

AXIS Camera Station S2216 Mk II Appliance

Inhalt

Funktionsweise.....	4
Das Gerät installieren	5
.....	5
Setup-Beispiele.....	5
Setup in unabhängigen Überwachungsnetzwerk	5
Setup in einem vorhandenen Netzwerk	6
Schließen Sie den Switch direkt an das Unternehmensnetzwerk an	7
Ihr Gerät konfigurieren	9
Erstes Setup des AXIS Recorders	9
Mit einem Server verbinden.....	9
Mit einem Remote-Server verbinden.....	10
Bei AXIS Secure Remote Access anmelden.....	10
AXIS Camera Station Pro konfigurieren.....	11
Das Video Management System starten	11
Geräte hinzufügen.....	11
Konfigurieren des Aufzeichnungsverfahrens	12
Live-Video ansehen.....	12
Aufzeichnungen anzeigen.....	12
Lesezeichen hinzufügen	12
Aufzeichnungen exportieren	12
Aufzeichnungen mit AXIS File Player wiedergeben und überprüfen	12
Netzwerkkonfiguration.....	13
Server-Port-Konfiguration	13
Hinweise zur Systemsicherheit.....	13
Ein System online lizenzieren.....	14
Ein System offline lizenzieren	14
Lokale Windows®-Benutzerkonten verwalten.....	15
Ein Benutzerkonto erstellen.....	15
Erstellen Sie ein Administratorenkonto	15
Eine lokale Benutzergruppe erstellen	15
Ein Benutzerkonto löschen	15
Das Kennwort eines Benutzerkontos ändern	16
Einen Kennworrücksetzdatenträger für ein Benutzerkonto erstellen.....	16
AXIS Camera Station Pro Benutzerkonten verwalten.....	17
Benutzerberechtigungen.....	17
Hinzufügen von Benutzern oder Gruppen.....	17
Benutzer-/Gruppenberechtigungen	18
Ihr Gerät verwalten.....	21
Secure-Boot-Zertifikate aktualisieren.....	21
Den Status Ihres Zertifikats prüfen	21
Empfohlene Aktionen.....	22
Zertifikat über das BIOS aktualisieren	22
Zertifikat über Windows Update aktualisieren.....	22
Aktuelle BIOS-Version überprüfen	23
BIOS aktualisieren	23
Windows® aktualisieren.....	23
Update-Einstellungen für Windows® konfigurieren	23
Hinzufügen von zusätzlichem Speicher.....	24
Blende entfernen.....	24
Festplatte installieren	24
Neuen Aufzeichnungsdatenträger hinzufügen	25
Erstellen eines RAID-Laufwerks.....	25
RAID-Laufwerk in Microsoft Windows® initiieren	26

Den integrierten Switch verwalten.....	27
Der integrierte Switch.....	27
Bei der Verwaltungsseite des Switches anmelden	27
Laufende Konfiguration	27
Übersicht.....	27
Verwaltung der Stromversorgung.....	28
Stromversorgung zuweisen.....	28
PoE aktivieren und deaktivieren.....	30
Netzwerkübersicht	30
Ports sperren und entsperren	31
Einstellungen.....	31
Netzwerkeinstellungen konfigurieren.....	31
Datum und Zeit konfigurieren	32
DHCP-Server konfigurieren	32
SNMP konfigurieren.....	32
Maintenance (Wartung):.....	32
Firmware aktualisieren.....	32
Den Switch neu starten	33
Switch-Einstellungen sichern.....	33
Switch-Einstellungen wiederherstellen	33
Zertifikate verwalten.....	33
Kennwort ändern.....	33
Webeinstellungen konfigurieren.....	34
Zurücksetzen auf die Werkseinstellungen	34
Protokolle.....	34
Switch-Berichte erstellen	34
Technische Daten.....	35
Produktübersicht.....	35
Vorder- und Rückseite	35
LED-Anzeigen	35
Fehlerbehebung	37
Server zurücksetzen.....	37
Eine Systemwiederherstellung durchführen.....	37
.....	37
Fehlerbehebung bei AXIS Camera Station Pro.....	38
Benötigen Sie Hilfe?.....	39
Nützliche Links	39
Support.....	39

Funktionsweise

Der Standardworkflow zum Konfigurieren eines AXIS Camera Station Pro 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 9*.
4. *Windows® konfigurieren. Wir empfehlen:*
 - Windows® auf die neuste Version aktualisieren. Siehe *Windows® aktualisieren, on page 23*.
 - Ein Standardbenutzerkonto erstellen. Siehe *Ein Benutzerkonto erstellen, on page 15*.
5. *AXIS Camera Station Pro auf die neuste Version aktualisieren.*
 - Wenn das System online ist: Öffnen Sie die App AXIS Recorder Toolbox und klicken Sie auf **Update AXIS Camera Station Pro (AXIS Camera Station Pro aktualisieren)**.
 - Wenn das System offline ist: Gehen Sie auf *axis.com* und laden Sie die aktuelle Version herunter.
6. *Starten Sie den AXIS Camera Station Pro Client.*
7. *Stellen Sie eine Verbindung zum AXIS Camera Station Pro-Server her.*
8. *AXIS Camera Station Pro konfigurieren, on page 11.*

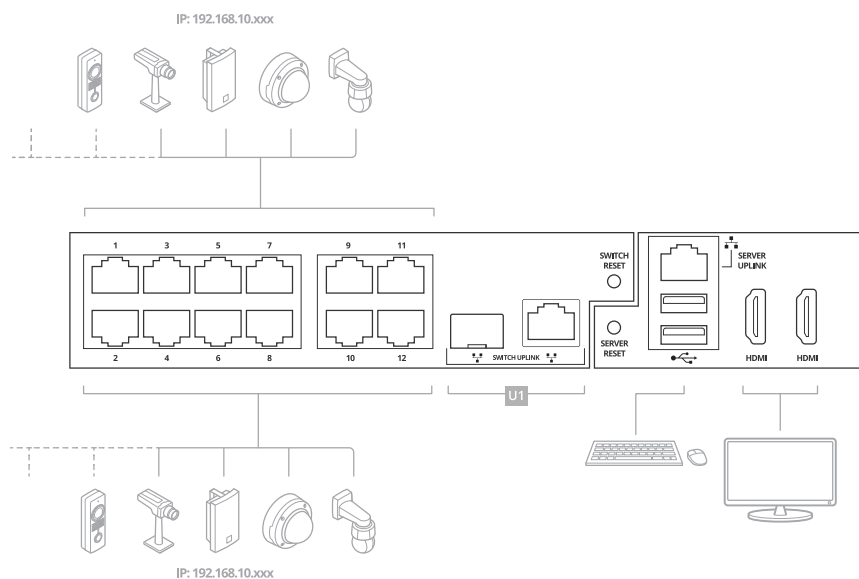
Das Gerät installieren

Hinweise zur Installation des Produkts finden Sie in der Installationsanleitung in der Verpackung oder auf der Produkt-Supportseite auf axis.com.

Setup-Beispiele

Setup in unabhängigen Überwachungsnetzwerk

Es kann ein unabhängiges Überwachungsnetzwerk erstellt werden, das keine Verbindung zu einem anderen externen Netzwerk hat. Dieses Setup ist eine einfache Plug-and-Play-Installation. Der DHCP-Server des integrierten Switches ist standardmäßig aktiviert. Sobald Kameras an die PoE-Ports angeschlossen werden, schalten sich die Kameras ein, erhalten eine IP-Adresse und können über AXIS Camera Station Pro abgerufen werden.



Schwierigkeitsgrad	Einfach
Vorteile	Dediziertes Überwachungsnetz ohne Verbindung zu einem anderen externen Netzwerk Sofort nach Installation einsatzbereit
Einschränkungen	Bandbreite PoE-Budget Kein Fernzugriff
Erforderliche Maßnahmen	Standardkennwort für den integrierten Switch ändern AXIS Camera Station Pro Lizenz registrieren

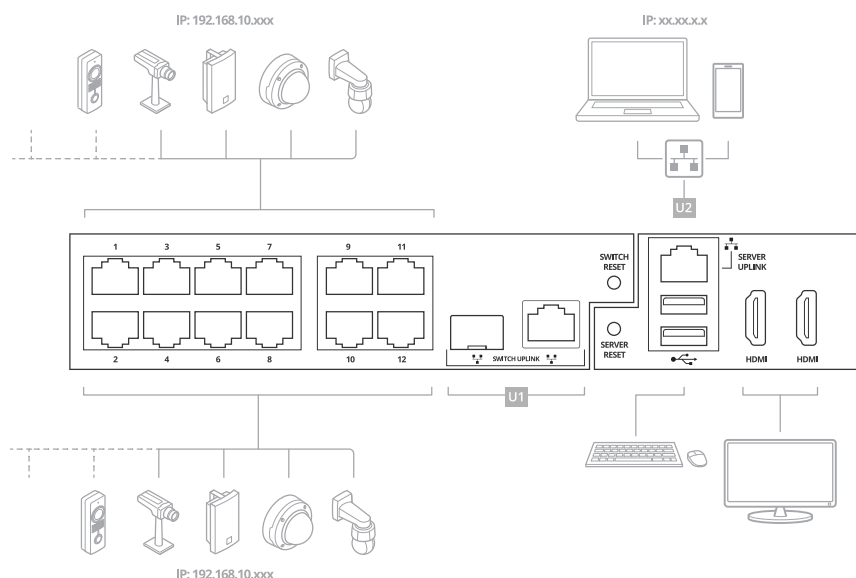
Verwendete Steckverbinder	PoE Ethernet-Ports USB 2.0-Ports (für Tastatur und Maus) Displayport™ oder HDMI-Anschluss
NICHT verwendete Steckverbinder	Uplink-Port für Switch Uplink-Port für Server USB 3.2-Port (Vorderseite) Universal-Audiostecker (Vorderseite)

Setup in einem vorhandenen Netzwerk

Ein Überwachungsnetzwerk kann innerhalb eines vorhandenen Netzwerks erstellt werden. Dies bedeutet, dass das Überwachungsnetz vom vorhandenen Netzwerk getrennt ist.

Hinweis

Bei Verwendung eines zusätzlichen Rekorders, z. B. AXIS S30 Recorder, leitet die Appliance keine Netzwerkdaten aus dem Überwachungsnetzwerk zur Aufzeichnung an das Servernetzwerk weiter. Stellen Sie sicher, dass AXIS S30 Recorder mit demselben Netzwerk wie die Kameras verbunden sind.

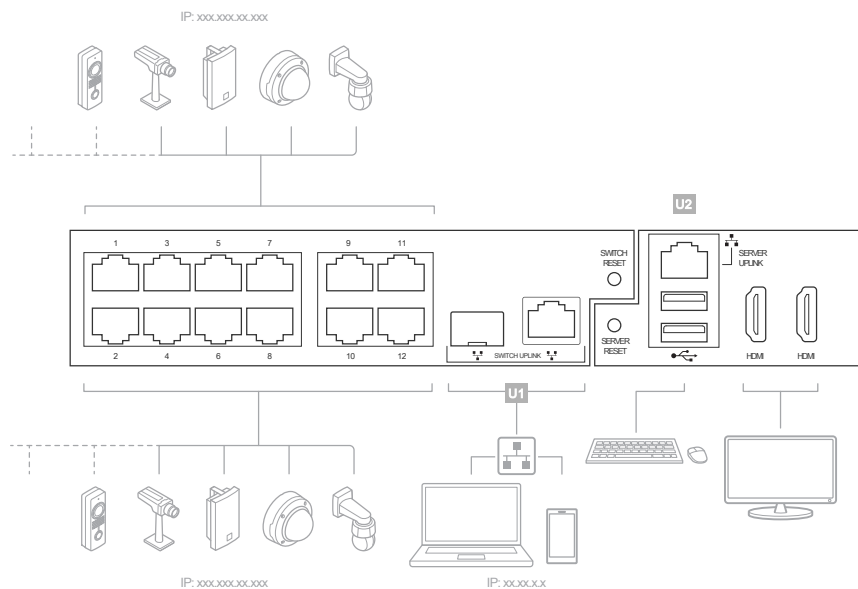


Schwierigkeitsgrad	Erweitert
Vorteile	Möglichkeit zur Verwendung eines AXIS Camera Station Pro Client, um über das Netzwerk eine Verbindung zur S22-Serie herzustellen. Netzwerk-Segregation
Einschränkungen	Ggf. ist die Befolgung der Netzwerkrichtlinien des Unternehmens erforderlich
Erforderliche Maßnahmen	Standardkennwort für den integrierten Switch ändern AXIS Camera Station Pro Lizenz registrieren

Verwendete Steckverbinder	PoE Ethernet-Ports Ethernet-Anschluss – Server-Uplink für die Verbindung zum Netzwerk (Optional) USB 2.0-Ports (für Tastatur und Maus) (Optional) Displayport™ oder HDMI-Anschluss
NICHT verwendete Steckverbinder	Uplink-Port für Switch USB 3.2-Port (Vorderseite) Universal-Audiostecker (Vorderseite)

Schließen Sie den Switch direkt an das Unternehmensnetzwerk an

Bei diesem Setup wird das System direkt in Ihr bestehendes Unternehmensnetzwerk integriert, so dass der Zugriff auf die Kameras und ihre Überwachung von jedem beliebigen Punkt des Netzwerks aus möglich ist.



Schwierigkeitsgrad	Erweitert
Vorteile	Die Kameras sind über das Unternehmensnetzwerk zugänglich und können mit einem SNMP-Server überwacht werden.
Einschränkungen	Ggf. ist die Befolgung der Netzwerkrichtlinien des Unternehmens erforderlich
Erforderliche Maßnahmen	Schalten Sie DHCP am Switch aus Ändern Sie die IP-Adresse des Switches in eine statische IP-Adresse im Unternehmensnetzwerk Stellen Sie die interne Netzwerkkarte des PCs auf DHCP oder eine statische IP im Unternehmensnetzwerk ein. Ändern Sie das Standard-Kennwort des Switches. Konfigurieren und Registrieren von AXIS Camera Station Pro

Verwendete Steckverbinder	PoE Ethernet-Ports Switch-Uplink-Port (U1) (Optional) USB 2.0-Ports (für Tastatur und Maus) (Optional) Displayport™ oder HDMI-Anschluss
NICHT verwendete Steckverbinder	PC-Uplink-Port (U2) USB 3.2-Port (Vorderseite) Universal-Audiostecker (Vorderseite)

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.

Hinweis

Die Einstellungen gelten für den Server. Wechseln Sie zur Verwaltungsseite des Switches, um die Einstellungen für den Switch zu ändern. Siehe *Einstellungen, on page 31*.

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.

Mit einem Server verbinden

Der AXIS Camera Station S2216 Mk II Appliance-Client erlaubt es Ihnen, sich auf verschiedene Weise mit einem oder mehreren Servern zu verbinden:

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 10*.

Hinweis

- Bei der ersten Verbindung mit einem Server überprüft der Client die Zertifikats-ID des Servers. Um sicherzustellen, dass Sie eine Verbindung zum richtigen Server herstellen, vergleichen Sie die Zertifikats-ID mit der in der Dienststeuerung von AXIS Camera Station S2216 Mk II Appliance angezeigten ID.

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 für alle verbundenen Server zu löschen, klicken Sie auf Delete saved passwords (Gespeicherte Kennwörter löschen) .
Proxy-Einstellungen des Klienten ändern	Wenn Sie keine Verbindung zu einem Server herstellen können, müssen Sie möglicherweise die Proxy-Einstellungen Ihres Clients aktualisieren. Client-Proxyeinstellungen ändern anklicken.

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 angeführt wird, 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

Für noch mehr Sicherheit und Funktionalität wird **Axis Secure Remote Access (v1)** auf **Axis Secure Remote Access v2** aktualisiert. Die aktuelle Version läuft am 1. Dezember 2025 aus und es wird dringend empfohlen, dass Sie Ihre Version vorher auf **Axis Secure Remote Access v2** aktualisieren.

Was bedeutet das für Ihr AXIS Camera Station S2216 Mk II Appliance System?

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

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 S2216 Mk II Appliance-Server** befindet, müssen Sie die Proxy-Einstellungen in Windows auf dem **AXIS Camera Station S2216 Mk II 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 Pro konfigurieren

Vorbereitungen:

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

Nach Abschluss der Konfiguration können Sie mit AXIS Camera Station Pro arbeiten:

1. *Das Video Management System starten*
2. *Geräte hinzufügen*
3. *Konfigurieren des Aufzeichnungsverfahrens, on page 12*
4. *Live-Video ansehen, on page 12*
5. *Aufzeichnungen anzeigen, on page 12*
6. *Lesezeichen hinzufügen, on page 12*
7. *Aufzeichnungen exportieren, on page 12*
8. *Aufzeichnungen mit AXIS File Player wiedergeben und überprüfen, on page 12*

Das Video Management System starten

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

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

Geräte hinzufügen

Wenn Sie AXIS Camera Station S2216 Mk II Appliance zum ersten Mal aufrufen, wird die Seite **Add devices (Geräte hinzufügen)** geöffnet, auf der das Netzwerk nach Geräten durchsucht wird, die hinzugefügt werden sollen.

1. Wählen Sie hinzuzufügende Geräte aus der Liste aus. Wenn Sie ein Gerät nicht finden können, klicken Sie auf **Manual search (Manuelle Suche)** oder geben Sie einen Suchbegriff ein, um die Ergebnisse einzugrenzen.
2. Klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf **Close (Schließen)**, um die Konfiguration zu überspringen und später fortzufahren. So fahren Sie jetzt mit der Konfiguration fort:
 - 3.1. Wählen Sie **Quick configuration (Schnellkonfiguration)** oder **Site Designer configuration (Site Designer Konfiguration)**. Weitere Informationen, siehe .
 - 3.2. Wählen Sie **Add image overlay for date, time, and text (Overlay für Datum, Uhrzeit und Text hinzufügen)**, um Overlays zu allen Axis Kameras hinzuzufügen, die noch keine haben.
 - 3.3. Klicken Sie auf **Next (Weiter)**.
 - 3.4. Wählen Sie Ihre bevorzugte **Aufzeichnungsmethode** aus.
 - 3.5. Klicken Sie auf **Next (Weiter)**.

- 3.6. Wählen Sie Ihre **Retention time (Aufbewahrungszeit)** und den **Recording storage (Aufzeichnungsspeicher)** aus und klicken Sie auf **Finish (Fertigstellen)**, um die Konfiguration zu übernehmen.

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.  anklicken.
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.  anklicken, 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.  anklicken, um die Aufzeichnungshinweise anzeigen zu können.
4. Die digitale Signatur überprüfen:
 - 4.1. Gehen Sie zu **Tools (Werkzeuge) > Verify digital signature (Digitale Signatur überprüfen)**.
 - 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. Anhand 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 die Proxy- oder Firewall-Einstellungen, bevor Sie AXIS Camera Station S2216 Mk II Appliance verwenden, falls sich Client, Server und die angeschlossenen Netzwerkgeräte in unterschiedlichen Netzwerken befinden.

Client-Proxyeinstellungen

Wenn sich ein Proxy-Server zwischen dem Client und dem Server befindet, müssen Sie die Proxy-Einstellungen in Windows auf dem Client-Computer konfigurieren. Weitere Informationen erhalten Sie vom Axis Support.

Proxyeinstellungen des Servers

Wenn sich der Proxy-Server zwischen dem Netzwerkgerät und dem Server befindet, müssen Sie die Proxy-Einstellungen in Windows auf dem Server konfigurieren. Weitere Informationen erhalten Sie vom Axis Support.

NAT und Firewall

Wenn ein NAT oder eine Firewall den Client und den Server voneinander trennt, konfigurieren Sie diese so, dass der in AXIS Camera Station S2216 Mk II Appliance „Service Control“ angegebene HTTP-Port, TCP-Port und Streaming-Port durchgelassen werden. Wenden Sie sich bitte an Ihren Netzwerk-Administrator, um Unterstützung zu erhalten.

Server-Port-Konfiguration

Der AXIS Camera Station S2216 Mk II Appliance-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 AXIS Camera Station S2216 Mk II Appliance-Server, die Kameras, Video-Encoder und Zusatzgeräte in einem sicheren, vom Büronetz separaten Netzwerk. Sie können den AXIS Camera Station S2216 Mk II 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.

Um die automatische Lizenzierung zu verwenden, müssen Sie Ihr System registrieren und mit einer Organisation verbinden.

1. Rufen Sie **Configuration (Konfiguration) > Licenses (Lizenzen) > Management (Verwaltung)** auf.
2. Stellen Sie sicher, dass **Automatic licensing (Automatische Lizenzierung)** eingeschaltet ist.
3. Klicken Sie auf **Register... (Registrieren...)**.
4. Melden Sie sich mit Ihrem MyAxis Konto an und befolgen Sie die Anweisungen auf dem Bildschirm.
5. Klicken Sie auf **Go to AXIS License Manager (AXIS License Manager aufrufen)**, um Ihre Lizenzen zu verwalten. Weitere Informationen finden Sie unter *My Systems – Benutzerhandbuch auf help.axis.com*.

Ein System offline lizensieren

So lizenzieren Sie Ihr System manuell:

1. Rufen Sie **Configuration (Konfiguration) > Licenses (Lizenzen) > Management (Verwaltung)** auf.
2. **Automatic licensing (Automatische Lizenzierung)** deaktivieren.
3. Klicken Sie auf **Export system file... (Systemdatei exportieren...)** und speichern Sie die Datei auf dem Computer.

Hinweis

Sie müssen über eine Internetverbindung verfügen, um auf AXIS License Manager zugreifen zu können. Falls Ihr Client-Computer nicht mit dem Internet verbunden ist, kopieren Sie die Systemdatei auf einen Computer mit Internetverbindung.

4. Öffnen Sie *AXIS License Manager*.
5. Im AXIS License Manager:
 - 5.1. Wählen Sie die richtige Organisation aus oder erstellen Sie eine, falls noch keine vorhanden ist. Weitere Informationen finden Sie unter *My Systems – Benutzerhandbuch auf help.axis.com*.
 - 5.2. Rufen Sie **System setup (Systemsetup)** auf.
 - 5.3. **Upload system file (Systemdatei hochladen)** anklicken.
 - 5.4. Klicken Sie auf **Upload system file (Systemdatei hochladen)** und wählen Sie die Systemdatei aus.
 - 5.5. **Upload system file (Systemdatei hochladen)** anklicken.
 - 5.6. Klicken Sie auf **Download license file (Lizenzdatei herunterladen)**.
6. Zurück zum AXIS Camera Station S2216 Mk II Appliance Client.
7. Klicken Sie auf **Import license file... (Lizenzdatei importieren...)** und wählen Sie Ihre Lizenzdatei aus.
8. Klicken Sie auf **Go to AXIS License Manager (AXIS License Manager aufrufen)**, um Ihre Lizenzen zu verwalten.

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. Rufen Sie **Settings > Accounts > Other users > Add other user** (Einstellungen > Konten > Andere Benutzer > Andere Benutzer hinzufügen) auf und klicken Sie auf **Add account** (Konto hinzufügen).
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.

Erstellen Sie ein Administratorenkonto

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 Pro Benutzerkonten verwalten

Benutzerberechtigungen

Rufen Sie **Configuration (Konfiguration) > Security (Sicherheit) > User permissions (Benutzerrechte)** auf, um die Benutzer und Gruppen in AXIS Camera Station S2216 Mk II Appliance anzuzeigen.

Hinweis

Administratoren von Computern, auf denen AXIS Camera Station S2216 Mk II Appliance Server ausgeführt werden, erhalten automatisch Administratorrechte in AXIS Camera Station S2216 Mk II 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 Zugriff auf Kamera X hat und gleichzeitig einer Gruppe angehört, die Zugriff auf die Kameras Y und Z hat, Zugriff auf alle 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 S2216 Mk II Appliance zugreifen. Um einen Benutzer zu AXIS Camera Station S2216 Mk II 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 **Add (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 S2216 Mk II 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 (Speichern)**.

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 erforderlich, um Zutritt zur Systemkonfiguration zu haben.

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 S2216 Mk II Appliance mit Ausnahme der Systemkonfiguration.

Viewer – 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	Erlaubt 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 für Kameras mit mechanischem PTZ-Antrieb und Auswahl von Mechanical PTZ (Mechanischer PTZ) verfügbar.

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 S2216 Mk II Appliance.
Edit (Bearbeiten):	Ermöglicht die Bearbeitung von Ansichten unter AXIS Camera Station S2216 Mk II 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 (Alarme 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.
Zugriffsverwaltung	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	Erlaubt das Konfigurieren der Systemzustandsüberwachung.
Auf Systemzustandsüberwachung zugreifen	Erlaubt den Zugriff auf die Systemzustandsüberwachung.

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 Geräts für die Aufzeichnung zu gewährleisten, führen Sie bitte die Installation der Zertifikate für das Jahr 2023 noch vor diesem Zeitpunkt durch.

Die Installation der Zertifikate für 2023 erfordert Windows 10 LTSC (Long-Term Servicing Channel) oder Windows 11 LTSC. Wenn Ihr Gerät noch unter die Garantie fällt, aber Windows 10 SAC (Semi-Annual Channel) anstelle einer LTSC-Version nutzt, wenden Sie sich bitte an den technischen Support von Axis. Dort kann man Ihnen mitteilen, ob eine Aktualisierung auf eine LTSC-Version möglich ist, 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 Updates für den Windows-Boot-Manager und Sperrlisten für neue Sicherheitslücken.

Den 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 den Registrierungseditor.
2. Wechseln Sie zu `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing`.
3. Prüfen Sie den Wert `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 (Windows-Sicherheit).
2. Rufen Sie Device security (Gerätesicherheit) auf.
3. Prüfen Sie unter Secure Boot (Sicheres Hochfahren) die Statusmeldung. Wenn das Zertifikat aktuell ist, wird auf der Karte Folgendes angezeigt: "Secure Boot is on and all required certificate updates have been applied. No further certificate changes are needed." (Secure Boot ist aktiviert und alle erforderlichen Aktualisierungen des Zertifikats wurden vorgenommen. Es sind keine weiteren Zertifikatsänderungen notwendig.)



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

Hinweis

„Windows-Sicherheit“ zeigt den Zertifikatsstatus nur an, wenn auf Ihrem Gerät das kumulative Update vom 14. April 2026 oder ein neueres Update installiert ist. Sollte keine Meldung zum Zertifikatsstatus angezeigt werden, 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 stattdessen die Zertifikate für 2023 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 ein BIOS-Update, sobald eines 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 (Sicheres Hochfahren)** auf, um den Status Ihres Zertifikats zu prüfen.

4. Falls das Zertifikat nach der Installation der neuesten Updates nicht aktualisiert wird, prüfen Sie den Registrierungswert **UEFICA2023Status**. Sollte Ihr Gerät weiterhin nicht für das automatische Update geeignet sein, aktualisieren Sie 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 Richtlinieneditor für die lokalen Gruppen 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 Benutzern 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**.

Hinzufügen von zusätzlichem Speicher

Der Speicherplatzbedarf kann variieren. Die Vorhaltezeit der gespeicherten Daten oder die Speicherung hochauflösender Aufzeichnungen erfordert häufig die Installation von mehr Speicher. In diesem Abschnitt wird erklärt, wie Sie eine zusätzliche Festplatte in Ihrem AXIS S22-Produkt installieren.

Hinweis

Die nachstehenden Anweisungen befolgen, um den entsprechenden AXIS S22-Produkten zusätzlichen Speicher hinzuzufügen. Diese Anweisungen gelten unverändert, und Axis Communications AB übernimmt keine Verantwortung für den Verlust von Daten oder Fehlkonfigurationen während dieser Schritte. Zur Sicherung geschäftskritischer Daten sollten die üblichen Vorsichtsmaßnahmen getroffen werden. Das folgende Verfahren zum Erweitern des Speichers wird vom technischen Support von Axis nicht unterstützt.

Hinweis

Um elektrostatische Entladungen zu vermeiden, empfehlen wir, bei Arbeiten an internen Systemkomponenten stets eine Antistatikmatte und ein Antistatikband zu verwenden.

Gewährleistung

Ausführliche Informationen zur Gewährleistung finden Sie unter: www.axis.com/support/warranty.



Rufen Sie zur Wiedergabe dieses Videos die Webversion dieses Dokuments auf.

Blende entfernen

1. Lösen Sie die beiden Flügelschrauben beidseits der Blende.
2. Blende entfernen.

Festplatte installieren

⚠ VORSICHT

- Verwenden Sie nur für den Betrieb mit der AXIS S22-Serie getestete und zugelassene Festplatten.
- Achten Sie beim Einbau einer Festplatte darauf, den Festplattenträger ganz einzuschieben. Der Laufwerksträger rastet mit einem hörbaren Klicken ein.
- Stellen Sie vor der Installation einer Festplatte sicher, dass das Netzkabel getrennt ist.

1. Fahren Sie das System herunter, und stellen Sie sicher, dass die Stromversorgung ausgeschaltet ist.
2. Ziehen Sie das Stromkabel.
3. Die Entriegelungstaste auf der Vorderseite des Festplattenträgers drücken und den Festplattenträgergriff öffnen.
4. Ziehen Sie den Festplattenträger am Griff heraus.
5. Setzen Sie eine Festplatte in den Festplattenträger ein.
6. Befestigen Sie die Festplatte mit vier Schrauben am Festplattenträger.
7. Schieben Sie den Festplattenträger in den Festplattenschacht, bis der Träger an der Rückwand einrastet.
8. Den Festplattenträgergriff schließen, um die Festplatte an ihrem Platz zu verriegeln.
9. Bringen Sie die Frontblende wieder an.
10. Starten Sie das System.

Neuen Aufzeichnungsdatenträger hinzufügen

1. Erstellen und formatieren Sie eine neue Festplattenpartition in Windows:
 - 1.1. Klicken Sie mit der rechten Maustaste auf das **Start menu (Startmenü)**, und wählen Sie **Disk Management (Datenträgerverwaltung)**.
 - 1.2. Klicken Sie auf **OK**, wenn das Popup-Fenster **Initialize Disk (Datenträger initialisieren)** erscheint. Falls es nicht erscheint, klicken Sie mit der rechten Maustaste auf die neue Festplatte und wählen Sie **Initialize Disk (Datenträger initialisieren)**.
 - 1.3. Klicken Sie mit der rechten Maustaste auf einen nicht zugeordneten Bereich des neu initialisierten Datenträgers und wählen Sie **New Simple Volume (Neues einfaches Laufwerk)** aus.
 - 1.4. Folgen Sie dem Assistenten, um die Datenträgergröße einzustellen, einen Laufwerksbuchstaben zuzuweisen und die Partition zu formatieren.
 - 1.5. Beenden Sie den Assistenten, um das neue einfache Laufwerk zu erstellen.
2. Fügen Sie einen neuen Speicher für die Aufzeichnung in AXIS Camera Station Pro hinzu:
 - 2.1. AXIS Camera Station Pro öffnen.
 - 2.2. Gehen Sie zu **Storage (Speicher) > Management**.
 - 2.3. Klicken Sie auf **Add... (Hinzufügen...)**
 - 2.4. Wählen Sie das neu hinzugefügte Laufwerk aus und klicken Sie auf **OK**.
 - 2.5. Gehen Sie zu **Storage (Speicher) > Selection (Auswahl)**.
 - 2.6. Wählen Sie die Geräte aus, deren Aufzeichnungen Sie auf das neue Laufwerk übertragen möchten.
 - 2.7. Wählen Sie in der Dropdown-Liste **Store to (Speichern unter)** das neue Laufwerk aus und klicken Sie auf **Apply (Übernehmen)**.

Weitere Informationen zur Speicherverwaltung finden Sie im *AXIS Camera Station Pro – Benutzerhandbuch*.

Erstellen eines RAID-Laufwerks

1. Stellen Sie sicher, dass die im RAID-Laufwerk zu verwendenden Festplatten erkannt werden.
 - 1.1. Schalten Sie das Gerät ein und drücken Sie sofort F12, bis das Axis Logo angezeigt wird.
 - 1.2. Im UEFI-Startmenü die Option **Device Configuration (Gerätekonfiguration)** auswählen und Enter drücken.
 - 1.3. Vergewissern Sie sich im Menü „Intel® Rapid Storage Technology“, dass die Festplatten unter **Non-RAID Physical Disks (Physische Nicht-RAID-Festplatten)** korrekt angezeigt werden.

Hinweis

Auf Geräten mit physischem Speicherplatz für nur ein zusätzliches Einzellaufwerk sind nur RAID 0 und RAID 1 verfügbar.

2. Wählen Sie im Menü „Intel Rapid Storage Technology“ die Option **Create RAID Volume (RAID-Laufwerk erstellen)** aus und bestätigen Sie mit Enter.
3. Geben Sie einen Namen für das Volume ein.
4. Wählen Sie den gewünschten RAID-Level aus.
 - 4.1. **RAID Level** (RAID-Ebene) auswählen und Enter drücken.
 - 4.2. Im Popup-Dialogfeld die gewünschte RAID-Ebene auswählen und Enter drücken.
5. Wählen Sie die für das Laufwerk zu verwendenden Festplatten aus.
 - 5.1. Eine Festplatte auswählen und Enter drücken.
 - 5.2. Wählen Sie **X** aus, um diese Festplatte in das Volume aufzunehmen.
 - 5.3. Wiederholen Sie diesen Vorgang, bis Sie alle Festplatten ausgewählt haben die Sie verwenden möchten.
6. Verwenden Sie für **Stripe Size (Stripe-Größe)** und **Capacity (Kapazität)** die Standardwerte, wenn nicht anders angegeben.
7. **Create Volume** (Volume erstellen) auswählen und Enter drücken.
8. Im Menü „Intel Rapid Storage Technology“ erscheint das neu erstellte RAID-Laufwerk unter **RAID Volumes (RAID-Laufwerke)**.
9. Drücken Sie Esc und dann Y, um zu speichern und zum UEFI-Menü zu gelangen.
10. STRG + ALT+ DELETE drücken, um Ihr Gerät neu zu starten.

RAID-Laufwerk in Microsoft Windows® initiieren

Neues Volume konfigurieren:

1. Klicken Sie mit der rechten Maustaste auf das **Start menu (Startmenü)**, und wählen Sie **Disk Management (Datenträgerverwaltung)**.
2. Wählen Sie im Pop-up-Fenster „Initialize Disk (Datenträger initialisieren)“ die Option **GPT** und klicken Sie auf **OK**.
3. Klicken Sie mit der rechten Maustaste auf die nicht zugewiesene Festplatte und wählen Sie **New Simple Volume (Neues einfaches Laufwerk)** aus.
 - Befolgen Sie die Anweisungen des Setup-Assistenten.
4. Wenn der Setup-Assistent abgeschlossen ist, zeigt **Disk Management (Datenträgerverwaltung)** das neue Laufwerk an. Schließen Sie **Disk Management (Datenträgerverwaltung)**, damit das System das neue Laufwerk verwenden kann.

Den integrierten Switch verwalten

Der integrierte Switch

Die AXIS Camera Station S22 Mk II Appliance Series verfügt über einen integrierten Power over Ethernet (PoE)-Switch. Es ist möglich, diesen integrierten Switch zu konfigurieren und verwalten.

Der Switch hat die Aufgabe, den Verkehr im Netzwerk so zu trennen, dass Sicherheitskameras und der damit verbundene, vom Switch verwaltete Verkehr (PoE und Switch-Uplink-Port) nicht mit anderen Netzwerken geteilt werden.

Für die Energieverwaltung des Switches gelten folgende Regeln:

- Jeder Port kann je nach PoE-Klasse des betriebenen Geräts eine bestimmte Leistung reservieren. Sie können einem Port auch manuell Strom zuweisen.
- Wenn der tatsächliche Stromverbrauch eines bestimmten Ports die für diesen Port reservierte Leistung überschreitet, wird er heruntergefahren.
- Die Ports werden heruntergefahren, wenn der tatsächliche Stromverbrauch für alle Ports die Gesamtleistung übersteigt, die das Netzteil liefern kann. Die Ports werden dann entsprechend der Portpriorität heruntergefahren, wobei eine niedrigere Portnummer für eine höhere Priorität steht.

Bei der Verwaltungsseite des Switches anmelden

1. Gehen Sie zur Menüleiste.
 - Im Webbrowser die IP-Adresse des Switches eingeben. Standardmäßige Vorgehensweise: 192.168.10.1
 - Von AXIS Recorder Toolbox aus **Switch > Open the switch configuration (Switch > Switch-Konfiguration öffnen)** aufrufen.
2. Melden Sie sich mit Ihrem Benutzernamen und Kennwort an.
 - Der Benutzername lautet `admin`
 - Ihr Kennwort befindet sich auf einem Aufkleber, der oben auf dem Gerät angebracht oder als selbstklebender Aufkleber im Lieferumfang enthalten ist.

Klicken Sie in der Menüleiste auf **Log out** (Abmelden), um die Verwaltungsseite des Switches zu verlassen.

Laufende Konfiguration

Bei der laufenden Konfiguration handelt es sich um die Einstellungen, die derzeit auf Ihrem Gerät im Netzwerk aktiv und in Betrieb sind. Sie spiegelt den aktuellen Zustand Ihres Geräts und seine Funktionsweise in Echtzeit wider. Diese Änderungen werden beim Neustart Ihres Geräts jedoch nicht gespeichert.

Die Startkonfiguration hingegen ist der Satz von Einstellungen, die im nichtflüchtigen Speicher Ihres Geräts gespeichert sind. Diese Konfiguration wird beim Start oder Neustart Ihres Geräts geladen und angewendet.

Wenn Sie Änderungen in der Weboberfläche vornehmen und auf **Save (Speichern)** klicken, werden diese Änderungen in die laufende Konfiguration übernommen.

Um Ihre Einstellungen in der Startkonfiguration zu speichern, klicken Sie auf das Speichersymbol in der oberen rechten Ecke der Weboberfläche.

Wenn Änderungen in der laufenden Konfiguration noch nicht gespeichert wurden, blinkt das Symbol gelb.

Übersicht

Klicken Sie in der Menüleiste auf **Overview** (Übersicht).

Allgemeine Informationen

Kategorie	Komponente	Beschreibung
Ports-Übersicht	Aktive Ports	Die Anzahl der verwendeten Ports.
	Ports mit PoE	Die Anzahl der verwendeten PoE-aktivierten Ports.
	Ports gesperrt	Die Anzahl der gesperrten Ports.
Leistungsaufnahme	Aktuelle Position:	Die PoE-Leistung in Watt, die von Geräten verbraucht wird, und der Prozentsatz der verbrauchten PoE-Leistung aus der gesamten dedizierten PoE-Leistung.
	Geforderte Leistung	Gesamtleistung in Watt und Prozentsatz, der auf die jeweiligen Geräte entfällt.
Port-Status	Aktiv	Der Port wird verwendet.
	Inaktiv	Der Port ist einsatzbereit.
	Gesperrt	Der Port ist gesperrt.

Hinweis

Sie können einen Port anklicken, um weitere Informationen über ihn zu erhalten.

Verwaltung der Stromversorgung

Klicken Sie in der Menüleiste auf **Power management** (Energieverwaltung).

Portliste

Komponente	Beschreibung
Anschluss	Die Portnummer, an die das Gerät angeschlossen ist.
PoE	Der PoE-Status. Per Klick auf das Symbol kann PoE am Port ein- oder ausgeschaltet werden.
PoE-Klassifizierung	Die PoE-Klasse des angeschlossenen Geräts.
Priorität	Die Priorität der Leistungszuweisung an das angeschlossene Gerät. Standardmäßig ist die Priorität die Portnummer.
Stromverbrauch (W)	Die Leistung in Watt, die das an den Port angeschlossene Gerät verbraucht.
Geforderte Leistung (W)	Die Leistung in Watt, die das an den Port angeschlossene Gerät anfordert.
Zugewiesene Stromversorgung (W)	Hier können Sie die dem Port zugewiesene Leistung manuell anpassen. Das ist jedoch nur möglich, wenn als Energiezuweisungsmethode Manual (Manuell) ausgewählt ist.

Stromversorgung zuweisen

PoE-Leistung kann den angeschlossenen Geräten auf folgenden Wegen zugewiesen werden:

- **PoE-Klasse:** Der Switch ordnet PoE-Leistung ausgehend von der PoE-Klasse des angeschlossenen Geräts zu.
- **Manual (Manuell):** Die dem angeschlossenen Gerät zugewiesene PoE-Leistung kann manuell angepasst werden.

- **LLDP-MED:** Der Switch kommuniziert mit dem angeschlossenen Gerät und weist dynamisch PoE-Leistung nach Bedarf zu.

Hinweis

Die LLDP-MED-Leistungszuweisung funktioniert nur bei Kameras mit AXIS OS 9.20 oder höher.

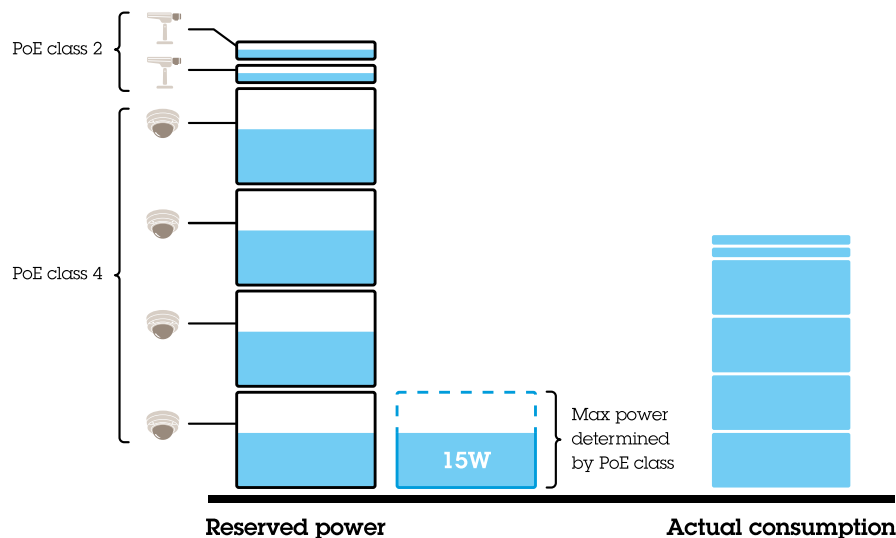
Energiezuweisungsmethode ändern:

1. Auf der Verwaltungsseite des Switches **Power management (Energieverwaltung)** aufrufen.
2. **PoE Class (PoE-Klasse), Manual (Manuell) oder LLDP-MED (LLDP-MED)** unter **Allocate power (Leistung zuweisen)** auswählen
3. Wenn Sie **Manual (Manuell)** ausgewählt haben, können Sie die dem angeschlossenen Gerät zugewiesene Leistung in der Spalte **Power allocated (Zugewiesene Leistung)** ändern.
4. Zum Ändern der Priorität des angeschlossenen Geräts eine Priorität für das entsprechende Gerät auswählen. Die Priorität anderer Geräte ändert sich automatisch.

Beispiel:

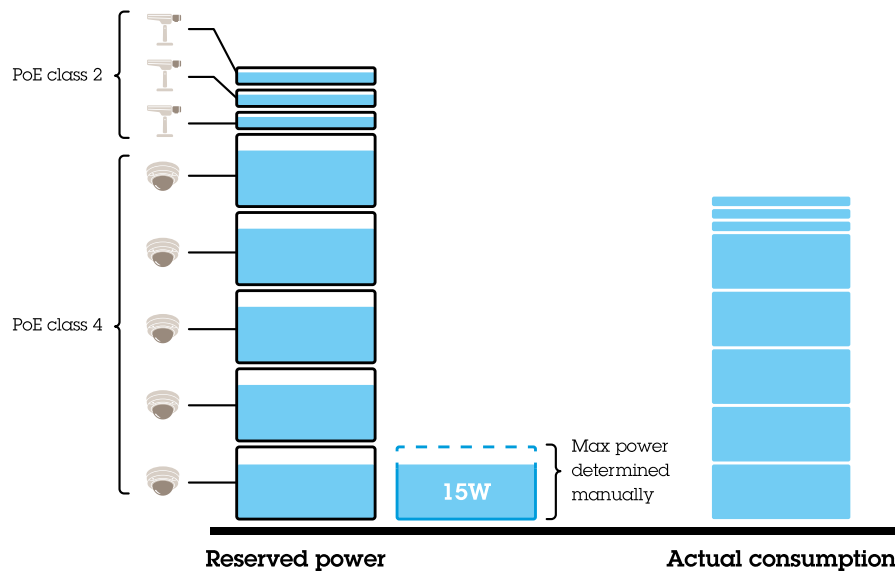
In diesem Beispiel hat der Switch ein Gesamtleistungsbudget von 135 W. Ein Gerät der PoE-Klasse 4 fordert 30 W Leistung an, verbraucht aber nur 15 W. Ein Gerät der PoE-Klasse 2 fordert 7 W Leistung an, verbraucht aber nur 5 W.

Leistung nach PoE-Klasse zuweisen



Die von jedem Gerät angeforderte Leistung wird von der PoE-Klasse bestimmt. Der Switch kann 4 Geräte der PoE-Klasse 4 und 2 Geräte der PoE-Klasse 2 mit Strom versorgen. Die angeforderte Gesamtleistung beträgt $(4 \times 30) + (2 \times 7) = 134$ W. Die tatsächlich verbrauchte Leistung beträgt $(4 \times 15) + (2 \times 5) = 70$ W. Auf diese Weise wird allen angeschlossenen Geräten ausreichend Strom garantiert und die Priorität ist weniger wichtig.

Energie manuell zuweisen



Die angeforderte Leistung wird für Geräte der PoE-Klasse 4 manuell auf 20 W eingestellt. Der Switch kann 5 Geräte der PoE-Klasse 4 und 3 Geräte der PoE-Klasse 2 mit Strom versorgen. Die angeforderte Gesamtleistung beträgt $(5 \times 20) + (3 \times 7) = 121$ W. Die tatsächlich verbrauchte Leistung beträgt $(5 \times 15) + (3 \times 5) = 90$ W. Auf diese Weise wird allen angeschlossenen Geräten ausreichend Strom garantiert und die Priorität ist weniger wichtig.

PoE aktivieren und deaktivieren

PoE an einem Port aktivieren

1. Klicken Sie in der Menüleiste auf **Overview** (Übersicht).
2. In der PoE-Spalte auf  klicken, um PoE am entsprechenden Port zu aktivieren.

PoE an einem Port deaktivieren

1. Klicken Sie in der Menüleiste auf **Overview** (Übersicht).
2. In der PoE-Spalte auf  klicken, um PoE am entsprechenden Port zu deaktivieren.

Ein- und Ausschalten von PoE an allen Ports

1. Klicken Sie in der Menüleiste auf **Power management** (Energieverwaltung).
2. Um PoE an allen Ports auszuschalten, öffnen Sie die Drop-down-Liste **PoE ports state** (Status PoE-Ports) und wählen Sie **Turn off all** (Alle ausschalten) aus.
3. Um PoE an allen Ports einzuschalten, öffnen Sie die Drop-down-Liste **PoE ports state** (Status PoE-Ports) und wählen Sie **Turn on all** (Alle einschalten) aus.

Netzwerkübersicht

Die Netzwerkübersicht liefert detaillierte Informationen über den Datenverkehr der einzelnen Ports.

PoE-Ports

Komponente	Beschreibung
Anschluss	Die Portnummer, an die das Gerät angeschlossen ist.
Gerät	Der Name des Geräts, das an den Port angeschlossen ist.
IP-Adresse	Die IP-Adresse des Geräts, das an den Port angeschlossen ist.
MAC-Adresse	Die MAC-Adresse des Geräts, das an den Port angeschlossen ist.

Receive (Empfangen)	Die durchschnittliche Datenrate in Megabit pro Sekunde für am Port eingehende Daten.
Transmit (Senden)	Die durchschnittliche Datenrate in Megabit pro Sekunde für am Port ausgehende Daten.
Packet sent (Gesendete Pakete)	Die Anzahl der Datenpakete, die der Switch an das Netzwerk übertragen hat.
Packet received (Empfangene Pakete)	Die Anzahl der Datenpakete, die der Switch vom Netzwerk empfangen hat.
Packet lost (Verlorene Pakete)	Anzahl und Prozentsatz der Datenpakete, die aufgrund von Netzwerkproblemen ihr Ziel nicht erreichen konnten.
Lock (Sperren)	Zeigt an, ob der Port gesperrt ist. Per Klick auf das Symbol kann der Port gesperrt oder entsperrt werden.

Ports sperren und entsperren

Ports können mit einer MAC-Adresse verknüpft werden, sodass nur Datenverkehr von der entsprechenden MAC-Adresse übergeben wird. Dadurch steigt die Sicherheit und es wird verhindert, dass nicht autorisierte Benutzer einen Laptop oder andere Geräte mit dem Sicherheitsnetzwerk verbinden.

Verknüpfen einer MAC-Adresse mit einem Port

1. Klicken Sie in der Menüleiste auf **Network overview** (Netzwerkübersicht).
2. Klicken Sie in der Spalte **Lock (Sperren)** auf , um den betreffenden Port zu verknüpfen.

Lösen der Verknüpfung einer MAC-Adresse von einem Port

1. Klicken Sie in der Menüleiste auf **Network overview** (Netzwerkübersicht).
2. Klicken Sie in der Spalte **Lock (Sperren)** auf , um die Verknüpfung des betreffenden Ports zu lösen.

Sperren oder Entsperren aller Ports

1. Klicken Sie in der Menüleiste auf **Network overview** (Netzwerkübersicht).
2. Um alle Ports zu sperren, öffnen Sie das Drop-down-Menü **Lock ports** (Ports sperren) und wählen Sie **Lock all** (Alle sperren).
3. Um alle Ports freizugeben, öffnen Sie das Drop-down-Menü **Lock ports** (Ports sperren) und wählen Sie **Unlock all** (Alle freigeben).

Einstellungen

Netzwerkeinstellungen konfigurieren

Es ist möglich, die IP-Adresse des Switches zu ändern. Für die meisten Kamerainstallation empfehlen wir jedoch die Verwendung der Standardeinstellungen. Der Grund dafür ist, dass ein Überwachungsnetzwerk normalerweise von anderen Netzwerken, z. B. einem Unternehmens-LAN, isoliert ist. In diesem Fall wird das Überwachungsnetzwerk nur zum Verwalten und Erfassen von Überwachungsgeräten und Daten aus der auf dem Server installierten Videoverwaltungssoftware verwendet.

1. Rufen Sie in der Menüleiste **Settings > Network settings** (Einstellungen > Netzwerkeinstellungen) auf.
2. Geben Sie den Verbindungstyp, die IP-Adresse, die Subnetzmaske, das Gateway, den primären und sekundären DNS sowie den Hostnamen ein.

Hinweis

Die werksseitige Standardeinstellung lautet: statische IP-Verbindung mit der Adresse 192.168.10.1 und Subnetzmaske mit der Adresse 255.255.255.0.

3. Klicken Sie auf **Save (Speichern)**.

Datum und Zeit konfigurieren

1. Rufen Sie in der Menüleiste **Settings > Date and time** (Einstellungen > Datum und Uhrzeit) auf.
2. Land und Zeitzone auswählen.
3. **Manual (Manuell)** auswählen, um die Zeit manuell einzustellen, und dann die Zeit manuell einstellen.
4. **NTP server (NTP-Server)** auswählen, um einen NTP-Server einzurichten, und die NTP-Server-Adresse eingeben.

Hinweis

NTP funktioniert nur, wenn der Switch mit einem Netzwerk verbunden und mit Internetzugriff konfiguriert ist.

5. Klicken Sie auf **Save (Speichern)**.

DHCP-Server konfigurieren

Der Switch kann so konfiguriert werden, dass er seinen internen DHCP-Server verwendet, um angeschlossenen Geräten IP-Adressen zuzuweisen. Wird die Switch-Uplink-Verbindung verwendet, um Geräten den Zugriff zu gestatten oder den Zugriff durch externe Anwendungen zu ermöglichen, müssen das Gateway und die DNS-Adressen angegeben werden.

1. Rufen Sie in der Menüleiste **Settings > DHCP server** (Einstellungen > DHCP-Server) auf.
2. Wählen Sie **Enable DHCP server (DHCP-Server aktivieren)** aus.
3. Geben Sie die Start-IP-Adresse, die End-IP-Adresse, die Subnetzmaske, das Gateway, den primären und sekundären DNS, die Leaselänge und den Domännennamen ein.
4. Klicken Sie auf **Save (Speichern)**.

SNMP konfigurieren

1. Rufen Sie in der Menüleiste **Settings > SNMP** (Einstellungen > SNMP) auf.
2. Server-Namen, Kontakt und Standort auswählen, die für die SNMP-Verbindung verwendet werden sollen.
3. Soll SNMPV1 oder SNMPV2c verwendet werden, dann **SNMPV1 / SNMPV2c** und Lesezugriff eingeben.
4. Soll SNMPV3 verwendet werden, **SNMPV3 (MD5)** auswählen und den Benutzernamen und das Kennwort eingeben.

Hinweis

Derzeit wird lediglich die MD5-Authentifizierung unterstützt, die für SNMP verwendet wird.

5. Klicken Sie auf **Save (Speichern)**.

Maintenance (Wartung):

Firmware aktualisieren

1. Rufen Sie in der Menüleiste **Maintenance > Update firmware** (Wartung > Firmware aktualisieren) auf.
2. Die Firmware-Datei ziehen und ablegen oder auf **Browse (Durchsuchen)** klicken und zur Firmware-Datei navigieren.
3. Klicken Sie auf **Upload (Hochladen)**.
4. Nachdem die Firmware aktualisiert wurde, starten Sie den Switch neu.

Den Switch neu starten

Wichtig

Während der Switch neu gestartet wird, verlieren alle angeschlossenen Geräte vorübergehend die Verbindung mit dem Switch einschließlich PoE.

1. Rufen Sie in der Menüleiste **Maintenance > Reboot switch** (Wartung > Switch neu starten) auf.
2. Auf **Reboot (Neustart)** und **Yes (Ja)** klicken.
3. Wenn der Switch nach einigen Minuten neu gestartet wird, mit Benutzernamen und Kennwort anmelden.

Switch-Einstellungen sichern

Hinweis

Die Sicherungsdatei enthält den Benutzernamen und das Kennwort.

1. Rufen Sie in der Menüleiste **Maintenance > Backup and restore** (Wartung > Sichern und Wiederherstellen) auf.
2. Auf **Create a backup file (Sicherungsdatei erstellen)** klicken. Dadurch wird eine Sicherungsdatei im .bin-Format erstellt und in Ihrem **Downloads**-Ordner gespeichert.

Switch-Einstellungen wiederherstellen

Hinweis

Damit die Einstellungen des Switch wiederhergestellt werden können, muss zuvor eine Sicherungsdatei erstellt worden sein.

1. Rufen Sie in der Menüleiste **Maintenance > Backup and restore** (Wartung > Sichern und Wiederherstellen) auf.
2. Sicherungsdatei ziehen und ablegen oder auf **Browse (Durchsuchen)** klicken und zur Sicherungsdatei navigieren.
3. Klicken Sie auf **Upload (Hochladen)**.

Die Wiederherstellung des Switches aus der Sicherungsdatei kann einige Minuten dauern. Nach Wiederherstellung der Einstellungen wird der Switch automatisch neu gestartet und Sie müssen sich erneut anmelden.

Zertifikate verwalten

1. Rufen Sie in der Menüleiste **Maintenance > Manage certificates** (Wartung > Zertifikate verwalten) auf.
2. Auf  klicken und zur eigenen Schlüsseldatei navigieren.
3. Auf  klicken und zur Zertifikatsdatei navigieren.
4. Auf  klicken und zur CA-Bundle-Datei navigieren.
5. Klicken Sie auf **Save (Speichern)**.
6. Den Switch neu starten.

Kennwort ändern

Das Standardkennwort des Switch kann zu einem selbst gewählten Kennwort geändert werden.

Wichtig

Wählen Sie ein Kennwort, das Sie sich merken können. Wenn Sie das Kennwort vergessen haben, erfahren Sie unter *Zurücksetzen auf die Werkseinstellungen, on page 34*, wie Sie das Kennwort wiederherstellen.

1. Rufen Sie in der Menüleiste **Maintenance > Change password** (Wartung > Kennwort ändern) auf.
2. Den Anweisungen entsprechend das alte und das neue Kennwort eingeben.
3. Klicken Sie auf **Save** (Speichern).

Webeinstellungen konfigurieren

1. Rufen Sie in der Menüleiste **Maintenance > Web settings** (Wartung > Interneteinstellungen) auf.
2. Geben Sie die Portnummer ein.

Hinweis

- Wenn Sie die Port-Nummer ändern, notieren Sie sich die neue Port-Nummer. Wenn Sie die neue Port-Nummer vergessen haben, erfahren Sie unter *Zurücksetzen auf die Werkseinstellungen, on page 34*, wie Sie die werksseitige Standardeinstellung wiederherstellen.
- Wir empfehlen, HTTPS aktiviert zu lassen.

Zurücksetzen auf die Werkseinstellungen

Halten Sie die Reset-Taste fünf Sekunden lang gedrückt, um den Switch auf seine werksseitigen Standardeinstellungen zurückzusetzen.

Sie können den Switch auch über die Weboberfläche zurücksetzen:

1. Rufen Sie in der Menüleiste **Maintenance > Reset to factory default settings** (Wartung > Zurücksetzen auf Werkseinstellungen) auf.
2. **Reset (Zurücksetzen)** und **Yes (Ja)** klicken.

Nach dem Zurücksetzen wird der Switch automatisch neu gestartet.

Protokolle

Klicken Sie in der Menüleiste auf **Logs** (Protokolle), um eine Liste der Protokolle anzuzeigen. Auf den Titel der Spalte klicken, um diese in alphabetischer Reihenfolge zu sortieren.

Komponente	Beschreibung
Time (Zeit)	Das Datum und die Uhrzeit des Protokollereignisses.
Level (Schweregrad)	Der Schweregrad, angezeigt in Form von Warnsymbolen.
Benutzer	Der Benutzer, der das Protokollereignis ausgelöst hat.
IP-Adresse	Die IP-Adresse des Benutzers, der das Protokollereignis ausgelöst hat.
Service	Der Dienst, mit dem das Protokollereignis zusammenhängt. Mögliche Werte sind Desktop, Netzwerk, System, ntpd, Speicher, dhcp usw.
Veranstaltung	Eine Beschreibung des Protokollereignisses.

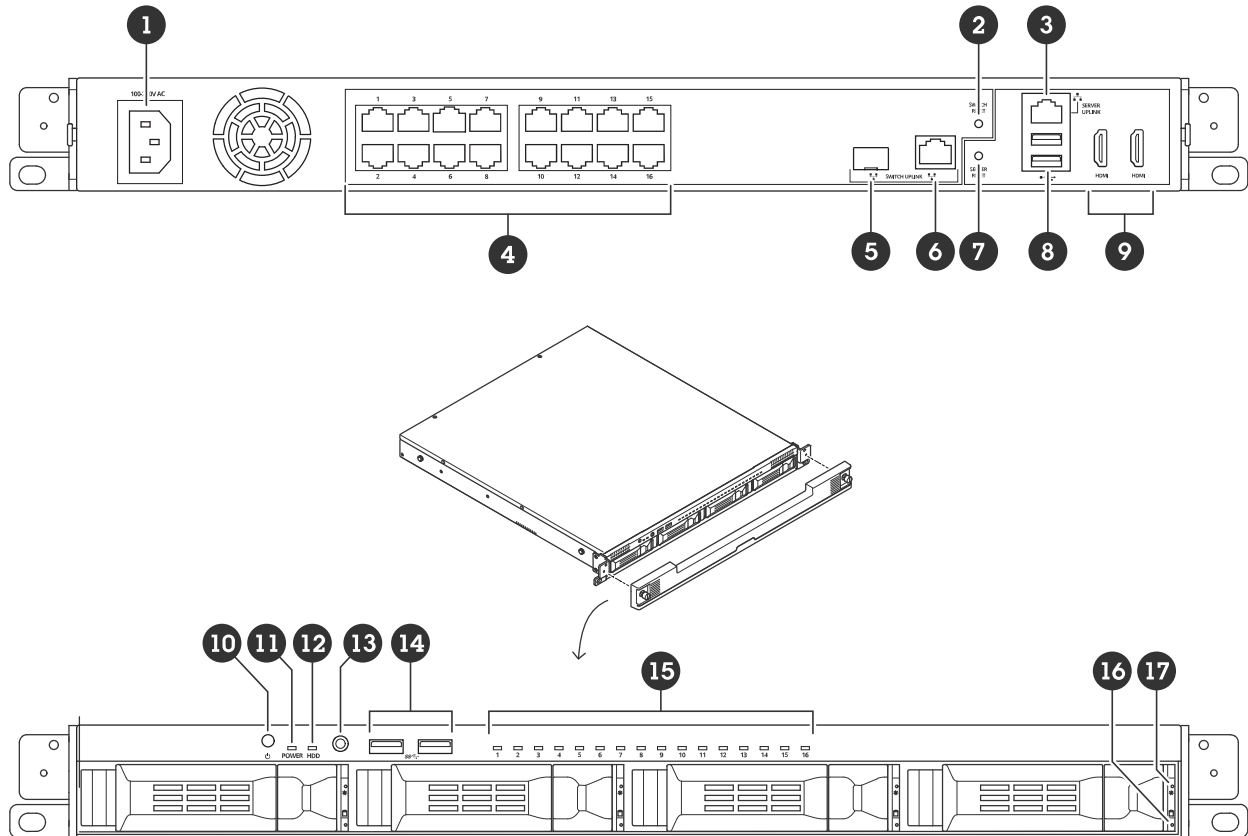
Switch-Berichte erstellen

Klicken Sie auf der Protokollseite auf **Export**, um eine Textdatei mit Switch-Informationen einschließlich der Protokolleinträge von der Protokollseite zu erstellen.

Technische Daten

Produktübersicht

Vorder- und Rückseite



- 1 Stromanschluss
- 2 Reset-Taste des Switches
- 3 1 GbE Ethernet-Port – Server-Uplink
- 4 1 GbE PoE Ethernet-Ports
- 5 1 GbE Ethernet-Port – Switch-Uplink (SFP)
- 6 1 GbE Ethernet-Port – Switch-Uplink (RJ45)
- 7 Reset-Taste des Servers
- 8 USB-2.0-Ports
- 9 HDMI™-Ports
- 10 Ein/-Ausschalter
- 11 Power-LED
- 12 LED für Laufwerksaktivität
- 13 Universalstecker Audio
- 14 USB 3.2 Ports
- 15 Status-LED für PoE Ethernet-Ports
- 16 LED für Laufwerksaktivität
- 17 Festplattenstatus-LED

LED-Anzeigen

Front-LEDs

Ein/-Ausschalter	Power-LED	Anzeige
Nicht gedrückt	Aus	PC und Switch sind ausgeschaltet
	Gelb	PC eingeschaltet, Switch ausgeschaltet
	Blinkt gelb	PC eingeschaltet, Switch wird gestartet
	Grün	PC eingeschaltet, Switch hat den Bootvorgang abgeschlossen
Gedrückt	Bis 0 Sekunden	Schaltet Switch und PC ein, falls diese ausgeschaltet sind
	Bis die Anzeige gelb blinkt (3 Sekunden)	Switch initiiert ordnungsgemäßes Herunterfahren
	Bis die Anzeige rot blinkt (6 Sekunden)	PC und Switch initiieren ein ordnungsgemäßes Herunterfahren
	Bis die Anzeige rot leuchtet (9 Sekunden)	PC initiiert erzwungenes Herunterfahren, Switch initiiert ordnungsgemäßes Herunterfahren

LED-Anzeige	Farbe	Anzeige
Festplatte (HDD)	Blinkt grün	Festplattenaktivität
	Rot	Möglicher Festplattenausfall
Status PoE Ethernet-Port	Grün	Linkstatus
	Gelb	Betriebenes Gerät, kein Verbindungsstatus
	Rot	PoE-Leistung überschritten
Festplattenstatus	Grün	Festplatte vorhanden
	Rot	Möglicher Festplattenausfall

LEDs hinten

Netzwerkgeschwindigkeit und -aktivität	Farbe	Anzeige
LED rechts	Gelb	10/100 Mbit/s
	Grün	1000 Mbit/s
LED links	Grün	PoE-Verbindung OK
	Rot	PoE-Leistung überschritten

Fehlerbehebung

Server zurücksetzen

Der Server kann über die Reset-Taste am Server zurückgesetzt werden. Das Zurücksetzen des Servers dauert mehr als eine Stunde.

1. Gerät ausschalten.
2. Server-Reset-Taste für 5 Sekunden gedrückt halten. Windows® RE wird gestartet.
3. Troubleshoot (Fehlerbehebung) auswählen.
4. Select Reset your PC (PC zurücksetzen).
5. Keep my files (Eigene Dateien beibehalten) oder Remove everything (Alles entfernen) auswählen. Keep my files (Eigene Dateien beibehalten) kann nur mit Administratorenkonto ausgewählt werden.
6. Die Anweisungen auf den Bildschirmseiten befolgen.
7. Der Server wird neu gestartet und das Zurücksetzen von Windows® auf die werksseitigen Standardeinstellungen wird eingeleitet.



Server auf die werksseitigen Standardeinstellungen zurücksetzen

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 Network Video Recorder 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. Laden Sie folgende Tools herunter: AXIS Network Video Recorder Recovery Kit and AXIS Network Video Recorder Recovery: ISO to USB Tool.
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. Führen Sie das AXIS Network Video Recorder Recovery: ISO to USB Tool aus und befolgen Sie die Anweisungen auf dem Bildschirm.

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. Ziehen Sie den USB-Stick nach der Beendigung des AXIS Network Video Recorder Recovery: ISO to USB Tools ab und schließen Sie ihn an Ihr Gerät an.
5. Gerät starten.
6. Wenn der AXIS Startbildschirm angezeigt wird, die Taste F12 drücken.
7. Auf **UEFI: USB-Laufwerk** klicken.
8. Wählen Sie Ihren USB-Stick aus und drücken Sie Enter. Das System startet mit dem AXIS Netzwerk-Videorekorder 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 Pro

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

Benötigen Sie Hilfe?

Nützliche Links

- *Benutzerhandbuch zu AXIS Camera Station Pro*
- *Bei AXIS Secure Remote Access anmelden*
- *Bei AXIS Secure Remote Access v2 anmelden*
- *Was in eine Antiviren-Freigabeliste für AXIS Camera Station aufgenommen werden sollte*

Support

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

T10207038_de

2026-09 (M6.2)

© 2024 – 2026 Axis Communications AB