Camera Station Service Control ändern.

Hinweise zur Systemsicherheit

Um unbefugten Zugriff zu Kameras und Aufzeichnungen zu verhindern:

- Verwenden Sie für alle Netzwerk-Geräte (Kameras, Video-Encoder und Zusatzgeräte) starke Kennwörter.
- Installiert den AXIS Camera Station S2108 Appliance-Server, die Kameras, Video-Encoder und Zusatzgeräte in einem sicheren, vom Büronetz separaten Netzwerk. Sie können den AXIS Camera Station

S2108 Appliance Client auf einem Computer eines anderen Netzwerks installieren, zum Beispiel einem Netzwerk mit Internetzugang.

- Sicherstellen, dass alle Benutzer starke Kennwörter verwenden.

Ein System online lizensieren.

Hierfür müssen sowohl der AXIS Camera Station-Client als auch der Server mit dem Internet verbunden sein.

1. **Konfiguration > Lizenzen > Verwaltung** aufrufen.
2. Stellen Sie sicher, dass die Option **Manage licenses online (Lizenzen online verwalten)** aktiviert ist.
3. Melden Sie sich mit Ihrem MyAxis-Konto an.
4. Der Lizenzschlüssel wird automatisch generiert und erscheint unter **License keys (Lizenzschlüssel)**.
5. Falls Sie Ihren Lizenzschlüssel separat erworben haben, geben Sie diesen unter **Add license key (Lizenzschlüssel hinzufügen)** ein.
6. Klicken Sie auf **Hinzufügen**.
7. Überprüfen Sie im AXIS Camera Station-Client, ob Ihre Lizenzschlüssel unter **Configuration > Licenses > Keys (Konfiguration > Lizenzen > Schlüssel)** angezeigt werden.

Ein System offline lizensieren

1. **Konfiguration > Lizenzen > Verwaltung** aufrufen.
2. Deaktivieren Sie **Manage licenses online (Lizenzen online verwalten)**.
3. **Systemdatei exportieren** anklicken.
4. Speichern Sie Ihre Systemdatei auf einem USB-Flashlaufwerk.
5. Melden Sie sich mit Ihrem MyAxis-Konto an.
6. Klicken Sie auf **Upload system file (Systemdatei hochladen)**, um die Systemdatei von Ihrem USB-Flashlaufwerk hochzuladen.
7. Der Lizenzschlüssel wird automatisch generiert und unter **License keys (Lizenzschlüssel)** angezeigt.
8. Falls Sie Ihren Lizenzschlüssel separat erworben haben, geben Sie diesen unter **Add license key (Lizenzschlüssel hinzufügen)** ein.
9. Klicken Sie auf **Hinzufügen**.
10. Klicken Sie unter Lizenzschlüssel auf **Lizenzdatei herunterladen** und speichern Sie die Datei auf einem USB-Stick.
11. Wechseln Sie im AXIS Camera Station-Client zu **Configuration > Licenses > Management (Konfiguration > Lizenzen > Verwaltung)**.
12. **Lizenzdatei importieren** anklicken und die auf dem USB-Stick gespeicherte Datei wählen.
13. Stellen Sie sicher, dass Ihre Lizenzschlüssel unter **Configuration > Licenses > Keys (Konfiguration > Lizenzen > Schlüssel)** angezeigt werden.

Lokale Windows®-Benutzerkonten verwalten

Ein Benutzerkonto erstellen

Um Ihre persönlichen Daten und Informationen besser zu schützen, empfehlen wir Ihnen, für jedes lokale Konto ein Kennwort hinzuzufügen.

Wichtig

Vergessen Sie die Kennwörter nicht, die Sie für die lokalen Konten erstellt haben! Es gibt keine Möglichkeit, verlorene Passwörter für lokale Konten wiederherzustellen.

1. **Settings > Accounts > Other people > Add someone else to this PC (Einstellungen > Konten > Andere Personen > Eine Person zu diesem PC hinzufügen)** aufrufen.
2. Auf **I don't have this person's sign-in information (Ich habe die Anmeldeinformationen dieser Person nicht)** klicken.
3. Auf **Add a user without a Microsoft account (Einen Benutzer ohne Microsoft-Konto hinzufügen)** klicken.
4. Einen Benutzernamen, ein Kennwort und einen Kennworthinweis eingeben.
5. Auf **Next (Weiter)** klicken und den Anweisungen folgen.

Administratorkonto erstellen

1. **Settings > Accounts > Other people (Einstellungen > Konten > Andere Personen)** aufrufen.
2. Zu dem Konto gehen, dessen Kontotyp geändert werden soll, und auf **Change account type (Kontotypen ändern)** klicken.
3. **Account type (Kontotyp)** aufrufen und **Administrator (Administrator)** auswählen.
4. Klicken Sie auf **OK**.
5. Gerät neu starten und mit dem neuen Administratorkonto anmelden.

Eine lokale Benutzergruppe erstellen

1. **Computer Management (Computerverwaltung)** aufrufen.
2. **Local Users and Groups > Group (Lokale Benutzer und Gruppen > Gruppe)** aufrufen.
3. Rechtsklick auf **Group (Gruppe)** und **New Group (Neue Gruppe)** auswählen.
4. Einen Gruppennamen und eine Beschreibung eingeben.
5. Gruppenmitglieder hinzufügen:
 - 5.1. Klicken Sie auf **Hinzufügen**.
 - 5.2. Klicken Sie auf **Erweitert**.
 - 5.3. Suchen Sie die Benutzerkonten, die zur Gruppe hinzugefügt werden sollen, und klicken Sie auf **OK**.
 - 5.4. Klicken Sie noch einmal auf **OK**.
6. Klicken Sie auf **Create (Erstellen)**.

Ein Benutzerkonto löschen

Wichtig

Nach Löschen eines Benutzerkontos erscheint dieses nicht mehr auf dem Anmeldebildschirm. Außerdem werden alle Dateien, Einstellungen und Programmdateien gelöscht, die im entsprechenden Benutzerkonto gespeichert sind.

1. **Settings > Accounts > Other people (Einstellungen > Konten > Andere Personen)** aufrufen.
2. Zu dem Konto gehen, das gelöscht werden soll, und **Remove (Entfernen)** klicken.

Das Kennwort eines Benutzerkontos ändern

1. Mit einem Administratorkonto anmelden.
2. **User Accounts > User Accounts > Manage another account in sequence (Benutzerkonten > Benutzerkonten > Anderes Konto verwalten)** aufrufen.
Es wird eine Liste mit allen Benutzerkonten auf dem Gerät angezeigt.
3. Das Benutzerkonto auswählen, dessen Kennwort geändert werden soll.
4. Auf **Change the password (Kennwort ändern)** klicken.
5. Neues Kennwort eingeben und auf **Change password (Kennwort ändern)** klicken.

Einen Kennwortrücksetzdatenträger für ein Benutzerkonto erstellen

Es wird empfohlen, einen Kennwortrücksetzdatenträger zu erstellen. Als Datenträger bietet sich ein USB-Stick an. Mit diesem können Sie das Kennwort zurücksetzen. Ohne Kennwortrücksetzdatenträger kann das Kennwort nicht zurückgesetzt werden.

Hinweis

Unter Windows® 10 oder höher ist ein Kennwortrücksetzdatenträger nicht notwendig. In diesem Fall können Sicherheitsfragen zum lokalen Benutzerkonto hinzugefügt werden. Die Sicherheitsfragen können folgendermaßen hinzugefügt werden: **Start (Start)** auswählen und auf **Settings > Sign-in options > Update your security questions (Einstellungen > Anmeldeoptionen > Sicherheitsfragen aktualisieren)** klicken.

1. Mit einem lokalen Benutzerkonto bei Ihrem Gerät anmelden. Für ein verbundenes Konto kann kein Kennwortrücksetzdatenträger erstellt werden.
2. Einen leeren USB-Stick an Ihr Gerät anschließen.
3. Vom Windows®-Suchfeld zu **Create a password reset disk (Kennwortrücksetzdatenträger erstellen)** wechseln.
4. Klicken Sie im Setup-Assistenten **Forgotten Password (Kennwort vergessen)** auf **Next (Weiter)**.
5. Ihren USB-Stick auswählen und auf **Next (Weiter)** klicken.
6. Ihr aktuelles Kennwort eingeben und auf **Next (Weiter)** klicken.
7. Den Anweisungen auf dem Bildschirm folgen.
8. Entfernen Sie den USB-Stick und bewahren Sie ihn an einem sicheren Ort auf. Wird das Kennwort geändert, muss kein neuer Kennwortrücksetzdatenträger erstellt werden – selbst dann nicht, wenn das Kennwort mehrfach geändert wird.

AXIS Camera Station Benutzerkonten verwalten

Benutzerberechtigungen

Rufen Sie **Configuration (Konfiguration) > Security (Sicherheit) > User permissions (Benutzerberechtigungen)** auf, um die Benutzer und Gruppen in AXIS Camera Station S2108 Appliance anzuzeigen.

Hinweis

Administratoren von Computern, auf denen der AXIS Camera Station S2108 Appliance-Server ausgeführt werden, erhalten automatisch Administratorrechte in AXIS Camera Station S2108 Appliance. Die Zugriffsrechte der Benutzergruppe „Administratoren“ können nicht geändert oder gelöscht werden.

Bevor Sie einen Benutzer oder eine Gruppe hinzufügen können, stellen Sie bitte sicher, dass diese auf dem lokalen Computer registriert sind oder über ein Windows® Active Directory-Konto verfügen. So fügen Sie Benutzer bzw. Gruppen hinzu: *Hinzufügen von Benutzern oder Gruppen*.

Wenn ein Benutzer einer Gruppe angehört, erhält er die höchste Rollenberechtigung, die ihm persönlich oder der Gruppe zugewiesen wurde. Beispielsweise hat ein Benutzer, der Zutritt zu Kamera X hat und gleichzeitig einer Gruppe angehört, die Zugriff zu den Kameras Y und Z hat, Zutritt zu allen drei Kameras.

	Gibt an, ob es sich um einen Einzelbenutzer handelt.
	Gibt an, ob es sich um eine Benutzergruppe handelt.
Bezeichnung	Der auf dem lokalen Computer oder in Active Directory angezeigte Benutzername.
Domäne	Domain, zu der der Benutzer oder die Benutzergruppe gehört.
Rolle	Die dem Benutzer oder der Benutzergruppe zugewiesene Zugriffsrolle. Mögliche Werte sind: Administrator, Bediener und Betrachter.
Details	Detaillierte Benutzerinformationen wie diese auf dem lokalen Rechner oder in Active Directory erscheinen.
Server	Server, zu der der Benutzer oder die Benutzergruppe gehört.

Hinzufügen von Benutzern oder Gruppen

Benutzer von Microsoft Windows® und Active Directory sowie Benutzergruppen können auf AXIS Camera Station S2108 Appliance zugreifen. Um einen Benutzer zu AXIS Camera Station S2108 Appliance hinzufügen zu können, müssen Sie zuerst Benutzer oder eine entsprechende Benutzergruppe in Windows® hinzufügen.

So fügen Sie einen Benutzer in Windows® 10 und 11 hinzu:

- Drücken Sie die Windows-Taste + X und wählen Sie **Computer Management (Computerverwaltung)**.
- Navigieren Sie im Fenster **Computer Management (Computerverwaltung)** zu **Local Users and Groups (Lokale Benutzer und Gruppen) > Users (Benutzer)**.
- Klicken Sie mit der rechten Maustaste auf **Users (Benutzer)** und wählen Sie **New user (Neuer Benutzer)**.
- Geben Sie im Popup-Dialog die Daten des neuen Benutzers ein und deaktivieren Sie **User must change password at next login (Benutzer muss bei der nächsten Anmeldung das Passwort ändern)**.
- Klicken Sie auf **Create (Erstellen)**.

Falls Sie eine Active Directory-Domäne verwenden, halten Sie bitte Rücksprache mit Ihrem Netzwerkadministrator.

Hinzufügen von Benutzern oder Gruppen

1. Gehen Sie zu **Configuration > Security > User permissions (Konfiguration > Sicherheit > Benutzerrechte)**.

2. Klicken Sie auf **Hinzufügen**. Die verfügbaren Benutzer und Gruppen werden in der Liste angezeigt.
3. Wählen Sie unter **Scope (Bereich)** aus, wo nach Benutzern und Benutzergruppen gesucht werden soll.
4. Wählen Sie unter **Show (Anzeigen)** aus, ob Sie Benutzer oder Benutzergruppen anzeigen möchten. Die Suchergebnisse werden möglicherweise nicht angezeigt, wenn zu viele Benutzer oder Gruppen vorhanden sind. Verwenden Sie den Filter, um die Ergebnisse einzugrenzen.
5. Wählen Sie Benutzer bzw. Gruppen und klicken Sie auf **Hinzufügen**.

Bereich	
Server	Wählen Sie diese Option, um auf Ihrem lokalen Rechner nach Benutzern oder Benutzergruppen zu suchen.
Domäne	Wählen Sie diese Option, um nach Active Directory-Benutzern oder -Benutzergruppen zu suchen.
Ausgewählter Server	Wenn eine Verbindung zu mehreren AXIS Camera Station S2108 Appliance-Servern besteht, wählen Sie einen Server aus, um auf diesem Server nach Benutzern oder Gruppen zu suchen.

Konfigurieren eines Benutzers oder einer Gruppe

1. Wählen Sie einen Benutzer oder eine Gruppe aus der Liste aus.
2. Wählen Sie unter **Role (Rolle)** eine der Optionen **Administrator**, **Operator (Bediener)** oder **Viewer (Betrachter)** aus.
3. Bei Auswahl von **Operator (Bediener)** oder **Viewer (Betrachter)** können Sie die entsprechenden Benutzer- oder Benutzergruppenberechtigungen konfigurieren. Siehe *Benutzer-/Gruppenberechtigungen*.
4. Klicken Sie auf **Save**.

Benutzer oder Benutzergruppe entfernen

1. Wählen Sie einen Benutzer oder eine Benutzergruppe aus.
2. Klicken Sie auf **Remove (Entfernen)**.
3. Wählen Sie **OK** in dem Dialogfenster, um den Benutzer oder die Gruppe zu löschen.

Benutzer-/Gruppenberechtigungen

Einem Benutzer oder einer Benutzergruppe können drei verschiedene Rollen zugewiesen werden. Weitere Informationen dazu, wie Sie die Rolle eines Benutzers oder einer Benutzergruppe definieren, finden Sie unter *Hinzufügen von Benutzern oder Gruppen*.

Administrator – Vollständiger Zugriff auf das gesamte System, einschließlich Zugriff auf Live-Videos und Video-Aufzeichnungen sämtlicher Kameras, alle I/O-Ports und Ansichten. Diese Rolle ist für den Zugriff auf die Systemkonfiguration erforderlich.

Bediener – Auswahl von Kameras, Ansichten und I/O-Ports für den Zugriff auf Live-Videos und Video-Aufzeichnungen. Ein Bediener hat vollen Zugriff auf alle Funktionen der AXIS Camera Station S2108 Appliance mit Ausnahme der Systemkonfiguration.

Betrachter – Zugriff auf Live-Videos bestimmter Kameras, I/O-Ports und Ansichten. Betrachter haben keinen Zugriff auf Video-Aufzeichnungen oder die Systemkonfiguration.

Kameras

Benutzern oder Benutzergruppen mit der Rolle **Operator (Bediener)** oder **Viewer (Betrachter)** können die folgenden Zugriffsrechte erteilt werden.

Zugriff	Gewährt dem Benutzer Zugriff auf die Kamera und alle Kamerafunktionen.
Video	Gewährt dem Benutzer Zugriff auf das Live-Video der Kamera.
Audio – Wiedergeben	Gewährt dem Benutzer Zugriff auf das Abhören der Kamera.
Audio – Sprechen	Gewährt dem Benutzer Zugriff auf das Sprechen über die Kamera.
Manuelle Aufzeichnung	Erlauben Sie das manuelle Starten und Beenden von Aufzeichnungen.
Mechanisches PTZ	Zugriff auf mechanische PTZ-Steuerungen gewähren. Nur für Kameras mit mechanischer PTZ-Steuerung verfügbar.
PZT-Priorität	Legen Sie die PTZ-Priorität fest. Eine niedrigere Zahl steht für eine höhere Priorität. Ist keine Priorität zugewiesen, beträgt die Einstellung 0. Ein Administrator hat die höchste Priorität. Wenn ein Rolle mit höherer Priorität eine PTZ-Kamera ansteuert, können andere Rollen dieselbe Kamera 10 Sekunden lang (Standardkonfiguration) nicht ansteuern. Nur möglich bei Kameras mit mechanischem PTZ-Antrieb, bei denen Mechanical PTZ (Mechanischer PTZ) ausgewählt ist.

Ansichten

Benutzern oder Benutzergruppen mit der Rolle **Operator (Bediener)** oder **Viewer (Betrachter)** können die folgenden Zugriffsrechte erteilt werden. Sie können mehrere Ansichten auswählen und die Zugriffsberechtigungen festlegen.

Zugriff	Gewährt Zugriff auf die Ansichten in AXIS Camera Station S2108 Appliance.
Bearbeiten	Ermöglicht die Bearbeitung von Ansichten in AXIS Camera Station S2108 Appliance.

I/O

Benutzern oder Benutzergruppen mit der Rolle **Operator (Bediener)** oder **Viewer (Betrachter)** können die folgenden Zugriffsrechte erteilt werden.

Zugriff	Gewährt dem Benutzer uneingeschränkten Zugriff auf den E/A-Port.
Lesen	Ermöglicht die Ansicht des Zustands des I/O-Ports, ohne diesen zu ändern.
Schreiben	Ermöglicht die Änderung des Zustands des I/O-Ports.

System

Ausgegraute Zugriffsrechte in der Liste können nicht konfiguriert werden. Mit einem Häkchen markiert bedeutet, dass die jeweiligen Benutzer oder Benutzergruppe standardmäßig über dieses Privileg verfügt.

Benutzern oder Benutzergruppen mit der Rolle **Operator (Bediener)** können die folgenden Zugriffsrechte erteilt werden. Die Option **Take snapshots (Momentaufnahmen erstellen)** ist ebenfalls für die Rolle **Viewer (Betrachter)** möglich.

Schnappschuss aufnehmen	Ermöglicht das Aufnehmen von Schnappschüssen in der Live-Ansicht und im Aufzeichnungsmodus.
Aufzeichnungen exportieren	Das Exportieren von Aufzeichnungen zulassen.
Vorfallsberichte erstellen	Das Erstellen von Vorfallsberichten zulassen.
Prevent access to recordings older than (Zugriff auf Aufzeichnungen verhindern, wenn älter als)	Verhindert den Zugriff auf Aufzeichnungen, die älter sind als die angegebene Minutenzahl. Benutzer können diese Aufzeichnungen bei der Suche nicht finden.
Zugriff auf Alarmer, Aufgaben und Protokolle	Erlaubt den Erhalt von Alarmbenachrichtigungen und den Zugriff auf die Funktionsleiste Alarms and tasks (Alarmer und Aufgaben) sowie die Registerkarte Logs (Protokolle) .
Access data search (Zugriff auf die Datensuche)	Ermöglicht die Suche nach Daten, um nachzuverfolgen, was zum Zeitpunkt eines Ereignisses passiert ist.
Ereignisse zu Kategorien hinzufügen	Ermöglicht das Hinzufügen von Kategorien zu Ereignissen auf der Registerkarte Recordings (Aufzeichnungen) .
Kategorien von Ereignissen entfernen	Ermöglicht das Entfernen von Kategorien aus Ereignissen auf der Registerkarte Recordings (Aufzeichnungen) .

Zutrittskontrolle

Benutzern oder Benutzergruppen mit der Rolle **Operator (Bediener)** können die folgenden Zugriffsrechte erteilt werden. Die Option **Access management (Zugriffsverwaltung)** ist ebenfalls für die Rolle **Viewer (Betrachter)** möglich.

Konfiguration der Zutrittskontrolle	Erlaubt die Konfiguration von Türen und Zonen, Identifikationsprofilen, Kartenformaten und PIN, verschlüsselter Kommunikation und Multi-Server.
Zutrittsverwaltung	Erlaubt die Zugriffsverwaltung und Zugriff auf die Einstellungen von Active Directory.

Die folgenden Zugriffsberechtigungen sind für Benutzer oder Gruppen mit der Rolle **Betrachter** verfügbar.

Systemzustand überwachen

Benutzern oder Benutzergruppen mit der Rolle **Operator (Bediener)** können die folgenden Zugriffsrechte erteilt werden. Die Option **Access to system health monitoring (Zugriff auf Systemzustandsüberwachung)** ist ebenfalls für die Rolle **Viewer (Betrachter)** möglich.

Konfigurieren der Überwachung des Systemzustands	Ermöglicht das Konfigurieren der Überwachung des Systemzustands.
Auf Systemzustandsüberwachung zugreifen	Ermöglicht den Zugriff auf die Überwachung des Systemzustands.

Ihr Gerät verwalten

Secure-Boot-Zertifikate aktualisieren

Microsoft wird die Secure-Boot-Zertifikate aus dem Jahr 2011 im Juni 2026 außer Kraft setzen und durch neue Zertifikate aus dem Jahr 2023 ersetzen. Um die Sicherheit Ihres Aufzeichnungsgeräts zu gewährleisten, installieren Sie die Zertifikate für 2023 bitte noch vor diesem Zeitpunkt.

Für die Installation der Zertifikate für das Jahr 2023 ist Windows 10 LTSC (Long-Term Servicing Channel) oder Windows 11 LTSC erforderlich. Falls Ihr Gerät noch unter die Garantie fällt, jedoch Windows 10 SAC (Semi-Annual Channel) anstelle einer LTSC-Version ausführt, wenden Sie sich bitte an den technischen Support von Axis. Dort kann man Ihnen mitteilen, ob Sie eine Aktualisierung auf eine LTSC-Version durchführen können, bevor Sie das BIOS aktualisieren oder Zertifikate ändern.

Hinweis

Nach Juni 2026 funktionieren Geräte ohne die Zertifikate aus dem Jahr 2023 zwar weiterhin wie gewohnt, erhalten jedoch keine neuen Sicherheitsmaßnahmen für den frühen Startvorgang mehr, darunter Aktualisierungen für den Windows-Boot-Manager und Sperrlisten für neue Sicherheitslücken.

Status Ihres Zertifikats prüfen

Um zu überprüfen, ob die Zertifikate für 2023 installiert sind und der Windows-Bootloader aktualisiert wurde, wenden Sie eine der folgenden Methoden an:

Methode 1:

1. Öffnen Sie **Registry Editor (Registrierungseditor)**.
2. Wechseln Sie zu `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing`.
3. Prüfen Sie den Wert von **UEFICA2023Status**. Wenn der Wert **Updated (Aktualisiert)** lautet, ist das Zertifikat für 2023 installiert.

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

Methode 2:

1. Öffnen Sie **Windows Security**.
2. Rufen Sie **Gerätesicherheit** auf.
3. Prüfen Sie unter **Secure Boot** die Statusmeldung. Sofern das Zertifikat auf dem neuesten Stand ist, wird auf der Karte Folgendes angezeigt: „Secure Boot ist aktiviert, und alle erforderlichen Aktualisierungen des Zertifikats wurden vorgenommen. Es müssen keine weiteren Zertifikate geändert werden.“



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

Hinweis

Windows Security zeigt den Zertifikatsstatus nur an, wenn auf Ihrem Gerät die Installation des kumulativen Updates vom 14. April 2026 oder eine neue Aktualisierung installiert ist. Sollten Sie keine Meldung zum Zertifikatsstatus sehen, führen Sie bitte die Installation des neuesten Windows-Updates durch oder wenden Sie stattdessen Methode 1 an.

Empfohlene Aktionen

Durch eine Aktualisierung des BIOS werden die Zertifikate für das Jahr 2023 dauerhaft in der Firmware gespeichert. Dies ist die zuverlässigste Methode, und wir empfehlen sie auch dann, wenn Sie die Zertifikate bereits über Windows Update installiert haben.

Wichtig

Wenn Sie die Zertifikate ausschließlich über Windows Update installieren und anschließend die BIOS-Secure-Boot-Schlüssel auf die werksseitigen Standardeinstellungen zurücksetzen, gehen die Zertifikate verloren, und das Gerät lässt sich bei eingeschaltetem Secure Boot nicht mehr starten. Aktualisieren Sie das BIOS, um die Zertifikate dauerhaft zu speichern, bevor Sie die Secure-Boot-Schlüssel zurücksetzen.

Zertifikat über das BIOS aktualisieren

Führen Sie die Installation der für Ihr Modell angegebenen BIOS-Version oder einer neueren Version durch. Sie können diese von der Produktseite auf [Axis.com](https://axis.com) herunterladen:

Modell	Mindestversion des BIOS
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

Zertifikat über Windows Update aktualisieren

Sollte für Ihr Modell noch keine Aktualisierung des BIOS verfügbar sein, können Sie die Zertifikate für 2023 stattdessen über Windows Update beziehen.

Wichtig

Während der Installation werden auf diese Weise installierte Zertifikate in der aktuellen Secure-Boot-Datenbank gespeichert, nicht in der Firmware. Wenn Sie die BIOS-Secure-Boot-Schlüssel auf die werksseitigen Standardeinstellungen zurücksetzen, gehen die Zertifikate verloren, und das Gerät kann möglicherweise nicht mehr gestartet werden, wenn Secure Boot eingeschaltet ist. Installieren Sie das BIOS-Update, sobald es für Ihr Modell verfügbar ist, auch wenn Sie diese Methode bereits angewendet haben.

So verwenden Sie diesen Pfad:

1. Stellen Sie sicher, dass auf Ihrem Gerät Windows 10 LTSC oder Windows 11 LTSC installiert ist.
2. Installieren Sie alle Windows-Updates, die am 14. April 2026 oder später veröffentlicht wurden.
3. Rufen Sie **Windows Security (Windows-Sicherheit) > Device security (Gerätesicherheit) > Secure Boot** auf, um den Status Ihres Zertifikats zu prüfen.
4. Falls das Zertifikat nach der Installation der neuesten Updates nicht aktualisiert wird, prüfen Sie den Registerwert **UEFICA2023Status**. Sollte Ihr Gerät weiterhin nicht für die automatische Aktualisierung geeignet sein, aktualisieren Sie bitte das BIOS oder wenden Sie sich an den technischen Support von Axis.

Wichtig

Widerrufen Sie das Zertifikat von 2011 nicht manuell, bevor Sie sich vergewissert haben, dass alle Wiederherstellungsmedien, Startumgebungen und Treiber in Ihrer Umgebung mit dem Zertifikat von 2023

signiert sind. Wenn Sie das Zertifikat aus dem Jahr 2011 zu früh widerrufen, kann Ihr Gerät bei eingeschaltetem Secure Boot nicht mehr gestartet werden.

Aktuelle BIOS-Version überprüfen

So überprüfen Sie das aktuelle BIOS:

1. Schalten Sie das Gerät ein und drücken Sie mehrmals **ENTF**, bis das Axis Logo angezeigt wird.
2. Die Versionsnummer wird unter **Haupt** als erster Eintrag angezeigt.

BIOS aktualisieren

Befolgen Sie die Anweisungen im BIOS-Handbuch, das auf der Download-Seite der BIOS-Datei verfügbar ist.

Windows® aktualisieren

Windows® sucht regelmäßig nach Updates. Wenn ein Update verfügbar ist, lädt Ihr Gerät das Update automatisch herunter – Sie müssen es jedoch manuell installieren.

Hinweis

Die Aufzeichnung wird während eines geplanten Systemneustarts unterbrochen.

So erfolgt die manuelle Suche nach Updates:

1. Rufen Sie **Settings > Windows Update** (Einstellungen > Windows-Update) auf.
2. Auf **Check for updates** (Auf Updates überprüfen) klicken.

Update-Einstellungen für Windows® konfigurieren

Sie können Ihrem Bedarf entsprechend ändern, wie und wann Windows® Updates durchführt.

Hinweis

Während eines geplanten Systemneustarts werden alle laufenden Aufzeichnungen angehalten.

1. Die Run-App öffnen.
 - **Windows System > Run** (Windows-System > Ausführen) aufrufen oder
2. Geben Sie `gpedit.msc` ein und klicken Sie auf **OK**. Der Editor für lokale Gruppenrichtlinien wird geöffnet.
3. **Computer Configuration > Administrative Templates > Windows Components > Windows Update** (Computerkonfiguration > Administrative Vorlagen > Windows-Komponenten > Windows-Update) aufrufen.
4. Einstellungen nach Bedarf konfigurieren; siehe Beispiel.

Beispiel:

Um Updates ohne Benutzerinteraktion automatisch herunterzuladen und zu installieren und das Gerät bei Bedarf außerhalb der Geschäftszeiten neu zu starten, muss die folgende Konfiguration vorgenommen werden:

1. **Always automatically restart at the scheduled time** (Immer automatisch zum geplanten Zeitpunkt neu starten) öffnen und folgende Option auswählen:
 - 1.1. **Aktiviert**
 - 1.2. **The restart timer will give users this much time to save their work (minutes)** (Der Neustart-Timer gibt Benutzer die angegebene Zeit (Minuten), um ihre Arbeit zu speichern): **15**.
 - 1.3. Klicken Sie auf **OK**.
2. **Configure Automatic Updates** (Automatische Updates konfigurieren) und folgende Option auswählen:
 - 2.1. **Aktiviert**
 - 2.2. **Configure Automatic updates** (Automatische Updates konfigurieren): **Automatisch herunterladen und Installation planen**

- 2.3. Schedule Install day (Installationstag planen): Jeden Sonntag
- 2.4. Schedule Install time (Installationszeit planen): 00:00
- 2.5. Klicken Sie auf OK.
3. Auf **Allow Automatic Updates immediate installation (Automatische Updates sofort installieren)** klicken und folgende Option auswählen:
 - 3.1. Aktiviert
 - 3.2. Klicken Sie auf OK.

Verwaltung der Stromversorgung

Das Gesamtleistungsbudget des Switchs beträgt 105 W. Dies ist die maximale Leistungsabgabe für alle angeschlossenen Geräte.

In den meisten Fällen verbrauchen die angeschlossenen Geräte weniger Strom als angefordert. Um den Stromverbrauch zu optimieren, können die angeschlossenen Geräte mit dem PoE-Controller bis zu 125 W anfordern und der tatsächliche Stromverbrauch wird auf 105 W gleichzeitig begrenzt.

Der Switch kann beispielsweise 8 PoE-Geräte der Klasse 3 mit Strom versorgen.

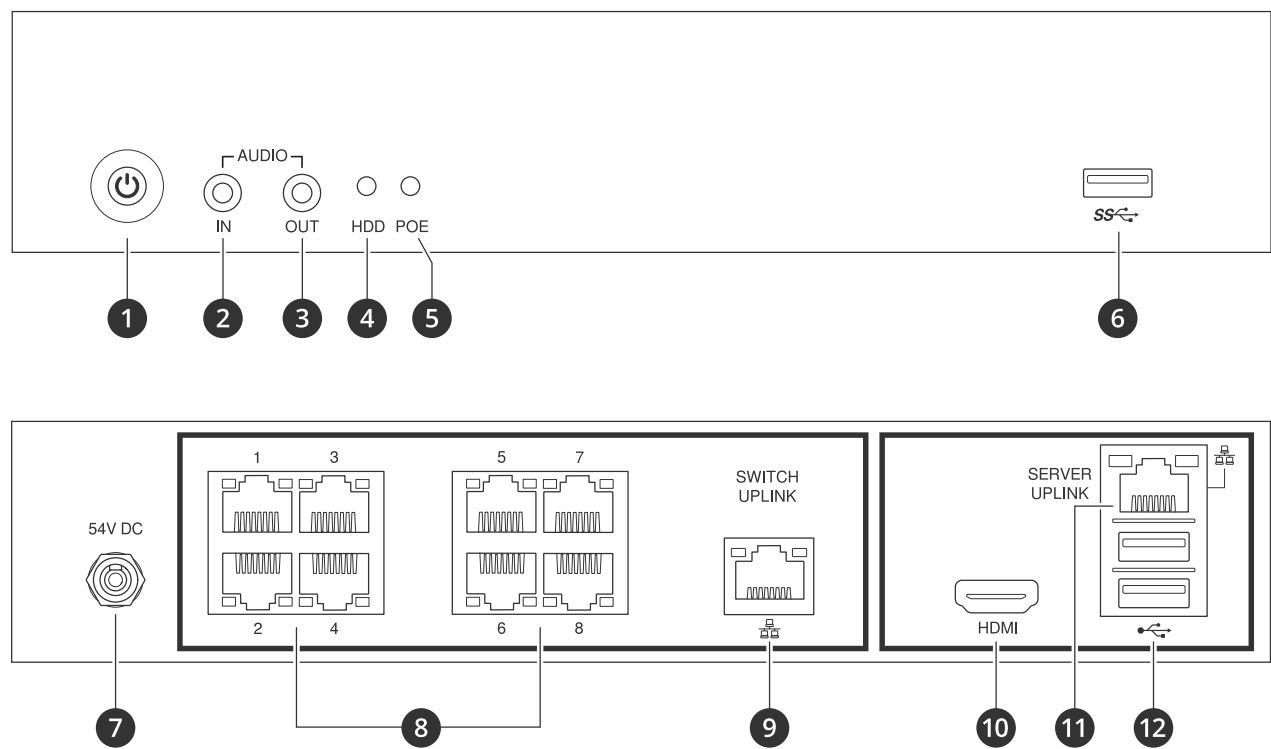
- Ein Gerät der PoE-Klasse 3 fordert eine Leistung von 15,4 W an.
- 8 PoE Klasse 3 Geräte fordern $(8 \times 15,4) = 123,2$ W Leistung an. Dies liegt innerhalb der vom PoE-Controller zulässigen 125-W-Grenze.
- Ein Gerät der PoE-Klasse 3 verbraucht in der Regel eine Leistung von 10 bis 12 W.
- 8 Geräte der PoE-Klasse 3 verbrauchen in der Regel eine Leistung von 80 bis 96 W. Dies liegt innerhalb der 105 W-Grenze des Gesamtleistungsbudgets.

⚠ WARNUNG

- Wenn die angeschlossenen Geräte eine Stromversorgung über 125 W anfordern:
 - Das letzte angeschlossene Gerät wird nicht gestartet.
 - Die PoE-Überlast-LED leuchtet rot, bis Sie das letzte angeschlossene Gerät trennen. Durch Entfernen anderer Geräte wird ausreichend PoE-Budget frei.
- Wenn die angeschlossenen Geräte tatsächlich mehr als 105 W verbrauchen:
 - Das letzte eingeschaltete Gerät wird heruntergefahren und versucht einen Neustart.
 - Die PoE-Überlast-LED wird nicht eingeschaltet.

Produktübersicht

Vorder- und Rückseite



- 1 Netzschalter/Netz-LED
- 2 Audio-Eingang
- 3 Audio-Ausgang
- 4 LED für Laufwerksaktivität
- 5 Status-LED der PoE-Ports
- 6 USB-3.0-Port
- 7 Stromanschluss
- 8 PoE-Ports
- 9 RJ45-Port Switch Uplink
- 10 HDMI-Port
- 11 RJ45-Port Server Uplink
- 12 USB-2.0-Ports

Technische Daten

Front-LEDs

LED-Anzeige	Farbe	Anzeige
Stromversorgung	Grün	Server an
Festplatte	Blinkt gelb	Festplattenaktivität
	Blinkt rot	Möglicher Festplattenausfall
Überlast PoE	Rot	Über PoE-Budget
	Aus	OK

LEDs hinten

Netzwerkgeschwindigkeit und -aktivität	Farbe	Anzeige
LED rechts	Gelb	10/100 Mbit/s
	Grün ¹	1000 Mbit/s
LED links	Blinkt grün	Netzwerkaktivität

1. Dies gilt nur für Switch-Uplink und Server-Uplink.

Fehlerbehebung

Eine Systemwiederherstellung durchführen

Nach einem kompletten Systemfehler muss das Windows®-System mit einem Wiederherstellungsabbild wiederhergestellt werden. Wenden Sie sich an den technischen Support von AXIS, um das AXIS Netzwerk-Videorecorder Recovery Kit herunterzuladen, und geben Sie die Seriennummer Ihres Geräts an.

Hinweis

Das AXIS Netzwerk-Videorecorder-Recovery-Kit ist in zwei Varianten erhältlich:

- **sb11** – für Geräte, die noch das Zertifikat aus dem Jahr 2011 verwenden.
- **sb23** – für Geräte, die auf das Zertifikat für 2023 umgestellt wurden.

Bitte überprüfen Sie den Status Ihres Zertifikats, bevor Sie das Recovery-Kit herunterladen, und wählen Sie die entsprechende Variante aus. Sollten Sie die falsche Variante auswählen, führt die Installation nicht zu einem bootfähigen Ergebnis, und Sie müssen mit dem richtigen Image von vorne beginnen. Dies wird Ihrem Gerät keinen Schaden zufügen.

Falls auf Ihrem Gerät bereits das Zertifikat von 2023 installiert ist, kann die Variante sb11 weiterhin sicher verwendet werden, solange das Zertifikat von 2011 nicht manuell widerrufen wurde. Sobald die Berechtigung widerrufen wurde, funktioniert nur noch sb23.

So wird das System wiederhergestellt:

1. AXIS Netzwerk-Videorecorder Recovery Kit und AXIS Netzwerk-Videorecorder Recovery: ISO to USB Tool herunterladen.
2. USB-Stick an Computer anschließen.
 - Der USB-Stick sollte mindestens 16 GB haben.
 - Der USB-Stick wird formatiert und alle vorhandenen Daten werden gelöscht.
3. AXIS Netzwerk-Videorecorder Recovery ISO: to USB Tool ausführen und die Anweisungen auf dem Bildschirm befolgen.
Es dauert ca. 10 bis 15 Minuten, bis die Daten auf den USB-Stick geschrieben wurden. Entfernen Sie den USB-Stick erst, wenn der Schreibvorgang abgeschlossen wurde.
4. Wenn AXIS Network Video Recorder Recovery: ISO to USB Tool vollständig ist, den USB-Stick nehmen und in das Gerät stecken.
5. Gerät starten.
6. Wenn der AXIS Startbildschirm angezeigt wird, die Taste F12 drücken.
7. Auf **UEFI: USB-Laufwerk** klicken.
8. Zum USB-Laufwerk navigieren und auf Enter drücken. Das System startet mit dem AXIS Netzwerk-Videorecorder Recovery Kit.
9. **Reinstall Operating System (Betriebssystem neu installieren)** anklicken.
Die Wiederherstellung dauert etwa 10 bis 15 Minuten. Eine detaillierte Anleitung ist im Download des Recovery-Kits enthalten.

Fehlerbehebung bei AXIS Camera Station

Informationen zur Behebung von Problemen bei AXIS Camera Station finden Sie im *Benutzerhandbuch zu AXIS Camera Station*.

Benötigen Sie Hilfe?

Nützliche Links

- *AXIS Camera Station Benutzerhandbuch*
- *Bei AXIS Secure Remote Access anmelden*
- *Was in eine Antiviren-Freigabeliste für AXIS Camera Station aufgenommen werden sollte*

Support

Weitere Hilfe erhalten Sie hier: axis.com/support.

T10181903_de

2026-07 (M7.2)

© 2022 – 2026 Axis Communications AB