AXIS Camera Station Pro

Benutzerhandbuch

Info

AXIS Camera Station Pro ist eine Videomanagementlösung zur Überwachung, Aufzeichnung und Verwaltung von Videostreams von Axis Netzwerkkameras. Sie unterstützt die Zutrittskontrolle, die Verwaltung mehrerer Standorte, die Kombination mit dem AXIS Audio Manager sowie die Integration in die Systeme von Drittanbietern.

Es ist mit allen gepflegten AXIS OS-Versionen der Kategorien „Active", „Long-Term Support" (LTS) und „Product Specific Support" (PSS)* kompatibel. Weitere Informationen finden Sie in den Versionshinweisen zu AXIS Camera Station Pro oder auf dem *AXIS OS-Portal*. Um zu überprüfen, welche Produkte mit AXIS Camera Station Pro funktionieren, siehe *Kompatible Produkte*.

*Wir sind bestrebt, die Kompatibilität mit älteren Versionen des AXIS OS zu gewährleisten, sofern dies wirtschaftlich vertretbar ist.

Zugriffsmöglichkeiten

AXIS Camera Station Pro Server – ist für die Kommunikation mit den Kameras, Videoencodern und Zusatzgeräten Ihres Systems zuständig. Informationen zu Systemanforderungen und Kapazitätsplanung finden Sie unter *Hardwarerichtlinien* in *AXIS Camera Station Pro - Installations- und Migrationsanleitung*.

AXIS Camera Station Pro Der Client – ermöglicht Zugriff auf Aufzeichnungen, Live-Video, Protokolle und Konfigurationen. Sie können ihn auf einem beliebigen Computer installieren, sodass er von jedem Punkt im Unternehmensnetzwerk aus – oder auch über das Internet – eingesehen und gesteuert werden kann.

Webclient für AXIS Camera Station – ermöglicht den Zugriff auf Aufzeichnungen von AXIS Camera Station Pro und Live-Video in Ihrem Webbrowser. Weitere Informationen dazu finden Sie in *Webclient für AXIS Camera Station - Benutzerhandbuch*.

AXIS Camera Station Pro mobile App – ermöglicht den Zugriff auf Aufzeichnungen und Live-Video mehrerer Systeme. Die App kann auf Android- und iOS-Geräten installiert werden und ermöglicht eine Fernanzeige.

Download-Optionen

Finden Sie den passenden Download oder die passende Aktualisierung für Ihre Anforderungen. Sie können AXIS Camera Station Pro kostenfrei testen, die mobile App herunterladen oder eine bestehende Installation aktualisieren. Gehen Sie zur *AXIS Camera Station Pro Download-Seite*, um zu starten.

- **Kostenfreie 90-Tage-Testversion mit vollem Funktionsumfang:** Testen Sie AXIS Camera Station Pro 90 Tage lang kostenfrei. Für den Einstieg ist keine Lizenz erforderlich.
- **Nur Ihren Client aktualisieren – Offline:** Aktualisiert den Client-Teil von AXIS Camera Station Pro, also den Teil der Anwendung, mit dem Sie direkt interagieren. Verwenden Sie diese Option, wenn Sie nur den Client und nicht den Server aktualisieren müssen.
- **Ihren Client und Server aktualisieren – Offline:** Ein komprimiertes Update-Paket für Server und Client. Entpacken Sie die ZIP-Datei nach dem Herunterladen, um Zugriff auf die MSI- und CAB-Dateien zu haben, und führen Sie anschließend die MSI-Datei aus, um die Aktualisierung zu starten.
- **Ihren Client und Server aktualisieren – Online:** Lädt die Aktualisierung herunter, extrahiert sie und führt die Installation automatisch durch. Führen Sie die EXE-Datei aus und befolgen Sie die Anweisungen. Ihr Computer muss während der gesamten Installation mit dem Internet verbunden bleiben.
- **Mobile app for iOS (Mobile App für iOS):** Die mobile App AXIS Camera Station Pro für iPhones und iPads. Downloads vom App Store.
- **Mobile App für Android:** Die mobile App AXIS Camera Station Pro für Android-Smartphones und -Tablets. Downloads von Google Play.

Lernvideos

Ausführliche Beispiele für die Verwendung des Systems finden Sie in *Tutorialvideos zu AXIS Camera Station Pro*.

Systemmerkmale

Weitere Informationen zu den Systemfunktionen finden Sie unter *Anleitung zu Funktionen von AXIS Camera Station Pro*.

News und Neuigkeiten

Die neuen Funktionen der einzelnen neuen Versionen von AXIS Camera Station Pro finden Sie unter *Was ist neu in AXIS Camera Station Pro*.

Hilfreiche Links für Administratoren

Hier sind einige Themen, die Sie interessieren könnten:

- *Mit einem Server verbinden, on page 9*
- *Geräte konfigurieren, on page 46*
- *Speicher konfigurieren, on page 74*
- *Aufzeichnung und Ereignisse konfigurieren, on page 80*
- *Verbundene Dienste konfigurieren, on page 124*
- *Server konfigurieren, on page 127*
- *Die Sicherheit konfigurieren, on page 138*

Weitere Handbücher

- *Webclient für AXIS Camera Station*
- *Anleitung zu AXIS Camera Station Pro Integrator*
- *Mobile App von AXIS Camera Station*
- *Videotutorials zu AXIS Camera Station Pro*
- *Anleitung zur Fehlerbehebung bei AXIS Camera Station Pro*
- *Anleitung zum Härten des Systems bei AXIS Camera Station Pro*

Hilfreiche Links für Bediener

Hier sind einige Themen, die Sie interessieren könnten:

- *Anleitung zu den ersten Schritten von Anwendern mit AXIS Camera Station Pro*
- *Mit einem Server verbinden, on page 9*
- *Client konfigurieren, on page 119*
- *Live-Ansicht, on page 13*
- *Aufzeichnungswiedergabe, on page 25*
- *Aufzeichnungen exportieren, on page 28*
- *AXIS Camera Station Pro Kurzanleitung – Ansicht und Export*

Schnellstart

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

Vorbereitungen:

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

Für Administratoren:

1. *Das Video Management System starten*
2. *Geräte hinzufügen*
3. *Konfigurieren des Aufzeichnungsverfahrens, on page 7*

Für Bediener:

1. *Live-Video ansehen, on page 7*
2. *Aufzeichnungen anzeigen, on page 7*
3. *Aufzeichnungen exportieren, on page 7*
4. *Aufzeichnungen mit AXIS File Player wiedergeben und überprüfen, on page 7*

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 Erststart des Clients versucht dieser, sich bei dem auf demselben Computer installierten AXIS Camera Station Pro Server anzumelden.

Sobald der Client geöffnet wird, werden Sie aufgefordert, Ihr System zu lizenzieren. Klicken Sie auf **License now (Jetzt lizenzieren)**, um die Seite **Manage licences (Lizenzen verwalten)** aufzurufen, auf der Sie den Server für ein Unternehmen registrieren können, um mit der Lizenzierung zu beginnen. Siehe *Verbundene Dienste verwalten, on page 124* und *Lizenzen verwalten, on page 137* für weitere Informationen. Sie müssen das System registrieren und mit einem Unternehmen verbinden, um auf verbundene Dienste wie den VMS-Webclient, die Überwachung des Systemzustands und die Online-Lizenzierung zuzugreifen.

Sie haben mehrere Möglichkeiten, um auf den AXIS Camera Station Pro Server zuzugreifen. Siehe *Mit einem Server verbinden*.

Geräte hinzufügen

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

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. Um die Konfiguration zu überspringen und später mit den hinzugefügten Geräten fortzufahren, klicken Sie auf **Close (Schließen)**. So fahren Sie mit der Konfiguration fort:
   3.1. Wählen Sie **Quick configuration (Schnellkonfiguration)** oder **Site Designer configuration (Site Designer Konfiguration)**. Weitere Informationen finden Sie unter *Site Designer-Projekte importieren, on page 50*.

3.2. Wählen Sie **Add image overlay for date, time, and text (Bildüberlagerung für Datum, Uhrzeit und Text hinzufügen)**, wenn Sie eine Überlagerung für die Axis Kameras hinzufügen möchten, für die noch keine Überlagerungen konfiguriert sind.

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 **Speicherdauer** und den **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.

Weitere Informationen finden Sie unter *Live-Ansicht, on page 13*.

Aufzeichnungen anzeigen

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

Weitere Informationen finden Sie unter *Aufzeichnungen, on page 25*.

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...**.

Weitere Informationen finden Sie unter *Aufzeichnungen exportieren, on page 28*.

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. **Überprüfen** anklicken. Die Seite mit dem entsprechenden Überprüfungsergebnis erscheint.

Hinweis

- Digitale Signatur unterscheidet sich von Signiertes Video. Mit signierten Videos lassen sich Videos auf die aufzeichnende Kamera rückverfolgen und Aufzeichnungen so auf etwaige Manipulationen überprüfen. 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.

Netzwerkkonfiguration

Wenn sich AXIS Camera Station Pro Client, AXIS Camera Station Pro Server und verbundene Geräte in verschiedenen Netzwerken befinden, müssen vor der Verwendung von AXIS Camera Station Pro Proxy- und Firewalleinstellungen konfiguriert werden.

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 Client und Server durch NAT, Firewall oder eine ähnliche Einrichtung getrennt sind, konfigurieren Sie diese so, dass die in AXIS Camera Station Pro 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.

Weitere Informationen finden Sie unter *Portliste für AXIS Camera Station Pro, on page 218*.

Server-Port-Konfiguration

AXIS Camera Station Pro-Server verwendet die Ports 29202 (TCP), 29204 (mobile Kommunikation) und 29205 (mobiles Streaming) für die Kommunikation zwischen dem Server und dem Client. Bei Bedarf können Sie die Ports über AXIS Camera Station Pro Service Control ändern.

Hinweis

Ändern Sie die Ports nur, wenn Sie AXIS Camera Station ohne Axis Secure Remote Access v2 oder einen unserer anderen Cloud-Dienste verwenden möchten.

Weitere Informationen finden Sie unter *Allgemeines* oder *Häufig gestellte Fragen (FAQ)*.

Hinweise zur Systemsicherheit

Um unbefugten Zugriff auf Kameras und Aufzeichnungen zu verhindern, Folgendes beachten:

- Verwenden Sie für alle Netzwerk-Geräte (Kameras, Video-Encoder und Zusatzgeräte) starke Kennwörter.
- Installiert AXIS Camera Station Pro-Server, die Kameras, Video-Encoder und Zusatzgeräte in einem sicheren, vom Büronetz separaten Netzwerk. Sie können den AXIS Camera Station Pro Client auf einem Computer eines anderen Netzwerks installieren, zum Beispiel einem Netzwerk mit Internetzugang.
- Sicherstellen, dass alle Benutzer starke Kennwörter verwenden. Windows® Active Directory bietet ein hohes Maß an Sicherheit.

Mit einem Server verbinden

Mit dem AXIS Camera Station Pro 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. Sie haben mehrere Möglichkeiten, um auf den AXIS Camera Station Pro Server zuzugreifen:

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 9*.

Axis Secure Remote Access v2 – Siehe *Bei AXIS Secure Remote Access v2 anmelden, on page 10*.

Hinweis

Bei der erstmaligen Verbindung mit einem Server überprüft der Client die Server-Zertifikat-ID. Um sicherzustellen, dass die Verbindung zum richtigen Server hergestellt wird, vergleichen Sie die Zertifikat-ID manuell mit der in der Dienststeuerung von AXIS Camera Station Pro angezeigten ID. Siehe *Allgemeines, on page 218*.

Damit eine Verbindung zwischen Client und Server hergestellt werden kann, müssen beide dieselbe Version nutzen. Sollten die Versionen bei der Verbindung mit einem lokalen System oder einem System mit Port-Mapping abweichen und Kompatibilitätsprobleme auftreten, kann der Client die korrekte, dem Server entsprechende Version herunterladen. Der Client wechselt dann zur übereinstimmenden Version.

Damit sich ein Client mit mehreren Servern verbinden kann, muss jeder Server über dieselbe Version verfügen. Standardmäßig verwendet die Client-Verknüpfung die neueste Version.

Es wird empfohlen, zur Authentifizierung der Clientbenutzer von AXIS Camera Station Pro **Kerberos** zu verwenden. Siehe hierzu *„Authentifizierung mit Kerberos" in der Anleitung zur Härtung des AXIS Camera Station Pro Systems* für weitere Informationen.

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. Siehe *Serverlisten*.
Serverliste importieren	Um eine Server-Listendatei zu importieren, die aus AXIS Camera Station Pro exportiert wurde, klicken Sie auf **Import server list (Server-Liste importieren)** und suchen Sie nach einer .msl-Datei. Siehe *Serverlisten*.
Gespeicherte Kennwörter löschen	Um die gespeicherten Benutzernamen und Kennwörter aller verbundenen Server zu löschen, klicken Sie auf **Delete saved passwords (Gespeicherte Kennwörter löschen)**.

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. Wenn der Server nicht aufgeführt ist, klicken Sie auf , um alle verfügbaren Remote-Server erneut zu laden. Wenn der Server so konfiguriert ist, dass er Clients auf einem anderen Port als dem Standardport 29202 zulässt, geben Sie die IP-Adresse gefolgt von der Portnummer ein, z. B.: 192.168.0.5:46001.
3. Sie haben hier folgende Möglichkeiten:
   - 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 v2 anmelden

1. Klicken Sie den Link **Bei AXIS Secure Remote Access v2 anmelden**.
2. Geben Sie die Anmeldedaten für Ihr MyAxis-Konto ein.
3. Klicken Sie auf **Anmelden**.
4. Wählen Sie eine Organisation aus und klicken Sie auf **OK**.
5. Wählen Sie den Server aus, bei dem Sie sich anmelden möchten.
6. Melden Sie sich mit Ihren Server-Zugangsdaten an.

Hinweis

Ihre Server-Zugangsdaten unterscheiden sich von den Zugangsdaten Ihres My Axis Kontos.

Die Statusleiste am unteren Rand des AXIS Camera Station Pro-Clients zeigt die Verwendung von Axis Secure Remote Access v2 an. **Im laufenden Monat genutztes Datenvolumen** zeigt das Gesamtvolumen der weitergeleiteten Daten an, die im Laufe des Monats von der Organisation verbraucht wurden. Der Zähler wird am Ersten jedes Monats um Mitternacht zurückgesetzt.

Unter *Axis Secure Remote Access v2, on page 126* finden Sie Informationen zum Aktivieren von Axis Secure Remote Access v2.

Axis Secure Remote Access v2 auf Mobilgeräten

So melden Sie sich mit Axis Secure Remote Access v2 auf einem Mobilgerät (iOS und Android) bei Ihrem Server an:

1. Rufen Sie auf Ihrem Mobilgerät *axis.com/products/axis-camera-station/overview* auf und laden Sie die mobile App AXIS Camera Station.
2. Installieren und öffnen Sie die App auf Ihrem Mobilgerät.
3. Melden Sie sich bei Axis Secure Remote Access v2 mit Ihren Zugangsdaten für Ihr Konto bei My Axis an.
4. Wählen Sie den Server aus, bei dem Sie sich anmelden möchten.
5. Melden Sie sich mit Ihren Server-Zugangsdaten an.

Hinweis

- Ihre Server-Zugangsdaten unterscheiden sich von den Zugangsdaten Ihres My Axis Kontos.
- Sie müssen eingeladen werden, der Organisation als Benutzer beizutreten, bevor Sie sich mit Ihrem My Axis Konto anmelden können.

In der mobilen App wird das Gesamtvolumen der weitergeleiteten Daten angezeigt, die im Laufe des Monats von der Organisation verbraucht wurden. Weitere Informationen finden Sie im *Benutzerhandbuch zur mobilen App AXIS Camera Station*.

Client-Proxyeinstellungen

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

AXIS Camera Station Pro Der Client

Bei der ersten Anwendung von AXIS Camera Station Pro öffnet sich auf der Registerkarte „Konfiguration" automatisch die Seite „Geräte hinzufügen". Siehe *Geräte hinzufügen*.

Registerkarten

Live-Ansicht	Live-Video von verbundenen Kameras anzeigen. Siehe *Live-Ansicht*.
Aufzeichnungen	Aufzeichnungen suchen, wiedergeben und exportieren. Siehe *Aufzeichnungen*.
Intelligente Suche 1	Mithilfe von Smart Search wichtige Ereignisse in Videoaufzeichnungen schnell auffinden. Siehe *Intelligente Suche 1*.
Datensuche	Nach Daten von einer externen Quelle oder einem externen System aus suchen und das genaue Geschehen bei einem Ereignis nachverfolgen. Siehe *Datensuche, on page 43*.
Konfiguration	Verwaltung und Wartung angeschlossener Geräte sowie Einstellungen von Client und Servern. Siehe *Konfiguration*.
Hotkeys	Eine Liste von Hotkeys für Aktionen. Siehe *Hotkeys*.
Protokolle	Protokolle zu Alarmen, Ereignissen und Audits. Siehe *Protokolle*.
Zutrittsverwaltung	Karteninhaber, Gruppen, Zugänge, Zonen und Zugangsregeln des Systems konfigurieren und verwalten. Siehe *Zutrittsverwaltung, on page 187*.
Intelligente Suche 2	Mithilfe von erweiterten Filtern Fahrzeuge und Personen anhand von Merkmalen finden. Siehe *Intelligente Suche 2, on page 37*.
Systemzustand überwachen	Überwachen Sie die Zustandsdaten über ein einzelnes oder über mehrere AXIS Camera Station Pro-Systeme. Siehe *Überwachung des Systemzustands BETA, on page 199*.
Warnmeldungen zur Live-Ansicht	Automatisches Wechseln zum Tab "Live-Ansicht" der Kamera oder Ansicht, wenn die Aktion "Live-Ansicht" ausgelöst wird. Siehe *Live-Ansichtsaktion erstellen*.
Warnmeldungen aufzeichnen	Wählen Sie einen Alarm in dem Tab "Alarme" oder "Protokolle" und klicken Sie auf **Zu Aufzeichnungen wechseln**, um den Tab "Aufzeichnungsalarme" zu öffnen. Siehe *Alarme* und *Protokolle*.

Hauptmenü

	Hauptmenü öffnen.
Server	Eine Verbindung mit einem neuen AXIS Camera Station Pro-Server herstellen und die Server-Listen

	und den Verbindungsstatus für alle Server anzeigen. Siehe *Server konfigurieren*.
Aktionen	Aufzeichnung manuell starten oder anhalten und den Status der I/O-Ports ändern. Siehe *Manuell aufzeichnen* und *E/A-Ports überwachen*.
Hilfe	Hilfeoptionen öffnen. Wechseln Sie zu **Help (Hilfe)** > **About (Über)**, um zu sehen, welche Version von AXIS Camera Station Pro Client Sie verwenden.
Abmelden	Hier können Sie die Serververbindung trennen und sich vom AXIS Camera Station Pro-Client abmelden.
Exit	Beenden und schließen Sie den AXIS Camera Station Pro Client.

Titelleiste

? oder F1	Hilfe öffnen.
	In den Vollbildmodus wechseln.
oder ESC	Den Vollbildmodus verlassen.

Statusleiste

Die Statusanzeige beinhaltet Folgendes:

- Ein Warnungssymbol taucht auf, wenn es eine Diskrepanz zwischen dem Client und dem Server gibt. Stellen Sie immer sicher, dass zur Vermeidung von Problemen mit der Zeitachse die Zeit von Client und Server synchron laufen.
- Die Server-Verbindungsstatus zeigt die Anzahl der verbundenen Server. Siehe *Verbindungsstatus*.
- Der Lizenzstatus zeigt die Anzahl von unlizensierten Geräten. Siehe .
- Die Nutzungsübersicht für Secure Remote Access v2 zeigt an, wie viel Datenvolumen Sie diesen Monat verbraucht haben.
- **AXIS Camera Station Pro update available (Aktualisierung für** verfügbar) wird angezeigt, wenn Sie als Administrator angemeldet sind. Siehe *AXIS Camera Station Pro aktualisieren, on page 130*.

Alarme und Aufgaben

Auf den Registerkarten „Alarme und Aufgaben" werden ausgelöste Ereignisse und Alarme des Systems angezeigt. Siehe *Alarme* und *Aufgaben*.

Live-Ansicht

In der Live-Ansicht werden die Ansichten und Kameras sowie Live-Videos der verbundenen Kameras angezeigt. Bei Verbindungen mit mehreren AXIS Camera Station Pro-Servern werden alle Ansichten und Kameras verbundener Server nach dem jeweiligen Servernamen gruppiert angezeigt.

Ansichten bietet Zugriff auf alle Kameras und Geräte, die zu AXIS Camera Station Pro hinzugefügt wurden. Eine Ansicht kann eine oder mehrere Kameras sowie eine Sequenz von Elementen, einen Lageplan oder eine Webseite umfassen. Die Live-Ansicht aktualisiert die Ansichten automatisch, wenn Sie dem System Geräte hinzufügen oder daraus entfernen.

Mit der Integration von AXIS Audio Manager Pro können Sie auch Audiobereiche mit Durchsageschnittstellen in der Live-Ansicht einrichten und hinzufügen. Weitere Informationen finden Sie unter *Verwendung von Durchsageschnittstellen in geteilten Ansichten, on page 20*

Alle Benutzer können auf „Ansichten" zugreifen. Informationen zu Benutzerrechten finden Sie unter *Benutzerberechtigungen, on page 138*.

Hilfe zur Konfiguration der Live-Ansicht finden Sie unter *Clienteinstellungen*.

Mehrere Monitore

So öffnen Sie eine Ansicht auf einem anderen Bildschirm:

1. Öffnen Sie eine Registerkarte „Live-Ansicht".
2. Wählen Sie eine oder mehrere Kameras, Ansichten oder Sequenzen.
3. Ziehen Sie sie per Drag & Drop auf den anderen Bildschirm.

So öffnen Sie eine Ansicht auf einem Monitor, der mit einem Axis Video Decoder verbunden ist:

1. Öffnen Sie eine Registerkarte „Live-Ansicht".
2. Wählen Sie eine oder mehrere Kameras, Ansichten oder Sequenzen.
3. Klicken Sie mit der rechten Maustaste auf Ihre Kameras, Ansichten oder Sequenzen und wählen Sie **Show on AXIS T8705 (Auf AXIS T8705 anzeigen)** oder **Show on AXIS D1110 (Auf AXIS D1110 anzeigen)**, abhängig davon, welchen Videodecoder Sie verwenden.

Hinweis

- AXIS T8705 unterstützt nur Axis Kameras.
- AXIS D1110 unterstützt bis zu 9 Streams in einer geteilten Ansicht.

Ansichten in der Live-Ansicht verwalten

+	Neue geteilte Ansichten, Sequenzen, Kameraansichten, Lagepläne, Webseiten oder Ordner hinzufügen.
✎	Den Namen einer Ansicht oder Kamera ändern. Informationen zur Bearbeitung der Kameraeinstellungen finden Sie unter *Kameraeinstellungen bearbeiten*

	Eine Ansicht entfernen. Sie müssen die Berechtigung haben, die Ansicht und alle sekundären Ansichten zu bearbeiten, um sie zu entfernen. Weitere Informationen zum Entfernen von Kameras von AXIS Camera Station Pro finden Sie unter *Kameras, on page 53*.
	Als Administrator können Sie die Ansicht sperren und damit verhindern, dass Bediener die Ansicht verschieben oder bearbeiten.

Bilderverwaltung in der Live-Ansicht

Navigieren	Um zur Kameraansicht zu wechseln, klicken Sie mit der rechten Maustaste auf ein Bild in einer geteilten Ansicht und wählen Sie **Navigieren**.
Momentaufnahme machen	Um einen Momentaufnahme zu machen, klicken Sie mit der rechten Maustaste auf ein Bild und wählen Sie **Momentaufnahme machen**. Das System speichert die Momentaufnahme in dem Momentaufnahmenordner, der unter **Configuration (Konfiguration) > Client > Settings (Einstellungen)** angegeben ist. Hinweis Axis Camera Station Pro verwendet normalerweise den Videostream, wenn Sie Momentaufnahmen machen, d. h. Sie erhalten eine Momentaufnahme mit der Auflösung des Videostreams. Bei Panorama- und Fischaugen-Kameras, die ein Zusammenfügen mehrerer Bilder oder eine Entzerrung erfordern, wird die Momentaufnahme jedoch auf der Client-Seite direkt vom Bildschirm aufgenommen. Diese Methode kann zu Bildern mit geringerer Auflösung führen, insbesondere wenn Sie Momentaufnahmen in Ansichten mit mehreren Kameras aufnehmen, bei denen jedes Bild auf dem Bildschirm kleiner erscheint.
Momentaufnahme der Exportliste hinzufügen	Um auf der Registerkarte „Export (Exportieren)" der Exportliste einen Momentaufnahme hinzuzufügen, klicken Sie mit der rechten Maustaste auf ein Bild und wählen Sie **Add snapshot to Export (Momentaufnahme der Exportliste hinzufügen)**.
Anzeigen auf	Um eine Ansicht auf einem anderen Bildschirm zu öffnen, klicken Sie mit der rechten Maustaste auf das Bild und wählen Sie **Anzeigen auf**.
Mechanisches PTZ verwenden	Die Option ist für PTZ-Kameras sowie für Kameras, in denen digitales PTZ über die Weboberfläche der Kamera aktiviert wurde, verfügbar. Um das mechanische PTZ zu verwenden, klicken Sie mit der rechten Maustaste in das Bild und wählen Sie **Mechanisches PTZ verwenden**. Verwenden Sie die Maus zum Zoomen, Schwenken und Neigen.

Zoom	Mit dem Mausrad ein- und auszoomen. Oder Sie drücken zum Heranzoomen CTRL + (+) und zum Herauszoomen CTRL + (-).
In dem Bereichs zoomen	Um einen Bildbereich zu vergrößern, ziehen Sie ein Rechteck um den zu vergrößernden Bereich. Verwenden Sie zum Auszoomen das Mausrad. Halten Sie, um einen Bereich nahe der Bildmitte zu vergrößern, die rechte Maustaste gedrückt und ziehen Sie ein Rechteck auf.
Schwenken und Neigen	Klicken Sie in das Bild dahin, wohin die Kamera zeigen soll. Um in der Live-Ansicht fortlaufend zu schwenken und zu neigen, bewegen Sie den Cursor in die Bildmitte, um den Navigationspfeil anzuzeigen. Halten Sie dann die Maustaste gedrückt, um in die Richtung des Navigationspfeils zu schwenken. Um das Bild schneller zu schwenken und zu neigen, halten Sie die Maustaste gedrückt, um den Navigationspfeil zu verlängern.
Fokus festlegen	Um den Fokus eines AXIS Geräts einzustellen, klicken Sie mit der rechten Maustaste auf das Bild und wählen Sie **Set focus (Fokus festlegen)**. Stellen Sie den Fokus manuell mit den Schiebereglern **Near (Nah)** und **Far (Fern)** ein oder klicken Sie auf **AF**, um den Fokus automatisch einzustellen. Um den Fokus eines ONVIF Geräts einzustellen, klicken Sie mit der rechten Maustaste auf das Bild und wählen Sie **Set focus (Fokus festlegen)**. Wählen Sie einen **Fokusmodus**. Bitte beachten Sie, dass sich das Dialogfeld je nach gewähltem Modus aktualisiert: • **Absolute (Absolut)**: Stellen Sie den Fokus auf eine bestimmte Position ein, indem Sie einen Wert eingeben und auf **Apply (Übernehmen)** klicken. • **Relative (Relativ)**: Stellen Sie den Fokus schrittweise ein. Verwenden Sie **Near (Nah)** für Objekte in der Nähe der Kamera und **Far (Fern)** für weiter entfernte Objekte. • **Continuous (Kontinuierlich)**: Verschieben Sie den Fokus mit **Nearer (Näher)** oder **Further (Weiter)** und klicken Sie auf „Stopp", wenn Sie fertig sind. • Um automatisch zu fokussieren, klicken Sie auf **AF**.
Fokusabrufzone	Um eine Fokusabrufzone hinzuzufügen oder zu entfernen, klicken Sie mit der rechten Maustaste auf das Bild und wählen Sie **Fokusabrufzone**.
Objektverfolgung ein/aus	Um automatische Nachverfolgung für eine Axis PTZ-Kamera mit AXIS PTZ Autotracking ein- oder auszuschalten, klicken Sie mit der rechten Maustaste auf das Bild und wählen Sie **Automatische Nachverfolgung ein/aus**.

Voreinstellungen	Um eine Voreinstellung aufzurufen, klicken Sie mit der rechten Maustaste in das Bild und wählen Sie erst **Voreinstellungen**, dann die gewünschte Voreinstellung. Um Voreinstellungen zu erstellen, siehe *PTZ-Voreinstellungen*.
Voreinstellung hinzufügen	Um eine Voreinstellung hinzuzufügen, ziehen Sie die Bildansicht an die gewünschte Position, klicken Sie mit der rechten Maustaste und wählen Sie **Voreinstellungen > Voreinstellung hinzufügen**.
Absolute PTZ-Bewegung	Diese Option ist für ONVIF-Geräte verfügbar, die eine absolute PTZ-Positionierung unterstützen. Verwenden Sie diese Funktion, um die Kamera für eine wiederholbare Positionierung auf präzise Koordinaten zu bewegen. Zur Nutzung der absoluten PTZ-Positionierung klicken Sie in der Live-Ansicht mit der rechten Maustaste auf die PTZ-Kamera und wählen Sie **Absolute PTZ Move (Absolute PTZ-Bewegung)** aus. Wählen Sie ein Koordinatensystem aus: **Generic (Generisch)** für Standardkoordinaten oder **Spherical (Sphärisch)** für gradbasierte Koordinaten. Geben Sie die Positionswerte für Schwenken, Neigen und Zoomen ein, legen Sie eine Bewegungsgeschwindigkeit fest und klicken Sie auf **OK** oder **Send (Senden)**.
Videostromprofil	Um das Videostreamprofil festzulegen, klicken Sie mit der rechten Maustaste auf ein Bild und wählen Sie **Videostreamprofil**. Siehe *Videostromprofile*.

Digitale Voreinstellungen hinzufügen

PTZ-Steuerung

Hinweis

Administratoren können mechanisches PTZ für Benutzer deaktivieren. Siehe *Benutzerberechtigungen*.

Aufzeichnung und unmittelbares Antworten in der Live-Ansicht

	Um die Registerkarte mit den Aufzeichnungen aufzurufen, wählen Sie eine Kamera oder eine geteilte Ansicht aus und klicken Sie auf .
	Zeigt eine laufende Aufzeichnung in der Live-Ansicht an.
	Zeigt an, dass Bewegung erkannt wurde.
	Um eine laufende Aufzeichnung wiederzugeben, bewegen Sie den Cursor über das Bild und klicken Sie auf **Instant replay (Sofortwiedergabe)**. Die Registerkarte „Aufzeichnungen" öffnet sich und die letzten 5 Sekunden der Aufzeichnung werden wiedergegeben.
REC	Um eine manuelle Aufzeichnung in der Live-Ansicht zu starten, bewegen Sie den Mauszeiger über das Bild und klicken auf **REC**. Die Taste wird gelb hinterlegt, um anzuzeigen, dass die Aufzeichnung läuft. Um die Aufzeichnung zu stoppen, klicken Sie erneut auf **REC**.

Um Einstellungen von manuellen Aufzeichnungen wie Auflösung, Komprimierung und Bildrate zu konfigurieren, navigieren Sie zu *Aufzeichnungsmethode*. Für weitere Informationen über Aufzeichnungen und Wiedergabe, siehe *Aufzeichnungswiedergabe*.

Hinweis

Administratoren können die manuelle Aufzeichnungsfunktion für Benutzer deaktivieren. Siehe *Benutzerberechtigungen*.

Audio in der Live-Ansicht

Audio steht zur Verfügung, wenn die Kamera Audiofunktionen unterstützt und in dem für die Live-Ansicht verwendeten Profil Audio eingeschaltet wurde.

Gehen Sie zu **Konfiguration > Geräte > Videostreamprofile** und konfigurieren Sie Audio für die Kamera. Siehe *Videostromprofile, on page 54*.

Lautstärke	Um die Lautstärke in einer Ansicht zu ändern, streichen Sie das Bild, dann die Lautsprechertaste und ändern Sie dann mithilfe des Schiebereglers die Lautstärke. Um Audio stummzuschalten oder die Stummschaltung wieder aufzuheben, klicken Sie auf .
Nur diese Ansicht anhören	Um andere Ansichten stummzuschalten und nur diese Ansicht anzuhören, bewegen Sie den Cursor über das Bild und klicken Sie auf .

Sprechen Sie über den Lautsprecher	Um im Vollduplexmodus über den konfigurierten Lautsprecher zu sprechen, bewegen Sie den Cursor über das Bild und klicken Sie auf .
Push-to-talk	Um im Simplex- und Halbduplexmodus über den konfigurierten Lautsprecher zu sprechen, bewegen Sie den Cursor über das Bild und halten Sie gedrückt. Um die **Sprechtaste** in allen Duplexmodi zu sehen, aktivieren Sie **Sprechtaste für alle Duplexmodi verwenden** unter **Konfiguration > Client > Streaming > Audio)**. Siehe *Streaming, on page 122*.

Hinweis

Als Administrator können Sie Audio für Benutzer deaktivieren. Siehe *Benutzerberechtigungen*.

Steuerung in der Live-Ansicht

Hinweis

Die Steuerung in der Live-Ansicht erfordert Firmware 7.40 oder später.

	Um in der Live-Ansicht auf die verfügbaren Kamerafunktionen, zuzugreifen, klicken Sie auf .

Geteilte Ansicht

In einer geteilten Ansicht werden mehrere Ansichten in einem Fenster dargestellt. In der geteilten Ansicht können Kameraansichten, Sequenzen, Webseiten, Lagepläne und weitere geteilte Ansichten dargestellt werden.

Hinweis

Bei Anschluss an mehrere AXIS Camera Station Pro Server können Sie jede Ansicht, jede Kamera, jedes Gerät oder jeden Audiobereich anderer Server zu Ihrer geteilten Ansicht hinzufügen.

Geteilte Ansicht hinzufügen:

1. Auf dem Tab "Live-Ansicht" + anklicken.
2. **Neue Geteilte Ansicht** wählen.
3. Geben Sie einen Namen für die Fensteraufteilung ein.
4. Wählen Sie aus dem Aufklappmenü **Vorlage** eine Vorlage aus, die Sie verwenden möchten.
5. Ziehen Sie eine(n) oder mehrere Ansichten, Kameras oder Audiobereiche per Drag & Drop in das Raster.
6. Klicken Sie auf **Ansicht speichern**, um die geteilte Ansicht auf dem aktuellen Server zu speichern.

Hotspot festlegen	Um das Bild eines Hotspot festzulegen, klicken Sie auf die rechte Maustaste und wählen Sie **Hotspot festlegen**. Wenn Sie auf ein anderes Bild klicken, wird es im Hotspot geöffnet. Hotspots sind insbesondere bei asymmetrischen Fensteraufteilungen mit einem großen und mehreren kleinen Teilfenstern praktisch. In der Regel ist das größte Bild der Hotspot.
Videostromprofil	Um das Videostreamprofil für die Kamera einzustellen, klicken Sie mit der rechten Maustaste auf eine Kamera in die Rasteransicht und wählen Sie **Videostreamprofil**. Siehe dazu *Videostromprofile*.

Fensteraufteilung hinzufügen

Zugangsdashboard in der geteilten Ansicht

Wenn Sie einen Zugang konfiguriert haben, können Sie Karteninhabern assistieren und den Status des Zugangs sowie neueste Transaktionen in einer geteilten Ansicht sehen.

1. Fügen Sie einen Zugang hinzu. Siehe *Hinzufügen eines Zugangs, on page 152*.
2. Mehr dazu, wie Sie ein Zugangsdashboard einer geteilten Ansicht hinzufügen, finden Sie in *Geteilte Ansicht, on page 18*.

Dashboard	Öffnen Sie die Registerkarte **Dashboard**, um Details zum Zugang, den Zugangsstatus und den Schlossstatus zu sehen. Auf dem Dashboard sehen Sie folgende Informationen: • Zutrittskontrollereignisse mit Einzelheiten zum Karteninhaber, inklusive Foto, z. B. wenn ein Karteninhaber eine Karte durch einen Leser zieht. • Alarme mit Informationen zum Auslöser des Alarms, z. B. wenn ein Zugang zu lange geöffnet ist. • Die letzte Transaktion.
	Klicken Sie auf , um ein Ereignis mit einem Lesezeichen zu markieren und es auf der Registerkarte Transaktionen verfügbar zu machen.
Zugriff	Klicken Sie auf **Zutritt**, um manuell Zugang zu gewähren. Dadurch wird der Zugang auf die gleiche Weise entriegelt wie beim Vorzeigen der Zugangsdaten. In der Regel verriegelt sich die Tür automatisch nach einer festgelegten Zeit.
Schloss	Zum manuellen Verriegeln der Tür klicken Sie auf **Verriegeln**.
Entriegeln	Um die Tür manuell zu entriegeln, klicken Sie auf **Entriegeln**. Die Tür bleibt entriegelt, bis Sie sie manuell wieder verriegeln.
Verriegelung	Klicken Sie auf **Absperren**, um den Zugang zur Tür zu vermeiden.
Transaktionen	Um die letzten und gespeicherten Transaktionen zu sehen, öffnen Sie die Registerkarte **Transaktionen**.

Überwachen und unterstützen über das Zugangsdashboard

AXIS Data Insights Dashboard in einer geteilten Ansicht

AXIS Data Insights Dashboard stellt die Analysedaten Ihrer Geräte in Grafiken und Diagrammen dar. So fügen Sie ein Dashboard zu einer geteilten Ansicht hinzu:

1. Dashboard konfigurieren. Siehe *AXIS Data Insights Dashboard, on page 181*.
2. Auf der Registerkarte Live-Ansicht + anklicken.
3. **Neue Geteilte Ansicht** wählen.
4. Erweitern Sie den Ordner für die **Dashboards**.
5. Ziehen und ablegen Sie ein Dashboard in das Raster.
6. Klicken Sie auf **Save view (Ansicht speichern)**.

Dashboards	
Audioanalyse	Zeigt Daten von AXIS Audio Analytics-Ereignissen an.
Zählung von Überquerungen	Zeigt Personenzähldaten aus dem Szenario der AXIS Object Analytics Querschnittszählung an.
Generisch	Zeigt Daten aus allen unterstützten Datenquellen an.
Bildqualität	Zeigt Daten von AXIS Image Health Analytics-Ereignissen an.
Belegung von Bereichen	Zeigt die Belegungsdaten von AXIS Object Analytics im Szenario "Belegung eines Bereichs" an.
Zählen der Eintritte und Austritte	Zeigt Daten aus dem Szenario der AXIS Object Analytics Personenzählung, dem AXIS People Counter und dem AXIS P8815-2 3D People Counter an.
Luftqualitätsmonitor	Zeigt Live-Daten zur Luftqualität in Innenräumen von Luftqualitätssensoren (AXIS Air Quality Sensors) an.
Air Quality Monitor Detailed (Luftqualitätsmonitor Detail)	Zeigt die aggregierten Daten von Luftqualitätssensoren (AXIS Air Quality Sensors) an.

Verwendung von Durchsageschnittstellen in geteilten Ansichten

Sie können Durchsageschnittstellen verwenden, um Live-Durchsagen zu machen, Anrufe zu tätigen oder Audiodateien auf Audiogeräten wiederzugeben. Hierfür ist die Integration von AXIS Audio Manager Pro erforderlich. Weitere Informationen finden Sie unter *Konfiguration von AXIS Audio Manager Pro, on page 177*.

So nutzen Sie Durchsageschnittstellen:

1. Bearbeiten Sie eine geteilte Ansicht oder fügen Sie eine neue hinzu.

2. Ziehen Sie eine oder mehrere Audiozonen per Drag & Drop in das Raster, um dort eine Durchsageschnittstelle zu erstellen.

Hinweis

Die Audiobereiche in AXIS Camera Station Pro entsprechen den Zonen, die Sie in Ihrem AXIS Audio Manager Pro-Server eingerichtet haben.

3. Wählen Sie die Option **Speak (Sprechen)**, **Call (Anrufen)** oder **Play a file (Datei abspielen)**.
   - Wählen Sie die Option **Speak (Sprechen)** für eine Einweg-Kommunikation wie Live-Durchsagen.
   - Wählen Sie die Option **Cal (Anrufen)** für die Zwei-Wege-Kommunikation, wenn Sie z. B. über eine IP-Türsprechanlage mit jemandem sprechen möchten.
   - Wählen Sie die Option **Play a file (Datei abspielen)**, um eine Datei auf dem AXIS Audio Pro-Server über den Lautsprecher wiederzugeben.

Sequenziell

Eine Sequenz wechselt zwischen Ansichten.

Hinweis

Bei Anschluss an mehrere AXIS Camera Station Pro Server können Sie jede Ansicht, Kamera oder jedes Gerät anderer Server zu Ihrer Sequenz hinzufügen.

Sequenz hinzufügen:

1. Auf dem Tab "Live-Ansicht" + anklicken.
2. **Neue Sequenz** wählen.
3. Geben Sie einen Namen für die Sequenz ein.
4. Ziehen Sie eine oder mehrere Ansichten oder Kameras per Drag & Drop in die Sequenzansicht.
5. Ordnen Sie die Ansichten in der Reihenfolge an, in der die Sequenz erstellt werden soll.
6. Legen Sie optional für jede Ansicht die individuelle Verweildauer fest.
7. Für Kameras mit PTZ-Funktionen, wählen Sie in der Dropdown-Liste **PTZ-Voreinstellung** eine PTZ-Voreinstellung aus. Siehe *PTZ-Voreinstellungen*.
8. Klicken Sie auf **Ansicht speichern**, um die Sequenz auf dem aktuellen Server zu speichern.

Verweildauer	Die Verweildauer gibt die Anzahl Sekunden an, für die eine Ansicht angezeigt wird, bevor zur nächsten gewechselt wird. Diese kann für jede Ansicht einzeln festgelegt werden.

Sequenz hinzufügen

Kamera-Ansicht

Eine Kameraansicht zeigt Live-Video einer Kamera. Sie können Kameraansichten in geteilten Ansichten, Sequenzen und Lageplänen verwenden.

Hinweis

Sind mehrere AXIS Camera Station Pro-Server verbunden, werden in der Liste alle Geräte aller verbundenen Server angezeigt.

So fügen Sie eine Kameraansicht hinzu:

1. In dem Tab Live-Ansicht oder der Aufzeichnungen + anklicken.
2. Wählen Sie **Neue Kameraansicht**.
3. Wählen Sie die Kamera in dem Auswahlmenü und klicken Sie auf **OK**.

Lageplan

Ein Lageplan ist ein importiertes Bild, in das Sie Kameraansichten, geteilte Ansichten, Audiobereiche, Sequenzen, Webseiten, andere Lagepläne und Zugänge einfügen können. Der Lageplan bietet einen Überblick und die Möglichkeit, einzelne Geräte zu finden und darauf zuzugreifen. Bei größeren Installationen lassen sich mehrere Lagepläne zu einem Übersichtsplan zusammenfassen.

Aktionstasten sind auch in der Lageplanansicht verfügbar. Siehe *Aktionsschaltflächenauslöser erstellen*.

Hinweis

Bei Anschluss an mehrere AXIS Camera Station Pro Server können Sie jede Ansicht, Kamera oder jedes Gerät anderer Server zu Ihrer Kartenansicht hinzufügen.

Lageplan hinzufügen:

1. Auf dem Tab "Live-Ansicht" + anklicken.
2. **Neuer Lageplan** wählen.
3. Geben Sie einen Namen für den Lageplan ein.
4. Klicken Sie auf **Bild wählen** und suchen Sie Lageplandatei. Die maximale Größe für eine hochgeladene Datei beträgt 20 MB und BMP, JPG, PNG und GIF werden unterstützt.
5. Ziehen Sie die Ansichten, Kameras, andere Geräte und Zugänge per Drag & Drop in den Lageplan.
6. Klicken Sie auf ein Symbol im Lageplan, um die Einstellungen zu bearbeiten.
7. Um den Lageplan zu beschriften, klicken Sie auf **Beschriftung hinzufügen**, geben Sie einen Namen und stellen Sie Größe, Schriftstil und Farbe ein.

Hinweis

Einige Einstellungen für Symbole und Lageplanbeschriftungen können gruppenweise bearbeitet werden.

8. Klicken Sie auf **Ansicht speichern**, um den Lageplan auf dem aktuellen Server zu speichern.

	Den physischen Zustand des Zugangs, wenn der Zugang mit einem Zugangsmonitor konfiguriert ist.
	Den physischen Zustand des Schlosses, wenn der Zugang nicht mit einem Zugangsmonitor konfiguriert ist.
	Ein rotes Warndreieck weist auf einen Alarm bei Manipulation an einer Tür, einem Leser oder einer Tür-Steuerung hin.
Symbol	Wählen Sie das Symbol aus, das Sie verwenden möchten. Diese Option steht nur für Kameras und andere Geräte zur Verfügung.
Größe	Die Größe des Symbols mit dem Schieberegler einstellen.

Farbe	Um die Farbe des Symbols zu ändern, anklicken.
Bezeichnung	Um die Bezeichnung des Symbols anzuzeigen, diese Option aktivieren. Um die Lage der Bezeichnung zu festzulegen, **Unten** oder **Oben** wählen.
Direction arrow (Richtungspfeil)	Mit dieser Option können Sie Richtungspfeile für das Sichtfeld der einzelnen Kameras anzeigen lassen. Die Anzeige der Pfeile ist mit oder ohne Überwachungsbereiche möglich.
Überwachungsbereich	Diese Option steht nur für Kameras und andere Geräte zur Verfügung. Mit dieser Option den Abdeckungsbereich auf dem Lageplan hervorheben. Sie können den Umfang (**Range**), die Breite (**Width**), die Richtung (**Direction**) und die Farbe des Erfassungsbereichs bearbeiten. Aktivieren Sie die Option **Flash (Blinken)**, wenn Sie möchten, dass der Erfassungsbereich bei aufzeichnender Kamera nach Auslösung durch die Bewegungserkennung oder andere Aktionsregeln blinkt. Sie können die Blinkfunktion für die Erfassungsbereiche in den Client-Einstellungen auf der entsprechenden Seite global für alle Geräte deaktivieren, siehe hierzu *Clienteinstellungen, on page 119*.
Entfernen	Um ein Symbol vom Lageplan zu entfernen, anklicken.

Hinzufügen eines Lageplans

Audio ab Lageplan auslösen

Webseite

Die Webseitenansicht zeigt den Inhalt einer Internetseite. Sie können eine Webseite, z. B. einer geteilten Ansicht oder Sequenz, hinzufügen.

Hinzufügen einer Webseite:

1. Auf dem Tab "Live-Ansicht" anklicken.

2. **New webpage (Neue Webseite)** wählen.
3. Geben Sie einen Namen für die Webseite ein.
4. Geben Sie die vollständige URL der Webseite ein.
5. Klicken Sie auf **OK**.

Ordner

Mit Ordnern werden Objekte in einer Strukturansicht dargestellt. Ordner können geteilte Ansichten, Sequenzen, Kameraansichten, Lagepläne, Webseiten und andere Ordner enthalten.

So fügen Sie einen Ordner hinzu:

1. In dem Tab Live-Ansicht oder der Aufzeichnungen + anklicken.
2. **Neuer Ordner** wählen.
3. Benennen Sie den Ordner und klicken Sie auf **OK**.

Aufzeichnungen

Über die Registerkarte „Recordings (Aufzeichnungen)" können Sie Aufzeichnungen suchen, wiedergeben und exportieren. Die Registerkarte enthält eine Ansicht der Aufzeichnung und zwei Bereiche, in denen Sie Ansichten, Bilder, Wiedergabetools und Kameras der verbundenen Server finden können, gruppiert nach dem Servernamen (siehe *Live-Ansicht*).

In der Hauptansicht der Aufnahme können Sie das Bild auf die gleiche Weise verwalten wie in der Live-Ansicht. Weitere Informationen finden Sie unter *Bilderverwaltung in der Live-Ansicht, on page 14*.

Informationen zum Ändern der Aufzeichnungsart und der Aufzeichnungseinstellungen wie Auflösung, Komprimierung und Bildrate finden Sie unter *Aufzeichnungsmethode*.

Hinweis

Sie können Aufzeichnungen nicht manuell von AXIS Camera Station Pro entfernen. Um alte Aufzeichnungen zu löschen, müssen Sie unter **Configuration > Storage > Selection (Konfiguration > Speicher > Auswahl)** die Vorhaltezeit ändern.

Aufzeichnungswiedergabe

Aufzeichnungen von mehreren Kameras werden gleichzeitig wiedergegeben, wenn die Wiedergabemarkierung über mehrere Aufzeichnungen auf der Zeitleiste positioniert wird.

Sie können Live- und aufgezeichnete Videos gleichzeitig anzeigen, wenn Sie mehrere Monitore verwenden.

Wiedergabe-Zeitleiste

Verwenden Sie die Zeitleiste, um in der Wiedergabe zu navigieren und herauszufinden, wann eine Aufnahme stattgefunden hat. Eine rote Linie in der Zeitleiste symbolisiert eine Bewegungserkennungsaufzeichnung. Eine blaue Linie in der Zeitleiste symbolisiert eine Aufzeichnung, die durch eine Aktionsregel ausgelöst wurde. Bewegen Sie den Mauszeiger über eine Aufzeichnung in der Zeitleiste, um Aufnahmetyp und -zeit anzuzeigen. Um eine bessere Ansicht zu erhalten und Aufzeichnungen zu finden, können Sie die Zeitleiste vergrößern, verkleinern und ziehen. Beim Ziehen der Zeitleiste wird die Wiedergabe vorübergehend angehalten und erst nach der Freigabe fortgesetzt. Verschieben Sie in einer Aufzeichnung die Zeitleiste (Scrubbing), um einen Überblick über den Inhalt zu erhalten und bestimmte Ereignisse zu finden.

Aufzeichnungen finden

	Klicken Sie, um ein Datum und eine Uhrzeit in der Zeitleiste auszuwählen.
	Verwenden Sie den Filter, um zu konfigurieren, welche Art von Aufzeichnungen in der Timeline angezeigt werden sollen.
	Verwenden Sie diese Option, um gespeicherte Lesezeichen zu finden, siehe *Lesezeichen*.
	Klicken Sie hierauf, um eine Liste mit Aufzeichnungen und Lesezeichen zu öffnen, die mit der Axis Body Worn-Kamera erstellt wurden. Hier können Sie nach Datum und Uhrzeit, der Aktivierungsmethode für die Aufzeichnung sowie nach beliebigen Kategorien und Anmerkungen suchen, die der Kamerabenutzer im AXIS Body Worn Assistant hinzugefügt hat.
Intelligente Suche 1	Verwenden Sie die intelligente Suche, um nach Aufzeichnungen zu suchen (siehe *Intelligente Suche 1*.

Aufzeichnungswiedergabe

	Die Aufzeichnung wiedergeben.
	Die Aufzeichnung unterbrechen.
	Zum Anfang der/des laufenden oder der/des vorherigen Aufzeichnung/Ereignisses springen. Klicken Sie mit der rechten Maustaste, um zu Aufzeichnungen, Ereignissen oder beidem zu gelangen.
	Zum Anfang der nächsten Aufzeichnung/des nächsten Ereignisses springen. Klicken Sie mit der rechten Maustaste, um zu Aufzeichnungen, Ereignissen oder beidem zu gelangen.
	Zum vorherigen Bild in einer Aufzeichnung springen. Unterbrechen Sie die Aufnahme, um diese Funktion zu nutzen. Klicken Sie mit der rechten Maustaste, um festzulegen, wie viele Bilder übersprungen werden sollen (bis zu 20 Bilder).
	Zum nächsten Bild in einer Aufzeichnung springen. Unterbrechen Sie die Aufnahme, um diese Funktion zu nutzen. Klicken Sie mit der rechten Maustaste, um festzulegen, wie viele Bilder übersprungen werden sollen (bis zu 20 Bilder).
	Ändern Sie die Wiedergabegeschwindigkeit mithilfe der Multiplikatoren im Drop-Down Menü.
	Stummschalten. Nur Aufnahmen mit Audio verfügen über diese Funktion.
Audio-Schieberegler	Schieben Sie, um die Lautstärke zu ändern. Nur Aufnahmen mit Audio verfügen über diese Funktion.
Alle Body Worn-Metadaten anzeigen	Zeigen Sie die Metadaten eines Body Worn-Systems sowie Anmerkungen und Kategorien aus dem AXIS Body Worn Assistant an.
Schwenken, Neigen und Zoomen	Klicken Sie auf das Bild und scrollen Sie nach oben oder unten, um das Bild zu vergrößern oder zu verkleinern und die Ansicht zu verschieben, um andere Teile des Bildes anzuzeigen. Um in einen Bereich hineinzuzoomen, den Cursor in den gewünschten Bereich stellen und scrollen.

Lesezeichen

Hinweis

- Sie können eine gesperrte Aufnahme nur löschen, wenn Sie sie manuell entsperren.
- Das System löscht gesperrte Aufzeichnungen, wenn Sie die Kamera aus AXIS Camera Station Pro entfernen.

	Klicken Sie, um alle Lesezeichen anzuzeigen. Um die Lesezeichen zu filtern, klicken Sie auf das Symbol.
	Ein neues Lesezeichen hinzufügen.

	Bedeutet, dass es sich um eine gesperrte Aufnahme handelt. Die Aufzeichnung umfasst mindestens 2,5 Minuten Video vor und nach dem Lesezeichen.
	Bearbeiten Sie den Namen und die Beschreibung des Lesezeichens und entsperren oder sperren Sie die Aufnahme.
	Lesezeichen entfernen. Zum Entfernen mehrerer Lesezeichen diese markieren und STRG oder SHIFT gedrückt halten.
Löschen von Aufzeichnungen verhindern	Wählen oder löschen Sie die Option, um die Aufnahme zu sperren oder zu entsperren.

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. Um das Lesezeichen einfacher ermitteln zu können, in der Beschreibung Schlüsselbegriffe angeben.
5. Wählen Sie **Löschen von Aufzeichnungen verhindern**, um die Aufzeichnung zu sperren.

Hinweis

Es ist nicht möglich, eine gesperrte Aufnahme zu löschen. Um die Aufzeichnung zu entsperren, Entfernen Sie die Markierung der Option auf oder löschen Sie das Lesezeichen.

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

Ereigniskategorien

Weisen Sie Aufzeichnungen Kategorien zu, um das Auffinden bestimmter Arten von Ereignissen, wie z. B. Überfälle oder Verkehrskontrollen, zu erleichtern. Bevor Sie beginnen, vergewissern Sie sich bitte, dass Sie über die erforderlichen Benutzerrechte verfügen. Siehe *Benutzer-/Gruppenberechtigungen, on page 140*.

Ereigniskategorien zuweisen

1. Suchen Sie auf der Registerkarte **Recordings (Aufzeichnung)** die Aufzeichnung, der Sie eine Ereigniskategorie zuweisen möchten.
2. Klicken Sie mit der rechten Maustaste auf die Aufzeichnung in der Zeitleiste und wählen Sie **Categorize event (Ereignis kategorisieren)**.
3. Fügen Sie eine oder mehrere Kategorien hinzu.
4. Klicken Sie auf **OK**.

Wenn Sie ein Ereignis kategorisieren, werden die ausgewählten Kategorien auf der Miniaturansicht der Aufzeichnung angezeigt. Wenn Sie der Kategorie eine Farbe zugewiesen haben, wird diese Farbe in der Zeitleiste angezeigt.

Ereigniskategorien entfernen

1. Suchen Sie auf der Registerkarte **Recordings (Aufzeichnungen)** die Aufzeichnung, aus der Sie Kategorien entfernen möchten.
2. Klicken Sie mit der rechten Maustaste auf die Aufzeichnung in der Zeitleiste und wählen Sie **Categorize event (Ereignis kategorisieren)**.
3. Wählen Sie in der Liste der zugewiesenen Kategorien die Kategorie aus, die Sie entfernen möchten.
4. Klicken Sie auf **Remove (Entfernen)**.

5. Wiederholen Sie die Schritte 3 und 4 für jede Kategorie, die Sie entfernen möchten.
6. Klicken Sie auf **OK**.

Hinweis

Sie können die Schaltfläche „Remove (Entfernen)" nur verwenden, wenn Sie die Berechtigung zum Entfernen von Kategorien haben oder wenn Sie eine nicht zugewiesene Kategorie aus der Liste auswählen.

Weitere Informationen finden Sie unter *Ereigniskategorien konfigurieren, on page 90*.

Aufzeichnungen exportieren

Von der Registerkarte **Export** können Sie Aufzeichnungen in einen lokalen Speicher oder einen Netzwerkspeicherort exportieren. Hier finden Sie auch Informationen und eine Vorschau der Aufzeichnung. Es ist möglich, mehrere Dateien gleichzeitig zu exportieren und sie in die Formate .asf, .mp4 und .mkv zu exportieren. Um Ihre Aufnahmen abzuspielen, verwenden Sie Windows Media Player (.asf) oder AXIS File Player (.asf, .mp4, .mkv). AXIS File Player ist eine kostenlose Video- und Audiowiedergabesoftware, die keine Installation erfordert.

Hinweis

Mit dem AXIS File Player können Sie die Wiedergabegeschwindigkeit von Aufzeichnungen im .mp4- und .mkv-Format ändern, jedoch nicht im .asf-Format.

Vor Exportbeginn sicherstellen, dass die entsprechende Berechtigung gegeben ist. Siehe *Benutzerrechte für das Exportieren, on page 31*.

Aufzeichnungen exportieren

1. Wählen Sie in der Registerkarte **Recordings (Aufzeichnungen)** eine Kamera oder eine Ansicht.
2. Die Aufzeichnungen der Exportliste hinzufügen. Aufnahmen in der Timeline, die nicht im Export enthalten sind, erhalten eine gestreifte Farbe.
   2.1. Klicken Sie auf , um die Auswahlmarkierungen anzuzeigen.
   2.2. Bewegen Sie die Markierungen, um die zu exportierenden Aufzeichnungen einzuschließen.
   2.3. Klicken Sie auf , um die Registerkarte **Export** zu öffnen.
3. Klicken Sie auf **Export... (Exportieren...)**.
4. Wählen Sie einen Ordner, um die Aufzeichnungen zu exportieren.
5. Klicken Sie auf **OK**. Die Aufgabe zum Exportieren von Aufzeichnungen wird im Tab **Tasks (Aufgaben)** angezeigt.

Der Inhalt des Exportordners:

- Die Aufzeichnungen im ausgewählten Format.
- Eine TXT-Datei mit Notizen, falls Sie **Include notes (Notizen hinzufügen)** auswählen.
- AXIS File Player, wenn Sie **Include AXIS File Player (AXIS File Player einbeziehen)** gewählt haben.
- Eine .asx-Datei mit einer Wiedergabeliste, falls Sie **Create playlist(.asx) (Playlist erstellen (.asx))** auswählen.

Aufzeichnungen exportieren

Registerkarte **Recordings (Aufzeichnungen)**	
	Um mehrere Aufnahmen auszuwählen, klicken Sie auf und verschieben Sie die Auswahlmarkierungen an den gewünschten Start und Stopp.
	Um Aufnahmen innerhalb der Abschnittsmarkierungen zu exportieren, klicken Sie auf .
Aufzeichnungen hinzufügen	Um eine einzelne Aufzeichnung zu exportieren, klicken Sie mit der rechten Maustaste auf eine Aufzeichnung und wählen Sie **Export > Add recordings (Exportieren > Aufnahmen hinzufügen)**.
Ereignisaufzeichnungen hinzufügen	Um alle Aufzeichnungen hinzuzufügen, die innerhalb der Zeit eines Ereignisses stattgefunden haben, klicken Sie mit der rechten Maustaste auf eine Aufzeichnung und wählen Sie **Export > Add event recordings (Exportieren > Ereignisaufzeichnungen hinzufügen)**.
Aufzeichnungen löschen	Um eine Aufnahme aus der Exportliste zu entfernen, klicken Sie mit der rechten Maustaste auf eine Aufnahme und wählen Sie **Export > Remove recordings (Exportieren > Aufnahmen entfernen)**.
Aufzeichnungen löschen	Um alle Aufzeichnungen innerhalb der Auswahlmarkierungen von der Exportliste zu entfernen, außerhalb einer Aufzeichnung rechtsklicken und **Export > Remove recordings (Exportieren > Aus der Exportliste entfernen)** wählen.

Registerkarte **Export**	
Audio	Um die Audiospur der exportierten Aufzeichnung auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen in der Spalte **Audio**. Um bei exportierten Aufzeichnungen grundsätzlich auch die Audiospur einzuschließen, wechseln Sie zu **Configuration** > **Server** > **Settings** > **Export** (Konfiguration > Server > Einstellungen > Export) und wählen die Option **Include audio when adding recordings to export (Audio beim Hinzufügen zu exportierender Aufzeichnungen miteinschließen)**.
	Zur Bearbeitung einer Aufzeichnung wählen Sie die entsprechende Aufzeichnung aus und klicken auf . Siehe *Aufzeichnungen vor dem Exportieren bearbeiten (Schwärzung), on page 31*.
	Zur Bearbeitung von Aufzeichnungshinweisen wählen Sie eine Aufzeichnung aus und klicken auf .
	Um eine Aufzeichnung aus der Exportliste zu löschen, wählen Sie die entsprechende Aufzeichnung aus und klicken auf .

Registerkarte **Export**	
Zum Export wechseln	Um die Registerkarte **Export** aufzurufen, auf der angezeigten Registerkarte **Incident report (Vorfallbericht) Switch to export (Export aufrufen)** anklicken.
Bevorzugtes Videostreamprofil	Wählen Sie im Feld **Bevorzugtes Videostreamprofil** das Videostreamprofil aus.
Vorschau	Zur Vorschau und zur Wiedergabe einer Aufzeichnung, diese in der exportierten Liste anklicken. Mehrere Aufzeichnungen können nur dann in der Vorschau angezeigt werden, wenn sie von ein und der selben Kamera stammen.
Speichern	Um die Exportliste als Datei zu speichern, **Speichern** anklicken.
Last	Wenn Sie eine zuvor gespeicherte Exportliste einschließen möchten, klicken Sie auf **Load (Laden)**.
Name of export (Exportname)	Sie können einen benutzerdefinierten Namen für den exportierten Ordner bzw. die Dateien eingeben oder das Feld leer lassen und die Standard-Namenskonvention in AXIS Camera Station Pro anwenden.
Append camera name and timestamp (Kameranamen und Zeitstempel anhängen)	Wählen Sie diese Option aus, um den Namen der Kamera und den Zeitstempel an den Namen des exportierten Ordners bzw. der Dateien anzuhängen.
Start- und Endzeit anpassen	Um die Start- und Endzeit der Aufnahme anzupassen, gehen Sie in der Vorschau zur Zeitleiste und passen Sie die Start- und Endzeiten an. Die Zeitleiste zeigt um die ausgewählte Aufzeichnung bis zu 30 Minuten vor und nach der Aufzeichnung an.
Schnappschuss hinzufügen	Um Momentaufnahmen hinzuzufügen, ziehen Sie die Zeitleiste in der Vorschau an eine bestimmte Position. Klicken Sie mit der rechten Maustaste auf die Vorschau und wählen Sie **Add snapshot (Momentaufnahme hinzufügen)**.

Erweiterte Einstellungen	
Notizen beifügen	Um die Notizen für die Aufzeichnungen mit einzubeziehen, wählen Sie **Notizen miteinbeziehen**. Die Notizen sind in dem exportierten Ordner als .txt-Datei oder als Lesezeichen bei der Aufzeichnung in AXIS File Player verfügbar.
Include AXIS File Player (AXIS File Player beifügen)	Klicken Sie auf **AXIS File Player einbeziehen** und der AXIS File Player wird den exportierten Aufzeichnungen automatisch beigefügt.
Create playlist(.asx) (Wiedergabeliste erstellen (.asx))	Erstellen Sie eine Wiedergabeliste im .asx-Format für Windows Media Player, indem Sie **Wiedergabeliste (.asx) erstellen** auswählen. Die Aufzeichnungen

Erweiterte Einstellungen	
	werden in der Reihenfolge wiedergegeben, in der Sie aufgezeichnet wurden.
Digitale Signatur hinzufügen	Um Bildmanipulationen zu verhindern, wählen Sie **Add digital signature (Digitale Signatur hinzufügen)**. Diese Option ist nur für Aufzeichnungen im .asf-Format verfügbar. Siehe *Exportierte Aufzeichnungen wiedergeben und überprüfen, on page 33*.
Export zu Zip-Datei	**Export to Zip file (Als ZIP-Datei exportieren)** auswählen, um Dateien als ZIP-Datei zu exportieren. Die exportierte ZIP-Datei kann mit einem Kennwort geschützt werden.
Exportformat	Wählen Sie aus dem Drop-Down Menü **Export format (Exportformat)** ein Format aus, in das Sie Ihre Aufzeichnungen exportieren möchten. Die Audioeingänge im Format G.711 oder G.726 werden nicht in die exportierten Aufzeichnungen aufgenommen, wenn Sie MP4 auswählen.
Edited video encoding (Bearbeitete Videocodierung)	Wenn ein Video bearbeitet wurde, können Sie das Videocodierungsformat unter **Edited video encoding (Bearbeitete Videocodierung)** auf `Automatic`, `H.264` oder `M-JPEG` festlegen. Bei der Einstellung `Automatic` werden M-JPEG für das M-JPEG-Format und H.264 für andere Formate verwendet.

Benutzerrechte für das Exportieren

Um Aufzeichnungen zu exportieren oder Vorfallberichte zu erstellen, benötigen Sie eine Berechtigung. Sie können die Berechtigung für einen oder beide haben. Wenn Sie in der Registerkarte **Recordings (Aufzeichnungen)** anklicken, öffnet sich die verbundene Registerkarte für den Export.

Zum Konfigurieren der Freigaben wechseln Sie zu *Benutzerberechtigungen, on page 138*.

Aufzeichnungen vor dem Exportieren bearbeiten (Schwärzung)

Ein sich bewegendes Objekt weichzeichnen

1. Auf der Registerkarte **Export** oder **Incident report (Vorfallsbericht)** eine Aufzeichnung auswählen und auf klicken.
2. Verschieben Sie die Zeitleiste zum ersten Vorkommen des sich bewegenden Objekts, das Sie abdecken möchten.
3. Klicken Sie auf **Bounding boxes > Add (Umgrenzungsfelder > Hinzufügen)**, um ein neues Umgrenzungsfeld hinzuzufügen.
4. Wechseln Sie zu **Bounding box options > Size (Optionen für Umgrenzungsrahmen > Größe)**, um die Größe anzupassen.
5. Verschieben Sie das Begrenzungsfeld und platzieren Sie es über dem Objekt.
6. Wechseln Sie zu **Bounding box options > Fill (Optionen für Umgrenzungsfelder > Befüllen)** und wählen Sie die Option **Pixelated (Verpixelt)** oder **Black (Schwarz)** aus.
7. Wenn die Aufnahme abgespielt wird klicken Sie mit der rechten Maustaste auf das Objekt und wählen Sie **Add key frame (Keyframe hinzufügen)** aus.

8. Um fortlaufende Keyframes hinzuzufügen, ziehen Sie das Umgrenzungsfeld so, dass er das Objekt bei der Wiedergabe der Aufzeichnung abdeckt.
9. Verschieben Sie die Zeitleiste und stellen Sie sicher, dass das Umgrenzungsfeld das Objekt während der gesamten Aufnahme abdeckt.
10. Um ein Ende festzulegen, klicken Sie mit der rechten Maustaste auf die Rautenform im letzten Keyframe und wählen Sie **Set end (Ende einstellen)**. Dadurch werden die Schlüsselbilder nach dem Endpunkt entfernt.

Hinweis

Dem Video können mehrere Umgrenzungsrahmen hinzugefügt werden. Überlappende Rahmenbereiche werden in folgender Reihenfolge gefüllt: schwarz, verpixelt und klar.

Alle entfernen	Um alle Begrenzungsrahmen zu entfernen, klicken Sie auf **Bounding boxes > Remove all (Begrenzungsrahmen > Alle entfernen)**.
Keyframe entfernen	Um einen Keyframe zu entfernen, mit der rechten Maustaste auf den gewünschten Keyframe klicken und **Remove key frame (Keyframe entfernen)** auswählen.

Sich bewegende Objekt vor anonymisierten Hintergrund anzeigen

1. Erstellen Sie einen Begrenzungsrahmen, siehe *Ein sich bewegendes Objekt weichzeichnen, on page 31*.
2. **Bounding box options > Fill (Optionen für Umgrenzungsrahmen > Füllen)** und die Option **Clear (Klar)** auswählen.
3. Wechseln Sie zu **Video background (Videohintergrund)** und wählen Sie die Option **Pixelated (Verpixelt)** oder **Black (Schwarz)** aus.

Alles außer dieses verpixeln	Es können mehrere Umgrenzungsfelder aus der Liste ausgewählt werden. Rechtsklicken und **Pixelate all but this (Alle außer diesem verpixeln)** auswählen. Die ausgewählten Umgrenzungsfeld werden **Clear (Klar)** und die nicht ausgewählten **Pixelated (Verpixelt)**.

Umgrenzungsrahmen erstellen

Um Umgrenzungsfelder aus den Analysedaten zu generieren, schalten Sie die Analysedaten der Kamera ein. Siehe *Videostromprofile, on page 54*.

1. Klicken Sie auf der Registerkarte **Export** oder **Incident report (Vorfallsbericht)** auf .
2. Klicken Sie auf **Generate bounding boxes (Umgrenzungsrahmen erstellen)**.
3. Stellen Sie sicher, dass die Umgrenzungsfelder das sich bewegende Objekt abdecken, und passen Sie sie gegebenenfalls an.
4. Wählen Sie eine Füllung für die Umgrenzungsfelder oder den Videohintergrund.

Videobearbeitung mit Axis Video Content Stream optimieren

Installieren Sie zur Verbesserung der Videobearbeitung die Anwendung AXIS Video Content Stream 1.0 auf Kameras mit der Firmware 5.50 bis 9.60. AXIS Camera Station Pro startet die Installation automatisch, wenn Sie eine Kamera zum System hinzufügen. Siehe *Kameraanwendung installieren*.

Aufzeichnungen vor dem Exportieren bearbeiten

Exportierte Aufzeichnungen wiedergeben und überprüfen

Um Bildmanipulationen vorzubeugen, können Sie den exportierten Aufnahmen eine digitale Signatur mit oder ohne Kennwort hinzufügen. Verwenden Sie AXIS File Player, um die digitale Signatur zu überprüfen und auf Änderungen der Aufzeichnung zu prüfen.

1. Wechseln Sie in den Ordner mit den exportierten Aufzeichnungen. Wenn die exportierte Zip-Datei passwortgeschützt ist, geben Sie Ihr Kennwort ein, um den Ordner zu öffnen.
2. Öffnen Sie AXIS File Player. Die exportierten Aufzeichnungen werden automatisch abgespielt.
3. Klicken Sie im AXIS File Player auf , um die den Aufzeichnungen beigefügten Notizen anzuzeigen.
4. Überprüfen Sie im AXIS File Player die digitale Signatur, wenn Sie **Add digital signature (Digitale Signatur hinzufügen)** für Aufnahmen ausgewählt haben.
   4.1. **Tools > Digitale Signatur überprüfen** aufrufen.
   4.2. Wählen Sie **Validate with password (Mit Kennwort überprüfen)** und das Kennwort eingeben, wenn sie mit Kennwort geschützt ist.
   4.3. Um die Verifizierungsergebnisse anzuzeigen, klicken Sie auf **Verify (Verifizieren)**.

Vorfallsberichte exportieren

Auf der Registerkarte „Vorfallbericht" können Sie Vorfallberichte in einen lokalen Speicher oder einen Netzwerkspeicherort exportieren. Hier können Sie Aufzeichnungen, Momentaufnahmen und Notizen in Ihre Vorfallberichte einbinden.

Vor Exportbeginn sicherstellen, dass die entsprechende Berechtigung gegeben ist. Siehe *Benutzerrechte für das Exportieren, on page 31*.

Meldung von Vorfällen

Vorfallsberichte erstellen

1. Wählen Sie in der Registerkarte **Recordings (Aufzeichnungen)** eine Kamera oder eine Ansicht.
2. Die Aufzeichnungen der Exportliste hinzufügen. Siehe *Aufzeichnungen exportieren, on page 28*.
3. Klicken Sie auf **Switch to incident report (Wechseln zum Vorfallbericht)**, um zur Registerkarte „Vorfallbericht" zu gelangen.
4. Auf **Create report (Bericht erstellen)** klicken.
5. Wählen Sie einen Ordner aus, in dem der Vorfallbericht gespeichert werden soll.

6. Klicken Sie auf **OK**. Die Aufgabe „Vorfallbericht exportieren“ wird in der Registerkarte **Tasks (Aufgaben)** angezeigt.

Der Inhalt des Exportordners:

- AXIS File Player.
- Die Aufzeichnungen im ausgewählten Format.
- Eine TXT-Datei, falls Sie **Include notes (Notizen hinzufügen)** auswählen.
- Der Vorfallsbericht.
- Im Falle mehrere exportierter Aufzeichnungen die Wiedergabeliste.

Audio	Um die Audiospur der exportierten Aufzeichnung auszuschließen, deaktivieren Sie das entsprechende Kontrollkästchen in der Spalte **Audio**. Um bei exportierten Aufzeichnungen grundsätzlich auch die Audiospur einzuschließen, wechseln Sie zu **Configuration** > **Server** > **Settings** > **Export** (Konfiguration > Server > Einstellungen > Export) und wählen die Option **Include audio when adding recordings to export (Audio beim Hinzufügen zu exportierender Aufzeichnungen miteinschließen)**.
	Zur Bearbeitung einer Aufzeichnung wählen Sie die entsprechende Aufzeichnung aus und klicken auf . Siehe *Aufzeichnungen vor dem Exportieren bearbeiten (Schwärzung), on page 31*.
	Zur Bearbeitung von Aufzeichnungshinweisen wählen Sie eine Aufzeichnung aus und klicken auf .
	Um eine Aufzeichnung aus der Exportliste zu löschen, wählen Sie die entsprechende Aufzeichnung aus und klicken auf .
Zu Vorfallbericht wechseln	Um zur Registerkarte **Incident report (Vorfallbericht)** zu wechseln, wenn die Registerkarte **Export** offen ist, wählen Sie **Switch to incident report (Vorfallbericht aufrufen)**.
Bevorzugtes Videostreamprofil	Wählen Sie im Drop-Down-Menü **Preferred stream profile (Bevorzugtes Videostreamprofil)** das Videostreamprofil aus.
Vorschau	Zur Vorschau und zur Wiedergabe einer Aufzeichnung, diese in der exportierten Liste anklicken. Mehrere Aufzeichnungen können nur dann in der Vorschau angezeigt werden, wenn sie von ein und der selben Kamera stammen.
Speichern	Um den Vorfallbericht als Datei zu speichern, **Save (Speichern)** anklicken.
Last	Wenn Sie einen zuvor gespeicherten Vorfallbericht einschließen möchten, klicken Sie auf **Load (Laden)**.
Beschreibung	Das Feld **Description (Beschreibung)** wird automatisch mit vordefinierten Daten aus der Beschreibungsvorlage gefüllt. Hier können auch ergänzende Informationen hinzugefügt werden.

Kategorie	Wählen Sie eine Kategorie aus, zu der der Bericht gehört.
Referenz-ID	Eine **Reference ID (Referenz-ID)** wird automatisch generiert und kann bei Bedarf manuell geändert werden. Die Referenz-ID identifiziert den Vorfallsbericht eindeutig.
Notizen beifügen	Um Anmerkungen zu den Aufzeichnungen und Schnappschüssen hinzuzufügen, **Include notes (Anmerkungen hinzufügen)** auswählen. Die Notizen sind in dem exportierten Ordner als .txt-Datei oder als Lesezeichen bei der Aufzeichnung in AXIS File Player verfügbar.
Edited video encoding (Bearbeitete Videocodierung)	Wenn ein Video bearbeitet wurde, können Sie das Videocodierungsformat unter **Edited video encoding (Bearbeitete Videocodierung)** auf `Automatic`, `H.264` oder `M-JPEG` festlegen. Bei der Einstellung `Automatic` werden M-JPEG für das M-JPEG-Format und H.264 für andere Formate verwendet.
Start- und Endzeit anpassen	Um die Start- und Endzeit der Aufnahme anzupassen, gehen Sie in der Vorschau zur Zeitleiste und passen Sie die Start- und Endzeiten an. Die Zeitleiste zeigt um die ausgewählte Aufzeichnung bis zu 30 Minuten vor und nach der Aufzeichnung an.
Schnappschuss hinzufügen	Um Momentaufnahmen hinzuzufügen, ziehen Sie die Zeitleiste in der Vorschau an eine bestimmte Position. Klicken Sie mit der rechten Maustaste auf die Vorschau und wählen Sie **Add snapshot (Momentaufnahme hinzufügen)**.

Manuell aufzeichnen

Hinweis

Wenn Sie eine Verbindung zu mehreren AXIS Camera Station Pro Servern herstellen, können Sie eine Aufzeichnung auf jedem verbundenen Server manuell starten und stoppen. Wählen Sie dazu den Server in der Dropdown-Liste **Selected server (Ausgewählter Server)** aus.

Eine Aufzeichnung kann auch im Hauptmenü gestartet und gestoppt werden:

1. Gehen Sie zu ☰ **> Actions > Record manually (> Aktionen > Manuell aufzeichnen)**.
2. Wählen Sie eine oder mehrere Kameras aus.
3. Klicken Sie auf **Start**, um die Wiedergabe der Aufzeichnung zu starten.
4. Klicken Sie auf **Stop**, um die Aufzeichnung anzuhalten.

Eine manuell gestartete Aufzeichnung von der **Live view (Live-Ansicht)** aus starten oder anhalten:

1. Die **Live-Ansicht** aufrufen.
2. Bewegen Sie den Mauszeiger in das Fenster Direktübertragung der Kamera.
3. **REC** anklicken, um die Aufzeichnung zu beenden. Während der Aufnahme erscheint im Ansichtsrahmen eine rote Anzeige.
4. **REC** anklicken, um die Aufzeichnung anzuhalten.

Intelligente Suche 1

Suchen Sie mit „Intelligente Suche 1“ nach Teilen einer Aufzeichnung, in der in einem definierten Bildbereich Bewegung stattfindet.

Um die Suchgeschwindigkeit zu erhöhen, wählen Sie **Analysedaten einschließen** in Videostreamprofilen. Siehe *Videostromprofile*.

So verwenden Sie „Intelligente Suche 1“:

1. Klicken Sie auf + und öffnen Sie eine Registerkarte **Smart search 1 (Intelligente Suche 1)**.
2. Wählen Sie die Kamera, nach der Sie suchen möchten.
3. Passen Sie den ausgewählten Bereich an. Der Form können bis zu 20 Punkte hinzugefügt werden. Um einen Punkt zu entfernen, klicken Sie darauf mit der rechten Maustaste.
4. Verwenden Sie den **Filter für kurzlebige Objekte** und den **Filter für kleine Objekte**, um unerwünschte Ergebnisse herauszufiltern.
5. Wählen Sie Start- und Endzeit sowie das Datum für die Suche aus. Wählen Sie mit der SHIFT-Taste einen Datumsbereich aus.
6. Klicken Sie auf **Suchen**.

Die Suchergebnisse werden auf der Registerkarte **Ergebnisse** angezeigt. Klicken Sie hier mit der rechten Maustaste auf eines oder mehrere Ergebnisse, um die Aufzeichnungen zu exportieren.

Filter für kurzlebige Objekte	Die Mindestzeit, die ein Objekt im ausgewählten Interesses vorhanden sein muss, um in die Suchergebnisse aufgenommen zu werden.
Filter für kleine Objekte	Die Mindestgröße, die ein Objekt haben muss, um in den Suchergebnissen aufgenommen zu werden.

Intelligente Suche 1

Intelligente Suche 2

Nutzen Sie „Intelligente Suche 2", um sich bewegende Personen und Fahrzeuge in den Aufnahmen zu finden.

Wenn Sie „Intelligente Suche 2" für eine Axis Kamera aktivieren, beginnt AXIS Camera Station Pro mit der Aufzeichnung von Metadaten dieser Kamera. „Intelligente Suche 2" verwendet die Metadaten, um Objekte in der Szene zu klassifizieren, und ermöglicht Ihnen die Verwendung von Filtern, um interessante Dinge zu finden.

Hinweis

Für „Intelligente Suche 2" gelten folgende Voraussetzungen:

- Streaming von Metadaten zur Analyse über RTSP.
- AXIS Video Content Stream auf Kameras mit AXIS OS vor 9.60. Siehe *Kameraanwendung installieren, on page 69*.
- Zeitsynchronisierung zwischen AXIS Camera Station Pro Server und Kameras.

Hinweis

Allgemeine Empfehlungen:

- Wir empfehlen die Verwendung einer kontinuierlichen Aufzeichnung. Die Bewegungserkennung kann zu Objekterfassungen führen, die keine Videoaufzeichnung auslösen.
- Wir empfehlen die Verwendung des H.264-Formats, wenn Sie Aufnahmen in der Vorschau im Suchergebnis anzeigen möchten.
- Stellen Sie sicher, dass die Lichtverhältnisse für eine optimale Farbklassifizierung innerhalb der Kameraspezifikation liegen. Nach Erfordernis zusätzliche Lichtquellen einsetzen.

Vorgehensweise

1. *Intelligente Suche 2 konfigurieren, on page 178*
2. Zeitsynchronisierung zwischen AXIS Camera Station Pro Server und Kameras konfigurieren. Siehe *Zeitsynchronisierung, on page 73*.
3. Erstellen Sie einen Filter oder laden Sie einen vorhandenen Filter. Siehe *Suche mit Filtern, on page 37*.
4. Suchergebnisse verwalten. Siehe *Ergebnisse der intelligenten Suche, on page 42*.

Suche mit Filtern

1. Gehe zu**Configuration > Smart search 2 > Settings (Konfiguration > Intelligente Suche 2 > Einstellungen)** und wählen Sie die Kameras aus, die Sie in „Smart search 2 (Intelligente Suche 2)" verwenden möchten.
2. Klicken Sie auf + und öffnen Sie die Registerkarte **Smart search 2 (Intelligente Suche 2)**.
3. Suchkriterien definieren.
4. Klicken Sie auf **Suchen**.

Wenn die Suche länger dauert als erwartet, versuchen Sie eines oder mehrere der folgenden Verfahren, um sie zu beschleunigen:

- Schalten Sie die Hintergrundverarbeitung des Server für wichtige oder häufig genutzte Kameras ein.
- Wenden Sie Eingangsfilter auf Kameras an, um irrelevante Erfassungen zu reduzieren.
- Verkürzung der Suchdauer.
- Reduzieren Sie die Anzahl der Kameras bei der Suche.
- Definieren Sie Bereich, Objektrichtung, Größe und Dauer, um die Datenmenge einzugrenzen.

Kameras	Um die Suche nach Kamera einzuschränken, klicken Sie auf **Cameras (Kameras)** und wählen Sie die Kameras aus, die Sie in die Suche einbeziehen möchten.
Suchzeitraum	Um die Suche zeitlich einzugrenzen, klicken Sie auf **Search interval (Suchzeitraum)** und wählen Sie einen Zeitbereich bzw. ein Zeitintervall von mehreren Tagen aus oder erstellen Sie ein benutzerdefiniertes Intervall.
Person	Um Personen zu erfassen, klicken Sie auf **Object characteristics** > **Pre-classified** (Objektmerkmale > Vorklassifiziert) und wählen die Option **Person (Personen)** sowie die Kleidungsfarben. Sie können mehrere Farben auswählen.
Fahrzeug	Um Fahrzeug zu erfassen, klicken Sie auf **Object characteristics** > **Pre-classified** (Objektmerkmale > Vorklassifiziert) und wählen die entsprechenden Fahrzeugtypen und -farben aus.. Sie können mehrere Fahrzeugtypen und -farben auswählen.
Visuelle Ähnlichkeit	Suchergebnisse mit darin abgebildeten Personen können verwendet werden, um nach optisch ähnlichen Personen zu suchen. Öffnen Sie das Kontextmenü ⋮ eines Suchergebnisses und wählen Sie **Use as visual similarity reference (Als optische Vergleichsreferenz verwenden)** aus. Klicken Sie dann auf **Suchen**. Hinweis Die Ähnlichkeitssuche erstellt abstrakte Darstellungen aus zugeschnittenen Bildern von Personen mit niedriger Auflösung und vergleicht sie mit anderen Darstellungen. Wenn zwei Darstellungen ähnlich sind, erhalten Sie einen Treffer bei Ihrer Suche. Bei der Ähnlichkeitssuche werden keine biometrischen Daten zur Identifizierung einer Person verwendet, sondern es können beispielsweise die allgemeine Form und die Farbe der Kleidung einer Person zu einem bestimmten Zeitpunkt erkannt werden.
Freitextsuche	Mit der Freitextsuche können Sie in natürlicher Sprache (nur Englisch) beschreiben, wonach Sie in den Aufzeichnungen suchen. Siehe *Freitextsuche, on page 40*.
Bereich	Klicken Sie auf **Area (Bereich)**, wählen Sie eine Kamera und aktivieren Sie **Filter by area on this camera (Auf dieser Kamera nach Bereich filtern)**, um nach Bereich zu filtern. Passen Sie den gewünschten Bereich im Bild an und fügen Sie bei Bedarf Punkte hinzu oder entfernen Sie sie.
Virtueller Stolperdraht	Klicken Sie auf **Line crossing (Überschreiten einer Linie)**, wählen Sie eine Kamera und aktivieren Sie **Filter by line crossing on this camera (Auf dieser Kamera nach Überschreiten einer Linie filtern)**, um nach Überschreiten einer Linie zu filtern. Passen Sie

	die Linie im Bild an und fügen Sie bei Bedarf Punkte hinzu oder entfernen Sie sie.
Größe und Dauer	Klicken Sie auf **Size and duration (Größe und Dauer)**, wählen Sie die Kamera aus und aktivieren Sie **Filter by size and duration on this camera (Auf dieser Kamera nach Größe und Dauer filtern)**, um nach Größe und Dauer zu filtern. Passen Sie die Mindesthöhe und -breite als Prozentwert des Gesamtbildes ein. Passen Sie die Mindestdauer in Sekunden an.
Geschwindigkeit	Klicken Sie auf **Speed (Geschwindigkeit)**, wählen Sie die Kamera und aktivieren Sie **Filter by speed on this camera (Auf dieser Kamera nach Geschwindigkeit filtern)**, um nach Geschwindigkeit zu filtern. Geben Sie den Geschwindigkeitsbereich an, nach dem gefiltert werden soll. Hinweis Der Geschwindigkeitsfilter steht für Produkte wie Radare und Fusionskameras zur Verfügung, die Geschwindigkeiten erfassen können.
Unbekannte Objekterfassungen	Um die Erkennungen einzuschließen, die „Intelligente Suche 2“ als unbekannt einstuft, wählen Sie **Object characteristics (Objekteigenschaften)** und dann **Unknown object detections (Unbekannte Objekterfassungen)**.
	Um einen Filter zu speichern, klicken Sie auf , geben Sie einen Filternamen ein und klicken Sie auf **Save (Speichern)**. Wählen Sie **Share with other users (Mit anderen Benutzern teilen)** aus, um den Filter mit anderen Benutzern zu teilen. Um einen vorhandenen Filter zu ersetzen, klicken Sie auf , wählen einen vorhandenen Filter aus und klicken auf **Replace (Ersetzen)**.
	Um eine aktuelle Suche zu laden, klicken Sie auf > **Recent searches (Aktuelle Suchen)** und wählen eine Suche aus. Um einen gespeicherten Filter zu laden, klicken Sie auf > **Saved filters (Gespeicherte Filter)** und wählen eine Filter aus. Um einen von anderen Benutzern freigegebenen Filter zu laden, klicken Sie auf > **Shared filters (Geteilte Filter)** und wählen einen Filter aus.
	Klicken Sie zum Zurücksetzen eines Filters auf und dann auf **Reset (Zurücksetzen)**.

Freitextsuche

Mit der Freitextsuche können Sie in Ihrer natürlichen Sprache beschreiben, wonach Sie in den Aufzeichnungen suchen.

Hinweis

- Die Freitextsuche erfordert mindestens 16 GB RAM.
- Für die Freitextsuche ist eine Internetverbindung erforderlich.
  - Die Freitextsuche nutzt die Internetverbindung, um das KI-Modell von axis.com herunterzuladen, wenn Sie es zum ersten Mal einrichten und wenn wir das Modell verbessern.
  - Die Freitextsuche stellt einmal wöchentlich eine Verbindung zu den Cloud-Diensten von Axis her um zu prüfen, ob die KI-Modelle aktualisiert werden müssen, um künftigen Vorschriften oder Anforderungen zu entsprechen. Wenn die Verbindung fehlschlägt, können Sie die Freitextsuche erst wieder nutzen, wenn Ihr System wieder verbunden ist.
  - Die Freitextsuche führt die gesamte Verarbeitung lokal auf Ihrem Server durch und **nutzt keine** Internetverbindung, um Videos, Bilder oder Eingabetexte zu versenden.

So schalten Sie die Freitextsuche ein:

1. Öffnen Sie eine Registerkarte **Configuration (Konfiguration)**.
2. Gehen Sie zu **Intelligente Suche 2** > **Einstellungen**.
3. Wählen Sie unter Freitextsuche **Use free text search (Freitextsuche verwenden)**. Das System lädt die erforderlichen Dateien von axis.com herunter.

Zur Freitextsuche:

1. Öffnen Sie die Registerkarte **Intelligente Suche 2**.
2. Klicken Sie auf **Objektmerkmale**.
3. Klicken Sie auf **Free text (Freitext)**.
4. Klicken Sie auf **Zeigen**, um Informationen zu Verwendungszweck, Einschränkungen und verantwortungsvoller Nutzung zu lesen.
5. Geben Sie ein, was Sie bei Ihrer Suche ein- und ausschließen möchten.
6. Klicken Sie auf **Suchen**.

Leitlinien für Eingabeaufforderungen

Wir empfehlen, folgende Struktur für Ihre Eingabeaufforderungen zu verwenden:

`{person, vehicle or other object} + {specific action or attributes of the person, vehicle, or object}`

Beschreiben Sie das Objekt gut mit einigen wenigen Schlüsseldeskriptoren. Zum Beispiel:

Eingabeaufforderung	Kommentar
Eine Dame mit rotem Pullover und schwarzem Hut	In etwa richtig
Dame in Rot	Ein wenig zu vage
Eine Frau, etwa 156 cm groß, mit einer kastanienbraunen Strickjacke mit gelben Akzenten und einem schwarzen Sonnenhut aus den späten 80er Jahren mit hellbrauner Borte	Viel zu viele Details

Beschreiben Sie die Situation so, als ob Sie mit einer Person sprechen würden, die kein Experte für Videosicherheit ist. Zum Beispiel:

Eingabeaufforderung	Kommentar
Ein gelber Pickup parkt neben einem Baum	In etwa richtig
Ein unbemanntes Fahrzeug ohne Personen, Fahrzeugkennzeichen: CHY67F, Klasse: Pickup, Farbe: gelb, Position: Neben der mächtigen Pappel.	Zu sehr wie ein Polizeibericht

Gute Deskriptoren, die bei der Freitextsuche sehr wahrscheinlich verstanden werden:

Bezeichnung	Beispiel
Objektklasse	Person, Auto, Fahrrad, Tier
Farbe	Gelb
Wetter	Sonnig
Bekannte Marken (Automarken, Logos)	UPS-Lastwagen

Schlechte Deskriptoren:

Bezeichnung	Beispiel
Text	Ein Ladenschild mit der Aufschrift “Zutritt für Tanzbären verboten“.
Emotionale Anhaltspunkte	Ein wütend aussehender Mann
Zählung	14 Menschen auf einem Marktplatz
Regionale Umgangssprache	Ein roter Staubsauger

Moderation von Suchanfragen

Suchanfragen, die beleidigende, schädliche oder toxische Inhalte enthalten, können blockiert werden, um eine sichere und respektvolle Umgebung zu gewährleisten. Unser System verwendet ein Modell zur Verarbeitung natürlicher Sprache, um jede Suchanfrage zu bewerten, sowie eine benutzerdefinierte Liste verbotener Suchkategorien und Wörter, um diese Fähigkeit zu verbessern.

Wenn Sie mit einem gesperrten Wort nicht einverstanden sind oder ein neues vorschlagen möchten, können Sie über die Benutzeroberfläche der Intelligenten Suche ein anonymes Feedback abgeben, das unserem Team zur Überprüfung übermittelt wird.

Hinweis

- Die Freitextsuche unterstützt nur Englisch.
- Die Freitextsuche analysiert Standbilder. Es kann schwierig sein, mit der Freitextsuche für Aktionen wie Fallen, Laufen oder Stehlen gute Ergebnisse zu erzielen, da sie mehr Kontext erfordern.
- Die Freitextsuche verwendet Bildausschnitte, was bedeutet, dass die Umgebung möglicherweise nicht berücksichtigt wird. Sie erhalten möglicherweise weniger genaue Ergebnisse, wenn Sie Szene-Deskriptoren wie Stadt, Urban, Park, Garten, See und Strand verwenden.
- Ausführlichere Informationen über die Freitextfunktion, einschließlich ihrer Einschränkungen und bewährter Verfahren, finden Sie in unserem Whitepaper *Freitextsuche in AXIS Camera Station Pro*.

Ergebnisse der intelligenten Suche

	Um Erkennungen zu gruppieren, die wahrscheinlich zum selben Ereignis gehören, können Sie sie in Zeitintervallen gruppieren. Wählen Sie im Dropdown-Menü ein Intervall aus.
Neuste zuerst	„Intelligente Suche 2" zeigt die Suchergebnisse in absteigender Reihenfolge an, wobei die neuesten Entdeckungen zuerst angezeigt werden. Klicken Sie auf **Oldest first (Älteste zuerst)**, damit die ältesten Erfassungen zuerst angezeigt werden.
Confidence level (Vertrauensniveau)	Um die Suchergebnisse weiter zu filtern, klicken Sie auf **Confidence level (Zuverlässigkeitsstufe)** und legen Sie die gewünschte Zuverlässigkeitsstufe fest. Bei einem hohen Vertrauensniveau werden unsichere Klassifikationen ignoriert.
Spalten	Um die Größe der Miniaturansichten im Suchergebnis anzupassen, klicken Sie auf **Columns (Spalten)** und ändern die Spaltenanzahl.
Erfassungsansicht	Wählen Sie **Detection view (Erfassungsansicht)**, um eine zugeschnittene Ansicht des erfassten Objekts als Miniaturansicht anzuzeigen.

Einschränkungen

- Die Intelligente Suche 2 unterstützt nur den primären (nicht beschnittenen) Sichtbereich.
- Die Intelligente Suche 2 unterstützt nur Erfassungsmodi ohne Beschnitt.
- Die Verwendung der Intelligenten Suche 2 mit gespiegelten und gedrehten Videostreams für Geräte mit ARTPEC-7 oder höher und einer Firmware-Version unter 10.6 kann einige Probleme verursachen.
- Eine hohe oder stark schwankende Netzwerkverzögerung kann zu Problemen bei der Zeitsynchronisation führen und die Erfassungsklassifizierung anhand analytischer Metadaten beeinträchtigen.
- Die Klassifizierung der Objekttypen sowie die Erfassungsgenauigkeit wird durch eine schlechte Bildqualität aufgrund hoher Komprimierungsraten, Witterungsverhältnisse wie Starkregen oder Schnee und – bei Kameras mit geringer Bildauflösung – durch starke Verzerrungen, ein großes Sichtfeld oder übermäßige Vibrationen negativ beeinflusst.
- „Intelligente Suche 2" erkennt möglicherweise keine kleinen und weit entfernten Objekte.
- Bei Dunkelheit oder IR-Beleuchtung ist keine Klassifizierung nach Farben möglich.
- Body Worn-Kameras werden nicht unterstützt.
- Radar erfasst nur Personen und andere Fahrzeuge. Bei Radarbildern ist keine Server-Klassifizierung im Hintergrund möglich.
- Die Objektklassifizierung hat bei Wärmebildkameras ein unbekanntes Verhalten.
- Bei jeder Änderung einer PTZ-Voreinstellung werden während einer kurzen Rekalibrierung nach der Positionsänderung keine sich bewegenden Objekte von „Intelligente Suche 2" erkannt.
- Linienüberquerungs- und Bereichsfilter bleiben von PTZ-Positionsänderungen unberührt.

Datensuche

Mit der Datensuche können Sie Daten aus einer externen Quelle finden. Eine Quelle ist ein System oder Gerät, das Daten generiert, die Sie verwenden können, um mehr darüber herauszufinden, was bei einem Ereignis passiert ist. Weitere Informationen finden Sie unter *Externe Datenquellen, on page 73*. Hier ein paar Beispiele:

- Ein Ereignis, das von einem Zutrittssystem generiert wurde.
- Ein Fahrzeugkennzeichen, das von AXIS License Plate Verifier erfasst wurde.
- Eine Geschwindigkeitserfassung über AXIS Speed Monitor.

Um die Zeit zum Speichern externer Daten in AXIS Camera Station Pro zu ändern, rufen Sie **Configuration > Server > Settings > External data (Konfiguration > Server > Einstellungen > Externe Daten)** auf.

So suchen Sie nach Daten:

1. Klicken Sie auf + und wählen Sie **Data search (Datensuche)** aus.
2. Wählen Sie ein Suchintervall aus .
3. Wählen Sie einen Datenquellentyp aus der Drop-Down-Liste aus.
4. Klicken Sie auf die Suchoptionen und wenden Sie weitere Filter an. Die Filter können abhängig vom Datenquellentyp variieren.
5. Geben Sie Schlüsselwörter in das Suchfeld ein. Siehe *Suche optimieren, on page 44*.
6. Klicken Sie auf **Suchen**.

Die Datensuche speichert die aus der Quelle generierten Daten als Lesezeichen, wenn Sie sie mit einer Ansicht konfiguriert haben. Klicken Sie auf die Daten in der Liste, um zur Aufzeichnung zu gehen und das damit verbundene Ereignis nachzuverfolgen.

Zeitintervall	
Live	Um nach Echtzeitdaten zu suchen, wählen Sie **Live** als Zeitintervall. Die Datensuche kann maximal 3000 Live-Datenereignisse anzeigen. Der Live-Modus unterstützt keine Suchoperatoren.
Letzte Stunde – Letzte 30 Tage	Um Daten aus einem Zeitraum mit Voreinstellung zu suchen, wählen Sie eine der verfügbaren Optionen aus: letzte Stunde, 4 Stunden, 12 Stunden, 24 Stunden, 48 Stunden, 7 Tage oder 30 Tage.
Benutzerdefiniert	Um Daten innerhalb eines bestimmten Zeitraums zu suchen, wählen Sie **Custom (Benutzerdefiniert)** und geben Sie ein Start- und Enddatum sowie eine Start- und Endzeit ein.

Sie können das Suchergebnis nach verschiedenen Quellentypen filtern:

Datenquellentyp	
All data (Alle Daten)	Diese Option umfasst Daten sowohl von Komponenten- als auch von externen Quellen.

Zutrittskontrolle	Die Zutrittskontrolle ist ein Beispiel für eine Komponente, die Daten erzeugt. Verwenden Sie diese Option, wenn Sie ausschließlich Daten von dieser bestimmten Komponente miteinbeziehen möchten. Mit der Zutrittskontrolle können Sie nach Zugängen und Zonen, Karteninhabern und Ereignistypen filtern.
Third party (Dritte)	Verwenden Sie diese Option, wenn Sie Daten von anderen Quellen als den konfigurierten Komponenten miteinbeziehen möchten.

Abhängig von der Datenquelle können Sie unterschiedliche Elemente in Ihrem Suchergebnis erhalten. Hier ein paar Beispiele:

Suchergebnisse	
Server	Der Server, an den die Ereignisdaten gesendet werden. Nur verfügbar, wenn mehrere Server verbunden werden.
Standort	Der Name des Zugangs und der Name des Netzwerk-Zugangscontrollers mit IP-Adresse.
Eintrittsgeschwindigkeit	Die Geschwindigkeit (Kilometer pro Stunde oder Meilen pro Stunde), wenn das Objekt in die RMD-Zone (Radar Motion Detection) eintritt.
Klassifizierung	Die Objektklassifizierung. Zum Beispiel: Fahrzeug.

Klicken Sie auf **Download search result (Suchergebnis herunterladen)**, um die Suchergebnisse in eine PDF- oder Textdatei zu exportieren. Sie können die Spalten neu anordnen und die Spaltenbreiten im Suchergebnis anpassen, um das Tabellenlayout in der PDF-Ausgabe zu verbessern. Die PDF-Datei enthält bis zu 10 Spalten.

Suche optimieren

Für genauere Ergebnisse können Sie die folgenden Suchoperatoren verwenden:

Verwenden Sie Anführungszeichen `" "`, um exakte Übereinstimmungen für Schlüsselwörter zu finden.	• Eine Suche nach `"door 1"` führt zu Ergebnissen, die “Zugang 1“ enthalten. • Eine Suche nach `door 1` führt zu Ergebnissen, die “Zugang“ und “1“ enthalten.
Verwenden Sie `AND`, um Übereinstimmungen mit allen Schlüsselwörtern zu finden.	• Eine Suche nach `door AND 1` führt zu Ergebnissen, die “Zugang“ und “1“ enthalten. • Eine Suche nach `"door 1" AND "door forced open"` führt zu Ergebnissen, die “ Zugang 1“ und “Unberechtigter Zugang “ enthalten.
Verwenden Sie `OR` oder `|`, um Übereinstimmungen in beliebiger Kombination zu finden.	• Eine Suche nach `"door 1" OR "door 2"` führt zu Ergebnissen, die “Zugang 1“ oder “Zugang 2“ enthalten. • Eine Suche nach `door 1 OR door 2` führt zu Ergebnissen, die “Zugang“ oder “1“ oder “2“ enthalten.
Verwenden Sie die Klammern `( )` zusammen mit `AND` oder `OR`.	• Eine Suche nach `(door 1 OR door 2) AND "Door forced open"` liefert Ergebnisse, die eines der folgenden Elemente enthalten:

	– "Tür 1" und "unberechtigter Zugang" – "Tür 2" und "unberechtigter Zugang" • Eine Suche nach `door 1 AND (door (forced open OR open too long))` liefert Ergebnisse, die eines der folgenden Elemente enthalten: – "Tür 1" und "unberechtigter Zugang" – "Tür 1" und "Tür zu lange geöffnet"
Verwenden Sie >, >=, < oder <=, um Zahlen in einer bestimmten Spalte zu filtern.	• Eine Suche nach `[Max speed] > 28` liefert Ergebnisse mit einem Wert über 28 in der Spalte Maximale Geschwindigkeit. • Eine Suche nach `[Average speed] <= 28` liefert Ergebnisse mit einem Wert bis maximal 28 in der Spalte Durchschnittliche Geschwindigkeit.
Verwenden Sie `CONTAINS`, um nach Text in bestimmten Spalten zu suchen.	• Die Suche `[Cardholder] CONTAINS Oscar` liefert Ergebnisse, bei denen sich in der Spalte „Kartenhalter" der Text „Oskar" befindet. • Die Suche `[Door] CONTAINS "door 1"` liefert Ergebnisse, bei denen sich in der Spalte „Zugang" der Text „Zugang 1" befindet.
Verwenden Sie = für genaue Übereinstimmungen in einer bestimmten Spalte.	Eine Suche nach `[CardholderId] = ABC123` gibt nur Ergebnisse mit Übereinstimmungen für „ABC123" in der Spalte „Karteninhaber" zurück.

Konfiguration

Der Tab Konfiguration wird zur Verwaltung und Wartung angeschlossener Geräte sowie Einstellungen von Client und Servern verwendet. Klicken Sie auf + und wählen Sie **Configuration (Konfiguration)** aus, um die Registerkarte zur Konfiguration aufzurufen.

Geräte konfigurieren

In AXIS Camera Station Pro bezieht sich der Begriff Gerät auf ein Netzwerk-Produkt mit einer IP-Adresse. Der Begriff "Kamera" bezieht sich auf die Videoquelle, wie eine Netzwerk-Kamera oder ein Videoport (mit angeschlossener analoger Kamera) an einem Video-Encoder mit mehreren Ports. Beispielsweise ist ein Videoencoder mit vier Ports ein Gerät mit vier Kameras.

Hinweis

- AXIS Camera Station Pro unterstützt ausschließlich Geräte mit IPv4-Adressen.
- Einige Video-Encoder haben für jeden Videoport eine IP-Adresse. Ist dies der Fall, wird jeder Videoport von AXIS Camera Station Pro als ein Gerät mit einer Kamera behandelt.

Bei einem Gerät kann es sich bei AXIS Camera Station Pro handeln um:

- eine Netzwerk-Kamera
- ein Video-Encoder mit einem oder mehreren Videoports
- ein Zusatzgerät wie etwa ein E/A-Audiogerät, ein Netzwerklautsprecher oder eine Türsteuerung
- eine IP-Türsprechanlage

Folgende Aktionen können auf den Geräten ausgeführt werden:

- Kameras und Geräte ohne Videofunktionen hinzufügen. Siehe *Geräte hinzufügen*.
- Einstellungen angeschlossener Kameras bearbeiten. Siehe *Kameras*.
- Einstellungen für Geräte ohne Kamera bearbeiten. Siehe *Andere Geräte*.
- Auflösung, Format und andere Einstellungen von Videostreamprofilen bearbeiten. Siehe *Videostromprofile*.
- Bildeinstellungen in Echtzeit anpassen. Siehe *Bildkonfiguration*.
- PTZ-Voreinstellungen hinzufügen oder entfernen. Siehe *PTZ-Voreinstellungen*.
- Verbundene Dienste verwalten und warten. Siehe *Geräteverwaltung*.
- Externe Datenquellen verwalten. Siehe *Externe Datenquellen, on page 73*.

Geräte hinzufügen

Hinweis

- Das System erkenn Ansichtbereiche als individuelle Kameras. Ansichtbereiche müssen zuerst in der Kamera erstellt werden, bevor sie verwendet werden können. Siehe *Ansichtsbereiche verwenden*.
- Wenn Sie ein Gerät hinzufügen, synchronisiert das Gerät seine Uhrzeit mit dem AXIS Camera Station Pro-Server.
- Wir empfehlen, im Hostnamen eines Geräts keine Sonderzeichen wie å, ä oder ö zu verwenden.

1. Suchen Sie nach Geräten, Videostreams oder vorab aufgezeichneten Videos.
   - *Geräte ermitteln, on page 48*
   - *Videostreams finden, on page 48*
   - *Auffinden von vorab aufgezeichneten Videos, on page 49*
2. *Hinzufügen von Geräten, Videostreams oder vorab aufgezeichneten Videos, on page 49*

Sie müssen alle in der Gerätestatusspalte angezeigten Probleme beheben, bevor Sie ein Gerät hinzufügen können.

(Leer)	Wenn kein Status vorhanden ist, können Sie das Gerät zu AXIS Camera Station Pro hinzufügen.
Communicating (Kommunikation erfolgt...)	AXIS Camera Station Pro Server versucht, auf das Gerät zuzugreifen.
Kein vertrauenswürdiges Gerätezertifikat	AXIS Camera Station Pro kann nicht überprüfen, ob das HTTPS-Zertifikat auf dem Gerät von einem vertrauenswürdigen Aussteller signiert wurde. Klicken Sie auf den Link, um ein neues HTTPS-Zertifikat auszustellen oder AXIS Camera Station Pro zu erklären, dass das vorhandene Zertifikat vertrauenswürdig ist.
Zertifizierungsstelle nicht mehr gültig	Die Zertifizierungsstelle, die das Zertifikat für das Gerät ausgestellt hat, ist nicht mehr gültig. Klicken Sie auf den Link, um ein neues HTTPS-Zertifikat auszustellen oder AXIS Camera Station Pro zu erklären, dass das vorhandene Zertifikat vertrauenswürdig ist.
Adresse im Gerätezertifikat stimmt nicht überein	Die Adresse des Geräts stimmt nicht mit der Adresse im Zertifikat überein. Klicken Sie auf den Link, um ein neues HTTPS-Zertifikat auszustellen oder AXIS Camera Station Pro zu erklären, dass das vorhandene Zertifikat vertrauenswürdig ist.
Kommunikationsfehler	AXIS Camera Station Pro kann nicht mit dem Gerät kommunizieren.
Kennwort eingeben	AXIS Camera Station Pro kennt die Anmeldedaten für den Zugriff auf das Gerät nicht. Auf den Link klicken, um einen Benutzernamen und ein Kennwort für ein Administratorkonto für das Gerät einzugeben. Die Kombination aus Benutzername und Kennwort wird von AXIS Camera Station Pro für alle Geräte verwendet, auf denen der Benutzer registriert ist.
Kennwort festlegen	Das Root-Konto und -Kennwort sind nicht eingerichtet oder das Gerät verwendet weiterhin das Standardkennwort. Auf den Link klicken, um das Root-Benutzerkennwort festzulegen. • Geben Sie Ihr Kennwort ein oder klicken Sie **Generate (Generieren)** um ein Kennwort zu bekommen. Es wird empfohlen, das erstellte Kennwort anzuzeigen und eine Kopie davon zu erstellen. • Optional kann dieses Kennwort für alle Geräte mit dem Status `Set password` verwendet werden.
Nicht unterstütztes Modell	AXIS Camera Station Pro unterstützt das Gerätemodell nicht.
Firmware veraltet	Die Firmware des Geräts ist alt und Sie müssen sie aktualisieren, bevor Sie das Gerät hinzufügen können.
Fehlerhaftes Gerät	Die von AXIS Camera Station Pro abgerufenen Geräteparameter sind beschädigt.
Neigungsausrichtung einstellen	Klicken Sie auf den Link und wählen Sie als Neigungsausrichtung Decke, Wand oder Schreibtisch,

	je nach Montage der Kamera. Die Einstellung der Neigungsausrichtung ist bei bestimmten Kameramodellen obligatorisch.
Nicht unterstütztes ONVIF-Gerät	AXIS Camera Station Pro unterstützt dieses Drittanbietergerät nicht.
Nicht unterstütztes Gerät	AXIS Camera Station Pro unterstützt diesen Typ von Geräten nicht.

Hinweis

Neue HTTPS-Zertifikate werden von AXIS Camera Station Pro ausgestellt und verlängern sich automatisch.

Geräte ermitteln

Um nicht aufgeführte Geräte zu ermitteln:

1. **Konfiguration > Geräte > Geräte hinzufügen** aufrufen.
2. Auf **Abbrechen** klicken, um die laufende Netzwerksuche abzubrechen.
3. Klicken Sie auf **Manual search (Manuelle Suche)**.
4. So finden Sie mehrere Geräte in einem oder mehreren IP-Bereichen:
   4.1. Wählen Sie **Search one or more IP ranges (Einen oder mehrere IP-Adressbereiche durchsuchen)** aus.
   4.2. Geben Sie den IP-Adressbereich ein. Zum Beispiel: 192.168.10.*, 192.168.20-22.*, 192.168.30.0-50
   - Für alle Adressen einer Gruppe Platzhalter verwenden.
   - Für Adressbereiche einen Bindestrich (-) verwenden.
   - Trennen Sie mehrere Bereiche mithilfe eines Kommas.

   4.1. Um den voreingestellten Port 80 zu ändern, den Portbereich eingeben. Zum Beispiel: 80, 1080-1090
   - Für Portbereiche einen Bindestrich (-) verwenden.
   - Trennen Sie mehrere Bereiche mithilfe eines Kommas.

   4.1. Klicken Sie auf **Suchen**.
5. So suchen Sie ein oder mehrere bestimmte Geräte:
   5.1. Wählen Sie **Enter one or more hostnames or IP addresses (Eine(n) oder mehrere Hostnamen oder IP-Adressen eingeben)** aus.
   5.2. Geben Sie die Host-Namen oder IP-Adressen durch Kommas voneinander getrennt ein.
   5.3. Klicken Sie auf **Suchen**.
6. Klicken Sie auf **OK**.

Videostreams finden

Sie können Videostreams hinzufügen, die Folgendes unterstützen:

- Protokoll: RTSP, HTTP, HTTPS
- Video-Codierung: M-JPEG für HTTP und HTTPS, H.264 für RTSP
- Audiocodierung: AAC und G.711 für RTSP

Unterstützte Videostream-URL-Schemata:

- `rtsp://<address>:<port>/<path>`
  Zum Beispiel: `rtsp://<address>:554/axis-media/media.amp`

- `http://<address>:80/<path>`
  Zum Beispiel: `http://<address>:80/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`
- `https://<address>:443/<path>`
  Zum Beispiel: `https://<address>:443/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`

1. **Konfiguration > Geräte > Geräte hinzufügen** aufrufen.
2. Klicken Sie auf **Enter stream URLs (Stream-URLs eingeben)** und geben Sie eine oder mehrere Videostream-URLs ein, die durch Komma getrennt sind.
3. Klicken Sie auf **Hinzufügen**.

Auffinden von vorab aufgezeichneten Videos

Sie können voraufgezeichnete Videos im .mkv-Format zu AXIS Camera Station Pro hinzufügen.

Anforderungen an die .mkv-Datei:

- Video-Codierung: M-JPEG, H.264, H.265
- Audiocodierung: AAC

1. Erstellen Sie einen Ordner **PrerecordedVideos** unter `C:\ProgramData\Axis Communications\AXIS Camera Station Server`.
2. Fügen Sie dem Ordner eine .mkv-Datei hinzu.
3. Fügen Sie eine .dewarp-Datei mit dem selben Namen wie die .mkv-Datei hinzu, um das vorab aufgezeichnete Video auszupacken. Weitere Informationen finden Sie unter *Bildkonfiguration, on page 59*.
4. Rufen Sie **Configuration > Devices > Add devices (Konfiguration > Geräte > Geräte hinzufügen)** und aktivieren Sie **Vorab aufgezeichnete Videos einbeziehen**.
   Das vorab aufgezeichnete Video und mehrere vorab aufgezeichnete Videos werden vom System bereitgestellt.

Hinzufügen von Geräten, Videostreams oder vorab aufgezeichneten Videos

1. Wählen Sie in einem System mit mehreren Servern einen Server aus der Dropdown-Liste **Selected server (Ausgewählter Server)** aus.
2. **Konfiguration > Geräte > Geräte hinzufügen** aufrufen.
3. Wählen Sie die Geräte, Videostreams oder vorab aufgezeichneten Videos aus. Klicken Sie auf **Hinzufügen**.
4. Um die Konfiguration zu überspringen und später mit den hinzugefügten Geräten fortzufahren, klicken Sie auf **Close (Schließen)**. So fahren Sie mit der Konfiguration fort:
   4.1. Wählen Sie **Quick configuration (Schnelle Konfiguration)**, wenn Sie nur die Grundeinstellungen konfigurieren möchten. Wenn Sie ein Site Designer Projekt importieren, wählen Sie **Site Designer configuration (Site Designer Konfiguration)**. Weitere Informationen finden Sie unter *Site Designer-Projekte importieren*.
   4.2. Wählen Sie **Add image overlay for date, time, and text (Bildüberlagerung für Datum, Uhrzeit und Text hinzufügen)**, wenn Sie eine Überlagerung für die Axis Kameras hinzufügen möchten, für die noch keine Überlagerungen konfiguriert sind.
   4.3. Klicken Sie auf **Next (Weiter)**.
   4.4. Wählen Sie Ihre bevorzugte **Aufzeichnungsmethode** aus.
   4.5. Klicken Sie auf **Next (Weiter)**.
   4.6. Wählen Sie Ihre **Speicherdauer** und den **Aufzeichnungsspeicher** aus und klicken Sie auf **Finish (Fertigstellen)**, um die Konfiguration zu übernehmen.

Site Designer-Projekte importieren

Der AXIS Site Designer ist ein Onlinedesign-Tool, das Sie beim Erstellen eines Standorts mit Produkten und Zubehör von Axis unterstützt.

Wenn Sie in AXIS Site Designer einen Standort erstellt haben, können Sie die Projekteinstellungen in AXIS Camera Station Pro importieren. Sie können mit einem Zugangscode oder einer heruntergeladenen Site Designer Setup-Datei auf das Projekt zugreifen.

Ein AXIS Site Designer Projekt in AXIS Camera Station Pro importieren:

1. Zugangscode für Ihr Site Design-Projekt erstellen oder eine Projektdatei herunterladen.
   1.1. Melden Sie sich unter *http://sitedesigner.axis.com* mit Ihrem MyAxis-Konto an.
   1.2. Ein Projekt auswählen und die Projektseite aufrufen.
   1.3. Auf **Share (Freigeben)** klicken.
   1.4. Klicken Sie auf **Generate code (Code erstellen)**, wenn der AXIS Camera Station Pro Server mit dem Internet verbunden ist. Oder klicken Sie auf **Download settings file (Einstellungsdatei herunterladen)**, wenn Ihr Server nicht mit dem Internet verbunden ist.
2. Rufen Sie im AXIS Camera Station Pro Client **Configuration > Devices > Add devices (Konfiguration > Geräte > Geräte hinzufügen)** auf.
3. Wählen Sie die Geräte aus und klicken Sie auf **Add** (Hinzufügen).
4. Wählen Sie **Site Designer-Konfiguration** aus und klicken Sie auf **Weiter**.
5. Wenn Sie einen Zugangscode generiert haben, wählen Sie **Zugangscode** und geben Sie ihn ein. Alternativ wählen Sie **Choose file (Datei auswählen)** aus und wechseln Sie zur bereits heruntergeladenen Einrichtungsdatei für Site Designer.
6. Klicken Sie auf **Import (importieren)**. AXIS Camera Station Pro versucht, das Site Designer Projekt anhand der IP-Adresse oder des Produktnamens mit den ausgewählten Geräten abzugleichen. Wenn der Abgleich fehlschlägt, können Sie im Dropdown-Menü das richtige Gerät auswählen.
7. Klicken Sie auf **Next** (Weiter).
8. Wählen Sie Ihre bevorzugte **Aufzeichnungsmethode** aus. Bitte beachten Sie, dass die Einstellungen auf die Kameras angewendet werden, die nicht mit der Konfiguration aus dem Site Designer Projekt übereinstimmen.
9. Klicken Sie auf **Next (Weiter)**.
10. Wählen Sie Ihre **Speicherdauer** und den **Aufzeichnungsspeicher** aus und klicken Sie auf **Finish (Fertigstellen)**, um die Konfiguration zu übernehmen.

AXIS Camera Station Pro importiert die folgenden Einstellungen aus dem Site Designer Projekt:

	Encoder, Video-Decoder, Türsteuerungen, Radarmelder und Lautsprecher	Kameras, Gegensprechanlagen und F/FA-Serien
Zeitpläne mit Namen und Zeitfenstern	✓	✓
Karten mit Name, Symbolfarbe, Symbolposition und Elementname	✓	✓
Bezeichnung	✓	✓
Beschreibung	✓	✓
Kontinuierliche Aufzeichnung: Zeitplan- und Aufzeichnungsprofil einschließlich Bildrate, Auflösung,		✓

	Encoder, Video-Decoder, Türsteuerungen, Radarmelder und Lautsprecher	Kameras, Gegensprechanlagen und F/FA-Serien
Video-Codierung und Komprimierung		
Bewegungsausgelöste Aufzeichnung: Zeitplan- und Aufzeichnungsprofil einschließlich Bildrate, Auflösung, Video-Codierung und Komprimierung		✓
Zipstream-Stärke		✓
Audio-Einstellungen für die Live-Ansicht und Aufzeichnungen		✓
Vorhaltezeit für Aufzeichnungen		✓

Hinweis

- Wenn Sie nur eines der Aufzeichnungsprofile definiert haben oder es im Site Designer Projekt zwei identische Aufzeichnungsprofile gibt, setzt AXIS Camera Station Pro das Profil auf Medium.
- Wenn Sie beide Aufzeichnungsprofile im Site Designer Projekt definiert haben, setzt AXIS Camera Station Pro das kontinuierliche Aufzeichnungsprofil auf Medium und die bewegungsgesteuerte Aufzeichnung auf Hoch.
- AXIS Camera Station Pro optimiert das Seitenverhältnis, was bedeutet, dass die Auflösung zwischen dem Import und dem Site Designer-Projekt unterschiedlich sein kann.
- AXIS Camera Station Pro kann die Audioeinstellungen festlegen, wenn das Gerät über ein integriertes Mikrofon oder einen Lautsprecher verfügt. Um ein externes Audiogerät zu verwenden, aktivieren Sie dieses nach der Installation manuell.
- AXIS Camera Station Pro wendet keine Audioeinstellungen auf IP-Türsprechanlagen an, auch wenn die Einstellungen in Site Designer unterschiedlich sind. Bei Gegensprechanlagen ist der Ton immer nur in der Live-Ansicht eingeschaltet.

Geräte anderer Hersteller hinzufügen

Geräte anderer Hersteller können auf die gleiche Weise wie Axis Produkte zu AXIS Camera Station Pro hinzugefügt werden. Siehe *Geräte hinzufügen*.

Hinweis

Sie können auch Geräte anderer Hersteller als Videostreams zu AXIS Camera Station Pro hinzufügen. Siehe *Videostreams finden, on page 48*.

Informationen zur Unterstützung von Geräten anderer Hersteller finden Sie in den *aktuellen technischen Unterlagen*.

AXIS Camera Station Pro unterstützt folgende Funktionen für Geräte von Drittanbietern gemäß IEC 62676-2-31 und IEC 62676-2-32:

- Kameraerkennung
- Video-Codierung: M-JPEG, H.264
- Audio-Codierungen: G.711 (unidirektional vom Gerät zu AXIS Camera Station Pro)
- Ein Videoprofil pro Kamera
- Live-Ansicht
- Kontinuierliche und manuelle Aufzeichnungen
- Wiedergabe
- Aufzeichnungen exportieren
- Geräte-Ereignisauslöser
- PTZ

Ansichtsbereiche verwenden

Einige Kameramodelle unterstützen Sichtbereiche. AXIS Camera Station Pro führt auf der Seite **Add devices (Geräte hinzufügen)** Sichtbereiche als Einzelkameras auf. Siehe *Geräte hinzufügen*.

Hinweis

- Alle Sichtbereiche einer Netzwerk-Kamera zählen in der laut AXIS Camera Station Pro Lizenz zulässigen Gesamtanzahl von Kameras als eine Kamera.
- Die Anzahl der Kameras, die Sie hinzufügen können, hängt von der Lizenz ab.
- Jeder AXIS Camera Station Pro Lizenz kann eine bestimmte Anzahl von Kameras hinzugefügt werden.

Um Sichtbereiche in AXIS Camera Station Pro verwenden zu können, müssen Sie diese zunächst in der Kamera aktivieren:

1. Wechseln Sie zu **Konfiguration > Geräte > Kameras**.
2. Die Kamera wählen und den Link in der Adressspalte anklicken.
3. Geben Sie auf der Konfigurationsseite der Kamera den Benutzernamen und das Kennwort für die Anmeldung ein.
4. Einstellungen werden je nach Kamera und Firmware unterschiedlich aktiviert. Die **Help (Onlinehilfe)** hilft beim Auffinden der Einstellungsoptionen.

Ein Gerät ersetzen

Sie können ein Gerät ersetzen und die vorhandene Konfiguration und die Aufzeichnungen behalten. Die Anzahl der konfigurierten Videostreams auf der neuen Kamera muss mit der der alten Kamera identisch sein.

Ein Gerät ersetzen:

1. Wenn das Gerät, das Sie ersetzen möchten, den Cloud-Speicher verwendet, gehen Sie zu **Cloud storage (Cloud-Speicher)** in My Systems und deaktivieren Sie den Cloud-Speicher für das Gerät.
2. Öffnen Sie eine Registerkarte **Configuration (Konfiguration)** und wechseln Sie zu **Devices (Geräte)** > **Management**.
3. Das zu ersetzende Gerät auswählen und anklicken.
4. Im Dialogfeld **Replace device (Geräte ersetzen)** das Gerät wählen, mit dem das alte ersetzt werden soll.
5. Klicken Sie auf **Finish** (Fertig).
6. Das Dialogfeld **Replaced device (Ersetztes Gerät)** wird angezeigt, um zu bestätigen, dass das Gerät erfolgreich ersetzt wurde. Klicken Sie auf **OK**.
7. Wenn das ersetzte Gerät den Cloud-Speicher verwendet hat, starten Sie den Dienst auf Ihrem AXIS Camera Station ProServer erneut und aktivieren Sie den Cloud-Speicher für das Gerät in My Systems. Siehe *Einschalten des Cloud-Speichers für Ihre einzelnen Kameras*.

8. Überprüfen Sie die Konfiguration des neuen Geräts, um sicherzustellen, dass die Einstellungen korrekt sind und das Gerät normal funktioniert. Falls zutreffend:
   8.1. Rekonfigurieren Sie die PTZ-Voreinstellungen auf dem Gerät.
   8.2. Fügen Sie entfernte I/O-Ports hinzu und aktualisieren Sie zugehörige Aktionsregeln.
   8.3. Rekonfigurieren Sie die Kameraeinstellungen, wenn die alte Kamera die integrierte Videobewegungserkennung anstelle der Videobewegungserkennung der ACAP-Anwendung verwendet hat.
   8.4. Legen Sie eine SD-Speicherkarte ein oder schalten Sie **Failover recording (Ausfallsichere Aufzeichnung)** in den Einstellungen für die Speicherauswahl aus, wenn die alte Kamera eine ausfallsichere Aufzeichnung verwendet hat.

Kameras

Wechseln Sie zu**Configuration > Devices > Cameras (Konfiguration > Geräte > Kameras)**, um die Liste aller im System hinzugefügten Kameras anzuzeigen.

Auf dieser Seite haben Sie folgende Möglichkeiten:

- Klicken Sie auf die Adresse einer Kamera, um deren Weboberfläche zu öffnen. Dies erfordert, dass zwischen dem AXIS Camera Station Pro Client und dem Gerät kein NAT oder keine Firewall vorhanden ist.
- Hier können Sie die Kameraeinstellungen bearbeiten. Siehe *Kameraeinstellungen bearbeiten*.
- Kameras entfernen. Dabei werden von AXIS Camera Station Pro alle Aufzeichnungen, einschließlich der gesperrten, die mit den gelöschten Kameras verknüpft sind.

Kameraeinstellungen bearbeiten

Um Kameraeinstellungen zu bearbeiten:

1. Wechseln Sie zu **Konfiguration > Geräte > Kameras**.
2. Die Kamera wählen und **Bearbeiten** anklicken.

Aktiviert	Deaktivieren Sie **Enabled (Aktiviert)**, um die Aufzeichnung und Anzeige des Videostreams zu verhindern Ermöglicht. Aufzeichnungen und Live-Ansicht können weiterhin konfiguriert werden.
Channel	Wenn **Channel (Kanal)** für Multiport Video-Encoder verfügbar ist, wählen Sie die Portnummer. Ist **Channel (Kanal)** für Sichtbereiche verfügbar, wählen Sie die jeweilige Nummer des Sichtbereichs aus.

Andere Geräte

Wechseln Sie zu**Configuration > Devices > Other devices (Konfiguration > Geräte > Andere Geräte)**, um eine Liste der Geräte ohne Videofunktionen anzuzeigen. Die Liste umfasst Türsteuerungen, Audiogeräte und E/A-Module.

Weitere Informationen zu unterstützten Produkten finden Sie auf *www.axis.com* unter *Audio von Zusatzgeräten verwenden*.

Auf dieser Seite haben Sie folgende Möglichkeiten:

- Klicken Sie auf die Adresse eines Geräts, um dessen Weboberfläche zu öffnen. Dies erfordert, dass zwischen dem AXIS Camera Station Pro Client und dem Gerät kein NAT oder keine Firewall vorhanden ist.

- Geräteeinstellungen wie Name, Adresse und Kennwort bearbeiten.
- Geräte entfernen.

Zusatzgeräteeinstellungen bearbeiten

So ändern Sie den Namen eines Zusatzgeräts, bei dem es sich nicht um eine Kamera handelt:

1. **Konfiguration > Geräte > Andere Geräte** aufrufen.
2. Das Gerät wählen und **Bearbeiten** anklicken.
3. Den neuen Namen für das Gerät eingeben.

Videostromprofile

Ein Videostreamprofil ist eine Gruppe von Einstellungen, die sich auf den Videostream auswirken, z. B. Auflösung, Videoformat, Bildrate und Komprimierung. Gehen Sie auf **Konfiguration > Geräte > Videostreamprofile)**, um die Seite mit den Videostreamprofilen zu öffnen. Auf der Seite wird eine Liste aller Kameras angezeigt.

Die folgenden Profile können für die Live-Ansicht und für Aufzeichnungseinstellungen verwendet werden:

Hoch – Optimiert für höchste Qualität und Auflösung.

Mittel – Optimiert für ausgewogene Qualität und Leistung.

Niedrig – Auf Leistung optimiert.

Hinweis

Das Videostreamprofil ist standardmäßig auf **Automatic (Automatisch)** in der Live-Ansicht und bei Aufzeichnungen eingestellt, d. h. das Videostreamprofil ändert sich automatisch zu**High (Hoch)**, **Medium (Mittel)** oder **Low (Niedrig)** abhängig von der verfügbaren Größe für den Videostream.

Videostreamprofile bearbeiten

1. Wechseln Sie zu **Configuration > Devices > Stream profiles (Konfiguration > Geräte > Videostreamprofile)** und wählen Sie die Kameras, die Sie konfigurieren möchten.
2. Unter **Video profiles (Videoprofile)** konfigurieren Sie Auflösung, Videoformat, Bildrate und Komprimierung.
3. Unter **Audio** konfigurieren Sie das Mikrofon und den Lautsprecher.
4. Unter **Advanced (Erweitert)** konfigurieren Sie Analysedaten, FFmpeg-Streaming, PTZ-Autotracking-Objektindikatoren und benutzerdefinierte Stream-Einstellungen. Diese Einstellungen sind nicht für alle Produkte verfügbar.
5. Klicken Sie auf **Anwenden**.

Videoprofile

Encoder	• Die verfügbaren Optionen hängen von den Konfigurationen des Video-Encoders auf dem Gerät ab. Diese Option steht nur für Geräte anderer Hersteller zur Verfügung. • Sie können eine Videoencoder-Konfiguration nur für ein Videoprofil verwenden. • Wenn das Gerät nur über eine Encoderkonfiguration verfügt, ist nur das **Medium**-Profil verfügbar.
Auflösung	Die verfügbaren Optionen hängen vom Kameramodell ab. Eine höhere Auflösung liefert ein detaillierteres

	Bild, erfordert jedoch eine höhere Bandbreite und mehr Speicherplatz.
Format	Die verfügbaren Optionen hängen vom Kameramodell ab. Die meisten Kameras unterstützen **H.264** und **M-JPEG**. H.264 erfordert weniger Bandbreite und Speicher als M-JPEG. Einige Kameras unterstützen auch **H.265**, das eine etwas bessere Komprimierung bietet, jedoch mehr Rechenleistung erfordert. Unsere Kameras der neuesten Generation unterstützen AV1, das eine gute Komprimierung und eine Reihe neuer Funktionen bietet, wie beispielsweise umschaltbare Overlays. Weitere Informationen zu AV1 erhalten Sie auf der *AV1-Produktseite*. Auf der *Seite mit dem kompatiblen Kameras* können Sie prüfen, ob Ihre Kamera AV1 unterstützt.
Bildfrequenz	Die tatsächliche Bildrate hängt vom Kameramodell, den Netzwerkbedingungen und der Computerkonfiguration ab.
Komprimierung	Eine niedrigere Komprimierung verbessert die Bildqualität, erfordert jedoch eine höhere Bandbreite und mehr Speicherplatz.

Hinweis

- In den Audio-Dropdown-Listen werden ausschließlich Kameras mit Firmware 5 und höher angezeigt.
- Wenn mehr als 5 Kameras dieselbe Audioquelle verwenden, kann die Quellkamera überlastet werden und weniger effizient arbeiten.

Zipstream

Stärke	Die Zipstream-Stärke bestimmt den Grad der Bitratenreduzierung in einem H.264- oder H.265-Stream in Echtzeit. Diese Option ist nur auf Axis Geräten verfügbar, die Zipstream unterstützen.	**Standard**	Verwenden Sie die über die Weboberfläche des Geräts konfigurierte Zipstream-Einstellung.
		Aus	Keine
		Niedrig	In den meisten Szenen kein sichtbarer Effekt
		Mittel	Sichtbarer Effekt in einigen Szenen: Weniger Bildrauschen und etwas niedrigere Detailstufe in weniger interessanten Beobachtungsbereichen
		Hoch	Sichtbarer Effekt in vielen Szenen: Weniger Bildrauschen und niedrigere Detailstufe in weniger interessanten Beobachtungsbereichen
		Höher	Sichtbarer Effekt in noch mehr Szenen: Weniger Bildrauschen und niedrigere Detailstufe in weniger interessanten Beobachtungsbereichen
		Extrem	Sichtbarer Effekt in den meisten Szenen: Weniger Bildrauschen und niedrigere Detailstufe in weniger interessanten Beobachtungsbereichen

Für Speicherung optimieren	Zipstream optimiert den Videostream für die Speicherung mithilfe des Profils **Optimize for storage (Optimierung für die Speicherung)**. Bei der Speicheroptimierung werden mit erweiterten Komprimierungstools im Vergleich zu den Standardeinstellungen von Zipstream zusätzliche Speichermedien eingespart. Dieses Profil kann die Bitrate selbst bei Szenen mit viel Bewegung noch weiter reduzieren. • Das asf-Format unterstützt keine B-Rahmen, die von dieser Funktion verwendet werden. • Diese Funktion wirkt sich nicht auf Videoaufzeichnungen mit Rekordern der AXIS S30-Serie aus. • Diese Funktion erfordert AXIS OS 11.7.59 oder höher.		

Audio

Mikrofon:	Um einer Kamera ein Mikrofon zuzuordnen, **Built-in microphone or line in (Integriertes Mikrofon oder Audioeingang)** oder das Mikrofon eines anderen Geräts wählen. Siehe *Audio von Zusatzgeräten verwenden*.
Lautsprecher:	Um einer Kamera einen Lautsprecher zuzuordnen, **Built-in speaker or line out (Integrierter Lautsprecher oder Audioausgang)** oder den Lautsprecher eines anderen Geräts wählen. Verwenden Sie ein am Computer angeschlossenes Mikrofon, um Ansprachen zu übermitteln. Siehe *Audio von Zusatzgeräten verwenden*.
Mikrofon verwenden für:	Aktivieren von Audio für ein oder zwei Videostreams. Audio kann für die Live-Ansicht und Aufzeichnungen, nur für die Live-Ansicht oder nur für Aufzeichnungen aktiviert werden.

Bei einer Verbindung mit AXIS Audio Manager Pro können Sie über einen AXIS Audio Manager Pro-Server auch Audiogeräte als verknüpftes Audiogerät für eine Kamera auswählen. Weitere Informationen finden Sie unter *Konfiguration von AXIS Audio Manager Pro, on page 177*.

Erweitert

Analysedaten einbeziehen	Um während des Videostreamings Daten für die intelligente Suche zu erfassen, **Include analytics data (Analysedaten einbeziehen)** wählen. Diese Option ist nur auf Axis Geräten verfügbar, die Analysedaten unterstützen. Das Sammeln von Daten für *Intelligente Suche 1* kann zu Verzögerungen im Streaming von Live-Video führen.
Verwenden Sie FFmpeg	Um die Kompatibilität mit Geräten anderer Hersteller zu verbessern, **FFmpeg verwenden**, um FFmpeg-Streaming zu aktivieren. Diese Option steht nur für Geräte anderer Hersteller zur Verfügung.
Objektindikatoren für PTZ-Autotracking anzeigen	Um die Objektanzeigen zu zeigen, die von einer PTZ-Kamera in der Live-Ansicht erkannt werden, wählen Sie Die Objektanzeigen für automatisches **Verfolgen von PTZ anzeigen** aus und legen Sie die Pufferzeit des Videostreams auf 2000 Millisekunden fest. Diese Option ist nur für Axis PTZ-Kameras mit AXIS PTZ Autotracking verfügbar. Für einen vollständigen Workflow zum Einrichten von AXIS PTZ Autotracking in AXIS Camera Station Pro siehe *AXIS PTZ Autotracking einrichten*.
Anpassen des Videostreams	Um die Stream-Einstellungen für ein bestimmtes Profil anzupassen, geben Sie die Einstellungen für das Profil getrennt durch `&` ein. Geben Sie beispielsweise `overlays=off&color=0` ein, um die Overlays dieser Kamera auszublenden. Die benutzerdefinierten Einstellungen überschreiben alle vorhandenen Einstellungen. Schließen Sie vertrauliche Informationen nicht in die benutzerdefinierten Einstellungen ein.

Die zu konfigurierende Kamera wählen, um die Profileinstellungen für Auflösung, Bildrate, Komprimierung, Videoformat und Audio **anzupassen**. Kameras des gleichen Modells mit den gleichen Konfigurationsmöglichkeiten können gleichzeitig zusammen konfiguriert werden. Siehe *Konfigurationseinstellungen*.

Weitere Informationen zum **Anpassen der Profileinstellungen für Aufzeichnungen** finden Sie unter *Aufzeichnungsmethode*.

Die **in der Live-Ansicht verwendete Auflösung und Bildrate kann begrenzt werden, um die genutzte Bandbreite zu reduzieren**, z. B. wenn eine langsame Verbindung zwischen dem AXIS Camera Station Pro Client und dem AXIS Camera Station Pro Server verwendet wird. Mehr über Bandbreitennutzung, siehe *Streaming*.

Audio von Zusatzgeräten verwenden

Audio von anderen Geräten, nicht-Kamera oder Zusatzgeräten kann zusammen mit den Videobildern einer Netzwerk-Kamera oder eines Video-Encoders für Live-Ansichten und Aufzeichnungen verwendet werden.

1. Fügen Sie Geräte, bei denen es sich nicht um Kameras handelt, zu AXIS Camera Station Pro hinzu. Siehe *Geräte hinzufügen*.
2. Die Kamera zum Verwenden von Audio des Geräts konfigurieren. Siehe *Videostromprofile*.
3. Aktivieren Sie die Audiofunktion für die Live-Ansicht bzw. Aufzeichnung. Siehe *Videostromprofile*.

Die folgenden Beispiele finden Sie in *AXIS Camera Station Pro Video Tutorials*:

- Einrichten von Audiogeräten und Live-Ansagen
- Eine Aktionstaste erstellen, um bei Bewegungserfassung ein Audio manuell wiederzugeben
- Automatische Wiedergabe von Audio bei Bewegungserkennung
- Hinzufügen eines Audioclips zum Lautsprecher und zu AXIS Camera Station Pro

Bildkonfiguration

Sie können die Bildeinstellungen für die mit AXIS Camera Station Pro verbundenen Kameras konfigurieren.

Hinweis

Vorgenommene Änderungen werden sofort umgesetzt.

Die Bildeinstellungen konfigurieren:

1. Unter **Configuration > Devices > Image configuration (Konfiguration > Geräte > Bildkonfiguration)** befindet sich eine Liste der zu AXIS Camera Station Pro hinzugefügten Kameras.
2. Die Kamera wählen und den Videostream unterhalb der Liste in Echtzeit wiedergeben. Verwenden Sie das Feld **Suchwort eingeben**, um eine bestimmte Kamera in der Liste zu finden.
3. Die Bildeinstellungen konfigurieren.

Bildeinstellungen

Helligkeit: Die Bildhelligkeit ändern. Höhere Werte ergeben ein helleres Bild.

Farbstufe: Die Farbsättigung anpassen. Niedrigere Werte ergeben eine geringere Farbsättigung. Farbstufe 0 ergibt ein Schwarzweißbild. Der Maximalwert ergibt maximale Farbsättigung.

Schärfe: Die Bildschärfe einstellen. Mehr Schärfe kann zu stärkerem Bildrauschen führen, besonders bei dunklen Lichtbedingungen. Eine hohe Schärfeeinstellung kann auch zu Bildfehlern um Bereiche mit hohem Kontrast führen, z. B. an scharfen Kanten. Eine niedrigere Schärfeeinstellung reduziert das Bildrauschen, führt jedoch zu einem weniger scharfen Bild.

Kontrast: Den Bildkontrast ändern.

Weißabgleich: Die Option für den Weißabgleich ist über die Drop-Down-Liste verfügbar. Mithilfe des Weißabgleichs werden Farben unabhängig von der Farbtemperatur der Lichtquelle gleich dargestellt. Die Kamera identifiziert bei Verwendung der Option **Automatic** bzw. **Auto** die Lichtquelle und gleicht automatisch deren

Farbe aus. Ist das Ergebnis nicht zufriedenstellend, wählen Sie eine Option aus, die zum Typ der Lichtquelle passt. Die verfügbaren Optionen hängen vom Kameramodell ab.

Bild drehen: Die Bilddrehung festlegen.

Automatische Bilddrehung: Aktivieren Sie diese Einstellung, damit die Bilddrehung automatisch erfolgt.

Mirror image (Bild spiegeln): Aktivieren Sie diese Option, um das Bild zu spiegeln.

Backlight compensation (Gegenlichtausgleich): Aktivieren, wenn eine helle Lichtquelle (z. B. eine Glühbirne) dazu führt, dass andere Bildbereiche zu dunkel dargestellt werden.

Dynamic Contrast (Wide Dynamic Range): Aktivieren, um diese Funktion zu verwenden. Ein großer Dynamikbereich kann bei deutlichem Kontrast zwischen hellen und dunklen Bildbereichen die Belichtung verbessern. Passen Sie den dynamischen Kontrast mit Hilfe des Schiebereglers an. Aktivieren Sie den dynamischen Kontrast bei starkem Gegenlicht. Deaktivieren Sie den dynamischen Kontrast bei schwacher Beleuchtung.

Custom dewarp settings (Einstellungen für benutzerdefinierte Entzerrung): Es kann eine DEWARP-Datei importiert werden, die die Objektiv-Parameter und Werte für die optische Zentrierung sowie die Neigungsausrichtung der Kamera enthält. Auf **Reset (Zurücksetzen)** klicken, um die Parameter auf die ursprünglichen Werte zurückzusetzen.

1. Eine DEWARP-Datei mit folgenden Parametern erstellen:
   - Erforderlich: `RadialDistortionX`, `RadialDistortionY`, `RadialDistortionZ` und `TiltOrientation`. Die möglichen Werte für `TiltOrientation` sind `wall`, `desk` und `ceiling`.
   - Optional: `OpticalCenterX` und `OpticalCenterY`. Wenn die optische Zentrierung festgelegt werden soll, müssen beide Parameter hinzugefügt werden.
2. Auf **Import** klicken und zur DEWARP-Datei navigieren.

Beispiel für eine DEWARP-Datei:

```
RadialDistortionX=-43.970703 RadialDistortionY=29.148499 RadialDistortionZ=715.732193
TiltOrientation=Desk OpticalCenterX=1296 OpticalCenterY=972
```

PTZ-Voreinstellungen

Schwenken, Neigen und Zoomen (PTZ) ist die Fähigkeit zu schwenken (Bewegung nach links und rechts), zu neigen (Bewegung nach oben und unten) sowie herein- und herauszuzoomen.

Unter **Konfiguration > Geräte > PTZ-Voreinstellungen** befindet sich eine Liste der zu Kameras, die mit PTZ verwendet werden können. Klicken Sie auf eine Kamera, um alle für die Kamera verfügbaren Voreinstellungen anzeigen zu können. **Aktualisieren** anklicken, um die Liste zu aktualisieren.

Sie können PTZ verwenden mit:

- PTZ-Kameras, also Kameras mit integriertem mechanischen PTZ.
- Feste Kameras mit aktiviertem digitalen PTZ.
- ONVIF-Kameras, die PTZ-Voreinstellungen unterstützen.

Digitales PTZ wird über die integrierten Setup-Seiten der Kamera aktiviert. Weitere Informationen finden Sie im Benutzerhandbuch der Kamera. Um die Setup-Seiten zu öffnen, den Arbeitsbereich Geräteverwaltung aufrufen, die Kamera wählen und den Link in der Spalte Adresse anklicken.

PTZ-Voreinstellungen können auf AXIS Camera Station Pro und der Konfigurationsseite der Kamera konfiguriert werden. Es wird empfohlen, die PTZ-Voreinstellungen in AXIS Camera Station Pro zu konfigurieren.

- Wenn auf der Konfigurationsseite der Kamera eine PTZ-Voreinstellung konfiguriert wird, können Sie den Videostream nur innerhalb der Voreinstellung anzeigen. Die PTZ-Bewegungen in der Live-Ansicht sind zu erkennen und werden aufgezeichnet.

- Wenn eine PTZ-Voreinstellung in AXIS Camera Station Pro konfiguriert ist, können Sie den vollständigen Videostream der Kamera anzeigen. Die PTZ-Bewegungen in der Live-Ansicht sind zu erkennen und werden aufgezeichnet.

Hinweis

PTZ kann nicht verwendet werden, wenn die Steuerungswarteschlange der Kamera aktiviert ist. Informationen zur Steuerungswarteschlange sowie zu deren Aktivierung und Deaktivierung finden Sie im Benutzerhandbuch der Kamera.

So fügen Sie eine Voreinstellung hinzu:

1. **Konfiguration > Geräte > PTZ-Voreinstellungen** aufrufen und eine Kamera aus der Liste auswählen.
2. Verwenden Sie bei Kameras mit mechanischem PTZ die PTZ-Steuerung, um die Kameraansicht in die gewünschte Position zu bewegen. Verwenden Sie bei Kameras mit digitalem PTZ das Mausrad, um die Kameraansicht zu vergrößern und in die gewünschte Position zu ziehen.
3. **Hinzufügen** anklicken und einen Namen für die neue Voreinstellung eingeben.
4. Klicken Sie auf **OK**.

Um eine Voreinstellung zu entfernen, wählen Sie die Voreinstellung aus und klicken Sie auf **Entfernen**. Dadurch wird die Voreinstellung aus AXIS Camera Station Pro und der Kamera entfernt.

Geräteverwaltung

Die Geräteverwaltung bietet Tools zum effizienten Verwalten und Warten von Geräten, die mit AXIS Camera Station Pro verbunden sind.

Gehen Sie zu **Konfiguration > Geräte > Management**, um die Geräteverwaltungsseite zu öffnen.

Wenn Sie in *Einstellungen zum Aktualisieren der Firmware, on page 125* die automatische Überprüfung auf neue Firmware-Versionen eingerichtet haben, wird ein Link angezeigt, wenn neue Firmware-Versionen für Geräte verfügbar sind. Um die neueste Firmwareversion zu aktualisieren, klicken Sie auf den Link. Siehe *Aktualisieren der Firmware*.

Wenn Sie in *AXIS Camera Station Pro aktualisieren, on page 130* die automatische Überprüfung auf neue Firmware-Versionen eingerichtet haben, wird ein Link angezeigt, wenn eine neue Firmware-Version für AXIS Camera Station Pro verfügbar ist. Klicken Sie auf den Link, um eine neue Version von AXIS Camera Station Pro zu installieren.

Eine Liste aller Geräte, die zu AXIS Camera Station Pro hinzugefügt wurden, wird angezeigt. Verwenden Sie das Feld **Suchwort eingeben**, um Geräte in der Liste zu finden. Um Spalten aus- und einzublenden, die Kopfzeile rechtsklicken die betreffenden Spalten wählen. Ziehen Sie an den Spaltenköpfen, um die Spalten in einer anderen Reihenfolge anzuordnen.

Die folgenden Informationen wird in der Geräteliste angezeigt:

- **Vor- und Nachname:** Wenn das Gerät ein Video-Encoder mit mehreren angeschlossenen Kameras oder eine Netzwerk-Kamera mit mehreren Ansichtsbereichen ist, wird der Gerätename oder eine Liste aller zugeordneten Kameranamen angezeigt.
- **MAC-Adresse:** Die MAC-Adresse des Geräts.
- **Status:** Der Status des Geräts.
  - **OK:** Der Standardstatus einer hergestellten Geräteverbindung.
  - **Maintenance (Wartung):** Das Gerät wird gewartet. Der Zugriff ist vorübergehend nicht möglich.
  - **Zugriff nicht möglich:** Es kann keine Verbindung zum Gerät hergestellt werden.
  - **Not accessible over set hostname (Kein Zugriff über eingestellten Hostnamen):** Über den Hostnamen kann keine Verbindung mit dem Gerät hergestellt werden.
  - **Zugriff auf Server nicht möglich:** Zu dem Server, mit dem das Gerät verbunden ist, kann keine Verbindung hergestellt werden.

- **Kennwort eingeben:** Keine Verbindung zu dem Gerät, bis gültige Anmeldeinformationen eingegeben wurden. Auf den Link klicken, um gültige Benutzeranmeldeinformationen bereitzustellen. Sofern das Gerät verschlüsselte Verbindungen unterstützt, wird das Kennwort verschlüsselt versendet.
- **Kennwort festlegen:** Das Root-Konto und -Kennwort sind nicht eingerichtet oder das Gerät verwendet weiterhin das Standardkennwort. Auf den Link klicken, um das Root-Benutzerkennwort festzulegen.
  - Geben Sie Ihr Kennwort ein oder klicken Sie auf **Generate (Erstellen)**, um automatisch ein Kennwort zu erstellen, das nicht länger als für das Gerät zulässig ist. Es wird empfohlen, das automatisch erstellte Kennwort anzuzeigen und eine Kopie davon zu erstellen.
  - Optional kann dieses Kennwort für alle Geräte mit dem Status `Set password` verwendet werden.
  - Wählen Sie bei Geräten, die dieses Protokoll unterstützen, **HTTPS aktivieren**.
- **Kennworttyp: unverschlüsselt:** Es wird keine Verbindung zu dem Gerät hergestellt, da das Gerät zuvor mithilfe eines verschlüsselten Kennworts verbunden war. Aus Sicherheitsgründen verweigert AXIS Camera Station Pro die Verwendung unverschlüsselter Kennwörter für Geräte, die zuvor mithilfe eines verschlüsselten Kennworts verbunden waren. Bei Geräten, die Verschlüsselung unterstützen, wird der Verbindungstyp über die Konfigurationsseite des Geräts konfiguriert.
- **Certificate error (Zertifikatfehler):** Fehler mit dem Zertifikat auf dem Gerät.
- **Das Zertifikat läuft demnächst ab:** Das Zertifikat auf dem Gerät läuft demnächst ab.
- **Certificate has expired (Zertifikat abgelaufen):** Das Zertifikat auf dem Gerät ist abgelaufen.
- **HTTPS certificate not trusted (Nicht vertrauenswürdiges HTTPS-Zertifikat):** Dem HTTPS-Zertifikat auf dem Gerät wird von AXIS Camera Station Pro nicht vertraut. Klicken Sie auf den Link, um ein neues HTTPS-Zertifikat auszustellen.
- **HTTP failed (HTTP fehlgeschlagen):** Es kann keine HTTP-Verbindung zum Gerät hergestellt werden.
- **HTTPS failed (HTTPS fehlgeschlagen):** Es kann keine HTTPS-Verbindung zum Gerät hergestellt werden.
- **HTTP and HTTPS failed (ping or UDP OK) (HTTP und HTTPS fehlgeschlagen (Ping oder UDP OK)):** Es kann keine HTTP- oder HTTPS-Verbindung zum Gerät hergestellt werden. Das Gerät reagiert auf Ping-Tests und das Benutzer-Datagramm-Protokoll (UDP).

- **Adresse:** Die Adresse des Geräts. Klicken Sie auf den Link, um die Konfigurationsseite des Geräts zu öffnen. Zeigt die IP-Adresse oder den Hostnamen an, je nach dem was verwendet wird, wenn das Gerät hinzugefügt wird. Siehe *Registerkarte Gerätekonfiguration, on page 72*.
- **Hostname:** Der Hostname des Geräts, falls verfügbar. Klicken Sie auf den Link, um die Konfigurationsseite des Geräts zu öffnen. Der angezeigte Hostname ist der vollständig qualifizierte Domainname. Siehe *Registerkarte Gerätekonfiguration, on page 72*.
- **Hersteller:** Der Hersteller des Geräts.
- **Modell:** Das Gerätemodell.
- **Firmware:** Die Firmwareversion, die das Gerät aktuell verwendet.
- **DHCP:** Gibt an, ob das Gerät mit dem Server über DHCP verbunden ist.
- **HTTPS:** Der HTTPS-Status des Geräts. Finden Sie in den Status HTTPS in *Sicherheit, on page 70*.
- **IEEE 802.1X:** Der IEEE 802.1X-Status des Geräts. Siehe IEEE 802.1X-Status in *Sicherheit, on page 70*.
- **Server:** Der AXIS Camera Station Pro-Server, mit dem das Gerät verbunden ist.
- **Tags:** Die dem Gerät zugeordneten Tags (in der Standardeinstellung ausgeblendet).
- **UPnP-Anzeigename:** Der UPnP-Anzeigename (in der Standardeinstellung ausgeblendet). Ein beschreibender Name zur einfacheren Identifizierung des Geräts.

Folgende Aktionen können auf den Geräten ausgeführt werden:

- Geräten IP-Adresse zuweisen. Siehe *Zuweisen einer IP-Adresse*.
- Ein Kennwort für Geräte festlegen. Siehe *Benutzerverwaltung*.
- Aktualisieren der Firmware für Geräte. Siehe *Aktualisieren der Firmware*.
- Geräte neu starten.
- Geräte wiederherstellen: Setzt die meisten Einstellungen auf die Werkseinstellungen zurück, einschließlich Kennwort. Die folgenden Einstellungen werden nicht zurückgesetzt: hochgeladene Kamera-Anwendungen, Boot-Protokoll (DHCP oder statisch), statische IP-Adresse, Standardrouter, Subnetzmaske, Systemzeit.

Hinweis

- Zum Schutz vor unbefugten Zugriffen wird dringend empfohlen, Geräte nach dem Wiederherstellungsvorgang wieder mit einem Kennwort zu schützen.
- Wenn das Gerät, das Sie zurücksetzen möchten, den Cloud-Speicher verwendet, gehen Sie zu **Cloud storage (Cloud-Speicher)** in My Systems und deaktivieren Sie den Cloud-Speicher für das Gerät, bevor Sie es zurücksetzen. Sobald das Gerät zurückgesetzt wurde, starten Sie den Dienst auf Ihrem AXIS Camera Station ProServer erneut und aktivieren Sie den Cloud-Speicher für das Gerät in My Systems. Siehe *Einschalten des Cloud-Speichers für Ihre einzelnen Kameras*.
- Kamera-Anwendung auf Geräte installieren. Siehe *Kameraanwendung installieren*.
- Geräte erneut laden, nachdem die Einstellungen über die Einstellungsseiten des Geräts geändert wurden.
- Geräte konfigurieren. Siehe *Geräte konfigurieren*.
- Benutzerverwaltung. Siehe *Benutzerverwaltung*.
- Zertifikate verwalten. Siehe *Sicherheit, on page 70*.
- Gerätedaten erfassen. Siehe *Gerätedaten sammeln*.
- Aktivieren Sie dieses Kontrollkästchen, um eine IP-Adresse oder einen Host-Namen zu verwenden. Siehe *Verbindung, on page 71*.
- Geräte mit Tags versehen. Siehe *Tags*.
- Anmeldeinformationen für Gerät eingeben. Das Gerät rechtsklicken und **Erweitert > Anmeldeinformationen für Gerät eingeben** wählen und Kennwort eingeben.
- Auf der Registerkarte Konfiguration des Geräts das Gerät konfigurieren. Siehe *Registerkarte Gerätekonfiguration, on page 72*.

Zuweisen einer IP-Adresse

AXIS Camera Station Pro kann mehreren Geräten eine IP-Adresse zuweisen. Neue IP-Adressen können automatisch von einem DHCP-Server bezogen oder aus einem IP-Adressbereich zugewiesen werden.

IP-Adressen zuweisen

1. Gehen Sie zu **Konfiguration > Geräte > Management**, um die Geräte auswählen, die Sie konfigurieren möchten.
2. Klicken Sie auf oder rechtsklicken und wählen Sie **IP-Adressen zuweisen**.
3. Sollten einige der ausgewählten Geräte nicht konfiguriert werden können, etwa weil kein Zugriff auf sie möglich ist, wird das Dialogfeld „Ungültige Geräte" angezeigt. **Continue (Fortfahren)** anklicken, um die Geräte, die nicht konfiguriert werden können, zu überspringen.
4. Wenn Sie einem Gerät eine IP-Adresse zuweisen, klicken Sie **Erweitert**, um die Seite "IP-Adresse zuweisen" zu öffnen.
5. Wählen Sie **IP-Adresse automatisch beziehen (DHCP)** aus, um automatisch eine IP-Adresse von einem DHCP-Server zu beziehen.

6. **Folgenden IP-Adressbereich zuweisen** wählen, um den ersten verfügbaren IP-Adressbereich, die Subnetzmaske und den Standardrouter festzulegen.
   IP-Bereich festlegen:
   - Platzhalter verwenden. Zum Beispiel: 192.168.0.* oder 10.*.1.*
   - Die erste und die letzten IP-Adresse durch Bindestrich getrennt eingeben. Zum Beispiel: 192.168.0.10-192.168.0.20 (dieser Adressbereich kann gekürzt als 192.168.0.10-20 eingegeben werden) oder 10.10-30.1.101
   - Platzhalter und Bereich kombinieren. Zum Beispiel: 10.10-30.1.*
   - Trennen Sie mehrere Bereiche mithilfe eines Kommas. Zum Beispiel: 192.168.0.*,192.168.1.10-192.168.1.20

Hinweis

Für die Zuweisung eines IP-Adressbereichs müssen die ausgewählten Geräte mit demselben AXIS Camera Station Pro Server verbunden sein.

7. Klicken Sie auf **Next** (Weiter).
8. Die aktuelle IP-Adresse und die neue IP-Adresse überprüfen. Um die IP-Adresse eines Geräts zu ändern, das Gerät wählen und **IP bearbeiten** anklicken.
   - Die aktuelle IP-Adresse, die Subnetzmaske und der Standardrouter werden in dem Bereich "Aktuelle IP-Adresse" angezeigt.
   - Bearbeiten Sie die Optionen im Bereich "Neue IP-Adresse" und klicken Sie auf **OK**.
9. Wenn Sie mit den neuen IP-Adressen zufrieden sind, klicken Sie auf **Fertigstellen**.

Geräte konfigurieren

Durch das Kopieren der Geräteeinstellungen von einem Gerät oder das Übertragen einer Konfigurationsdatei können einige Einstellungen auf mehrere Geräte gleichzeitig konfiguriert werden.

Hinweis

Um alle Einstellungen eines einzelnen Geräts zu konfigurieren gehen Sie auf die Konfigurationsseite des Geräts. Siehe *Registerkarte Gerätekonfiguration, on page 72*.

- Weitere Informationen zum Konfigurieren von Geräten finden Sie unter *Konfigurationsmethoden*.
- Weitere Informationen zum Erstellen einer Konfigurationsdatei finden Sie unter *Konfigurationsdatei erstellen*.
- Weitere Informationen zu den kopierbaren Einstellungen finden Sie unter *Konfigurationseinstellungen*.

Konfigurationsmethoden

Es gibt verschiedene Methoden, Geräte zu konfigurieren. AXIS Device Management versucht, alle Geräte gemäß den in der Methode gewählten Einstellungen zu konfigurieren. Siehe *Geräte konfigurieren*.

Konfiguration des gewählten Gerätes verwenden

Hinweis

Diese Methode ist nur für die Konfiguration eines einzelnen Gerätes gültig.Dabei werden einige oder alle vorhandenen Einstellungen weiterverwendet.

1. **Konfiguration > Geräte > Verwaltung** aufrufen.
2. Auf ein Gerät rechtsklicken und **Geräte konfigurieren > Konfigurieren** wählen.
3. Die zu übernehmenden Einstellungen wählen. Siehe *Konfigurationseinstellungen, on page 66*.
4. **Weiter** anklicken, um die zu übernehmenden Einstellungen zu überprüfen.
5. **Fertigstellen** anklicken, um die ausgewählten Einstellungen für das gewählte Gerät zu übernehmen.

Konfiguration von einem anderen Gerät kopieren

1. **Konfiguration > Geräte > Verwaltung** aufrufen.

2. Geräte rechtsklicken und **Geräte konfigurieren > Konfigurieren** wählen. Es lassen sich Geräte verschiedener Modelle und mit unterschiedlicher Firmware auswählen.
3. **Gerät** anklicken, um Geräte mit verwendbaren Konfigurationen anzuzeigen.
4. Ein Gerät, von dem Einstellungen zu kopieren sind, wählen **OK** anklicken.
5. Die zu übernehmenden Einstellungen wählen. Siehe *Konfigurationseinstellungen, on page 66*.
6. **Weiter** anklicken, um die zu übernehmenden Einstellungen zu überprüfen.
7. **Fertigstellen** anklicken, um die ausgewählten Einstellungen für die Geräte zu übernehmen.

Konfigurationsdatei verwenden

Eine Konfigurationsdatei enthält die für ein Gerät gewählten Einstellungen. Sie kann verwendet werden, um mehrere Geräte gleichzeitig zu konfigurieren und ein Gerät neu zu konfigurieren, z. B. wenn ein Gerät auf die Werkseinstellungen zurück gesetzt wurde. Eine für ein Gerät erstellte Konfigurationsdatei lässt sich auf verschiedene Gerätemodelle und Geräte mit unterschiedlicher Firmware anwenden. Dies trifft auch zu, wenn bestimmte Einstellungsoptionen nicht für alle gewählten Geräte gegeben sind.

Wenn bestimmte Einstellungen nicht vorhanden sind oder sich nicht anwenden lassen, wird der Aufgabenstatus Fehler auf der Registerkarte „Tasks (Aufgaben)" unten im AXIS Camera Station Pro-Client angezeigt. Klicken Sie mit der rechten Maustaste auf die Aufgabe und wählen Sie Anzeigen, um Informationen über die nicht anwendbaren Einstellungen anzeigen zu lassen.

Hinweis

Diese Methode darf nur von erfahrenen Nutzern verwendet werden.

1. **Konfiguration > Geräte > Verwaltung** aufrufen.
2. Geräte rechtsklicken und **Geräte konfigurieren > Konfigurieren** wählen.
3. **Konfigurationsdatei** anklicken, um die Konfigurationsdatei aufzurufen. Wie Sie eine Konfigurationsdatei erstellen, erfahren Sie unter *Konfigurationsdatei erstellen, on page 65*.
4. Suchen Sie die .cfg-Datei und klicken Sie auf **Öffnen**.
5. **Weiter** anklicken, um die zu übernehmenden Einstellungen zu überprüfen.
6. **Fertigstellen** anklicken, um die ausgewählten Einstellungen für die Geräte zu übernehmen.

Konfigurationsdatei erstellen

Eine Konfigurationsdatei enthält die für ein Gerät gewählten Einstellungen. Diese Einstellungen können auch auf andere Geräte angewendet werden. Weitere Informationen zum Verwenden von Konfigurationsdateien finden Sie unter *Konfigurationsmethoden*.

Die angezeigten Geräteeinstellungen werden über AXIS Device Management bearbeitet. Um eine bestimmte Einstellung zu finden, verwenden Sie das Feld **Suchwort eingeben**.

Eine Konfigurationsdatei erstellen:

1. **Konfiguration > Geräte > Verwaltung** aufrufen.
2. Das Gerät wählen, auf dem die Konfigurationsdatei erstellt werden soll.
3. Wählen Sie, nach einem Rechtsklick mit der Maus **Geräte konfigurieren > Konfigurationsdatei erstellen**.
4. Die einzubeziehenden Einstellungen wählen und die Werte nach Erfordernis anpassen. Siehe *Konfigurationseinstellungen*.
5. **Weiter** anklicken, um die Einstellungen zu überprüfen.
6. **Fertigstellen** anklicken, um die Konfigurationsdatei zu erstellen.
7. **Speichern** anklicken, um die gewählten Einstellungen in einer .cfg-Datei zu speichern.

Konfigurationseinstellungen

Wenn Sie Geräte konfigurieren, können Sie die Parameter, Aktionsregeln und zusätzliche Einstellungen der Geräte konfigurieren.

Parameter

Parameter sind interne Geräteparameter, über die das Geräteverhalten gesteuert werden kann. Allgemeine Informationen und Parameter finden Sie in dem Benutzerhandbuch des Produkts unter *www.axis.com*

Hinweis

- Parameter sollten nur von erfahrenen Benutzern angepasst werden.
- Nicht alle Geräteparameter sind über AXIS Device Management zugänglich.

In einige Textfelder können Variablen eingefügt werden. Die Variablen werden vor der Übertragung auf ein Gerät durch Text ersetzt. Um eine Variable einzufügen, das Textfeld rechtklicken und Folgendes wählen:

- **Variable für die Seriennummer des Geräts einfügen:** Diese Variable wird durch die Seriennummer des Geräts ersetzt, auf das die Konfigurationsdatei angewendet wird.
- **Variable für den Gerätenamen einfügen:** Diese Variable wird durch den Namen des Geräts ersetzt, das beim Anwenden der Konfigurationsdatei verwendet wird. Der Gerätename ist auf der Seite Geräteverwaltung in der Spalte "Name" aufgeführt. Um ein Gerät umzubenennen, gehen Sie auf die Seite "Kameras" oder "Andere Geräte".
- **Variable für den Server-Namen einfügen:** Diese Variable wird durch den Namen des Servers ersetzt, der beim Anwenden der Konfigurationsdatei verwendet wird. Der Server-Name ist auf der Seite "Geräteverwaltung" in der Spalte "Server" aufgeführt. Um einen Server umzubenennen, die Dienststeuerung von AXIS Camera Station Pro verwenden.
- **Variable für die Zeitzone des Servers einfügen:** Diese Variable wird durch die POSIX-Zeitzone des Servers ersetzt, der beim Anwenden der Konfigurationsdatei verwendet wird. Diese kann mit dem Parameter POSIX-Zeitzone verwendet werden, um für alle Geräte in einem Netzwerk mit Servern in verschiedenen Zeitzonen die richtige Zeitzone einzustellen.

Aktionsregeln

Aktionsregeln können durch Kopieren auf andere Geräten übertragen werden. Nur erfahrene Benutzer sollten Aktionsregeln bearbeiten. Weitere allgemeine Informationen zu Aktionsregeln finden Sie unter *Aktionsregeln*.

Weitere Einstellungen

- **Streamprofile:** Ein Videostreamprofil ist eine vorprogrammierte Live-Ansichtskonfigurationsprofil für Videoencoding sowie für Bild- und Toneinstellungen. Videostreamprofile können durch Kopieren auf andere Geräte übertragen werden.
- **Bewegungserfassungsfenster:** Bewegungserkennungsfenster werden verwendet, um bestimmte Bereiche im Sichtfeld der Kamera zu definieren. Normalerweise wird ein Alarm ausgelöst, wenn in den bestimmten Bereichen eine Bewegung einsetzt (oder beendet wird). Bewegungserkennungsfenster können durch Kopieren auf andere Geräte übertragen werden.

Benutzerverwaltung

Gehen Sie zu **Konfiguration > Geräte > Verwaltung**, wo Sie die Benutzer der Geräte verwalten können.

Wenn Sie ein Kennwort einstellen oder Benutzer von verschiedenen Geräten entfernen, werden Benutzer, die nicht mehr auf allen Geräten verfügbar sind mit markiert. Jeder Benutzer wird nur einmal in der Liste aufgeführt, auch wenn er auf verschiedenen Geräten mit unterschiedlichen Rollen registriert ist.

Hinweis

Die Konten sind gerätespezifisch und nicht mit den Benutzerkonten von AXIS Camera Station Pro verknüpft.

Kennwort festlegen

Hinweis

- Geräte mit Firmware 5.20 oder neuer unterstützen Kennwörter mit einer Länge von bis zu 64 Zeichen. Geräte mit früheren Firmwareversionen unterstützen Kennwörter mit einer Länge von bis zu 8 Zeichen. Es wird empfohlen, Kennwörter auf Geräten mit älterer Firmware separat festzulegen.
- Beim Festlegen eines Kennworts für mehrere Geräte, die unterschiedliche Kennwortlängen unterstützen, darf das Kennwort nicht länger als die kürzeste unterstützte Länge sein.
- Um unbefugte Zugriffe zu verhindern und die Sicherheit zu erhöhen, wird dringend empfohlen, dass Sie alle zu AXIS Camera Station Pro hinzugefügten Geräte mit Kennwörtern versehen.

Folgende Zeichen können in Kennwörtern verwendet werden:

- Buchstaben A-Z, a-z
- Zahlen 0-9
- Leerzeichen, Komma (,), Punkt (.), Doppelpunkt (:), Semikolon (;)
- !, ", #, $, %, &t, ', (, +, *, -,), /, <, >, =, ?, [, \, ^, -, `, {, |, ~, @,], }

Kennwort für Benutzer auf gewählten Geräten festlegen:

1. Rufen Sie **Configuration > Devices > Management > Manage devices (Konfiguration > Geräte > Verwaltung > Geräte verwalten)** auf.
2. Wählen Sie die Geräte aus und klicken Sie auf . Oder klicken Sie mit der rechten Maustaste auf die Geräte und wählen Sie **User Management > Set password (Geräteverwaltung > Kennwort einstellen)** aus.
3. Wählen Sie einen Benutzer aus.
4. Geben Sie Ihr Kennwort ein oder klicken Sie auf **Generate (Erstellen)**, um ein starkes Kennwort zu erstellen.
5. Klicken Sie auf **OK**.

Benutzer hinzufügen

Lokale Benutzer oder Active-Directory-Benutzer zu AXIS Camera Station Pro hinzufügen:

1. Rufen Sie **Configuration > Devices > Management > Manage devices (Konfiguration > Geräte > Verwaltung > Geräte verwalten)** auf.
2. Klicken Sie mit der rechten Maustaste auf die Geräte und wählen Sie **User Management > Add user (Geräteverwaltung > Benutzer hinzufügen)** aus.
3. Geben Sie einen Benutzernamen und Kennwort ein und bestätigen Sie es. Für eine Liste zulässiger Zeichen, siehe "Kennwort festlegen".
4. Die Benutzerzugriffsrechte aus dem Aufklappmenü aus dem Feld **Rolle**:
   - **Administrator (Administrator):** Uneingeschränkter Zugriff auf das Gerät.
   - **Operator (Bediener):** – Zugriff auf Videostream, Ereignisse und alle Einstellungen mit Ausnahme der Systemoptionen.
   - **Viewer (Betrachter):** Zugriff auf den Videostream.
5. **PTZ-Steuerung aktivieren** - Aktivieren Sie dieses Kontrollkästchen, damit der Benutzer in der Live-Ansicht Schwenken, Neigen und Zoomen kann.
6. Klicken Sie auf **OK**.

Benutzer entfernen

Benutzer von gewählten Geräten entfernen:

1. Rufen Sie **Configuration > Devices > Management > Manage devices (Konfiguration > Geräte > Verwaltung > Geräte verwalten)** auf.

2. Klicken Sie mit der rechten Maustaste auf die Geräte und wählen Sie **User Management > Remove user (Geräteverwaltung > Benutzer entfernen)** aus.
3. Wählen Sie die zu löschenden Benutzer aus dem Aufklappmenü aus dem Feld **Benutzer**.
4. Klicken Sie auf **OK**.

Benutzer anzeigen

Um alle Benutzer der gewählten Geräte und deren Benutzerrechte aufzulisten:

1. Rufen Sie **Configuration > Devices > Management > Manage devices (Konfiguration > Geräte > Verwaltung > Geräte verwalten)** auf.
2. Klicken Sie mit der rechten Maustaste auf die Geräte und wählen Sie **User Management > List users (Geräteverwaltung > Benutzer auflisten)** aus.
3. Verwenden Sie das Feld **Suchwort eingeben**, um bestimmte Benutzer in der Liste zu finden.

Aktualisieren der Firmware

Unter Firmware versteht man jene Software, die die Funktionalität des Axis-Produkts bestimmt. Mit der aktuellen Firmware können Sie sicher sein, dass Ihr Gerät über die neuesten Funktionen und Verbesserungen verfügt.

Neue Firmware kann durch AXIS Camera Station Pro heruntergeladen oder durch eine auf einer Festplatte oder einer Speicherkarte gespeicherte Datei importiert werden. Firmwareversionen, die zum Herunterladen bereitstehen, enthalten nach der Versionsnummer den Zusatz **Herunterladen**. Firmwareversionen, die auf dem lokalen Client bereitstehen, enthalten nach der Versionsnummer den Zusatz **Datei**.

Wenn Sie die Firmware aktualisieren, können Sie den Upgrade-Typ auswählen:

- **Standard:** Aktualisieren Sie auf die ausgewählte Firmware-Version und behalten Sie die vorhandenen Einstellwerte bei.
- **Werkseinstellung:** Aktualisieren Sie auf die ausgewählte Firmware-Version und setzen Sie alle Einstellungen auf die werkseitigen Standardwerte zurück.

Firmware aktualisieren:

1. Gehen Sie zu **Konfiguration > Geräte > Management**, um die Geräte auswählen, die Sie konfigurieren möchten.
2. Klicken Sie oder rechtsklicken und wählen Sie **Firmware aktualisieren**.
3. Sollten einige der ausgewählten Geräte nicht konfiguriert werden können, etwa weil kein Zugriff auf sie möglich ist, wird das Dialogfeld „Ungültige Geräte" angezeigt. **Continue (Fortfahren)** anklicken, um die Geräte, die nicht konfiguriert werden können, zu überspringen.
4. Während der Aktualisierung der Firmware kann nicht auf das Gerät zugriffen werden. Klicken Sie auf **Ja**, um fortzufahren. Wenn Sie dies bestätigt haben und es nicht erneut angezeigt bekommen möchten, wählen Sie **Dieses Dialogfenster nicht erneut anzeigen** und klicken Sie auf **Ja**.
5. Das Dialogfeld Upgrade-Firmware listet das Gerätemodell, die Anzahl der Geräte jedes Modells, die vorhandene Firmware-Version, die verfügbaren Firmware-Versionen zum Upgrade und den Upgrade-Typ auf. Die Geräte in der Liste sind standardmäßig vorausgewählt, wenn neue Firmware-Versionen zum Herunterladen bereitstehen und die aktuelle Firmware-Version ist für jedes Gerät vorausgewählt.

5.1. Um die Liste der zum Herunterladen bereitgestellten Firmware-Versionen zu aktualisieren, die Schaltfläche **Nach Aktualisierungen suchen** anklicken. Um nach einer oder mehreren auf dem lokalen Client gespeicherten Firmwaredateien zu suchen, die Schaltfläche **Durchsuchen** anklicken.

5.2. Wählen Sie die Geräte, die Firmware-Versionen, die Sie aktualisieren möchten, und den Upgrade-Typ.

5.3. Klicken Sie auf **OK**, um das Upgrade der Geräte in der Liste zu starten.

Hinweis

Die Firmware-Updates erfolgen standardmäßig gleichzeitig für alle ausgewählten Geräte. Die Reihenfolge der Aktualisierungen kann geändert werden. Siehe *Einstellungen zum Aktualisieren der Firmware*.

Kameraanwendung installieren

Eine Kamera-Anwendung ist eine Software, die in Netzwerk-Video-Produkte von Axis hochgeladen und dort installiert werden kann. Anwendungen erweitern den Funktionsumfang des Geräts, z. B. Erfassungs-, Erkennungs-, Tracking- und Zählfunktionen.

Manche Anwendungen lassen sich direkt über AXIS Camera Station Pro installieren. Andere Anwendungen müssen zuerst von *www.axis.com/global/en/products/analytics-and-other-applications* oder der Website des Anwendungsanbieters heruntergeladen werden.

Anwendungen lassen sich auf Geräten installieren, die die AXIS Camera Application Platform unterstützen. Manche Anwendungen erfordern außerdem eine bestimmte Firmware-Version oder ein bestimmtes Kameramodell.

Falls für die Anwendung eine Lizenz erforderlich ist, kann die Lizenzschlüsseldatei gleichzeitig mit der Anwendung oder später mit Hilfe der Einrichtungsseiten des Geräts installiert werden.

Um die Lizenzschlüsseldatei zu erhalten, muss der mitgelieferte Lizenzcode der Anwendung unter *www.axis.com/se/sv/products/camera-applications/license-key-registration#/registration* registriert werden.

Sollte sich eine Anwendung nicht installieren lassen, *www.axis.com* aufrufen und prüfen, ob das Gerätemodell und die Firmware-Version die AXIS Camera Application Platform unterstützen.

Verfügbare Kamera-Anwendungen:

AXIS Video Motion Detection 4 – Eine Anwendung, die Objektbewegungen innerhalb eines ausgewählten Bereichs erkennt. Die Anwendung erfordert keine Lizenz und lässt sich auf Kameras mit Firmware 6.50 oder neuer installieren. In den Versionshinweisen des Produkt finden sich Angaben, ob Video Motion Detection 4 unterstützt wird.

AXIS Video Motion Detection 2 – Eine Anwendung, die Objektbewegungen innerhalb eines ausgewählten Bereichs erkennt. Die Anwendung erfordert keine Lizenz und lässt sich auf Kameras mit Firmware 5.60 oder neuer installieren.

AXIS Video Content Stream – Diese Anwendung ermöglicht Axis Kameras das Senden von Daten zur Verfolgung beweglicher Objekte an AXIS Camera Station Pro. Sie kann auf Kameras mit Firmware der Versionen 5.50 bis 9.59 installiert werden. Die Verwendung von AXIS Video Content Stream ist nur in Verbindung mit AXIS Camera Station Pro zulässig.

Andere Anwendungen – Eine Anwendung wählen, die Sie installieren möchten. Bevor Sie mit der Installation beginnen, laden Sie die Anwendung auf Ihren Computer herunter.

Um Kameraanwendungen zu installieren:

1. **Konfiguration > Geräte > Verwaltung** aufrufen.
2. Wählen Sie die Kameras, auf die Sie die Anwendungen installieren möchten. Klicken Sie oder rechtsklicken und **Kamera-Anwendung installieren** wählen.

3. Wählen Sie die Kamera-Anwendung, die Sie auf den Kameras installieren möchten. Wenn Sie andere Anwendungen installieren möchten, klicken Sie auf **Browse** und gehen Sie zur lokalen Anwendungsdatei. Klicken Sie auf **Next** (Weiter).
4. Wenn Sie die Anwendung installiert haben, können Sie **Anwendung überschreiben erlauben**, um die Anwendung erneut zu installieren oder wählen Sie **Anwendungs-Downgrade erlauben**, um eine vorherige Version der Anwendung zu installieren.

Hinweis

Das Rückstufen oder das Überschreiben setzt auf den Geräten die Anwendungseinstellungen zurück.

5. Wenn eine Anwendung eine Lizenz erfordert, erscheint das Dialogfenster "Lizenzen installieren"
   5.1. Um Lizenzen zu installieren, **Ja** klicken und dann **Weiter** anklicken.
   5.2. Klicken Sie auf **Browse**, wählen Sie die Lizenzdatei und klicken dann auf **Weiter**.

Hinweis

Beim Installieren von AXIS Video Motion Detection 2, AXIS Video Motion Detection 4 oder AXIS Video Content Stream wird keine Lizenz erfordert.

6. Prüfen Sie die Informationen und klicken Sie auf **Fertigstellen**. Der Kamerastatus wechselt von `OK` auf `Maintenance` und zurück auf `OK`, wenn die Installation abgeschlossen ist.

Sicherheit

Wenn Sie HTTPS oder IEE 802.1X aktivieren, signiert die Zertifizierungsstelle (CA) von AXIS Camera Station Pro Zertifikate für Clients und Server und verteilt sie automatisch auf Geräte. Die CA ignoriert vorinstallierte Zertifikate. Weitere Informationen zur Konfiguration von Zertifikaten finden Sie unter *Zertifikate, on page 143*.

HTTPS oder IEEE 802.1X-Zertifikate verwalten

Hinweis

Stellen Sie vor der Aktivierung von IEEE 802.1X sicher, dass die Zeit auf den Axis Geräten in AXIS Camera Station Pro synchronisiert ist.

1. **Konfiguration > Geräte > Verwaltung** aufrufen.
2. Rechtsklicken Sie die Geräte:
   - Wählen Sie **Sicherheit > HTTPS > Aktivieren/Aktualisieren**, um HTTPS zu aktivieren oder die HTTPS-Einstellungen für die Geräte zu aktualisieren.
   - Wählen Sie **Sicherheit > IEEE 802.1X > Aktivieren/Aktualisieren**, um IEEE 802.1X zu aktivieren oder die IEEE 802.1X-Einstellungen für die Geräte zu aktualisieren.
   - Wählen Sie **Sicherheit > HTTPS > Deaktivieren**, um HTTPS für Geräte zu deaktivieren.
   - Um IEEE 802.1X für die Geräte zu deaktivieren, wählen Sie **Sicherheit > IEEE 802.1X > Deaktivieren**.
   - Wählen Sie **Zertifikate...**, um eine Übersicht zu erhalten, Zertifikate zu löschen oder detaillierte Informationen zu einem bestimmten Zertifikat zu erhalten.

Hinweis

Wenn das gleiche Zertifikat auf mehreren Geräten installiert ist, wird es nur einmal angezeigt. Durch das Löschen des Zertifikats, wird es von allen Geräten entfernt, auf denen es installiert ist.

Status des HTTPS und IEEE 802.1X

Auf der Seite Geräteverwaltung wird der Status von HTTPS und IEEE 802.1X aufgeführt.

	Status	Beschreibung
HTTPS	Ein	AXIS Camera Station Pro verwendet HTTPS, um eine Verbindung mit dem Gerät herzustellen.
	Aus	AXIS Camera Station Pro verwendet HTTP, um eine Verbindung mit dem Gerät herzustellen.

	Unbekannt	Das Gerät ist nicht erreichbar.
	Nicht unterstützte Firmware	HTTPS wird nicht unterstützt, da die Firmware des Geräts zu alt ist.
	Nicht unterstütztes Gerät	HTTPS wird auf diesem Gerätemodell nicht unterstützt.
IEEE 802.1X	Aktiviert	IEEE 802.1X ist auf dem Gerät aktiv.
	Deaktiviert	IEEE 802.1X ist nicht aktiv, aber bereit, auf dem Gerät aktiviert zu werden.
	Nicht unterstützte Firmware	IEEE 802.1X wird nicht unterstützt, da die Firmware des Geräts zu alt ist.
	Nicht unterstütztes Gerät	IEEE 802.1X wird von diesem Gerätemodell nicht unterstützt.

Gerätedaten sammeln

Diese Option wird in der Regel für die Fehlersuche verwendet. Mit dieser Option eine .zip-Datei mit einem Datensammelbericht für einen bestimmten Speicherort auf den gewählten Geräten erstellen.

Gerätedaten erfassen:

1. **Konfiguration > Geräte > Verwaltung** aufrufen.
2. Die Geräte rechtsklicken und **Gerätedaten erfassen** wählen.
3. In dem Bereich "Datenquelle für ausgewählte Geräte":
   - Klicken Sie **Voreinstellung** und wählen Sie einen aus dem Aufklappmenü der meist genutzten Befehle.

   Hinweis

   Einige Voreinstellungen funktionieren nicht auf allen Geräten. Z. B. funktioniert PTZ-Status nicht auf Audio-Geräten.
   - Klicken Sie **Benutzerdefiniert** und geben Sie den Pfad zur Datensammlung auf den gewählten Servern an.
4. In dem Bereich "Speichern als", geben Sie den Dateinamen und den Speicherort für die .zip-Datei mit der Datensammlung an.
5. Wählen Sie **Ordner automatisch öffnen, wenn fertiggestellt**, um den Ordner automatisch zu öffnen, sobald die Datenerfassung abgeschlossen wurde.
6. Klicken Sie auf **OK**.

Verbindung

Zur Kommunikation mit Geräten unter Verwendung der IP-Adresse oder des Host-Namens:

1. **Konfiguration > Geräte > Verwaltung** aufrufen.
2. Wählen Sie die Geräte aus, klicken Sie mit der rechten Maustaste und wählen Sie **Connection (Verbindung)**.
   - Um eine Verbindung mit den Geräten über die IP-Adresse herzustellen, wählen Sie **Use IP (IP verwenden)**.
   - Um eine Verbindung mit den Geräten über den Host-Namen herzustellen, wählen Sie **Use hostname (Host-Namen verwenden)**.
   - Zum Ändern der Zugangsdaten oder der Adress- und Porteinstellungen wählen Sie **Edit (Bearbeiten)** aus.

Tags

Tags organisieren auf der Seite Geräteverwaltung die Geräte. Ein Gerät kann mehrere Tags besitzen.

Geräte können beispielsweise mit Kameragruppen nach Modell oder Standort versehen werden. Wenn Sie beispielsweise Geräte nach Modell getagged werden, können Sie alle Kameras dieses Modells schnell auffinden und aktualisieren.

Geräte mit einem Tag versehen:

1. **Konfiguration > Geräte > Verwaltung** aufrufen.
2. Ein Gerät rechtsklicken und **Geräte mit Tags versehen** wählen.
3. Wählen Sie **Vorhandene Gruppe verwenden** und wählen Sie eine Gruppe aus oder wählen Sie **Neue Gruppe erstellen** und geben Sie einen Namen für die Gruppe ein.
4. Klicken Sie auf **OK**.

Ein Tag von einem Gerät entfernen:

1. Rufen Sie **Configuration > Devices > Management (Konfiguration > Geräte > Management)** auf und klicken Sie oben rechts auf .
2. Einen Tag im Ordner "Tags" wählen. Es werden alle Geräte mit diesem Tag angezeigt.
3. Wählen Sie die Geräte aus. Rechtsklicken und **Tags von Geräten entfernen** wählen.
4. Klicken Sie auf **OK**.

So verwalten Sie Tags:

1. Rufen Sie **Configuration > Devices > Management (Konfiguration > Geräte > Management)** auf und klicken Sie oben rechts auf .
2. Auf der Seite Gerätetags:
   - Um ein Tag zu erstellen, **Tags** rechtsklicken und **Neues Tag**wählen.
   - Um ein Tag umzubenennen, dieses rechtsklicken und **Tag umbenennen** wählen und einen neuen Namen eingeben.
   - Um ein Tag zu löschen, dieses rechtsklicken und **Löschen** wählen.
   - Um Geräte-Tags an die Seite anzuheften, anklicken.
   - Klicken Sie auf einen Tag, um alle zugehörigen Geräte anzuzeigen. Klicken Sie auf „All devices (Alle Geräte)", um alle Geräte anzuzeigen, die mit AXIS Camera Station Pro verbunden sind.
   - Klicken Sie auf **Warnungen/Fehler**, um Geräte anzuzeigen, die Ihre Aufmerksamkeit erfordern, z. B. Geräte, auf die nicht zugegriffen werden kann.

Registerkarte Gerätekonfiguration

So konfigurieren Sie alle Einstellungen auf einem einzelnen Gerät:

1. **Konfiguration > Geräte > Verwaltung** aufrufen.
2. Klicken Sie auf die Adresse oder den Host-Namen des Geräts, um zur Registerkarte Konfiguration des Geräts zu wechseln.
3. Server-Einstellungen ändern Informationen zur Konfiguration Ihres Geräts finden Sie im Benutzerhandbuch des Geräts.
4. Schließen Sie die Registerkarte und das Gerät wird neu geladen, um sicherzustellen, dass die Änderungen in AXIS Camera Station Pro implementiert werden.

Einschränkungen

- Die automatische Authentifizierung für Geräte von Drittanbietern wird nicht unterstützt.

- Die allgemeine Unterstützung für Geräte von Drittanbietern kann nicht garantiert werden.
- Die Registerkarte Gerätekonfiguration mit aktiven Videostreams erhöht die Last und kann sich auf die Leistung auf dem Server-Computer auswirken.

Externe Datenquellen

Eine externe Datenquelle ist ein System oder eine Quelle, die Daten erzeugt, mit denen nachverfolgt werden kann, was zum Zeitpunkt eines jeden Ereignisses passiert ist. Siehe *Datensuche, on page 43*.

Rufen Sie **Configuration > Devices > External data sources (Konfiguration > Geräte > Externe Datenquellen)** auf, um eine Liste aller externen Datenquellen anzuzeigen. Klicken Sie auf eine Spaltenüberschrift, um nach dem Inhalt der Spalte zu sortieren.

Komponente	Beschreibung
Bezeichnung	Der Name der externen Datenquelle.
Quellenschlüssel	Der eindeutige Bezeichner der externen Datenquelle.
Ansehen	Die Ansicht, mit der die externe Datenquelle verknüpft ist.
Server	Der Server, mit dem die Datenquelle verbunden ist. Nur verfügbar, wenn mehrere Server verbunden werden.

Eine externe Datenquelle wird automatisch hinzugefügt, wenn

- Rufen Sie **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugänge und Zonen)** auf und fügen Sie einen Zugang hinzu.
  Die vollständige Vorgehensweise zum Einrichten eines Axis Network Door Controller in AXIS Camera Station Pro finden Sie unter *Einrichten eines Axis Network Door Controllers*.
- Das erste Ereignis wird von dem Gerät empfangen, das mit dem AXIS License Plate Verifier.
  Für einen vollständigen Workflow zum Einrichten von AXIS License Plate Verifier in AXIS Camera Station Pro, siehe *Set up AXIS License Plate Verifier (Einrichten von AXIS License Plate Verifier)*.

Wenn ein Zugang mit einer Ansicht konfiguriert wurde, werden die vom Zugang erzeugten Daten in der Zeitachse der Ansicht auf der Registerkarte zur Datensuche automatisch mit Lesezeichen versehen. So verbinden Sie einen Zugang mit einer Ansicht:

1. Rufen Sie **Configuration > Devices > External data sources (Konfiguration > Geräte > Externen Datenquellen)** auf.
2. Wählen Sie einen Zugang als Datenquelle aus und klicken Sie auf **Edit (Bearbeiten)**.
3. Wählen Sie eine Ansicht aus dem Aufklappmenü **View (Ansicht)** aus.
4. Klicken Sie auf **OK**.

Zeitsynchronisierung

Gehen Sie auf **Configuration > Devices > Time synchronization**, um die Zeitsynchronisation zu öffnen.

Eine Liste aller Geräte, die zu AXIS Camera Station Pro hinzugefügt wurden, wird angezeigt. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie die Spalten aus, die angezeigt werden sollen. Ziehen Sie an den Spaltenköpfen, um die Spalten in einer anderen Reihenfolge anzuordnen.

Die folgenden Informationen wird in der Geräteliste angezeigt:

- **Vor- und Nachname:** Wenn das Gerät ein Video-Encoder mit mehreren angeschlossenen Kameras oder eine Netzwerk-Kamera mit mehreren Ansichtsbereichen ist, wird der Gerätename oder eine Liste aller zugeordneten Kameranamen angezeigt.

- **Adresse:** Die Adresse des Geräts. Klicken Sie auf den Link, um die Konfigurationsseite des Geräts zu öffnen. Zeigt die IP-Adresse oder den Hostnamen an, je nach dem was verwendet wird, wenn das Gerät hinzugefügt wird. Siehe *Registerkarte Gerätekonfiguration, on page 72*.
- **MAC-Adresse:** Die MAC-Adresse des Geräts.
- **Modell:** Das Gerätemodell.
- **Aktiviert:** Zeigt an, ob die Zeitsynchronisierung aktiviert ist.
- **NTP-Quelle:** Die für das Gerät konfigurierte NTP-Quelle.
  - **Statisch:** Die NTP-Server des Geräts werden manuell unter **Primärer NTP-Server** und **Sekundärer NTP-Server** angegeben.
  - **DHCP:** Das Gerät empfängt den NTP-Server dynamisch vom Netzwerk. **Primärer NTP-Server** und **Sekundärer NTP-Server** sind nicht verfügbar, wenn **DHCP** ausgewählt ist.
- **Primärer NTP-Server:** Der primäre NTP-Server, der für das Gerät konfiguriert ist. Nur verfügbar, wenn **Statisch** ausgewählt ist.
- **Sekundärer NTP-Server:** Der sekundäre NTP-Server, der für das Gerät konfiguriert ist. Nur verfügbar für AXIS Geräte, die sekundäres NTP unterstützen und wenn **Statisch** ausgewählt ist.
- **Zeitversatz beim Server:** Der Zeitunterschied zwischen Gerät und Server.
- **UTC-Zeit:** Die koordinierte Weltzeit (UTC) auf dem Gerät.
- **Synchronisiert:** Zeigt an, ob die Zeitsynchronisierungseinstellungen tatsächlich angewendet werden. Dies ist nur für Geräte mit Firmware 9.1 oder höher möglich.
- **Dauer bis zur nächsten Synchronisierung:** Die verbleibende Zeit bis zur nächsten Synchronisierung.

Der Windows Time-Dienst (W32Time) verwendet NTP (Network Time Protocol), um Datum und Uhrzeit für AXIS Camera Station Pro Server zu synchronisieren. Die folgenden Informationen werden angezeigt:

- **Server:** Der AXIS Camera Station Pro Server, auf dem der Windows Time-Dienst ausgeführt wird.
- **Status:** Der Status des Windows Time-Dienstes. Entweder `Running` oder `Stopped`.
- **NTP-Server:** Der NTP-Server, der für den Windows Time-Dienst konfiguriert ist.

Zeitsynchronisierung konfigurieren

1. Gehen Sie zu **Configuration > Devices > Time synchronization (Konfiguration > Geräte > Zeitsynchronisierung)**.
2. Wählen Sie Ihre Geräte und aktivieren Sie **Zeitsynchronisierung aktivieren**.
3. Wählen Sie die NTP-Quelle **Statisch** oder **DHCP** aus.
4. Wenn Sie **Statisch** ausgewählt haben, konfigurieren Sie den primären und sekundären NTP-Server.
5. Klicken Sie auf **Anwenden**.

Bei einer Zeitdifferenz zwischen Server und Gerät über 2 Sekunden Alarm senden	Mit dieser Option ergeht ein Alarm, wenn die Zeitdifferenz zwischen Server und Gerät mehr als 2 Sekunden beträgt.
Zeitzone manuell über die Schnittstelle des Geräts einstellen	Mit dieser Option wird nicht die Zeitzone des Servers, sondern die am Standort des Geräts geltende Zeitzone verwendet. Mit dieser Option müssen Sie die Zeitzone manuell über die Weboberfläche des Geräts einstellen.

Speicher konfigurieren

Gehen Sie zu **Konfiguration > Speicher > Management**, um die Speicherverwaltungsseite zu öffnen. Auf der Seite „Manage storage (Speicher verwalten)" wird eine Übersicht des lokalen Speichers und des Netzwerk-Speichers angezeigt, der in AXIS Camera Station Pro existiert.

Liste	
Standort	Pfad und Name des Speichers.
Zugewiesen:	Die maximale Menge an Speicherplatz, die den Aufzeichnungen zugewiesen wird.
Used (Verwendet)	Der von Aufzeichnungen derzeit belegte Speicherplatz.

Liste	
Status	Der Speicherstatus. Mögliche Werte sind: • **OK** • **Speicher voll:** Der Speicher ist voll. Das System überschreibt die ältesten freigegebenen Aufzeichnungen. • **Nicht verfügbar:** Die Speicherinformationen sind zurzeit nicht verfügbar. Dies kann der Fall sein, wenn ein Netzwerk-Speicher entfernt oder getrennt wurde. • **Eindringende Daten:** Daten anderer Anwendungen belegen Speicherplatz, der AXIS Camera Station Pro zugeordnet ist. Oder es sind Aufzeichnungen ohne Datenbankverbindung vorhanden, sogenannte nicht indizierte Aufzeichnungen, die den Speicherplatz belegen, der AXIS Camera Station Pro zugeordnet ist. • **Keine Berechtigungen:** Der Benutzer hat keine Lese- oder Schreibberechtigung für den Speicher. • **Wenig freier Speicherplatz:** Auf dem Laufwerk sind weniger als 15 GB Speicherplatz frei, was AXIS Camera Station Pro als zu wenig erachtet. Um Fehler oder Beschädigungen zu vermeiden, führt AXIS Camera Station Pro zum Schutz des Laufwerks unabhängig vom Platzieren des Speicherschiebers eine erzwungene Bereinigung durch. Während der erzwungenen Bereinigung verhindert AXIS Camera Station Pro das Durchführen von Aufzeichnungen, bis mehr als 15 GB Speicherplatz verfügbar sind. • **Unzureichende Kapazität**: Die Festplattengröße beträgt insgesamt weniger als 32 GB, was für AXIS Camera Station Pro nicht ausreicht. AXIS OS Recorder, die RAID unterstützen, können auch folgende Status aufweisen: • **Online** Das RAID-System funktioniert ordnungsgemäß. Wenn eine der physischen Festplatten des RAID-Systems ausfällt, ist Redundanz vorhanden. • **Verringert:** Eine der physischen Festplatten des RAID-Systems ist defekt. Das Aufzeichnen sowie die Wiedergabe von gespeicherten Aufzeichnungen sind weiterhin möglich. Es ist jedoch keine Redundanz vorhanden. Wenn eine weitere physische Festplatte ausfällt, ändert sich der RAID-Status zu **Failure (Fehler)**. Wir empfehlen, die defekte physische Festplatte so schnell wie möglich zu ersetzen. Nach dem Ersetzen einer defekten Festplatte ändert sich der RAID-Status von **Degraded (Verringert)** zu **Syncing (Synchronisierung)**. • **Synchronisierung:** Die RAID-Festplatten werden synchronisiert. Das Aufzeichnen sowie die Wiedergabe von gespeicherten Aufzeichnungen sind weiterhin möglich. Es ist jedoch keine Redundanz vorhanden, wenn eine der physischen Festplatten ausfällt. Nach der Synchronisierung der physischen Festplatten ist im RAID-System Redundanz vorhanden und der RAID-Status ändert sich zu **Online**. Wichtig Vermeiden Sie es, während der Synchronisierung eine RAID-Festplatte zu entfernen. Dies kann einen Festplattenausfall zur Folge haben. • **Fehler:** Mehrere physische Festplatten im RAID-System sind ausgefallen. In diesem Fall gehen alle Aufzeichnungen im Speicher

Liste	
	verloren. Neue Aufzeichnungen sind erst nach dem Ersetzen der beschädigten physischen Festplatten möglich.
Server	Der Server, auf dem der lokale Speicher oder der Netzwerk-Speicher angelegt ist.

Übersicht	
Used (Verwendet)	Derzeit für Aufzeichnungen verwendeter Speicherplatz. Nicht in der Datenbank indizierte Dateien im Aufzeichnungsverzeichnis fallen in die Kategorie **Other data (Andere Daten)**. Zum Erfassen nicht indizierte Dateien, siehe *Speicher verwalten, on page 77*.
Frei	Verbleibender freier Speicherplatz des Speicherorts. Diese Wert entspricht dem in Windows unter den Eigenschaften des Speicherorts als frei angezeigten Wert.
Andere Daten	Von nicht indizierten Aufzeichnungen belegter Speicherplatz, der deshalb AXIS Camera Station Pro nicht bekannt ist. Andere Daten: Gesamtspeicher minus belegter Speicher minus freier Speicher
Gesamtkapazität	Die Gesamtgröße des Speicherplatzes. Diese Wert entspricht dem in Windows unter den Eigenschaften des Speicherorts als Gesamtspeicher angezeigten Wert.
Zugewiesen:	Der Speicherplatz, der für AXIS Camera Station Pro Aufzeichnungen verwendet werden kann. Um die Größe des zugewiesenen Speicherplatzes verändern, den Schieberegler entsprechend verschieben und **Apply (Anwenden)** anklicken.

Netzwerk-Speicher	
Pfad:	Der Pfad der Netzwerk-Freigabe.
Benutzername	Der für die Verbindung zur Netzwerk-Freigabe verwendete Benutzername.
Kennwort	Das für die Verbindung zur Netzwerk-Freigabe verwendete Benutzerkennwort.

Speicher verwalten

Gehen Sie zu **Konfiguration > Speicher > Management**, um die Speicherverwaltungsseite zu öffnen. Auf dieser Seite können Sie den Ordner für gespeicherte Aufzeichnungen festlegen. Es sollte ein Maximalwert für den von AXIS Camera Station Pro verwendeten Speicher festgelegt werden, um zu verhindern, dass der Speicher komplett beschrieben wird. Sie können zusätzliche lokale Speicher und Netzwerklaufwerke hinzufügen. Dadurch erhalten Sie mehr Sicherheit und Speicherplatz.

Hinweis

- Bei einer Verbindung zu mehreren AXIS Camera Station Pro-Servern wählen Sie zur Verwaltung des Speichers einen beliebigen Server aus dem Dropdown-Menü **Selected server (Ausgewählter Server)** aus.
- Wenn der Dienst zur Anmeldung das Systemkonto verwendet, ist es nicht möglich, Netzwerklaufwerke hinzuzufügen, die auf gemeinsam genutzte Ordner auf anderen Computern verweisen. Siehe *Zugriff auf Netzwerk-Speicher nicht möglich*.
- Sie können den lokalen Speicher oder den Netzwerk-Speicher nicht entfernen, wenn Kameras für das Aufzeichnen auf dieses Speichermedium festgelegt wurden.

Einen lokalen Speicher oder ein freigegebenes Netzwerklaufwerk hinzufügen

1. **Konfiguration > Speicher > Verwaltung** aufrufen.
2. Klicken Sie auf **Hinzufügen**.
3. Um einen lokalen Speicher hinzuzufügen, wählen Sie zunächst **Local storage (Lokaler Speicher)** und anschließend einen Speicher aus dem Drop-Down Menü aus.
4. Um ein freigegebenes Netzwerklaufwerk hinzuzufügen, wählen Sie **freigegebenes Netzwerklaufwerk** und geben den Pfad für das freigegebene Netzwerklaufwerk ein. Zum Beispiel: \\ip_address\share.
5. Klicken Sie auf **OK** und geben Sie den Benutzernamen und das Kennwort des freigegebenen Netzwerklaufwerks ein.
6. Klicken Sie auf **OK**.

Einen lokalen Speicher oder ein freigegebenes Netzwerklaufwerk entfernen

Um einen lokalen Speicher oder ein freigegebenes Netzwerklaufwerk zu entfernen, wählen Sie einen lokalen Speicher oder ein freigegebenes Netzwerklaufwerk aus der Speicherliste und klicken Sie auf **Entfernen**.

Aufzeichnungen in einen neuen Ordner verschieben

1. **Konfiguration > Speicher > Verwaltung** aufrufen.
2. Wählen Sie aus der Speicherliste einen lokalen Speicher oder ein freigegebenes Netzwerklaufwerk aus.
3. Geben Sie unter **Overview (Übersicht)** in das Feld **Move recordings to a new folder (Aufzeichnungen in einen neuen Ordner verschieben)** einen Ordnernamen ein, um den Speicherort für Aufzeichnungen zu ändern. Mit dieser Aktion werden auch vorhandene Aufzeichnungen aus dem bisherigen Ordner in den neuen Ordner verschoben.
4. Klicken Sie auf **Anwenden**.

Passen Sie die Speicherkapazität an

1. **Konfiguration > Speicher > Verwaltung** aufrufen.
2. Wählen Sie aus der Speicherliste einen lokalen Speicher oder ein freigegebenes Netzwerklaufwerk aus.
3. Verwenden Sie unter **Overview (Übersicht)** den Schieber, um den maximalen, von AXIS Camera Station Pro zu verwendenden Speicherplatz festzulegen.
4. Klicken Sie auf **Anwenden**.

Hinweis

- Für eine optimale Leistung empfehlen wir, mindestens 5 % des Speicherplatzes frei zu lassen.
- Die Mindestgröße für den Speicher, der zu AXIS Camera Station Pro hinzugefügt wird, beträgt mindestens 32 GB, wobei mindestens 15 GB freier Speicherplatz zur Verfügung stehen müssen.
- Wenn weniger als 15 GB freier Speicherplatz verfügbar sind, beginnt AXIS Camera Station Pro automatisch, alte Aufzeichnungen zu löschen, um freien Speicherplatz zu schaffen.

Nicht indizierte Dateien erfassen

Nicht indizierte Dateien können einen beträchtlichen Teil von **Other data (Andere Daten)** im Speicher einnehmen. Bei einer nicht indizierten Datei handelt es sich um Daten im Aufzeichnungsordner, die nicht zur aktuellen Datenbank gehören. Die Datei kann Aufzeichnungen von vorherigen Installationen oder verloren gegangene Daten enthalten, wenn ein Wiederherstellungspunkt verwendet wurde.

Die gesammelten Dateien werden vom System nicht gelöscht, sondern erfasst und im Ordner **Non-indexed files (Nicht indizierte Daten)** im Aufzeichnungsspeicher abgelegt. Dieser Speicher kann sich je nach Ihrer Konfiguration auf demselben Computer wie der Client oder auf einem Remote-Server befinden. Um auf den Ordner **Non-indexed files (Nicht indizierte Dateien)** zuzugreifen, benötigen Sie Zugriff auf den Server. AXIS Camera Station Pro platziert die Daten in den Ordnern nach der Reihenfolge, in der sie gefunden wurden, zuerst durch den Server und dann die mit diesem bestimmten Server verbundenen Geräte.

Sie können entweder nach einer bestimmten Aufzeichnung bzw. einem verloren gegangenen Protokoll suchen oder einfach den Inhalt löschen, um Speicherplatz freizugeben.

Erfassung nicht indizierter Dateien zur Überprüfung oder Entfernung:

1. **Konfiguration > Speicher > Verwaltung** aufrufen.
2. Wählen Sie aus der Speicherliste einen lokalen Speicher oder ein freigegebenes Netzwerklaufwerk aus.
3. Klicken Sie unter **Collect non-indexed files (Nicht indizierte Dateien erfassen)** auf **Collect (Erfassen)**, um eine Aufgabe zu starten.
4. Rufen Sie nach Abschluss der Aufgabe **Alarms and Tasks > Tasks (Alarme und Aufgaben)** auf und doppelklicken Sie auf die Aufgabe, um das Ergebnis anzuzeigen.

Das anzuschließende Geräte wählen

Hinweis

Die Aufzeichnungen werden als .acsm-Dateien gespeichert und müssen konvertiert werden, bevor Sie sie abspielen können. Wenden Sie sich an den technischen Support von Axis, wenn Sie Hilfe bei der Konvertierung Ihrer Dateien benötigen.

Gehen Sie zu **Konfiguration > Speicher > Auswahl**, um die Speicherverwaltungsseite zu wählen. Auf dieser Seite finden Sie eine Liste mit allen Kameras in AXIS Camera Station Pro und Sie können angeben, wie viele Tage lang die Aufzeichnungen für bestimmte Kameras gespeichert werden sollen. Wenn angewählt, wird die Speicherinformation unter Aufzeichnungsspeicher angezeigt. Sie können mehrere Kameras gleichzeitig konfigurieren.

Bezeichnung	Wenn das Gerät ein Video-Encoder mit mehreren angeschlossenen Kameras oder eine Netzwerk-Kamera mit mehreren Ansichtsbereichen ist, wird der Gerätename oder eine Liste aller zugeordneten Kameranamen angezeigt.
Adresse	Die Adresse des Geräts. Klicken Sie auf den Link, um die Konfigurationsseite des Geräts zu öffnen. Zeigt die IP-Adresse oder den Host-Namen an, je nachdem, was Sie beim Hinzufügen des Geräts verwendet haben. Siehe *Registerkarte Gerätekonfiguration, on page 72*.
MAC-Adresse	Die MAC-Adresse des Geräts.
Hersteller	Der Hersteller des Geräts.
Modell	Das Gerätemodell.
Verwendeter Speicher	Der von Aufzeichnungen derzeit belegte Speicherplatz.
Standort	Pfad und Name des Speichers.
Aufbewahrungszeit	Die für die Kamera konfigurierte Vorhaltezeit.
Älteste Aufzeichnung	Der Zeitpunkt der ältesten Aufzeichnung der Kamera, die im Speicher aufbewahrt wird.
Failover-Aufzeichnung	Zeigt an, ob die Kamera eine ausfallsichere Aufzeichnung verwendet.
Ausweichoption-Aufzeichnung	Zeigt an, ob die Kamera eine Fallback-Aufzeichnung verwendet.
Server	Der Server, auf dem der lokale Speicher oder der Netzwerk-Speicher angelegt ist.

Sobald Kameras zu AXIS Camera Station Pro hinzugefügt werden, wird der entsprechende Aufzeichnungsspeicher konfiguriert. Um die Speichereinstellungen einer Kamera zu bearbeiten:

1. **Konfiguration > Speicher > Auswahl** aufrufen.
2. Wählen Sie die Kamera aus, deren Speichereinstellungen Sie bearbeiten möchten.
3. Legen Sie unter **Recording storage (Aufzeichnungsspeicher)** den Speicherort und die Vorhaltezeit fest.
4. Klicken Sie auf **Anwenden**.

Aufzeichnungsspeicher	
Store to (Speichern auf)	Wählen Sie aus dem Drop-down-Menü den Speicher aus, auf dem die Aufzeichnungen gespeichert werden sollen. Verfügbare Optionen sind der lokale Speicher und Netzwerk-Freigaben.
Failover-Aufzeichnung	Um die Aufzeichnungen auf der SD-Speicherkarte der Kamera zu speichern, wenn die Verbindung zwischen AXIS Camera Station Pro und der Kamera während des Aufzeichnens unterbrochen wird, wählen Sie diese Option aus. Bei Wiederherstellung der Verbindung werden die ausfallsicheren Aufzeichnungen an AXIS Camera Station Pro übermittelt. Hinweis Diese Funktion ist nur für Kameras mit SD-Speicherkarte und Firmware 5.20 oder höher verfügbar.
Unbegrenzt	Wählen Sie die Vorhaltezeit für die Aufzeichnungen aus, bis der Speicher voll ist.
Begrenzt	Wählen Sie die maximale Anzahl an Tagen aus, für die Aufzeichnungen aufbewahrt werden sollen. Hinweis Wenn der für AXIS Camera Station Pro reservierte Speicherplatz nicht ausreicht, werden Aufzeichnungen ggf. noch vor Ablauf der angegebenen Aufbewahrungsfrist gelöscht.
Maximum days to keep recordings (Max. Aufbewahrungszeit der Aufzeichnungen in Tagen)	Die Aufbewahrungszeit für Ihre Aufzeichnungen in Tagen eingeben.

Aufzeichnung und Ereignisse konfigurieren

AXIS Camera Station Pro konfiguriert beim Hinzufügen von Kameras automatisch die Bewegungs- oder Daueraufzeichnung. Sie können die Aufzeichnungsart später an Ihre Bedürfnisse anpassen, siehe *Aufzeichnungsmethode, on page 86*.

Bewegungsaufzeichnung

Die Bewegungserkennung kann zusammen mit allen Axis Netzwerk-Kameras und Video-Encodern verwendet werden. Nur bei durch eine Kamera erfasster Bewegung aufzuzeichnen spart im Vergleich zur kontinuierlichen Aufzeichnung sehr viel Speicherplatz. Die Bewegungsaufzeichnung kann unter **Recording method (Aufzeichnungsart)** eingeschaltet und unter **Motion detection (Bewegungserkennung)** konfiguriert werden. Sie können beispielsweise die Einstellungen konfigurieren, wenn die Kamera zu viele oder wenige bewegte Objekte erkennt oder wenn die Größe der aufgenommenen Dateien zu groß für den verfügbaren Speicherplatz ist.

Konfigurieren der Einstellungen für die Bewegungsaufzeichnung:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode** aufrufen.
2. Eine Kamera wählen
3. Aktivieren Sie das Kontrollkästchen **Motion detection (Bewegungserkennung)**.
4. Klicken Sie auf **Motion settings (Bewegungseinstellungen)**, um die Bewegungserkennungseinstellungen zu konfigurieren, z. B. die Anzahl der erkennbaren Objekte. Die verfügbaren Einstellungen sind für

verschiedene Kameras unterschiedlich, siehe *Die integrierte Bewegungserkennung bearbeiten* und *Bearbeiten von AXIS Video Motion Detection 2 und 4*.

5. Wählen Sie ein **Profile (Profil)** im Drop-Down Menü, **High (Hoch)**-Profil ist Standard.
6. Wählen Sie einen Zeitplan oder klicken Sie auf **New schedule... (Neuer Zeitplan...)**, um einen neuen benutzerdefinierten Zeitplan zu erstellen.
7. Legen Sie die Zeiteinstellungen für den Vor- und Nachpuffer sowie die Auslösedauer fest.
8. Klicken Sie auf **Anwenden**.

Hinweis

Die Bewegungsaufzeichnung kann über Aktionsregeln konfiguriert werden. Stellen Sie sicher, dass Sie **Motion detection (Bewegungserkennung)** in **Recording method (Aufnahmemethode)** deaktivieren, bevor Sie Aktionsregeln verwenden.

Profil	Verwenden Sie eine niedrigere Auflösung, um die Aufzeichnungsgröße zu verringern. Hier können Sie die Kameraeinstellungen bearbeiten: *Videostromprofile*.
Zeitschema	Der Zeitplan für die Aufzeichnungen. Um die Belastung Ihres Speicherplatzes zu verringern, zeichnen Sie nur in bestimmten Zeiträumen auf.
Ereigniskategorie	Die gewünschte Ereigniskategorie, der die Aufzeichnung gegebenenfalls zugeordnet werden soll.
Vorpuffer:	Die Zeit in Sekunden vor der erkannten Bewegung, die in eine Aufnahme einbezogen werden sollen.
Nachpuffer:	Die Zeit in Sekunden nach der erkannten Bewegung, die in eine Aufnahme einbezogen werden sollen.
Trigger period (Auslösedauer)	Das Intervall zwischen zwei aufeinanderfolgenden Auslösern zur Reduzierung der Anzahl aufeinanderfolgender Aufzeichnungen. Tritt innerhalb dieses Intervalls ein weiterer Auslöser ein, wird die Aufzeichnung fortgesetzt und der Auslösezeitraum neu gestartet.
Alarm auslösen	Löst einen Alarm aus, wenn die Kamera eine Bewegung detektiert.

Konfigurieren der Bewegungserkennung

Objekterkennung

Die Aufzeichnung bei Objekterfassung zeichnet Videodaten auf, wenn AXIS Object Analytics Objekttypen wie Personen und Fahrzeuge detektiert und klassifiziert. Es wird empfohlen, diese Funktion in Verbindung mit der Bewegungserkennung oder der kontinuierlichen Aufzeichnung zu verwenden, um sicherzustellen, dass alle Ereignisse erfasst werden. AXIS Object Analytics unterstützt bis zu 10 Szenarien pro Kamera.

Hinweis

Zur Unterstützung dieser Funktion muss Ihre Kamera mit Firmware-Version 12.4.26 oder höher, einem Einzelsensor und AXIS Object Analytics ACAP ausgestattet sein.

Zur Nutzung der Objekterkennung:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode** aufrufen.
2. Eine Kamera wählen
3. Aktivieren Sie das Kontrollkästchen **Object detection (Objekterkennung)**.
4. Nehmen Sie Ihre Einstellungen vor. Weitere Informationen finden Sie in der Tabelle unten.
5. Klicken Sie auf **Anwenden**.

- Objekterkennungsereignisse erscheinen in der Zeitleiste in Rosa.

Object detection settings... (Einstellungen für Objekterfassung...)	Klicken Sie auf diese Option, um die AXIS Object Analytics-Weboberfläche zu öffnen und die gewünschten Objekttypen (Personen, Fahrzeuge) als Auslöser für Aufzeichnungen, die Mindestgröße der Objekte, die Erkennungsbereiche und die Einstellungen für die Verweildauer im Bereich festzulegen.
Profil	Wählen Sie im Auswahlmenü unter **Profile (Profil)** ein Profil. Standardmäßig ist das Profil **High (Hoch)** ausgewählt. Verwenden Sie eine niedrigere Auflösung, um die Aufzeichnungsgröße zu verringern. Hier können Sie die Kameraeinstellungen bearbeiten: *Videostromprofile*.
Zeitschema	Legen Sie den Zeitplan für die Aufzeichnungen fest. Um die Belastung Ihres Speicherplatzes zu verringern, zeichnen Sie nur in bestimmten Zeiträumen auf.
Ereigniskategorie	Wählen Sie die Ereigniskategorie aus, der die Aufzeichnung gegebenenfalls zugeordnet werden soll. Weitere Informationen finden Sie unter *Ereigniskategorien, on page 27*.
Vorpuffer:	Legen Sie die Anzahl der Sekunden vor der Erkennung des Objekts fest, die in eine Aufnahme einbezogen werden sollen.
Nachpuffer:	Legen Sie die Anzahl der Sekunden nach der Erkennung des Objekts fest, die in eine Aufnahme einbezogen werden sollen.
Trigger period (Auslösedauer)	Stellen Sie ein Intervall zwischen zwei aufeinanderfolgenden Auslösern ein, um die Anzahl aufeinanderfolgender Aufzeichnungen zu verringern. Tritt innerhalb dieses Intervalls ein weiterer Auslöser ein, wird die Aufzeichnung fortgesetzt und der Auslösezeitraum neu gestartet.
Alarm auslösen	Wählen Sie diese Option aus, um bei der Erkennung eines Objekts durch AXIS Object Analytics einen Alarm auszulösen.

Kontinuierliche und geplante Aufzeichnung

Bei der kontinuierlichen Aufnahme werden Bilder fortlaufend gespeichert und benötigen mehr Speicherplatz als bei anderen Aufnahmeoptionen. Um die Dateigröße zu reduzieren, sollten Sie eine Aufzeichnung mit Bewegungserkennung erwägen.

Um kontinuierlich aufzuzeichnen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode** aufrufen.
2. Eine Kamera wählen
3. Aktivieren Sie das Kontrollkästchen **Continuous (Kontinuierlich)**, um kontinuierlich aufzuzeichnen.
4. Nehmen Sie Ihre Einstellungen vor. Weitere Informationen finden Sie in der Tabelle unten.
5. Klicken Sie auf **Anwenden**.

Profil	Wählen Sie im Auswahlmenü unter **Profile (Profil)** ein Profil. Standardmäßig ist das Profil **High (Hoch)** ausgewählt. Verwenden Sie eine niedrigere Auflösung, um die Aufzeichnungsgröße zu verringern. Hier können Sie die Kameraeinstellungen bearbeiten: *Videostromprofile*.
Zeitschema	Legen Sie den Zeitplan für die Aufzeichnungen fest. Um die Belastung Ihres Speicherplatzes zu verringern, zeichnen Sie nur in bestimmten Zeiträumen auf.
Durchschnittliche Bitrate	Aktivieren Sie diese Option und legen Sie den maximalen Speicherplatz fest. Die angezeigte geschätzte durchschnittliche Bitrate wird vom System auf Grundlage des angegebenen maximalen Speicherplatzes und der Vorhaltezeit berechnet. Die maximale durchschnittliche Bitrate beträgt 50000 KBit/s (siehe *Durchschnittliche Bitrate einstellen, on page 86*).

Manuelle Aufzeichnung

Weitere Informationen zur manuellen Aufnahme finden Sie unter *Manuell aufzeichnen*.

So konfigurieren Sie die Einstellungen der manuellen Aufzeichnung:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode** aufrufen.
2. Eine Kamera wählen
3. Aktivieren Sie das Kontrollkästchen **Manual (Manuell)**.
4. Nehmen Sie Ihre Einstellungen vor. Weitere Informationen finden Sie in der Tabelle unten.
5. Klicken Sie auf **Anwenden**.

Profil	Wählen Sie ein **Profile (Profil)** im Drop-Down Menü, **High (Hoch)**-Profil ist Standard. Verwenden Sie eine niedrigere Auflösung, um die Aufzeichnungsgröße zu verringern. Hier können Sie die Kameraeinstellungen bearbeiten: *Videostromprofile*.
Ereigniskategorie	Wählen Sie die Ereigniskategorie aus, der die Aufzeichnung gegebenenfalls zugeordnet werden soll.

Vorpuffer:	Legen Sie die Zeit in Sekunden fest, die vor dem Auslösen der Aufnahme in die Aufzeichnung einbezogen werden sollen.
Nachpuffer:	Legen Sie die Zeit in Sekunden fest, die nach dem Beenden der Aufnahme in die Aufzeichnung einbezogen werden sollen.
Bookmark when recording (Lesezeichen bei Aufzeichnung)	Aktivieren Sie diese Option, wenn bei jedem Start einer manuellen Aufzeichnung Details zu dieser als Lesezeichen eingefügt werden sollen. Lesezeichen helfen Ihnen dabei, bestimmte Aufzeichnungen später leichter wiederzufinden und zu identifizieren. Diese Einstellung gilt nur für Bediener und Administratoren und ist standardmäßig deaktiviert.
Dauer maximal	Legen Sie die maximale Länge einer Aufzeichnung ohne Vorpuffer- und Nachpufferzeiten fest. Für eine unbegrenzte Dauer stellen Sie 0 ein.

Von Regeln getriggerte Aufzeichnung

Durch Regeln ausgelöstes Aufzeichnen wird gemäß den in Aktionsregeln erstellten Regeln gestartet und gestoppt. Mit Regeln können beispielsweise Aufzeichnungen erzeugt werden, die durch Signale von I/O-Ports oder Geräteereignissen ausgelöst wurden. Eine Regel kann mehrere Trigger besitzen.

Informationen zum Erstellen einer durch eine Regel ausgelösten Aufzeichnung finden Sie unter *Aktionsregeln*.

Hinweis

Achten Sie darauf, die Bewegungsaufzeichnung zu deaktivieren, wenn sie über eine Regel konfiguriert wird, um doppelte Aufzeichnungen zu vermeiden.

Failover-Aufzeichnung

Nutzen Sie die Failover-Aufzeichnung, wenn sicherstellen möchten, dass Aufzeichnungen bei einem Ausfall der Verbindung mit AXIS Camera Station Pro gespeichert werden. Bei aktivierter Failover-Aufzeichnung speichert die Kamera Aufzeichnungen auf ihrer integrierten SD-Karte, falls die Verbindung länger als 20 Sekunden ausfällt. In der Kamera muss eine SD-Karte installiert und die Funktion muss aktiviert sein. Ausfallsichere Aufzeichnungen sind nur bei Aufzeichnungen im H.264-Format möglich.

Ausfallsichere Aufzeichnung aktivieren:

1. **Konfiguration > Speicher > Auswahl** aufrufen.
2. Wählen Sie eine Kamera aus, welche ausfallsichere Aufzeichnungen unterstützt.
3. Wählen Sie **Failover recording (Ausfallsichere Aufzeichnung)**.
4. Klicken Sie auf **Anwenden**.

Hinweis

- Ein Neustart des AXIS Camera Station Pro-Servers löst keine Failover-Aufzeichnung aus. Beispielsweise, wenn Sie eine Datenbanksicherung durchführen, die Dienststeuerung der AXIS Camera Station Pro neu starten, oder den Computer neu starten, auf dem der Server installiert ist.
- Die Aktivierung der Failover-Aufzeichnung setzt alle bestehenden Failover-Einstellungen für diese Kamera auf anderen Servern außer Kraft.
- Die Failover-Aufzeichnung kann für jede Kameraansicht jeweils nur für einen AXIS Camera Station Pro-Server aktiv sein.

Sobald die Verbindung wiederhergestellt ist, importiert AXIS Camera Station Pro automatisch die Failover-Aufzeichnungen und markiert sie in der Zeitleiste in Dunkelgrau.

Die Kamera verwendet einen 20-sekündigen Vor- und Nachpuffer, um Aufzeichnungslücken zu minimieren. Dennoch kann es zu kurzen Lücken von etwa 1 bis 4 Sekunden kommen. Für Failover-Aufzeichnungen wird immer das Streamingprofil mit hoher Auflösung verwendet. Wenn die entsprechende Funktion in der Kamera aktiviert ist und Audio vor Aktivierung der Failover-Aufzeichnung Teil des Streams ist, wird Audio eingeschlossen.

Aufzeichnungsarten	
Bewegungserkennung mit Vorpuffer	Fällt die Verbindung länger als 20 Sekunden aus, zeichnet die Kamera fortlaufend solange auf die SD-Karte auf, bis die Verbindung wiederhergestellt oder die SD-Karte voll ist.
Bewegungserkennung ohne Vorpuffer	• Wenn keine durch eine Bewegung ausgelöste Aufzeichnung läuft und die Verbindung länger als 20 Sekunden ausfällt, wird die Failover-Aufzeichnung nicht gestartet. • Sollte die Verbindung während einer durch eine Bewegung ausgelösten Aufzeichnung länger als 20 Sekunden ausfallen, wird die Failover-Aufzeichnung gestartet und fortgesetzt, bis die Verbindung wiederhergestellt oder die SD-Karte voll ist.
Kontinuierliches Aufzeichnen	Fällt die Verbindung länger als 20 Sekunden aus, zeichnet die Kamera fortlaufend solange auf die SD-Karte auf, bis die Verbindung wiederhergestellt oder die SD-Karte voll ist.

Hinweis

Geräte mit einer AXIS OS-Version vor 11.11.42 verwenden eine Vorgängerversion der Failover-Aufzeichnung. Die Hauptunterschiede sind die folgenden:

- Die Kamera startet die Failover-Aufzeichnung bereits 10 Sekunden nach dem Verbindungsausfall.
- Die Kamera verwendet einen internen Puffer von 10 Sekunden anstelle eines Puffers von 20 Sekunden für Voralarm- und Nachalarmbilder.

SD-Karte für Failover-Aufzeichnung verwenden

Ausweichoption-Aufzeichnung

Sie können auf einem Gerät, das als Aufzeichnungsspeicher AXIS S3008 Recorder verwendet, Fallback-Aufzeichnung aktivieren. Bei Aktivierung der Option Fallback-Aufzeichnung startet das Gerät bei einem Verbindungsabbruch zwischen AXIS Camera Station Pro und Rekorder automatisch eine Daueraufzeichnung. Das Gerät verwendet für Fallback-Aufzeichnungen ein Videostream-Profil mit mittlerer Auflösung.

Hinweis

- Dafür ist AXIS Camera Station 5.36 oder höher, AXIS S3008 Recorder Firmware 10.4 oder höher, Firmware für Axis Geräte 5.50 oder höher erforderlich.
- Falls zum Startzeitpunkt der Fallback-Aufzeichnung bereits eine Daueraufzeichnung läuft, beginnt eine neue Daueraufzeichnung. Das System erstellt Duplikate des Videostreams auf dem Rekorder.

Fallback-Aufzeichnung aktivieren:

1. Stellen Sie sicher, dass Sie den AXIS S3008 Recorder und die erforderlichen Geräte hinzugefügt und den Rekorder als Aufzeichnungsspeicher für das Gerät ausgewählt haben. Siehe *AXIS OS Recorder einrichten*.
2. **Konfiguration > Speicher > Auswahl** aufrufen.
3. Wählen Sie das Gerät und dann **Fallback-Aufzeichnung**.
4. Klicken Sie auf **Anwenden**.

Aufzeichnungsmethode

AXIS Camera Station Pro konfiguriert beim Hinzufügen von Geräten automatisch die Bewegungs- oder Daueraufzeichnung.

Ein Häkchen in der Liste zeigt an, welche Aufzeichnungsart ein Gerät verwendet. Zum Anpassen der Profileinstellungen für Video und Audio, siehe *Videostromprofile*.

Aufzeichnungsart ändern:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode** aufrufen.
2. Wählen Sie ein oder mehrere Geräte aus.
   Mehrere Geräte desselben Modells lassen sich gleichzeitig konfigurieren.
3. Schalten Sie im Bild **Recording method (Aufzeichnungsart)** eine Aufzeichnungsart ein oder aus.

Hinweis

Anzeigebereiche unterstützen keine Bewegungserkennung.

Durchschnittliche Bitrate einstellen

Mit der durchschnittlichen Bitrate wird die Bitrate über einen längeren Zeitraum hinweg automatisch angepasst. Dadurch können Sie die angegebene Bitrate erreichen erfüllen und gute Videoqualität auf Grundlage des angegebenen Speichers bereitstellen.

Hinweis

- Diese Option ist nur für kontinuierliches Aufzeichnen verfügbar. Die Kameras müssen zudem die Funktion Durchschnittliche Bitrate unterstützen und mit der Firmwareversion 9.40 oder später ausgestattet sein.
- Die Einstellungen der durchschnittlichen Bitrate beeinflussen die Qualität des ausgewählten Videostreamprofils.

1. **Configuration > Storage > Selection (Konfiguration > Speicher >Auswahl)** aufrufen und sicherstellen, dass die Vorhaltezeit für die Kamera begrenzt ist.
2. Wechseln Sie zu **Configuration > Devices > Stream profiles (Konfiguration > Geräte > Videostreamprofile)** und vergewissern Sie sich, dass für das Videoprofil für das kontinuierliche Aufzeichnen das Format H.264 oder H.265 eingestellt ist.
3. **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode** aufrufen.
4. Wählen Sie die entsprechende Kamera und aktivieren Sie **Kontinuierlich**.
5. Das konfigurierte Profil unter **Video settings (Videoeinstellungen)** auswählen.
6. Aktivieren Sie **Average bitrate (Durchschnittliche Bitrate)** und stellen Sie **Max storage (Max. Speicherplatz)** ein. Die angezeigte geschätzte durchschnittliche Bitrate wird vom System auf Grundlage des angegebenen maximalen Speicherplatzes und der Vorhaltezeit berechnet. Die maximale durchschnittliche Bitrate beträgt 50.000 KBit/s.

Hinweis

Die Option **Max storage (Max. Speicherplatz)** bezieht sich auf den maximalen Speicherplatz für die Aufzeichnung im Rahmen der Vorhaltezeit. Es garantiert nur, dass die Aufnahmen den angegebenen Speicherplatz nicht überschreiten, es garantiert jedoch nicht, dass genügend Platz für die Aufnahmen vorhanden ist.

7. Klicken Sie auf **Anwenden**.

Bewegungseinstellungen bearbeiten

Wenn Ihr Gerät einen AXIS Object Analytics verwendet, können Sie dort die Einstellungen für die Bewegungsaufzeichnung bearbeiten.

Hinweis

Für AXIS Object Analytics in AXIS Camera Station Pro ist AXIS OS 12.4 erforderlich.

1. Öffnen Sie eine Registerkarte **Configuration (Konfiguration)**.
2. Rufen Sie **Recording and events (Aufzeichnung und Ereignisse)** > **Recording method (Aufzeichnungsmethode)** auf.
3. Wählen Sie die Kamera aus, die Sie konfigurieren möchten.
4. **Bewegungserkennung** aktivieren.
5. Klicken Sie auf **Motion settings (Bewegungseinstellungen)**.

Weitere Informationen finden Sie im *AXIS Object Analytics Benutzerhandbuch* zur Konfiguration von AXIS Object Analytics auf Ihrem Gerät.

Bearbeiten von AXIS Video Motion Detection 2 und 4

Die Kamera-Anwendungen AXIS Video Motion Detection 2 und 4 lassen sich auf Produkten installieren, die AXIS Camera Application Platform unterstützen. Wenn auf der Kamera AXIS Video Motion Detection 2 oder 4 installiert ist, werden in einem ausgewählten Bereich Bewegungen erkannt. Für Motion Detection 2 ist Firmware 5.60 oder höher erforderlich, und für AXIS Video Motion Detection 4 ist Firmware 6.50 oder höher erforderlich. In den Versionshinweisen des Produkt finden sich Angaben, ob Video Motion Detection 4 unterstützt wird.

Wenn beim Hinzufügen von Kameras zu AXIS Camera Station Pro die Bewegungsaufzeichnung ausgewählt ist, werden AXIS Video Motion Detection 2 und 4 nur auf Kameras mit der erforderlichen Firmware installiert. Kameras ohne die erforderliche Firmware nutzen die integrierte Bewegungserkennung. Einige Anwendungen lassen sich direkt manuell von der Device Manager-Seite aus installieren. Siehe *Kameraanwendung installieren*.

Mit AXIS Video Motion Detection 2 und 4 lässt sich folgendes erstellen:

- **Ausgewählter Bereich**: Ein Bereich in einer Aufzeichnung, in dem die Kamera sich bewegende Objekte erkennt. Objekte außerhalb des ausgewählten Bereichs werden mit dieser Funktion grundsätzlich ignoriert. Der Bereich wird in Form eines Polygons über dem Videobild angezeigt. Der Bereich hat 3 bis 20 Punkte (Eckpunkte).
- **Ausschlussbereich**: Ein Ausschlussbereich ist ein Bereich innerhalb des ausgewählten Bereichs, in dem sich bewegende Objekte ignoriert werden sollen.
- **Ignorierfilter**: Filter, die erstellt werden, um sich bewegende Objekte zu ignorieren, die von der Anwendung erkannt wurden. Verwenden Sie so wenige Filter wie möglich, und konfigurieren Sie diese mit Bedacht, damit keine wichtigen Objekte ignoriert werden. Die einzelnen Filter nacheinander aktivieren und konfigurieren.
  - **Objekte, die nur kurz erscheinen**: Dieser Filter ignoriert Objekte, die nur für kurze Zeit in einem Bild auftauchen. Zum Beispiel Lichtstrahlen eines vorbeifahrenden Autos und sich schnell bewegende Schatten. Die Mindestdauer, für die Objekte in der Szene erscheinen müssen, um einen Alarm auszulösen. Die Zeit wird ab dem Moment der Erfassung des Objekts durch die Applikation gemessen. Der Filter verzögert Alarme und löst sie nicht aus, wenn das Objekt innerhalb der angegebenen Zeit aus dem Bild verschwindet.
  - **Kleine Objekte**: Dieser Filter ignoriert kleine Objekte wie etwa kleine Tiere. Stellen Sie die Breite und Höhe als Prozentwert des Gesamtbildes ein. Objekte, die kleiner als die angegebenen Werte für Breite und Höhe sind, werden vom Filter ignoriert und lösen keinen Alarm aus. Das Objekt muss kleiner als die Werte für Breite und Höhe sein, damit der Filter es ignoriert.
  - **Schaukelnde Objekte**: Dieser Filter ignoriert Objekte, die sich nur über kurze Entfernung hin- und herbewegen wie etwa Zweige und Fahnen im Wind sowie deren Schatten. Distanz als Prozentwert des Gesamtbildes einstellen. Objekte, die sich über eine Entfernung bewegen, die

geringer ist als die Strecke zwischen der Mitte der Ellipse und einer der Pfeilspitzen, werden vom Filter ignoriert. Die Ellipse ist das Maß der Bewegung und wird auf alle Objekte im Bild angewendet.

Konfigurieren der Einstellungen für die Bewegungserkennung:

Hinweis

Änderungen an dieser Stelle beeinflussen die Einstellungen in der Kamera.

1. **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode** aufrufen.
2. Wählen Sie eine Kamera mit AXIS Video Motion Detection 2 oder 4 und klicken Sie auf **Bewegungserkennung**.
3. Ausgewählten Bereich bearbeiten.
4. Den Ausschlussbereich bearbeiten.
5. Ignorier-Filter erstellen.
6. Klicken Sie auf **Anwenden**.

Einen neuen Punkt hinzufügen	Um einen neuen Punkt zu Ihrem ausgewählten Bereich hinzuzufügen, klicken Sie auf die Linie zwischen zwei Punkten.
Remove Point (Punkt entfernen)	Um einen Punkt aus Ihrem Interessengebiet zu entfernen, klicken Sie auf den Punkt und dann auf **Remove Point (Punkt entfernen)**.
Add Exclude Area (Ausschlussbereich hinzufügen)	Um einen Ausschlussbereich zu erstellen, klicken Sie auf **Add Exclude Area (Ausschlussbereich hinzufügen)** und klicken Sie auf die Linie zwischen zwei Punkten.
Remove Exclude Area (Ausschlussbereich entfernen)	Um den Ausschlussbereich zu entfernen, klicken Sie auf **Ausschlussbereich entfernen**.
Short lived objects filter (Filter für nur kurz erscheinende Objekte)	Um einen Filter für nur kurz erscheinende Objekte zu aktivieren, wählen Sie **Short lived objects filter (Filter für kurz erscheinende Objekte)** und stellen Sie die Mindestdauer, die ein Objekt im Bild erscheinen muss, um einen Alarm auszulösen, über den Schieberegler **Time (Zeit)** ein.
Filter für kleine Objekte	Um einen Filter für kleine Objekte zu aktivieren, wählen Sie **Small objects filter (Filter für kleine Objekte)** und stellen Sie die Größe der zu ignorierenden Objekte über den Schieberegler für **Width (Breite)** und **Height (Höhe)** ein.
Swaying objects filter (Filter für schaukelnde Objekte)	Um einen Filter für schaukelnde Objekte zu aktivieren, wählen Sie **Swaying objects filter (Filter für schaukelnde Objekte)** und stellen Sie die Größe der Ellipse über den Schieberegler **Distance (Distanz)** ein.

Die integrierte Bewegungserkennung bearbeiten

Mit der integrierten Bewegungserkennung erkennt die Kamera Bewegungen innerhalb eines oder mehrerer Bereiche und ignoriert alle anderen Bewegungen. Ein Einschlussbereich ist ein Bereich, der Bewegungen erkennt. Sie können einen Ausschlussbereich innerhalb eines Einschlussbereichs platzieren, um Bewegungen zu ignorieren. Es können mehrere Bewegungs- und Ausschlussbereiche verwendet werden.

So können Sie einen Einschlussbereich hinzufügen und bearbeiten:

Hinweis

Änderungen an dieser Stelle beeinflussen die Einstellungen in der Kamera.

1. **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode** aufrufen.
2. Wählen Sie eine Kamera mit integrierter Bewegungserkennung und klicken Sie auf **Bewegungseinstellungen**.
3. Klicken Sie **Add (Hinzufügen)** im Bereich Fenster.
4. Wählen Sie **Include (Einschließen)** aus.
5. Um nur den von Ihnen bearbeiteten Bereich anzuzeigen, wählen Sie **Show selected window (Ausgewähltes Fenster anzeigen)**.
6. Verschieben Sie die Form im Videobild und ändern Sie ihre Größe. Dies ist der Einschlussbereich.
7. Passen Sie **Object size (Objektgröße)**, **History (Verlauf)** und **Sensitivity manually (Empfindlichkeit manuell)** an.
8. Vordefinierte Einstellungen verwenden. Wählen Sie **Low (Niedrig)**, **Moderate (Mittel)**, **High (Hoch)** oder **Very High (Sehr hoch)**. **Niedrig** erfasst größere Objekte mit kürzerem Verlauf. **Sehr hoch** erfasst kleinere Objekte mit längerem Verlauf.
9. In dem Bereich **Activity (Aktivität)** überprüfen Sie die erkannte Bewegung im Einschlussbereich. Rote Spitzen zeigen Bewegung an. Nutzen Sie das Feld **Activity (Aktivität)** bei der Einstellung von **Object size (Objektgröße)**, **History (Verlauf)** und **Sensitivity (Empfindlichkeit)**.
10. Klicken Sie auf **OK**.

Objektgröße	Die Objektgröße ist relativ zur Bereichsgröße definiert. Bei einem hohen Wert werden von der Kamera nur sehr große Objekte erfasst. Bei einem niedrigen Wert werden auch sehr kleine Objekte von ihr erfasst.
Verlauf	Die Objektspeicherdauer legt fest, wie lange sich ein Objekt in einem Bereich befinden muss, damit es als unbeweglich erkannt wird. Bei einem hohen Wert ist der Zeitraum lang, in dem ein Objekt die Bewegungserkennung auslöst. Bei einem niedrigen Wert lösen Objekte eine Bewegungserkennung über einen kurzen Zeitraum aus. Wenn sich im erfassten Bereich keine Objekte befinden sollen, wählen Sie einen sehr hohen Verlaufswert aus. Dies löst eine Bewegungserkennung aus, wenn sich das Objekt in der Umgebung befindet.
Empfindlichkeit	Helligkeitsunterschied zwischen Hintergrund und Objekt. Bei einer hohen Empfindlichkeit erkennt die Kamera durch Objekte mit gewöhnlicher Farbgebung auf gewöhnlichem Hintergrund. Mit geringer Empfindlichkeit erkennt sie nur sehr helle Objekte auf dunklem Hintergrund. Wenn nur Lichtblitze erkannt werden sollen, wählen Sie eine niedrige Empfindlichkeit. Andernfalls wird ein hoher Empfindlichkeitswert empfohlen.

So können Sie einen Ausschlussbereich hinzufügen und bearbeiten:

1. Klicken Sie im Bildschirm **Edit Motion Detection (Bewegungserkennung bearbeiten)** im Fensterbereich auf **Add (Hinzufügen)**.
2. Wählen Sie **Exclude (Ausschluss)**.
3. Verschieben Sie die schattierte Form im Videobild und ändern Sie ihre Größe.

4. Klicken Sie auf **OK**.

Entfernen eines neuen Einschluss- oder Ausschlussfensters:

1. Wählen Sie im Bildschirm **Edit Motion Detection (Bewegungserkennung bearbeiten)** einen Bereich zum Entfernen aus.
2. Klicken Sie auf **Remove (Entfernen)**.
3. Klicken Sie auf **OK**.

Ereigniskategorien konfigurieren

Ereigniskategorien erleichtern das Auffinden von Aufzeichnungen eines bestimmten Typs, z. B. Überfall oder Verkehrskontrolle. So erstellen Sie eine Ereigniskategorie:

1. Rufen Sie **Configuration (Konfiguration)** > **Recording and events (Aufzeichnung und Ereignisse)** > **Event categories (Ereigniskategorien)** auf.
2. Auf **Neu** klicken.
3. Geben Sie einen Namen für die Ereigniskategorie ein.
4. Optional können Sie eine Farbe für die Ereigniskategorie und eine benutzerdefinierte Speicherdauer für die Ereigniskategorie einstellen.
5. Klicken Sie auf **Anwenden**.

Bezeichnung	Wir empfehlen, einen Namen für die Kategorie zu verwenden, der für eine Art von Ereignis steht, z. B. Überfall oder Verkehrskontrolle.
Aufbewahrungszeit	Sie können für jede Ereigniskategorie eine benutzerdefinierte Aufbewahrungszeit einstellen, die die Standard-Aufbewahrungszeit der Kamera überschreibt. Die benutzerdefinierte Aufbewahrungszeit der Ereigniskategorie gilt nur, wenn sie länger ist als der Standard.

Weitere Informationen finden Sie unter *Ereigniskategorien, on page 27*.

E/A-Ports

Viele Kameras und Video-Encoder verfügen für den Anschluss von externen Geräten über E/A-Ports. Auch manche Zusatzgeräte können I/O-Ports besitzen.

Es gibt zwei Arten von E/A-Ports:

Eingangsanschluss – Wird für den Anschluss von Geräten, die zwischen offenem und geschlossenem Stromkreis umschalten können, verwendet. Beispielsweise für Tür- und Fensterkontakte, Rauchmelder, Glasbruchmelder und PIRs (Passive Infrarot-Melder).

Ausgangs-Port – Zum Anschließen von Geräten wie Relais, Türen, Schlössern und Alarmen. AXIS Camera Station Pro kann Geräte steuern, die an Ausgangs-Ports angeschlossen sind.

Hinweis

- Bei Verbindung zu mehreren AXIS Camera Station Pro Servern, können Sie auf jedem verbundenen Server I/O-Ports erstellen oder verwalten, indem der Server im Drop-Down Menü **Selected server (Ausgewählter Server)** markiert wird.
- Administratoren können I/O-Ports für Benutzer deaktivieren. Siehe *Benutzerberechtigungen*.

Aktionsregeln verwenden I/O-Ports als Auslöser oder Aktionen. Auslöser verwenden Eingangssignale: AXIS Camera Station Pro empfängt ein Signal von einem an einen Eingangsanschluss angeschlossenen Gerät und führt die festgelegten Aktionen aus. Aktionen verwenden Ausgangsanschlüsse: Wenn eine Regel aktiviert wird,

kann AXIS Camera Station Pro ein an einen Ausgangsanschluss angeschlossenes Gerät aktivieren oder deaktivieren. Siehe *Aktionsregeln*.

Informationen zum Anschließen von Geräten und zum Konfigurieren von I/O-Ports finden Sie im Benutzerhandbuch oder der Installationsanleitung des Axis Produkts. Einige Produkte besitzen Ports, die als Eingang oder Ausgang dienen können.

Sie können Ausgangsport manuell steuern. Siehe *E/A-Ports überwachen*.

E/A-Ports hinzufügen

E/A-Ports hinzufügen:

1. **Konfiguration > Aufzeichnung und Ereignisse > E/A-Ports** aufrufen.
2. Klicken Sie **Add (Hinzufügen)** an, um eine Liste von I/O-Ports zu sehen, die hinzugefügt werden können.
3. Wählen Sie den Port aus und klicken Sie auf **OK**.
4. Überprüfen Sie die Informationen unter **Type (Typ)** und **Device (Gerät)**. Ändern Sie die Informationen bei Bedarf.
5. Geben Sie einen Namen für **Port**, **Active State (Aktiver Status)** und **Inactive State (Inaktiver Status)** ein. Die Namen werden auch in Aktionsregeln, Protokollen und I/O-Überwachung angezeigt.
6. Für Ausgangsanschlüsse können Sie den Anfangsstatus festlegen, wenn AXIS Camera Station Pro eine Verbindung mit dem Gerät herstellt. Wählen Sie **On startup set to (Beim Start festlegen auf)** und wählen Sie den Anfangszustand im Drop-Down Menü **State (Status)** aus.

Bearbeiten	Um einen Port zu bearbeiten, wählen Sie den Port aus und klicken Sie auf **Bearbeiten**. Aktualisieren Sie die Port-Informationen und klicken Sie **OK** in dem Dialogfenster.
Entfernen	Um einen Port zu entfernen, wählen Sie den Port aus und klicken Sie auf **Entfernen**.
E/A-Ports neu laden	Wenn I/O-Ports über die Setup-Seiten des Geräts konfiguriert wurden, klicken Sie zum Aktualisieren der Liste auf **Reload I/O Ports (I/O-Ports neu laden)**.

E/A-Ports überwachen

Hinweis

Bei Verbindung zu mehreren AXIS Camera Station Pro Servern, können Sie auf jedem verbundenen Server I/O-Ports überwachen, indem der Server im Drop-Down Menü **Selected server (Ausgewählter Server)** markiert wird.

Ausgangsport manuell steuern:

1. Rufen Sie **Actions > I/O Monitoring (Aktionen > Überwachung von E/A)** auf.
2. Ausgangsanschluss auswählen.
3. Klicken Sie auf **Change state (Status ändern)**.

Aktionsregeln

Mit Aktionsregeln können Sie automatische Reaktionen auf Ereignisse konfigurieren. Dazu gehören zum Beispiel das Versenden einer E-Mail, wenn eine Kamera außerhalb der Geschäftszeiten eine Bewegung detektiert, Interaktionen mit an I/O-Ports angeschlossenen Geräten und die Alarmierung des Bedienpersonals bei wichtigen Ereignissen.

Für jede Regel gibt es Auslöser (Ereignisse, die die Regel aktivieren), Aktionen (Maßnahmen bei Auslösung) und optional einen Zeitplan. Bei Aktivierung eines Auslösers veranlasst die Regel alle Aktionen.

Hinweis

- Bei Verbindung mit mehreren AXIS Camera Station Pro-Servern können Sie auf jedem verbundenen Server Aktionsregeln erstellen oder verwalten, indem Sie den Server im Auswahlmenü **Selected Server (Ausgewählter Server)** auswählen.
- Bei Geräten anderer Hersteller können die verfügbaren Aktionen je nach Gerät unterschiedlich sein. Für viele dieser Ereignisse muss das Gerät zusätzlich konfiguriert werden.

Erstellen Sie eine neue Aktionsregel

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Klicken Sie auf **New... (Neu...)**.
3. Geben Sie im Feld **Name** einen Namen für die Regel ein.
4. Wählen Sie unter **Schedule (Zeitplan)** die Option **Always (Immer)** oder **Custom schedule (Benutzerdefinierter Zeitplan)** aus, um einen Zeitplan aus dem Auswahlmenü zu wählen. Sie können auch einen neuen Zeitplan erstellen oder einen vorhandenen bearbeiten.
5. Wählen Sie unter **Triggers (Auslöser)** die Option **Add... (Hinzufügen...)** und dann den Typ des Auslösers aus, konfigurieren Sie ihn und klicken Sie auf **OK**. Weitere Informationen erhalten Sie unter *Auslöser hinzufügen*.
6. Wählen Sie unter **Actions (Aktionen)** die Option **Add... (Hinzufügen...)** und dann den Typ der Aktion aus, konfigurieren Sie sie und klicken Sie auf **OK**. Weitere Informationen erhalten Sie unter *Aktionen hinzufügen*.
7. Klicken Sie auf **Anwenden**.
   - Die Regel wird automatisch aktiviert, wenn Sie sie speichern.

Bearbeiten	Um eine vorhandene Regel zu bearbeiten, wählen Sie die Regel aus und klicken Sie auf **Bearbeiten**.
Kopieren	Um eine vorhandene Regel zu kopieren, wählen Sie die Regel aus und klicken Sie auf **Copy... (Kopieren...)**.
Entfernen	Um eine Regel zu entfernen, wählen Sie die Regel aus und klicken Sie auf **Remove (Entfernen)**.

Konfiguration mehrerer Aktionsregeln

Bei der Auswahl mehrerer Regeln werden nur Auslöser und Aktionen angezeigt, die in allen ausgewählten Regeln identisch sind. Alle von Ihnen vorgenommenen Änderungen werden auf alle ausgewählten Regeln angewendet.

- **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln aufrufen.**
- Mehrere Regeln auswählen.
- Nehmen Sie Ihre Einstellungen vor:
  - Fügen Sie Auslöser oder Aktionen hinzu, die für alle ausgewählten Regeln gelten sollen.
  - Entfernen Sie gemeinsame Auslöser oder Aktionen aus allen ausgewählten Regeln.
  - Ändern Sie den Zeitplan für alle ausgewählten Regeln.
- Klicken Sie auf **Anwenden**.

Hinweis

Es ist nicht möglich, einzelne Auslöser oder Aktionen zu bearbeiten, wenn mehrere Regeln ausgewählt sind. Würden Ihre Änderungen eine Regel ungültig machen, können Sie diese nicht anwenden.

Auslöser hinzufügen

Auslöser aktivieren Regeln und eine Regel kann mehrere Auslöser haben. Die Regel bleibt aktiv, solange einer der Auslöser aktiv ist. Wenn die Regel nur aktiv sein soll, wenn alle Auslöser aktiv sind, wählen Sie **All triggers must be active simultaneously to trigger the actions (Alle Auslöser müssen gleichzeitig aktiv sein, um die Aktionen auszulösen)**. Erhöhen Sie die Dauer der Auslöser, wenn diese Einstellung für Impulsauslöser verwendet wird. Impulsauslöser sind Auslöser, die zu einem bestimmten Moment aktiv werden.

Es stehen folgende Trigger zur Verfügung:

Bewegungserkennung – Registrierte Bewegungen innerhalb eines definierten Bereichs aktivieren den Bewegungserkennungsauslöser. Siehe *Bewegungserkennungsauslöser erstellen, on page 93*.

Daueraktiv – Dieser Auslöser ist dauerhaft aktiviert. Sie können diesen Auslöser beispielsweise mit einem jederzeit verfügbaren Zeitplan und einer Aufzeichnungsaktion mit einem Low-Profil kombinieren für eine zweite kontinuierliche Aufzeichnung, die für Geräte mit beschränkter Leistung geeignet ist.

Live-Ansicht – Der Auslöser für die Live-Ansicht wird ausgelöst, wenn ein Benutzer den Videostream einer bestimmten Kamera öffnet. Sie können ihn beispielsweise verwenden, um Personen in der Nähe einer Kamera mit den LEDs der Kamera mitzuteilen, dass jemand sie beobachtet. Siehe *Auslöser für Live-Ansicht erstellen, on page 94*.

Systemereignis und Fehler – Der Auslöser Systemereignis und Systemfehler wird aktiviert, wenn Aufnahmefehler auftreten, ein Speicher voll ist, auf eine Netzwerk-Freigabe nicht zugegriffen werden kann oder die Verbindung zu einem oder mehreren Geräten unterbrochen ist. Siehe *Systemereignis- und Fehler-Auslöser erstellen, on page 94*.

Eingabe/Ausgabe – Der Auslöser Eingang/Ausgang (I/O) wird aktiviert, wenn der I/O-Port eines Geräts ein Signal von beispielsweise einer verbundenen Tür, einem Rauchmelder oder einem Schalter empfängt. Siehe *Auslöser Eingang/Ausgang erstellen, on page 95*. Wir empfehlen, nach Möglichkeit Geräteereignisse anstelle von Ein-/Ausgängen als Auslöser zu verwenden.

Geräteereignis – Dieser Trigger nutzt Ereignisse direkt von der Kamera oder dem Zusatzgerät. Verwenden Sie dies, wenn in AXIS Camera Station Pro kein passender Auslöser verfügbar ist. Siehe *Geräte-Ereignisauslöser erstellen, on page 96*.

Aktionsschaltfläche – Aktionsschaltflächen dienen zum Starten und Stoppen von Aktionen aus der Live-Ansicht. Dabei können Sie eine Schaltfläche in verschiedenen Regeln verwenden. Siehe *Aktionsschaltflächenauslöser erstellen, on page 101*.

Axis Entry Manager-Ereignis – Dieser Auslöser wird bei Eingang von im AXIS Entry Manager konfigurierten Türsignalen in AXIS Camera Station Pro aktiviert. Zum Beispiel, wenn Türen gewaltsam geöffnet werden, zu lange geöffnet bleiben oder der Zutritt verweigert wird. Siehe *Axis Entry Manager-Auslöser für Ereignisse erstellen, on page 103*.

HTTPS (extern) – Dank des externen HTTPS-Auslösers können durch externe Anwendungen über HTTPS-Kommunikation Ereignisse in AXIS Camera Station Pro ausgelöst werden. Siehe *Externen HTTPS-Auslöser erstellen, on page 103*.

Bewegungserkennungsauslöser erstellen

Der Auslöser Bewegungserkennung wird aktiviert, wenn die gewählte Kamera innerhalb eines bestimmten Bereichs eine Bewegung erkennt. Da die Verarbeitung der Erfassung durch die Kamera erfolgt, wird AXIS Camera Station Pro nicht weiter belastet.

Hinweis

Verwenden Sie zum Starten einer Aufzeichnung keine Bewegungserkennungs-Auslöser, wenn die Bewegungsaufzeichnung in der Kamera aktiviert ist. Schalten Sie die Bewegungsaufzeichnung aus, bevor Sie Bewegungserkennungs-Auslöser verwenden. Um die Aufzeichnung von Bewegung zu deaktivieren, wechseln Sie zu **Configuration > Recording and events > Recording method (Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsart)**.

Um einen Bewegungserkennungsauslöser zu erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen** und wählen Sie **Bewegungserkennung** aus.
4. Klicken Sie auf **OK**.
5. Auf dem Popup-Bildschirm:
   5.1. Wählen Sie die Kamera aus, die Bewegungen erkennen soll.
   5.2. Stellen Sie einen Intervall zwischen zwei aufeinanderfolgenden Auslösern ein, um die Nummer von aufeinanderfolgenden Aufzeichnungen zu verringern. Tritt innerhalb dieses Intervalls ein weiterer Auslöser ein, wird die Aufzeichnung fortgesetzt und der Auslösezeitraum neu gestartet.
   5.3. Klicken Sie auf **Bewegungseinstellungen**, um Bewegungserkennungseinstellungen zu konfigurieren. Die verfügbaren Bewegungseinstellungen unterscheiden sich zwischen verschiedenen Kameras. Siehe *Die integrierte Bewegungserkennung bearbeiten* und *Bearbeiten von AXIS Video Motion Detection 2 und 4*.
6. Klicken Sie auf **OK**.

Auslöser für Live-Ansicht erstellen

Der Auslöser für die Live-Ansicht wird ausgelöst, wenn ein Benutzer den Videostream einer bestimmten Kamera öffnet. Sie können ihn beispielsweise verwenden, um Personen in der Nähe einer Kamera mit den LEDs der Kamera mitzuteilen, dass jemand sie beobachtet.

So erstellen Sie einen Auslöser für eine Live-Ansicht:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. **Hinzufügen** anklicken und **Live-Ansicht** wählen.
4. Klicken Sie auf **OK**.
5. Die Auslöserkamera auswählen.
6. Klicken Sie auf **OK**.

Systemereignis- und Fehler-Auslöser erstellen

Wählen Sie ein oder mehrere Systemereignisse und -fehler aus, die Sie als Auslöser verwenden möchten. Beispiele für Systemereignisse sind Aufzeichnungsfehler, ein voller Speicher, der fehlende Verbindungsaufbau zu einem Netzwerkspeicher oder der Verbindungsabbruch zu einem oder mehreren Geräten.

Systemereignis- und Fehler-Auslöser erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. **Hinzufügen** anklicken und **Systemereignis und Fehler** wählen.
4. Klicken Sie auf **OK**.
5. Wählen Sie zur Erstellung des Auslösers ein Systemereignis oder einen Fehler aus.
6. Klicken Sie auf **OK**.

Bei Aufnahmefehler	**Bei Aufnahmefehler** wählen, um den Auslöser zu aktivieren, wenn während der Aufzeichnung ein Fehler auftritt, z. B. Unterbrechung eines Kamerastreams.
Bei vollem Datenträger	**Bei vollem Laufwerk** wählen, um den Auslöser zu aktivieren, wenn ein Speicher für Aufzeichnungen voll ist.

Bei Verbindungsabbruch zum Netzwerkdatenträger	Wählen Sie die **Option On no contact with network storage (Bei Verbindungsausfall zum Netzwerkspeicher)**, um den Auslöser zu bei Zugriffsproblemen auf einen Netzwerkspeicher zu aktivieren.
On lost connection to camera (Bei Verbindungsabbruch zur Kamera)	Wählen Sie die Option **On lost connection to camera (Bei Verbindungsabbruch zur Kamera)**, um den Auslöser bei Verbindungsstörungen zu den Kameras zu aktivieren. • Wählen Sie **All (Alle)** aus, um alle zu AXIS Camera Station Pro hinzugefügten Kameras zu verwenden. • Wählen Sie **Selected (Ausgewählt)** und klicken Sie auf **Cameras (Kameras)**, um eine Liste aller zu AXIS Camera Station Pro hinzugefügten Kameras anzuzeigen. Verwenden Sie **Select all (Alle auswählen)**, um alle Kameras auswählen, oder **Deselect all (Alle abwählen)**, um alle Kameras abzuwählen.

Auslöser Eingang/Ausgang erstellen

Ein- und Ausgangsauslöser (E/A-Auslöser) werden bei Eingang eines Signals (z. B. von einer verbundenen Tür, einem Rauchmelder oder einem Schalter) am I/O-Port des Geräts aktiviert.

Hinweis

- Sie müssen den I/O-Port zu AXIS Camera Station Pro hinzufügen, bevor Sie einen I/O-Trigger verwenden. Siehe *E/A-Ports*.
- Verwenden Sie als Auslöser nach Möglichkeit Geräteereignisse anstelle von Ein-/Ausgängen. Geräteereignis-Auslöser ermöglichen insgesamt ein besseres Nutzungserlebnis. Weitere Informationen finden Sie unter *Geräte-Ereignisauslöser erstellen, on page 96*.

Auslöser Eingang/Ausgang erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. **Hinzufügen** anklicken und **Eingang/Ausgang** wählen.
4. Klicken Sie auf **OK**.
5. Konfigurieren Sie unter **Trigger port and state (Auslöse-Port und Zustand)** den I/O-Port und die Auslöseeinstellungen.
6. Klicken Sie auf **OK**.

Triggerschnittstelle und Status	
E/A-Port	Wählen Sie unter **I/O port (I/O-Port)** den gewünschten Ein- oder Ausgangsport aus.
Trigger state (Auslösezustand)	Wählen Sie unter **Trigger state (Auslösezustand)** aus, in welchem E/A-Zustand der Auslöser aktiviert werden soll. Die verfügbaren Auslösezustände richten sich nach der Konfiguration des Ports.
Trigger period (Auslösedauer)	Stellen Sie unter **Trigger period (Auslösedauer)** ein Zeitintervall zwischen zwei aufeinanderfolgenden Auslösern ein, um die Anzahl der aufeinanderfolgenden Aufzeichnungen zu reduzieren. Tritt innerhalb dieses Intervalls ein weiterer Auslöser ein, wird die Aufzeichnung fortgesetzt und der Auslösezeitraum neu gestartet.

Geräte-Ereignisauslöser erstellen

Dieser Trigger nutzt Ereignisse direkt von der Kamera oder dem Zusatzgerät. Verwenden Sie diesen, wenn in AXIS Camera Station Pro kein passender Auslöser verfügbar ist. Die Ereignisse unterscheiden sich von Kamera zu Kamera und umfassen einen oder mehrere Filter, die gesetzt werden müssen. Filter sind Bedingungen, die erfüllt sein müssen, damit der Geräte-Ereignisauslöser aktiviert werden kann. Informationen zu Ereignissen und Filtern für Axis Produkte finden Sie in der VAPIX®-Dokumentation unter *axis.com/partners* und *axis.com/vapix*

Um einen Geräte-Ereignisauslöser zu erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. **Hinzufügen** anklicken und **Gerätereignis** wählen.
4. Klicken Sie auf **OK**.
5. Konfigurieren Sie unter **Configure device event trigger (Geräte-Ereignisauslöser konfigurieren)** den gewünschten Ereignisauslöser.

Hinweis

Welche Ereignisse ausgewählt werden können, ist vom jeweiligen Gerät abhängig. Bei Geräten von Drittanbietern ist bei einigen dieser Ereignisse möglicherweise eine zusätzliche Konfiguration des Geräts erforderlich.

6. Wählen Sie unter **Filters (Filter)** die gewünschten Filter aus.
7. Überprüfen Sie unter **Activity (Aktivität)** den aktuellen Status des als Zeitfunktion angezeigten Geräte-Ereignisauslösers. Ein Ereignis kann einen Status haben oder nicht. Die Aktivität eines statusbehafteten Ereignisses wird in Form einer Stufenfunktion dargestellt. Die Aktivität eines statuslosen Ereignisses wird durch eine bei Auslösung des Ereignisses gerade Linie mit Impulsen dargestellt.
8. Klicken Sie auf **OK**.

Geräte-Ereignistrigger konfigurieren	
Gerät	Wählen Sie unter **Device (Gerät)** die entsprechende Kamera oder das Zusatzgerät aus.
Veranstaltung	Wählen Sie unter **Event (Ereignis)** das Ereignis aus, das als Auslöser verwendet werden soll.
Trigger period (Auslösedauer)	In dem Feld **Trigger period (Auslöserzeitspanne)**, stellen Sie einen Intervall zwischen zwei aufeinanderfolgenden Auslösern ein, um die Nummer von aufeinanderfolgenden Aufzeichnungen zu verringern. Tritt innerhalb dieses Intervalls ein weiterer Auslöser ein, wird die Aufzeichnung fortgesetzt und der Auslösezeitraum neu gestartet.

Beispiele für Geräteereignisse

Kategorie	**Geräteereignis**
Verstärker	Verstärkerüberlastung
Audiosteuerung	Digitaler Signalstatus
Audioquelle	Audioerkennung
Autorisierung	Zutrittsanfrage gewährt
	Zutrittsanfrage verweigert
Anrufen	Status
	Status wechseln
	Netzwerkqualität
	SIP-Kontostatus
	Eingehendes Video
Gehäuse	Gehäuse geöffnet
Gerät	Ringstrom-Überstromschutz
Gerätesensoren	Systembereitschaft
	PIR-Sensor
Gerätestatus	Systembereitschaft
Tür	Zugang erzwungen
	Manipulation der Zugangsinstallation erkannt
	Tür verriegelt
	Tür zu lange geöffnet
	Türposition
	Tür entriegelt
Ereignispuffer	Anfang

Ereignisaufzeichnung	Verworfene Alarme
	Verworfene Ereignisse
	Alarm
Lüfter	Status
Globale Szenenänderung	Bilddienst
Hardwarefehler	Speicherfehler
	Lüfter Fehler
Heizung	Status
Eingangsanschlüsse	Virtueller Eingang
	Digitaler Eingangs-Port
	Manueller Auslöser
	Überwachter Eingangs-Port
	Digitaler Ausgangsanschluss
	Externer Eingang
Licht	Status
Lichtstatus geändert	Status
Medien	Profil geändert
	Konfiguration geändert
Überwachen	Heatbeat
Bewegungsbereichmelder	Bewegung
Netzwerk	Netzwerkverlust Gilt nur für vom Gerät verwendete Ereignisse, nicht für von AXIS Camera Station Pro verwendete Ereignisse.
	Adresse hinzugefügt
	Adresse entfernt
PTZ-Bewegung	PTZ-Bewegung auf Kanal
PTZ-Voreinstellungen	PTZ-Voreinstellung auf Kanal erreicht
PTZ-Steuerung	Automatisches Nachführen
	PTZ-Steuerungswarteschlange
	PTZ-Fehler
	PTZ-Bereit
Aufzeichnungskonfiguration	Aufzeichnung erstellen
	Aufzeichnung löschen
	Nachführungskonfiguration
	Konfiguration für Aufzeichnungen

	Aufzeichnungskonfiguration
Remote-Kamera	Vapix-Status
	PTZ-Position
Zeitschema	Impuls
	Intervall
	Geplantes Ereignis
Status	Aktiv
Speicherung	Speicherunterbrechung
	Aufzeichnung läuft
Systemmeldung	Aktion fehlgeschlagen
Sabotage	Neigung erkannt
	Erschütterung festgestellt
Temperaturfühler	Über der Betriebstemperatur
	Unter der Betriebstemperatur
	Innerhalb der Betriebstemperatur
	Oberhalb oder unterhalb der Betriebstemperatur
Trigger	Relais und Ausgänge
	Digitaleingang
Videobewegungserkennung	VMD 4: Profil <Profilname>
	VMD 4: jedes Profil
Video Motion Detection 3	VMD 3
Videoquelle	Bewegungsalarm
	Zugriff auf Livestream
	Tag-/Nachtsicht
	Kamera-Manipulation
	Durchschnittlicher Bitratenabfall
	Angeschlossene Videoquelle

Geräteereignisse des Axis Netzwerk-Tür-Controller

Geräteereignis	**Aktionsregel auslösen**
Autorisierung	
Zutrittsanfrage gewährt	Das System gewährte einem Karteninhaber Zutritt, wenn er mit seinen Zugangsdaten identifiziert wurde.
Zwang	Jemand hat seine Zwangs-PIN verwendet. Dies kann beispielsweise dazu verwendet werden, einen stillen Alarm auszulösen.

Zutrittsanfrage verweigert	Das System gewährte einem Karteninhaber keinen Zutritt, wenn er mit seinen Zugangsdaten identifiziert wurde.
Double Swipe	Ein Karteninhaber hat seine Karte zweimal durchgezogen. Mit dem doppelten Durchziehen kann der Karteninhaber den aktuellen Status einer Tür überschreiben. Dies kann beispielsweise dazu verwendet werden, eine Tür außerhalb des regulären Zeitplans zu entriegeln.
Anti-Passback-Erkennung	Jemand hat die Daten eines Karteninhabers verwendet, der eine Zone vor ihm betreten hat.
Authorization with two-person rule (Autorisierung mit Zwei-Personen-Regel)	
Zugangsanfrage anstehend	Der erste von zwei Karteninhabern hat sich anhand seiner Zugangsdaten identifiziert.
Zutrittsanfrage gewährt	Das System gewährte dem letzten Karteninhaber Zutritt, wenn er mit seinen Zugangsdaten identifiziert wurde.
Gehäuse	
Gehäuse geöffnet	Jemand hat das Gehäuse des Netzwerk-Tür-Controllers geöffnet oder entfernt. Verwenden Sie diese Option z. B., um bei einer Öffnung des Gehäuses zu Wartungszwecken oder Manipulationsversuchen eine Benachrichtigung an den Administrator zu versenden.
Gerätestatus	
Systembereitschaft	Das System ist betriebsbereit. Das Axis-Produkt erkennt beispielsweise den Systemstatus und sendet nach dem Systemstart eine Benachrichtigung an den Administrator. Wählen Sie **Ja** aus, um die Aktionsregel auszulösen, wenn sich das Produkt im Status „Bereit" befindet. Hinweis: Die Regel wird nur ausgelöst, nachdem alle erforderlichen Dienste, wie etwa das Ereignissystem, gestartet wurden.
Tür	
Zugang erzwungen	Der Zugang wurde erzwungen.
Manipulation der Zugangsinstallation erkannt	Wenn das System Folgendes erkennt: • Öffnen oder Schließen des Gerätegehäuses • Gerätebewegung • Ab- oder Ausbau des verbundenen Lesers • Manipulation des verbundenen Türmonitors, Lese- oder REX-Geräts. Aktivieren Sie bei Verwendung dieses Auslösers die Option Supervised Input (Überwachter Eingang), und überprüfen Sie die Installation der Leitungsabschlusswiderstände an den entsprechenden Eingangsanschlüssen der Tür-Verbindung.
Tür verriegelt	Das Zugangstürschloss ist verriegelt.
Tür zu lange geöffnet	Die Zugangstür ist zu lange geöffnet.
Türposition	Der Türmonitor zeigt an, dass die Zugangstür geöffnet oder geschlossen ist.
Tür entriegelt	Das Zugangstürschloss bleibt entriegelt. Dieser Zustand kann z. B. verwendet werden, wenn Besucher die Tür öffnen dürfen, ohne sich ausweisen zu müssen.

Eingangsanschlüsse	
Virtueller Eingang	Schaltzustandsänderung eines virtuellen Eingangs. Virtuelle Eingänge können von einem Client wie z. B. einer Steuerung verwendet werden, um verschiedene Aktionen auszulösen. Wählen Sie den Eingangsanschluss aus, der die Aktionsregel auslösen soll, wenn er aktiv wird.
Digitaler Eingangs-Port	Schaltzustandsänderung eines digitalen Eingangsanschlusses. Verwenden Sie diesen Auslöser, um verschiedene Aktionen wie z. B. den Versand einer Benachrichtigung oder die Einschaltung der Status-LED mit Blinklicht auszulösen. Wählen Sie den Eingangsanschluss aus, der bei Aktivierung die Aktionsregel auslösen soll, oder wählen Sie **Any (Beliebige)**, um die Aktionsregel bei Aktivierung eines beliebigen Eingangsanschlusses auszulösen.
Manueller Auslöser	Aktiviert den manuellen Auslöser. Verwenden Sie diesen Auslöser, um die Aktionsregel manuell über die VAPIX-API zu starten oder zu stoppen.
Externer Eingang	Notfalleingang aktiv oder inaktiv.
Netzwerk	
Netzwerkverlust	Das Netzwerk verliert die Verbindung. Gilt nur für vom Gerät verwendete Ereignisse, nicht für von AXIS Camera Station Pro verwendete Ereignisse.
Adresse hinzugefügt	Es wurde eine neue IP-Adresse hinzugefügt.
Adresse entfernt	Die IP-Adresse wurde entfernt.
Zeitschema	
Geplantes Ereignis	Zustandsänderungen eines vordefinierten Zeitplans. Mit dieser Funktion können Sie Videos in bestimmten Zeiträumen aufzeichnen, z. B. während der Bürozeiten, an Wochenenden usw. Wählen Sie im Dropdown-Menü **Schedule (Zeitplan)** einen Zeitplan aus.
Systemmeldung	
Aktion fehlgeschlagen	Eine Aktionsregel ist fehlgeschlagen und löst die Systemmeldung „Action failed" (Aktion fehlgeschlagen) aus.
Trigger	
Digitaler Eingang	Ein physischer digitaler Eingangsanschluss ist aktiv oder inaktiv.

Aktionsschaltflächenauslöser erstellen

Aktionsschaltflächen dienen zum Starten und Stoppen von Aktionen in der Live-Ansicht (**Live view**). Die Aktionsschaltflächen befinden sich unten in der Live-Ansicht oder werden in Lageplänen angezeigt. Sie können eine Schaltfläche mit mehreren Kameras und Lageplänen belegen und mehrere Aktionsschaltflächen für eine Kamera oder einen Lageplan erstellen. Sie können die Schaltflächen für eine Kamera beim Hinzufügen oder bei der Bearbeitung der Aktionsschaltfläche entsprechend anordnen.

Es gibt zwei Arten von Aktionsschaltflächen:

Befehlsschaltflächen – Befehlsschaltflächen dienen dazu, eine Aktion manuell zu starten. Verwenden Sie Befehlsschaltflächen für Aktionen, die keine Stopptaste erfordern. Eine Befehlsschaltfläche hat eine Schaltflächenbeschriftung und einen Tooltip. Die Schaltflächenbezeichnung ist der auf der Schaltfläche angezeigten Beschriftungstext. Bewegen Sie den Mauszeiger über die Schaltfläche, um den Tooltip anzuzeigen.

Beispiel: Erstellen einer Schaltfläche zur Aktivierung eines Ausgangs über eine vorbestimmte Zeit, Auslösung eines Alarms oder Versendung einer E-Mail.

Wechselschaltflächen – Umschaltflächen dienen dazu, eine Aktion manuell zu starten und zu stoppen. Die Schaltfläche hat zwei Status: Betätigung und Nichtbetätigung. Klicken Sie zum Umschalten zwischen den beiden Schaltzuständen auf die Schaltfläche. Die Aktion wird standardmäßig beim Umschalten auf „Eingeschaltet" gestartet, kann jedoch auch umgekehrt, d. h. bei Umschalten auf „Ausgeschaltet", erfolgen.

Umschaltflächen umfassen eine entsprechende Bezeichnung im eingeschalteten sowie ausgeschalteten Zustand und einen Tooltip. Der im ein- bzw. ausgeschalteten Zustand angezeigte Schaltflächenbeschriftungstext entspricht der jeweiligen Schaltflächenbezeichnung. Bewegen Sie den Mauszeiger über die Schaltfläche, um den Tooltip anzuzeigen.

Beispiel: Erstellen einer Schaltfläche zum Öffnen und Schließen von Türen, Verwendung einer Ausgangsaktion mit Impuls auf „solange ein Auslöser aktiv ist".

Aktionsschaltflächenauslöser erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. **Hinzufügen** anklicken und **Aktionsschaltfläche** wählen.
4. Klicken Sie auf **OK**.
5. Wählen Sie **Neue Schaltfläche erstellen** oder **Vorhandene Schaltfläche verwenden**. Klicken Sie auf **Next (Weiter)**.
6. Bei Auswahl von **Create new button (Neue Schaltfläche erstellen)**:
   6.1. Wählen Sie **Befehlsschaltfläche** bzw. **Wechselschaltfläche**. Wenn Sie die Wechselschaltfläche verwenden möchten, um die Aktion im Status Nichtbetätigung zu starten, wählen Sie **Auslöser bei Nichtbetätigung**.
   6.2. Klicken Sie auf **Next (Weiter)**.
   6.3. Fügen Sie entsprechenden Bezeichnungen und Tooltips für die Schaltfläche hinzu.

Hinweis

Der Buchstabe oder die Number nach dem ersten Unterstrich auf der Beschriftung der Aktionsschaltfläche wird zum Zugangs-Key für die Aktionsschaltfläche. ALT und die Zugriffstaste drücken, um die Aktionstaste zu aktivieren. Wenn Sie z. B. eine Aktionsschaltfläche mit A_BC benennen, wird der Name der Aktionsschaltfläche in der Live-Ansicht auf ABC geändert. ALT + B drücken, um die Aktionstaste zu aktivieren.

7. Bei Auswahl von **Use existing button (Bestehende Schaltfläche verwenden)**:
   7.1. Suchen Sie nach der gewünschten Schaltfläche, oder klicken Sie auf die Schaltfläche, die Sie verwenden möchten.
   7.2. Bei Verwendung einer bestehenden Umschalttaste wählen Sie **Trigger on toggle (Auslösung bei Einschalten)** oder **Trigger on untoggle (Auslösung bei Ausschalten)**.
   7.3. Klicken Sie auf **Next** (Weiter).
   7.4. Beschriftungen und Tooltips der Schaltflächen bearbeiten.
8. Wählen Sie die gewünschte Kamera bzw. den entsprechenden Lageplan aus dem Dropdown-Menü aus.
9. **Zu mehreren Kameras hinzufügen** oder **Zu mehreren Lagepläne hinzufügen** anklicken, um die Schaltfläche zu mehreren Kameras oder Lageplänen hinzuzufügen.
10. Falls einer Kamera mehrere Aktionsschaltflächen zugeordnet sind, klicken Sie auf **Arrange (Anordnen)**, um die Reihenfolge der Schaltflächen zu ändern. Klicken Sie auf **OK**.
11. Klicken Sie auf **Next (Weiter)**.

Axis Entry Manager-Auslöser für Ereignisse erstellen

AXIS Camera Station Pro Dieser Auslöser wird bei Eingang von im AXIS Entry Manager konfigurierten Türsignalen in aktiviert. Zum Beispiel, wenn Türen gewaltsam geöffnet werden, zu lange geöffnet bleiben oder der Zutritt verweigert wird.

Hinweis

Ereignisauslöser für AXIS Entry Manager stehen nur zur Verfügung, wenn die Türsteuerung AXIS A1001 Network Door Controller in AXIS Camera Station Pro hinzugefügt wurde.

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen** und wählen **Sie das EREIGNIS AXIS Entry Manageraus.**
4. Klicken Sie auf **OK**.
5. Wählen Sie ein Ereignis und eine Tür aus, um den Auslöser zu aktivieren.
6. Klicken Sie auf **OK**.

Externen HTTPS-Auslöser erstellen

Dank des externen HTTPS-Auslösers können durch externe Anwendungen über HTTPS-Kommunikation Ereignisse in AXIS Camera Station Pro ausgelöst werden. Dieser Auslöser unterstützt nur HTTPS-Kommunikation und erfordert die Angabe eines gültigen AXIS Camera Station Pro Benutzernamen sowie Domainnamen und Kennwort in den HTTPS-Anfragen.

Die folgenden Anfragen werden mit der HTTP-Methode GET* unterstützt. Möglich ist auch die Verwendung von POST mit JSON-Daten im Textkörper der Anfrage.

Hinweis

- Die Anfragen an externe HTTPS-Auslöser können nur in Google Chrome getestet werden.
- Der externe HTTPS-Auslöser nutzt die gleichen Ports wie die mobile Anzeige-App, siehe Mobiler Kommunikationsport und Mobiler Streamingport, wie beschrieben in *Allgemeines*.
- Aktivieren des Auslösers mit der ID „trigger1“: `https://[address]:29204/Acs/Api/TriggerFacade/ActivateTrigger?{"triggerName":"trigger1"}`
- Deaktivieren des Auslösers mit der ID „trigger1“: `https://[address]:29204/Acs/Api/TriggerFacade/DeactivateTrigger?{"triggerName":"trigger1"}`
- Aktivieren des Auslösers mit der ID „trigger1“ und anschließendes automatisches Deaktivieren des Auslösers nach 30 Sekunden: `https://[address]:29204/Acs/Api/TriggerFacade/ActivateDeactivateTrigger?{"triggerName":"trigger1","deactivateAfterSeconds":"30"}`

Hinweis

Der Timer für die automatische Deaktivierung wird abgebrochen, wenn an diesen Auslöser ein anderer Befehl gesendet wird.

- Impuls an den Auslöser mit der ID „trigger1“ senden (Aktivierung des Auslösers gefolgt von sofortiger Deaktivierung): `https://[address]:29204/Acs/Api/TriggerFacade/PulseTrigger?{"triggerName":"trigger1"}`

Externen HTTPS-Auslöser erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Hinzufügen** und wählen **Externe HTTPS**.
4. Klicken Sie auf **OK**.
5. Geben Sie unter **Trigger name (Auslösername)** den Namen des Auslösers ein.

6. Überprüfen Sie die Beispiel-URL, die die gleiche Server-Adresse wie der Client beim Anmelden verwendet. Die URLs funktionieren erst nach Abschluss der Aktionsregel.
7. Klicken Sie auf **OK**.

Für externe HTTPS-Auslöser geeignete Aktionen

- Anfragen zum Aktivieren und Deaktivieren des Auslösers sind für Aktionen geeignet, die Aufzeichnungen starten und beenden.
- Pulsationsanforderungen eigenen sich für Auslöseaktionen wie **Raise Alarm (Alarm auslösen)** oder **Send Email (E-Mail versenden)**.

Auslöser mit der Funktion Intelligente Suche 2 erstellen

So erstellen Sie einen Auslöser mit der Funktion Intelligente Suche 2:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Add (Hinzufügen)** und wählen Sie die Option **Smart search 2 (Intelligente Suche 2)**.
4. Klicken Sie auf **OK**.
5. Wählen Sie einen Auslöser aus und konfigurieren Sie diesen:
   - Weitere Informationen zur Erstellung intelligenter Suchfilter als Auslöser finden Sie unter *Trigger, on page 179*.
   - Wählen Sie die Option **High processing delay (Hohe Verarbeitungsverzögerung)**, um den Auslöser immer dann zu aktivieren, wenn die Funktion Intelligente Suche 2 mehr als eine Minute benötigt, um Erfassungen zu verarbeiten.
6. Klicken Sie auf **OK**.

Erstellung von Auslösern in Audio Manager

So erstellen Sie einen Auslöser im Audio Manager:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Add (Hinzufügen)** und wählen Sie **Audio Manager** aus.
4. Klicken Sie auf **OK**.
5. Wählen Sie einen Auslöser aus und konfigurieren Sie diesen.
6. Klicken Sie auf **OK**.

Gerätestatus geändert	Wählen Sie die Option **Device status changed (Gerätestatus geändert)**, um den Auslöser zu aktivieren, wenn sich der Gerätestatus ändert, z. B. wenn das Gerät online oder offline geht.
Wiedergabestatus geändert	Wählen Sie die Option **Playback status changed (Wiedergabestatus geändert)**, um den Auslöser zu aktivieren, wenn sich der Wiedergabestatus ändert, also die Wiedergabe gestartet bzw. gestoppt wird.

Ziel aktiviert oder deaktiviert	Wählen Sie die Option **Target enabled or disabled (Ziel aktiviert oder deaktiviert)**, um den Auslöser zu aktivieren, wenn das Auslöserziel aktiviert oder deaktiviert wird.
Lautstärkeregler-Lautstärke geändert	Wählen Sie die Option **Volume controller volume changed (Lautstärkeregler-Lautstärke geändert)**, um den Auslöser zu aktivieren, wenn sich die Einstellung des Lautstärkereglers ändert.

Aktionen hinzufügen

Eine Regel kann mehrere Aktionen besitzen. Die Aktionen werden bei Aktivierung der Regel ausgelöst.

Es stehen folgende Aktionen zur Verfügung:

Aufzeichnen – Diese Aktion startet eine Aufzeichnung über die gewählte Kamera. Siehe *Aufzeichnungsaktion erstellen*.

Alarm auslösen – Diese Aktion sendet einen Alarm an alle verbundenen AXIS Camera Station Pro Clients. Siehe *Die Aktionen "Alarm auslösen" erstellen*.

Ausgang einstellen – Diese Aktion setzt den Status eines Ausgangsports. Verwenden Sie diese Funktion, um das mit dem Ausgangsport verbundene Gerät zu anzusteuern, z. B. zur Einschaltung einer Leuchte oder Verriegelung einer Tür. Siehe *Ausgangsaktionen erstellen*.

Send email (E-Mail senden) – Diese Aktion sendet eine E-Mail an einen oder mehrere Empfänger. Siehe *Erstellen einer E-Mail-Senden-Aktion*.

Live-Ansicht – Diese Aktion öffnet den Arbeitsbereich Live-Ansicht einer bestimmten Kamera, Ansicht oder voreingestellten Position in allen verbundenen AXIS Camera Station Pro Clients. Live-Ansichtsaktionen können auch dazu verwendet werden, um geöffnete AXIS Camera Station Pro-Clients aus der Taskleiste herauszuholen oder in anderen geöffneten Anwendungen einzublenden. Siehe *Live-Ansichtsaktion erstellen*.

HTTP-Meldung senden – Diese Aktion sendet eine HTTP-Anfrage an eine Kamera, eine Tür-Steuerung oder einen externen Web-Server. Siehe *Aktion "HTTP-Meldung" erstellen*.

Sirene und Licht – Diese Aktion löst auf einem kompatiblen Gerät entsprechend einem vorkonfigurierten Profil ein Sirenen- und Lichtmuster aus. Siehe *Sirenen- und Lichtaktionen erstellen, on page 111*.

Virtuelle Ein- und Ausgänge – Diese Aktion löst einen bestimmten virtuellen Eingangs-Port eines Geräts aus. Siehe *Aktionen für virtuelle Ein-/Ausgänge erstellen, on page 111*

AXIS Entry Manager – Mit dieser Aktion können Zugänge freigegeben oder mit einer über AXIS Entry Manager konfigurierten Tür-Steuerung verbundene Zugänge entriegelt oder verriegelt werden. Siehe *Axis Entry Manager-Aktionen erstellen, on page 112*.

Benachrichtigung mit mobiler App senden – Diese Aktion sendet eine individuelle Nachricht an die mobile App von AXIS Camera Station. Siehe *Erstellen von Aktionen zum Versenden von Benachrichtigungen an die mobile App, on page 112*.

Regeln aktivieren oder deaktivieren – Aktivieren oder deaktivieren Sie mithilfe dieser Aktion andere Aktionsregeln. Siehe *Aktion erstellen, die andere Aktionsregeln ein- oder ausschaltet, on page 113*.

Senden an Video-Decoder – Verwenden Sie diese Aktion, um eine Ansicht an einen Video-Decoder zu senden, damit sie für eine bestimmte Zeit auf einem Bildschirm angezeigt wird. Siehe *Eine Aktion erstellen, die eine Ansicht an einen Video-Decoder sendet, on page 113*

Zutrittskontrolle – Diese Aktion umfasst Zugangs- und Zonenaktionen in AXIS Camera Station Secure Entry. Siehe *Zugangskontroll-Aktion erstellen, on page 114*.

Aufzeichnungsaktion erstellen

Aufzeichnungsaktionen starten die Aufzeichnung durch die Kamera. Die entsprechende Aufzeichnung kann über die Registerkarte **Recordings (Aufzeichnungen)** aufgerufen und wiedergegeben werden.

Aufzeichnungsaktion erstellen:

1. Geben Sie einen Speicherort für die Aufzeichnung an, und wechseln Sie zu **Configuration > Storage > Selection (Konfiguration > Speicher > Auswahl)**.
2. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
3. Auf **Neu** klicken.
4. Klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen. Klicken Sie auf **Next (Weiter)**. Siehe *Auslöser hinzufügen*.
5. **Hinzufügen** anklicken und **Live-Ansicht** wählen.
6. Klicken Sie auf **OK**.
7. Wählen Sie unter **Camera (Kamera)** die Kamera aus, über die Sie aufzeichnen möchten.
8. Konfigurieren Sie unter **Video setting (Videoeinstellung)** das Profil, den Vorpuffer und den Nachpuffer.
9. Wählen Sie unter **Event setting (Ereignisgruppe)** die Ereigniskategorie aus, der die Aufzeichnung gegebenenfalls zugeordnet werden soll.
10. Klicken Sie auf **OK**.

Videoeinstellung	
Profil	Wählen Sie im Dropdown-Menü unter **Profile (Profil)** ein Profil aus. Hier können Sie die Kameraeinstellungen bearbeiten: *Videostromprofile*.
Vorpuffer:	Legen Sie die Anzahl der Sekunden vor der erkannten Bewegung fest, die in eine Aufnahme einbezogen werden sollen.
Nachpuffer:	Wählen Sie aus, wie viele Sekunden nach Ende der Aktion in die Aufzeichnung eingeschlossen werden sollen.

Die Aktionen "Alarm auslösen" erstellen

Alarmauslösende Aktionen senden einen Alarm an alle mit AXIS Camera Station Pro verbundenen Clients. Der Alarm erscheint auf der Registerkarte **Alarms (Alarme)** und als Benachrichtigung in der Taskleiste. Es besteht die Möglichkeit, dem Alarm Alarmierungsanweisungen in Form einer Datei beizufügen. Der Alarmvorgang wird über den Tab **Alarme** und **Protokolle** aufgerufen.

Die Aktionen "Alarm auslösen" erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen. Klicken Sie auf **Next (Weiter)**. Siehe *Auslöser hinzufügen*.
4. **Hinzufügen** anklicken und **Alarm auslösen** wählen.
5. Klicken Sie auf **OK**.
6. Konfigurieren Sie unter **Alarm message (Alarmmeldung)** Titel, Beschreibung und Alarmdauer.
7. Unter **Alarm procedure (Alarmierungsanweisungen)**:
   7.1. Wählen Sie **Alarmvorgang bei Alarm anzeigen**.
   7.2. Klicken Sie auf **Upload (Hochladen)**, und suchen Sie die gewünschte Datei.

7.3. Klicken Sie auf **Vorschau**, um die hochgeladene Datei in einem Vorschaufenster zu öffnen.

7.4. Klicken Sie auf **OK**.

Alarmmeldung	
Title (Titel)	Einen Titel für den Alarm eingeben. Der Titel erscheint unter **Alarms (Alarme)** auf der Registerkarte **Alarms (Alarme)** und als Benachrichtigung in der Taskleiste.
Beschreibung	Eine Beschreibung für den Alarm eingeben. Die Titel erscheint unter **Alarms > Description (Alarme > Beschreibung)** auf der Registerkarte **Alarms (Alarme)** und als Benachrichtigung in der Taskleiste.
Alarmdauer (s)	Legen Sie für die Popup-Alarme die Dauer zwischen 1 und 600 Sekunden fest.

Ausgangsaktionen erstellen

Die Ausgangsaktion legt den Status eines Ausgangsports fest. Verwenden Sie diese Funktion, um das mit dem Ausgangsport verbundene Gerät zu anzusteuern, z. B. zur Einschaltung einer Leuchte oder Verriegelung einer Tür.

Hinweis

Vor Verwendung eines Ausgangsports müssen Sie zuerst einen Ausgangsport zu AXIS Camera Station Pro hinzufügen. Siehe *E/A-Ports*.

So erstellen Sie eine Ausgangsaktion:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen. Klicken Sie auf **Next (Weiter)**. Siehe *Auslöser hinzufügen*.
4. **Hinzufügen** anklicken und **Ausgang einstellen** wählen.
5. Klicken Sie auf **OK**.
6. Wählen Sie unter **Output port (Ausgangsport)** den entsprechenden Ausgangsport aus.
7. Wählen Sie unter **State on action (Schaltzustand bei Aktion)** aus, auf welchen Schaltzustand der Port gesetzt werden soll. Die verfügbaren Optionen richten sich nach der Konfiguration des Ports.
8. Wählen Sie **Impuls**, um festzulegen, wie lange der Ausgangsport den neuen Status beibehalten soll.

Hinweis

Damit der Port nach der Aktion den neuen Status komplett beibehält, heben Sie die Markierung **Impuls** auf.

9. Klicken Sie auf **OK**.

Solange irgendein Trigger aktiv ist	Damit der Port den neuen Status beibehält, solange alle Trigger in der Regel aktiv sind, wählen Sie **Solange irgendein Trigger aktiv ist**.
Keep the state for a fixed time (Für bestimmte Zeit setzen)	Um den Port für eine bestimmte Zeit auf den neuen Schaltzustand zu setzen, wählen Sie die zweite Option und geben die Anzahl der Sekunden an.

Erstellen einer E-Mail-Senden-Aktion

Die E-Mail-Aktion sendet eine E-Mail an einen oder mehrere Empfänger. Es besteht die Möglichkeit, Kamera-Momentaufnahmen als E-Mail-Anhang anzufügen.

Hinweis

Um E-Mails versenden zu können, müssen Sie zunächst einen SMTP-Server konfigurieren. Siehe *Servereinstellungen*.

Erstellen einer E-Mail-Senden-Aktion:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen. Klicken Sie auf **Next (Weiter)**. Siehe *Auslöser hinzufügen*.
4. **Hinzufügen** anklicken und **E-Mail senden** wählen.
5. Klicken Sie auf **OK**.
6. Fügen Sie unter **Recipients (Empfänger)** die gewünschten E-Mail-Empfänger hinzu:
   6.1. Geben Sie unter **New Recipient (Neuer Empfänger)** die E-Mail-Adresse ein und wählen die Optionen **To (An)**, **Cc (Kopie)** oder **Bcc (Blindkopie)** aus.
   6.2. Klicken Sie auf **Add (Hinzufügen)**, um die E-Mail-Adresse den Empfängern unter **Recipients** hinzuzufügen.
7. Geben Sie unter **Contents (Inhalt)** den Betreff und die E-Mail-Nachricht ein.
8. Konfigurieren Sie unter **Advanced (Erweitert)** etwaige Anhänge, die Anzahl der E-Mails und die entsprechenden Versandintervalle.
9. Klicken Sie auf **OK**.

Erweitert	
Attach snapshots (Momentaufnahmen anfügen)	Um der E-Mail-Benachrichtigung Kamera-Momentaufnahmen im .jpg-Format als Anhang anzufügen, wählen Sie die Option **Attach snapshots (Momentaufnahmen anhängen)** und klicken anschließend auf **Cameras (Kameras)**. Es erscheint eine Liste mit allen zu AXIS Camera Station Pro hinzugefügten Kameras. Mit **Select all (Alle auswählen)** können Sie alle Kameras auswählen, mit **Deselect all (Alle abwählen)** alle Kameras abwählen.
Send one email for each event (Eine E-Mail pro Ereignis versenden)	**Für jedes Ereignis eine E-Mail senden** - Wählen Sie diese Option, wenn Sie nicht möchten, dass für ein Ereignis mehrere E-Mails gesendet werden.
Don't send another email for (Keine weitere E-Mail senden für)	So verhindern Sie, dass E-Mails zu schnell hintereinander verschickt werden. Wählen Sie hierzu **Don't send another email for (Keine weitere E-Mail senden für)**, und legen Sie im Dropdown-Menü das Mindestzeitintervall zwischen dem Versand zweier E-Mails fest.

Live-Ansichtsaktion erstellen

Live-Ansichtsaktionen öffnen die Registerkarte **Live view (Live-Ansicht)** für eine bestimmte Kamera, Bildansicht oder voreingestellte Position. Die Registerkarte **Live view (Live-Ansicht)** wird in allen angeschlossenen AXIS Camera Station Pro Clients geöffnet. Wird in der Live-Ansicht auf der Registerkarte **Live view** eine geteilte Ansicht mit einem Hotspot angezeigt, wird die in der Live-Ansichtsaktion ausgewählte Kamera in den Hotspot geladen. Weitere Informationen zu Hotspots finden Sie unter *Geteilte Ansicht*.

Live-Ansichtsaktionen können auch dazu verwendet werden, um geöffnete AXIS Camera Station Pro-Clients aus der Taskleiste herauszuholen oder in anderen geöffneten Anwendungen einzublenden.

Aktion "Live-Ansicht" erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen. Klicken Sie auf **Next (Weiter)**. Siehe *Auslöser hinzufügen*.
4. **Hinzufügen** anklicken und **Live-Ansicht** wählen.
5. Klicken Sie auf **OK**.
6. Konfigurieren Sie unter **Live view actions (Live-Ansichtsaktionen)**, was bei aktiver Aktion angezeigt werden soll.
7. Konfigurieren Sie unter **Shown in (Anzeigen in)**, wie die ausgewählte Ansicht angezeigt werden soll.
8. Wählen Sie unter **Bring to front (In den Vordergrund)** die Option **On trigger bring application to front (Anwendung bei Auslösung in den Vordergrund holen)**, um geöffnete AXIS Camera Station Pro-Clients aus der Taskleiste zu holen oder die Clients bei Starten der Live-Ansichtsaktion in anderen geöffneten Anwendungen einzublenden.
9. Klicken Sie auf **OK**.

Direktübertragungsaktionen	
Ansehen	Zum Öffnen einer Ansicht wählen Sie **View (Ansicht)** und anschließend die gewünschte Ansicht aus dem Dropdown-Menü aus.
Kamera	Zum Öffnen einer Kameraansicht wählen Sie **Camera (Kamera)** und anschließend die gewünschte Kamera aus dem Dropdown-Menü aus. Bei Kameras mit PTZ-Voreinstellung wählen Sie **Go to preset (Zur Voreinstellung wechseln)** und wählen zum Öffnen einer voreingestellten Position einen Bereich aus dem Dropdown-Menü aus.
Keine Aktion	Um keine Ansicht zu öffnen, wählen Sie die Option **No action (Keine Aktion)**.

Shown in (Anzeigen in)	
Registerkarte Live-Warnung	Wählen Sie die Registerkarte **Live alert (Live-Warnung)**, um die ausgewählte Bild- oder Kameraansicht auf der Registerkarte **Live alert (Live-Warnung)** zu öffnen.
Hotspot in view (Hotspot in Ansicht)	Wählen Sie die Option **Hotspot in view (Hotspot in Ansicht)** und anschließend eine Ansicht mit Hotspot aus dem Dropdown-Menü aus. Ist der Hotspot bei Auslösung der Aktion in der Live-Ansicht zu sehen, wird die Kameraansicht im Hotspot angezeigt.

Beispiel:
Wechseln Sie zum Öffnen einer **Live-View**-Registerkarte in die Hotspot-Ansicht, und zeigen Sie im Hotspot eine Kameraansicht an. Konfigurieren Sie hierzu in derselben Aktionsregel zwei Live-Ansichtsaktionen:

1. Erstellen Sie eine Live-Ansichtsaktion zur Anzeige der Hotspot-Ansicht auf der Registerkarte **Live alert (Live-Warnung)**.
   1.1. Wählen Sie unter **Live view actions (Live-Ansichtsaktionen)** die Option **View (Ansicht)**.
   1.2. Wählen Sie die Option **Hotspot view (Hotspot-Ansicht)** aus.
   1.3. Wählen Sie unter **Anzeigen in** die Registerkarte **Live-Alarm**.

1.4. Wählen Sie **Anwendung bei Trigger in den Vordergrund ziehen**.

2. Erstellen Sie eine weitere Live-Ansicht-Aktion, um die Hotspot-Ansicht aufzurufen, und zeigen Sie die Kameraansicht im Hotspot an.
   2.1. Wählen Sie unter **Live-Ansicht-Aktionen** die Option **Kamera** und eine Kameraansicht.
   2.2. Wählen Sie unter **Show in (Anzeigen in)** die Option **Hotspot in view (Hotspot in Ansicht)** aus.
   2.3. Wählen Sie die Option **Hotspot view (Hotspot-Ansicht)** aus.

Aktion "HTTP-Meldung" erstellen

Die Aktion HTTP-Meldung erstellen sendet eine HTTP-Anfrage an einen Empfänger. Der Empfänger kann eine Kamera, eine Türsteuerung, ein externer Webserver oder ein beliebiger Server sein, der HTTP-Anforderungen entgegennehmen kann. HTTP-Benachrichtigungen können z. B. dazu verwendet werden, eine Kamerafunktion ein- oder auszuschalten oder eine mit einer Türsteuerung verbundene Tür zu öffnen, zu schließen, zu verriegeln oder zu entriegeln.

Unterstützte Methoden: GET, POST und PUT.

Hinweis

Um HTTP-Meldungen an Empfänger außerhalb des lokalen Netzwerks zu senden, müssen unter Umständen die Proxy-Einstellungen des AXIS Camera Station Pro-Servers angepasst werden. Weitere Informationen erhalten Sie vom Axis Support.

Aktion "HTTP-Meldung" erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen. Klicken Sie auf **Next (Weiter)**. Siehe *Auslöser hinzufügen*.
4. **Hinzufügen** anklicken und **HTTP-Meldung senden** wählen.
5. Klicken Sie auf **OK**.
6. Geben Sie unter **URL** die Adresse des Empfängers und das Skript ein, das die Anforderung abarbeitet. Zum Beispiel: `https://192.168.254.10/cgi-bin/notify.cgi`.
7. Wählen Sie **Authentifizierung erforderlich**, wenn der Empfänger eine Authentifizierung erfordert. Geben Sie den Benutzernamen und das Kennwort ein.
8. Wählen Sie eine Authentifizierungsmethode aus.
9. Klicken Sie auf **Erweitert**, um die erweiterten Einstellungen anzuzeigen.
10. Klicken Sie auf **OK**.

Authentifizierungsmethode	
Digest	Wir empfehlen die Verwendung dieser Option, da sie den besten Schutz vor Abhören bietet.
Digest mit Basic als Fallback	Verwenden Sie diese Option, wenn Sie nicht sicher sind, welche Authentifizierungsmethode das Gerät verwendet.

Erweitert	
Methode	Wählen Sie im Drop-Down Menü unter **Method (Methodel)** HTTP als Methode aus.
Inhaltstyp	Wählen Sie für die Methoden POST und PUT unter **Content type (Inhaltstyp)** den entsprechenden Inhaltstyp aus dem Dropdown-Menü aus.

Erweitert	
Textkörper	Geben Sie für die Methoden POST und PUT unter **Body (Nachrichtenkörper)** den Nachrichtenkörper der Anforderung ein.
Trigger data (Auslösedaten)	Es besteht auch die Möglichkeit, ebenfalls vordefinierte Auslösedaten aus dem Dropdown-Menü einzufügen. Weitere Informationen siehe unten.

Trigger data (Auslösedaten)	
Typ	Auslöser, der die Aktionsregel aktiviert hat.
Source ID (Quell-ID)	Die Quell-ID bezeichnet die Quelle, welche die Aktionsregel ausgelöst hat, und steht oft für eine Kamera oder einen anderen Gerätetyp. Nicht alle Quellen besitzen eine Quell-ID.
Source Name (Quellname)	Der Quellname bezeichnet die Quelle, welche die Aktionsregel ausgelöst hat, und steht oft für eine Kamera oder einen anderen Gerätetyp. Nicht alle Quellen besitzen einen Quellnamen.
Uhrzeit (UTC)	UTC-Datum und -Uhrzeit der Aktionsregelauslösung.
Time (local) (Uhrzeit (lokal))	Server-Datum und -Uhrzeit der Aktionsregelauslösung.

Aktionen für virtuelle Ein-/Ausgänge erstellen

Verwenden Sie Aktionen für virtuelle Ein-/Ausgänge, um einen bestimmten virtuellen Eingangs-Port eines Geräts auszulösen. Jeder Port eines Geräts kann für eine Aktion verwendet werden.

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen. Klicken Sie auf **Next (Weiter)**. Siehe *Auslöser hinzufügen*.
4. Klicken Sie **Add (Hinzufügen)** an und wählen Sie **Virtual I/O (Virtuelle Ein- und Ausgänge)** aus.
5. Klicken Sie auf **OK**.
6. Wählen Sie das Gerät und den Port aus, den Sie auslösen möchten.
7. Klicken Sie auf **OK**.

Sirenen- und Lichtaktionen erstellen

Sirenen- und Lichtaktionen aktivieren in der AXIS D4100-E Network Strobe Siren ein Sirenen- und Lichtmuster anhand eines konfigurierten Profils.

Hinweis

Um diese Aktion zu verwenden, muss auf der Konfigurationsseite des Geräts ein Profil konfiguriert werden.

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen. Klicken Sie auf **Next (Weiter)**. Siehe *Auslöser hinzufügen*.
4. Klicken Sie auf **Hinzufügen** und wählen Sie **Sirene und Licht**.

5. Klicken Sie auf **OK**.
6. Wählen Sie im Dropdown-Menü unter **Device (Gerät)** ein Gerät aus.
7. Wählen Sie im Dropdown-Menü unter **Profile (Profil)** ein Profil aus.
8. Klicken Sie auf **OK**.

Axis Entry Manager-Aktionen erstellen

Mit AXIS Entry Manager-Aktionen lassen sich Zugänge freigeben oder mit einer in AXIS Entry Manager konfigurierten Türsteuerung verbundene Türen entriegeln oder verriegeln.

Hinweis

AXIS Entry Manager-Aktionen sind nur möglich, wenn die Türsteuerung AXIS A1001 Network Door Controller in AXIS Camera Station Pro verfügbar ist.

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen. Klicken Sie auf **Next (Weiter)**. Siehe *Auslöser hinzufügen*.
4. Klicken Sie auf **Hinzufügen** und wählen Sie **AXIS Entry Manager** aus.
5. Klicken Sie auf **OK**.
6. Wählen Sie eine Aktion und eine Tür aus, um die Aktion durchzuführen.
7. Klicken Sie auf **OK**.

Erstellen von Aktionen zum Versenden von Benachrichtigungen an die mobile App

Mit der Aktion„ Benachrichtigung an mobile App sende"n wird eine benutzerdefinierte Nachricht an die mobile App von AXIS Camera Station gesendet. Klicken Sie auf die eingegangene Benachrichtigung, um eine bestimmte Kameraansicht aufzurufen. Weitere Informationen Finden Sie im *Benutzerhandbuch der mobilen App von AXIS Camera Station*.

Zum Erstellen einer Aktion zum Versenden von Benachrichtigungen an die mobile App:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen. Klicken Sie auf **Next (Weiter)**. Siehe *Auslöser hinzufügen*.
4. Klicken Sie auf **Hinzufügen** und wählen Sie **Benachrichtigung an mobile App senden**.
5. Klicken Sie auf **OK**.
6. Geben Sie unter **Message (Nachricht)** den Nachrichtentext ein, der in der mobilen App angezeigt werden soll.
7. Konfigurieren Sie unter **Click notification and go to (Benachrichtigung anklicken und aufrufen)**, was beim Anklicken der Benachrichtigung angezeigt werden soll.
8. Klicken Sie auf **OK**.

Click notification and go to (Benachrichtigung anklicken und aufrufen)	
Kamera	Wählen Sie im Dropdown-Menü unter **Camera (Kamera)** die Kameraansicht aus, die beim Anklicken der Benachrichtigung in der mobilen App angezeigt werden soll.
Standard	Wählen Sie **Default (Standard)**, um beim Klicken der Benachrichtigung die Startseite der mobilen App aufzurufen.

Aktion erstellen, die andere Aktionsregeln ein- oder ausschaltet

Verwenden Sie Aktionen zur Aktivierung oder Deaktivierung von Aktionsregeln, um z. B. die Bewegungserkennung in einem Büro zu deaktivieren, wenn ein Mitarbeiter seine Zutrittskarte benutzt.

Aktion zur Aktivierung oder Deaktivierung von Aktionsregeln erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen. Klicken Sie auf **Next (Weiter)**. Siehe *Auslöser hinzufügen*.
4. Klicken Sie auf **Hinzufügen** und wählen Sie **Ein- oder Ausschaltregeln**.
5. Klicken Sie auf **OK**.
6. Wählen Sie eine oder mehrere Aktionsregeln.
7. Wählen Sie, ob Sie die ausgewählten Aktionsregeln ein- oder ausschalten möchten.
8. Geben Sie eine Verzögerung ein, wenn zwischen Auslöser und Zustandsänderung eine bestimmte Zeit verstreichen soll.
9. Wählen Sie **Zurück zum vorherigen Status, wenn der Auslöser nicht mehr aktiv ist**, wenn die ausgewählte Aktionsregel bei nicht aktivem Auslöser nicht geändert werden soll. Im obigen Beispiel heißt dies, dass sich die Bewegungserkennung wieder einschaltet, wenn der Mitarbeiter seine Zutrittskarte aus dem Kartenleser zieht.
10. Klicken Sie auf **OK**.

Aktion „Lesezeichen erstellen"

So erstellen Sie eine Aktion „Lesezeichen erstellen":

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen. Klicken Sie auf **Next (Weiter)**. Siehe *Auslöser hinzufügen*.
4. Klicken Sie auf **Add (Hinzufügen)** und wählen Sie die Option **Add bookmark (Lesezeichen hinzufügen)**.
5. Klicken Sie auf **OK**.
6. Konfigurieren Sie das Lesezeichen, indem Sie einen Namen und optional eine Beschreibung eingeben.
7. Klicken Sie auf **OK**.

Eine Aktion erstellen, die eine Ansicht an einen Video-Decoder sendet

Verwenden Sie diese Aktion, um eine Ansicht an einen Video-Decoder zu senden, damit sie für eine bestimmte Zeit auf einem Bildschirm angezeigt wird.

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen. Klicken Sie auf **Next (Weiter)**. Siehe *Auslöser hinzufügen*.
4. Klicken Sie auf **Add (Hinzufügen)** und wählen Sie **Send to video decoder (An Videodecoder senden)**.
5. Klicken Sie auf **OK**.
6. Wählen Sie unter **Decoder** den Video-Decoder aus, an den die Ansicht gesendet werden soll.
7. Wählen Sie unter **View (Ansicht)** die zu sendende Kamera oder Ansicht aus.
8. Geben Sie unter **Duration (Dauer)** die Zeitspanne in Sekunden ein, für die der Bildschirm angezeigt werden soll.

9. Klicken Sie auf **OK**.

Zugangskontroll-Aktion erstellen

Die Aktion Zutrittskontrolle kann die folgenden Aktionen auf einem AXIS Camera Station Secure Entry durchführen:

- **Door actions (Zugangsaktionen):** Zugang gewähren; ausgewählte Zugänge verriegeln, entriegeln, zurücksetzen oder blockieren.
- **Zone actions (Zonenaktionen):** Ausgewählte Zugänge in den ausgewählten Zonen verriegeln, entriegeln, zurücksetzen oder blockieren.
- **Access rule actions (Aktionen für Zugriffsregeln)**: Zugangsregeln aktivieren oder deaktivieren.

Hinweis

Die Aktion Zutrittskontrolle ist nur für ein AXIS Camera Station Secure Entry verfügbar.

Zutrittskontrollaktion erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen. Klicken Sie auf **Next (Weiter)**. Siehe *Auslöser hinzufügen*.
4. Wählen Sie **Zutrittskontrolle** und klicken Sie auf **Weiter**.
5. Klicken Sie auf **OK**.
6. So führen Sie Türaktionen durch:
   6.1. Wählen **Sie unter** "Zugangskontrolle" **die Option Türaktionen** aus.
   6.2. Wählen **Sie unter** "Aktion konfigurieren" die Türen und die Aktion aus.
7. So führen Sie Zonenaktionen durch:
   7.1. Wählen **Sie unter** Zugangskontrolle **Zonenaktionen** aus.
   7.2. Wählen Sie unter **Configure action (Aktion konfigurieren)** die gewünschten Zonen, Zugangarten und Aktionen aus.
8. Zum Aktivieren oder Deaktivieren von Zugangsregeln:
   8.1. Wählen Sie unter **Access control (Zutrittskontrolle) Action rule actions (Zugangsregelaktionen)** aus.
   8.2. Wählen Sie unter **Configure action (Aktion konfigurieren)** die Zugangsregel aus, die Sie aktivieren oder deaktivieren möchten.
   8.3. Wählen Sie unter **Action (Aktion) Enable (Aktivieren)** oder **Disable (Deaktivieren)** aus.
9. Klicken Sie auf **OK**.
- Um einen Bericht als Teil der Aktion zu speichern, wählen Sie **Save report (Bericht speichern)** aus und wählen Sie die gewünschten Berichtseinstellungen.

Erstellung von Aktionen in Audio Manager

So erstellen Sie eine Aktion im Audio Manager:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Klicken Sie auf **Hinzufügen**, um einen neuen Auslöser hinzuzufügen. Klicken Sie auf **Next (Weiter)**. Siehe *Auslöser hinzufügen*.
4. Klicken Sie auf **Add (Hinzufügen)** und wählen Sie **Audio Manager** aus.
5. Klicken Sie auf **OK**.

6. Wählen Sie die auszulösende Aktion aus und konfigurieren Sie diese.
7. Klicken Sie auf **OK**.

Aktionen in Audio Manager	
Audiodatei abspielen	Wählen Sie die Option **Play audio file (Audiodatei abspielen)**, um eine ausgewählte Audiodatei wiederzugeben.
Wiedergabe der Audiodatei beenden	Wählen Sie **Stop audio file (Wiedergabe der Audiodatei beenden)**, um die laufende Wiedergabe einer Audiodatei zu beenden. Die Start-ID muss mit der Start-ID übereinstimmen, die für die Aktion „Play audio file" (Audiodatei abspielen) verwendet wurde.
Ziel aktivieren/deaktivieren	Wählen Sie **Enable or disable target (Ziel aktivieren oder deaktivieren)** aus, um Zielgeräte zu aktivieren oder zu deaktivieren.
Stummschalten	Wählen Sie **Mute volume (Stummschalten)** aus, um den Lautstärkeregler stummzuschalten.
Lautstärke festlegen	Wählen Sie **Set volume (Lautstärke festlegen)** aus, um eine neue Lautstärke festzulegen.
Lautstärke anpassen	Wählen Sie **Offset volume (Lautstärke anpassen)** aus, um die Lautstärke relativ zum aktuellen Pegel zu erhöhen oder zu verringern.

Zeitschemata

Die Seite Zeitpläne enthält alle Zeitpläne, die Sie auf Aufzeichnungen, Aktionsregeln und Komponenten wie AXIS Secure Entry anwenden können. AXIS Site Designer erstellt einige Zeitpläne während der Installation.

Mit der Funktion „Zeitpläne" können Sie individuelle Tages- und Wochenpläne erstellen und bearbeiten sowie Zeitpläne überschreiben. Überschreibungszeitpläne gelten immer täglich, können jedoch an besonderen Tagen wie Feiertagen sowohl auf tägliche Zeitpläne als auch auf wöchentliche Zeitpläne angewendet werden.

Die Registerkarte **Zeitpläne** ist die Hauptansicht für die Verwaltung Ihrer täglichen und wöchentlichen Zeitpläne:

- **Name**: Der Name des Zeitplans.
- **Typ**: Zeigt an, ob es sich bei dem Zeitplan um einen Tages- oder Wochenplan handelt.
- **Wird verwendet**: Zeigt an, ob eine Komponente, eine Aufzeichnungsregel oder eine Aktionsregel derzeit den Zeitplan verwendet.
- **Außer-Kraft-Setzen-Zeitpläne**: Listet auf, welche Außer-Kraft-Setzen-Zeitpläne für diesen Zeitplan gelten.

Die Registerkarte **Zeitpläne außer Kraft setzen** ist die Hauptansicht für die Verwaltung Ihrer Außer-Kraft-Setzen-Zeitpläne, in der Sie sehen können, auf welche Tages- und Wochenzeitpläne sie angewendet wurden.

Hinweis

Bei einer Verbindung zu mehreren AXIS Camera Station Pro-Servern können Sie auf jedem verbundenen Server Zeitpläne hinzufügen und verwalten. Um Ihre Zeitpläne zu verwalten, wählen Sie den entsprechenden Server aus dem Dropdown-Menü unter **Selected server (Ausgewählter Server)** aus.

Verwaltung der Tages- und Wochenzeitpläne

Zur Verwaltung der Tages- und Wochenzeitpläne gehen Sie auf die Registerkarte **Zeitpläne**.

Um einen neuen Tages- und Wochenzeitplan zu erstellen, klicken Sie auf **Neuer Zeitplan**.

Um einen Zeitplan zu löschen, wählen Sie ihn aus der Liste und klicken dann auf **Löschen**. Bevor Sie versuchen, den Zeitplan zu löschen, sollten Sie sich vergewissern, dass er nicht in Gebrauch ist.

Erstellen oder wählen Sie einen Tages- und Wochenzeitplan aus, um dessen Details auf dem Bildschirm anzuzeigen.

- Wenn es sich um einen Tageszeitplan handelt, klicken Sie auf **Daten hinzufügen** , um dem Zeitplan einen neuen Datumsbereich hinzuzufügen. Sie können demselben Zeitplan mehrere Datumsbereiche hinzufügen.
- Um ein Zeitfenster hinzuzufügen, klicken Sie entweder auf **+** oder doppelklicken Sie auf die Zeile.
- Um einen Datumsbereich oder ein Zeitfenster zu bearbeiten, klicken Sie mit der linken Maustaste darauf.
- Um einen Zeitplan hinzuzufügen, wählen Sie ihn aus der Drop-down-Liste aus und klicken Sie auf **Hinzufügen**. Um einen Außer-Kraft-Setzen-Zeitplan zu entfernen, diesen aus der Liste wählen und **Entfernen** anklicken.
- Klicken Sie **Anwenden** an, um Ihre Änderungen zu speichern.

Verwaltung von Außer-Kraft-Setzen-Zeitplänen

- Zur Verwaltung von Außer-Kraft-Setzen-Zeitplänen gehen Sie auf die Registerkarte **Außer-Kraft-Setzen-Zeitpläne**.
- Klicken Sie auf **Daten hinzufügen** , um dem Zeitplan einen neuen Datumsbereich hinzuzufügen. Sie können demselben Außer-Kraft-Setzen-Zeitplan mehrere Datumsbereiche hinzufügen.
- Um ein Zeitfenster hinzuzufügen, klicken Sie entweder auf **+** oder doppelklicken Sie auf die Zeile.
- Um einen Datumsbereich oder ein Zeitfenster zu bearbeiten, klicken Sie mit der linken Maustaste darauf.
- Klicken Sie **Anwenden** an, um Ihre Änderungen zu speichern.

Beispiele für Aktionsregeln

Beispiel: Tür wurde aufgebrochen

Tür wurde aufgebrochen

Das folgende Beispiel zeigt, wie Sie in AXIS Camera Station Pro eine Aktionsregel erstellen, die bei gewaltsamer Öffnung der Eingangstür eine Aufzeichnung und einen Alarm auslöst.

Bevor Sie anfangen, ist eventuell Folgendes erforderlich:

- Installieren Sie einen Axis Netzwerk-Tür-Controller. Siehe *Geräte hinzufügen, on page 46*.
- Konfigurieren Sie den Netzwerk-Tür-Controller. Siehe *Hinzufügen eines Zugangs, on page 152*.

Aktionsregel erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Fügen Sie den Auslöser für das Ereignis eines aufgebrochenen Zugangs hinzu.
   3.1. **Hinzufügen** anklicken und **Gerätereignis** wählen.
   3.2. Klicken Sie auf **OK**.
   3.3. Konfigurieren Sie unter **Configure device event trigger (Geräte-Ereignisauslöser konfigurieren)** den gewünschten Auslöseeinstellungen..
   3.4. Konfigurieren Sie unter **Filters (Filter)** die Filtereinstellungen.
   3.5. Überprüfen Sie unter **Activity (Aktivität)**, ob der Auslöser eine Aktivität auf der Signalleitung anzeigt.
   3.6. Klicken Sie auf **OK**.
4. Klicken Sie auf **Next (Weiter)**.
5. Fügen Sie eine Aufzeichnungsaktion hinzu.

5.1. **Hinzufügen** anklicken und **Live-Ansicht** wählen.

5.2. Klicken Sie auf **OK**.

5.3. Wählen Sie im Dropdown-Menü unter **Camera (Kamera)** eine Kamera aus.

5.4. Konfigurieren Sie unter **Video setting (Videoeinstellung)** das Profil, den Vorpuffer und den Nachpuffer.

5.5. Klicken Sie auf **OK**.

6. Fügen Sie eine Aktion zum Auslösen eines Alarms hinzu.

6.1. **Hinzufügen** anklicken und **Alarm auslösen** wählen.

6.2. Klicken Sie auf **OK**.

6.3. Geben Sie unter **Alarm message (Alarmnachricht)** einen Namen und eine Beschreibung für den Alarm ein. Beispiel: Der Haupteingang wurde aufgebrochen.

6.4. Klicken Sie auf **OK**.

7. Klicken Sie auf **Weiter** und wählen Sie **Always (Immer)** als Zeitplan aus.

8. Klicken Sie auf **Finish** (Fertig).

Geräte-Ereignistrigger konfigurieren	
Gerät	Wählen Sie im Dropdown-Menü unter **Device (Gerät)** den Axis Netzwerk-Tür-Controller aus.
Veranstaltung	Wählen Sie im Dropdown-Menü unter **Event (Ereignis)** die Option **Door > Door forced (Zugang > Unberechtigter Zugang)** aus.
Trigger period (Auslösedauer)	Legen Sie für **Trigger period (Auslöseperiode)** einen Wert von 10 Sekunden fest.

Filter	
Türname	Wählen Sie im Dropdown-Menü unter **Door name (Zugangsname)** den gewünschten Zugangspunkt aus.
Türstatus	Wählen Sie im Dropdown-Menü unter **Door status (Zugangsstatus)** die Option **Forced (Unberechtigt)** aus.

Videoeinstellung	
Profil	Wählen Sie im Dropdown-Menü unter **Profile (Profil)** die Option **High (Hoch)** aus.
Vorpuffer:	Legen Sie für **Prebuffer (Vorpuffer)** einen Wert von 3 Sekunden fest.
Nachpuffer:	Legen Sie für **Postbuffer (Nachpuffer)** einen Wert von 5 Sekunden fest.

Beispiel: Bei Ankunft einer wichtigen Person

Bei Ankunft einer wichtigen Person

Das folgende Beispiel zeigt, wie Sie in AXIS Camera Station Pro eine Aktionsregel erstellen, die eine Begrüßungsansage abspielt und den Aufzug ruft, sobald eine wichtige Person das Gebäude betritt.

Bevor Sie anfangen, ist Folgendes erforderlich:

- Installieren und konfigurieren Sie einen Axis Netzwerk-Tür-Controller und fügen Sie Karteninhaber hinzu. Siehe *Konfigurieren der Zutrittskontrolle, on page 148* und *Zutrittsverwaltung, on page 187*.
- Installieren Sie ein Axis Netzwerk-Audiogerät und verbinden Sie das Audiogerät mit einer Kamera. Siehe *Videostromprofile, on page 54*.
- Installieren Sie das AXIS A9188 Network I/O Relay Module, verbinden Sie den I/O-Anschluss mit dem Fahrstuhl und fügen Sie die I/O-Ports des Netzwerk-I/O-Relaismoduls zu AXIS Camera Station Pro hinzu. Siehe *E/A-Ports, on page 90*.

Aktionsregel erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Auf **Neu** klicken.
3. Fügen Sie einen Geräte-Ereignisauslöser hinzu.
   3.1. **Hinzufügen** anklicken und **Gerätereignis** wählen.
   3.2. Klicken Sie auf **OK**.
   3.3. Konfigurieren Sie unter **Configure device event trigger (Geräte-Ereignisauslöser konfigurieren)** den gewünschten Ereigniseinstellungen.
   3.4. Konfigurieren Sie unter **Filters (Filter)** die Filtereinstellungen.
   3.5. Überprüfen Sie unter **Activity (Aktivität)**, ob der Auslöser eine Aktivität auf der Signalleitung anzeigt.
   3.6. Klicken Sie auf **OK**.
4. Klicken Sie auf **Next (Weiter)**.
5. Fügen Sie eine HTTP-Benachrichtigungsaktion zur Wiedergabe einer Begrüßungsansage hinzu.
   5.1. Klicken Sie auf **Hinzufügen** und wählen Sie **Send HTTP notification (HTTP-Meldung senden)** aus.
   5.2. Klicken Sie auf **OK**.
   5.3. Geben Sie unter **URL** die URL des Audioclips der Begrüßungsansage ein.
   5.4. Wählen Sie **Authentication required (Authentifizierung erforderlich)** aus und geben Sie Benutzername und Kennwort des Audiogeräts ein.
   5.5. Klicken Sie auf **OK**.
6. Fügen Sie eine Aktion zum Einstellen des Ausgangs hinzu.
   6.1. **Hinzufügen** anklicken und **Ausgang einstellen** wählen.
   6.2. Klicken Sie auf **OK**.
   6.3. Wählen Sie im Dropdown-Menü unter **Output port (Ausgangsanschluss)** den Ausgangsanschluss des E/A-Moduls aus, der mit dem Aufzug verbunden ist.
   6.4. Wählen Sie im Dropdown-Menü unter **State on action (Schaltzustand bei Aktion)** den Schaltzustand des E/A-Moduls für die Anforderung des Aufzugs aus.
   6.5. Wählen Sie **Pulse (Impuls)** aus und legen Sie einen Wert von 60 Sekunden fest, für die der Port in diesem Status verbleibt.
   6.6. Klicken Sie auf **OK**.
7. Klicken Sie auf **Weiter** und wählen Sie **Always (Immer)** als Zeitplan aus.
8. Klicken Sie auf **Finish** (Fertig).

Geräte-Ereignistrigger konfigurieren	
Gerät	Wählen Sie im Dropdown-Menü unter **Device (Gerät)** einen Axis Netzwerk-Tür-Controller aus.
Veranstaltung	Wählen Sie im Dropdown-Menü unter **Event (Ereignis)** die Option **Authorization > Access request granted (Autorisierung > Zutrittsanfrage gewährt)**.
Trigger period (Auslösedauer)	Legen Sie für **Trigger period (Auslöseperiode)** einen Wert von 10 Sekunden fest.

Filter	
Türname	Wählen Sie im Dropdown-Menü unter **Door name (Zugangsname)** den gewünschten Zugangspunkt aus.
Door side (Türseite)	Wählen Sie im Dropdown-Menü unter **Door side (Zugangsseite)** die gewünschte Zugangsseite aus.
Kartennummer	Wählen Sie **Card number (Kartennummer)**, und geben Sie die Kartennummer der betreffenden Person ein.

Client konfigurieren

Konfiguration > Client aufrufen, um:

- Clientspezifische Einstellungen wie Design und Sprache bearbeiten. Siehe *Clienteinstellungen, on page 119*.
- Benutzerspezifische Einstellungen wie Benachrichtigungen und Startoptionen bearbeiten. Siehe *Benutzereinstellungen, on page 120*.
- Clientspezifische Einstellungen für das Leistungsverhalten beim Streaming, wie etwa Video-Skalierung und Hardware-Decodierung, anzupassen. Siehe *Streaming, on page 122*.

Clienteinstellungen

Diese Einstellungen greifen für alle AXIS Camera Station Pro Benutzer auf dem Computer. Wechseln Sie zu **Configuration > Client > Client settings (Konfiguration > Client > Client-Einstellungen)**, um die Client-Einstellungen von AXIS Camera Station Pro zu konfigurieren.

Design	
System, Light (Hell), Dark (Dunkel)	Das Design für den Client wählen. **System** ist das Standarddesign für neue Installationen. Wenn Sie **System** wählen, verwendet das System je nach Windows-Systemthema das helle oder dunkle Thema.

Allgemeines	
Anwendung beim Start von Windows ausführen	Aktivieren Sie diese Option, wenn AXIS Camera Station Pro automatisch beim Start von Windows ausgeführt werden soll.

Live-Ansicht	
Kameranamen in Live-Ansichten anzeigen	Anzeige des Kameranamens in der Live-Ansicht.
	Um Aufzeichnungstypen anzuzeigen, schalten Sie **Show recording indicators in live views and maps (In Live-Ansichten und Lageplänen Aufzeichnungsindikatoren anzeigen)** ein.
	Aktivieren Sie die Option **Show event indicators in live views and maps (Ereignisanzeigen in Live-Ansichten und Lageplänen einblenden)**, um anzuzeigen, dass eine durch die Bewegungserkennung oder eine Aktionsregel gestartete Aufzeichnung stattfindet.

Lagepläne	
Allow flashing coverage areas for all maps (Blinkende Erfassungsbereiche für alle Lagepläne zulassen)	Verwenden Sie diese Option, um bei Aktivierung von **Flash (Blinken)** die Blinkfunktion für alle Erfassungsbereiche global zu verbieten oder zu erlauben. Diese globale Einstellung hat keine Auswirkungen auf die lokalen Lageplaneinstellungen. Siehe *Lageplan, on page 22*.

Sprache
Ändern Sie die Sprache des AXIS Camera Station Pro Clients. Die Änderung wird nach dem Neustart des Clients wirksam.

Feedback	
Share anonymous client usage data with Axis Communications to help improve the application and user experience (Anonymisierte Client-Nutzungsdaten zur Verbesserung der Anwendung und Benutzerfreundlichkeit mit Axis Communications teilen)	Teilen Sie anonymisierte Daten mit Axis, um die Benutzerfreundlichkeit zu verbessern. Weitere Informationen zur Optionsänderung für den Server finden Sie unter *Servereinstellungen, on page 127*.

Benutzereinstellungen

Diese Einstellungen gelten für den angemeldeten AXIS Camera Station Pro-Benutzer. Wechseln Sie zu **Configuration > Client > User settings (Konfiguration > Client > Benutzereinstellungen)**, um die Client-Benutzereinstellungen von AXIS Camera Station Pro zu konfigurieren.

Navigationssystem	
Strukturansicht der Navigation	Standardmäßig aktiviert zur Einblendung der Strukturnavigationsleiste mit den entsprechenden Ansichten und Kameras.
Show in navigation (In Navigation anzeigen)	Wählen Sie im Dropdown-Menü aus, ob Ansichten oder Kameras oder beides angezeigt werden sollen.
Beim Navigieren in der Ansicht Dateipfad anzeigen.	Aktivieren Sie diese Option, um den Navigationspfad bei der Navigation in einer geteilten Ansicht oben in der Ansicht anzuzeigen.

Benachrichtigungen	
Benachrichtigung bei Alarm in Taskleiste anzeigen	Aktivieren Sie diese Option, um bei Auslösung eines Alarms eine Benachrichtigung in der Windows-Taskleiste anzuzeigen.
Benachrichtigung für Aufgaben in der Taskleiste anzeigen	Aktivieren Sie diese Option, um eine Benachrichtigung in der Windows-Taskleiste anzuzeigen, wenn jemand eine Aufgabe hinzufügt oder abschließt.
Benachrichtigungen in der Geräteverwaltung anzeigen	Aktivieren Sie diese Option, um Benachrichtigungen anzuzeigen, wenn eine neue Firmware zum Download zur Verfügung steht.
Show intercom notification window (Benachrichtigungsfenster für IP-Türsprechanlage anzeigen)	Aktivieren Sie diese Option, um ein Benachrichtigungsfenster anzuzeigen, wenn jemand die Ruftaste einer verbundenen IP-Türsprechanlage betätigt.

Schnappschuss	
Nachricht bei Aufnahme eines Schnappschusses anzeigen	Aktivieren Sie diese Option, um eine Meldung anzuzeigen, wenn jemand eine Momentaufnahme anfertigt.
Schnappschussordner bei Aufnahme eines Schnappschusses öffnen	Aktivieren Sie diese Option, um den Ordner für Momentaufnahmen zu öffnen, wenn jemand eine Momentaufnahme anfertigt.
Durchblättern	Klicken Sie auf **Browse (Durchsuchen)**, um den den Speicherordner für Momentaufnahmen auszuwählen.

Start	
Im Vollbildmodus starten	Aktivieren Sie diese Option, um AXIS Camera Station Pro im Vollbildmodus zu starten.
Zuletzt verwendete Registerkarten speichern	Aktivieren Sie diese Option, um AXIS Camera Station Pro mit denselben geöffneten Registerkarten, Bild- und Kameraansichten zu starten wie beim letzten Beenden von AXIS Camera Station Pro.
Zuletzt verwendete Monitore speichern	Aktivieren Sie diese Seite, um AXIS Camera Station Pro auf demselben Monitor zu starten, der zuletzt verwendet wurde, als AXIS Camera Station Pro geschlossen wurde.

Hinweis

- Bild- und Kameraansichten werden pro Registerkarte gespeichert. Das System merkt sich nur, wann sich der Client erneut mit demselben Server verbindet.
- Remember tabs in order to remember monitors, views and camera views (Registerkarten zur Abspeicherung von Monitoren, Ansichten und Kameraansichten merken)
- Das System merkt sich keine dynamischen Ansichten, die Sie per Drag&Drop in die Live-Ansicht ziehen.
- Bei Verbindung zu mehreren Servern mit verschiedenen Benutzern wird die Funktion **Remember last used tabs (Zuletzt verwendete Registerkarten merken)** nicht unterstützt.

Alarmton	
Kein Ton	Wählen Sie diese Option, wenn kein Alarmsignalton ausgegeben werden soll.
Signalton	Wählen Sie diese Option, wenn ein typischer Piepton als Alarmsignalton ausgegeben werden soll.
Sound file (Audiodatei)	Klicken Sie auf **Browse (Durchsuchen)**, und wählen Sie die gewünschte Audiodatei aus, wenn Sie einen benutzerdefinierten Alarmsignalton verwenden möchten. Sie können jedes Dateiformat verwenden, das von Windows Media Player unterstützt wird.
Wiedergabe	Klicken Sie auf diese Option, um den Signalton zu testen.

Akustisches Signal bei eingehendem Anruf	
Kein Ton	Wählen Sie diese Option, wenn bei eingehenden Anrufen kein Rufsignalton ausgegeben werden soll.
Signalton	Wählen Sie diese Option, wenn bei eingehenden Anrufen ein typischer Piepton als Rufsignalton ausgegeben werden soll.
Sound file (Audiodatei)	Klicken Sie auf **Browse (Durchsuchen)**, und wählen Sie die gewünschte Audiodatei aus, wenn Sie einen benutzerdefinierten Rufsignalton verwenden möchten. Sie können jedes Dateiformat verwenden, das von Windows Media Player unterstützt wird.
Wiedergabe	Klicken Sie auf diese Option, um den Signalton zu testen.

Merkmale	
Intelligente Suche 1 anzeigen	„Intelligente Suche 1" wird standardmäßig angezeigt. Deaktivieren Sie diese Option, um die Funktion auszublenden.

Warnungsdialoge anzeigen	
Warnung vor ungültigem Zertifikat	Schalten Sie ein, um diese Warnung anzuzeigen, wenn sie zutrifft.

Streaming

Gehen Sie zu **Configuration > Client > Streaming (Konfiguration > Client > Streaming)**, um die Streaming-Optionen des AXIS Camera Station Pro Client zu konfigurieren.

Videoskalierung	
Automatisch skalieren	Wählen Sie diese Option, um das Videobild über die gesamte verfügbare Bildfläche anzuzeigen, ohne das Seitenverhältnis zu verändern oder das Bild zuzuschneiden.
Videobereich ausfüllen (Ränder werden evtl. abgeschnitten)	Wählen Sie diese Option, um das Videobild bei gleichem Seitenverhältnis an die verfügbare Bildfläche anzupassen. Falls die verfügbare Bildfläche ein anderes Seitenverhältnis als das Videobild aufweist, wird das Videobild zugeschnitten.

Hardware-Decodierung	
Modus	• **Automatic (Automatisch)** Verwendung der Grafikkarte zur Dekodierung von Streams mit einer Auflösung über 3840 x 2160 p bei 25 Bildern pro Sekunde (auch als 4K oder UHD bekannt) (sofern unterstützt). • **On (Ein)** Verwendung der Grafikkarte zur Dekodierung von Streams mit einer Auflösung über 1920 x 1080 p bei 25 Bildern pro Sekunde (auch als 1080p oder HD bekannt) (sofern unterstützt). • **Off (Aus)** Die Hardware-Dekodierung ist deaktiviert, und AXIS Camera Station Pro verwendet zur Videodekodierung die CPU.
Grafikkarte	Wählen Sie eine Grafikkarte aus dem Dropdown-Menü aus.

Hinweis

- Bei der Hardware-Dekodierung wird das Videomaterial mithilfe Ihrer Grafikkarte dekodiert. Eine Hochleistungs-Grafikkarte kann mittels Hardware-Dekodierung insbesondere beim Streamen hochauflösender Videobilder die Leistung erhöhen und die CPU-Auslastung verringern. Die Hardware-Dekodierung unterstützt M-JPEG und H.264.
- Bei Kameras mit einer Auflösung unter 1080 p ist auch bei aktivierter Funktion (Einstellung **On**) keine Hardware-Dekodierung möglich.
- Falls Ihre Grafikkarte keine 4K-Dekodierung unterstützt, erfolgt die Hardware-Dekodierung auch bei aktivierter Funktion (Einstellung **On**) nur bei Streams mit einer Auflösung von 1080 p.

Bandbreitennutzung	
Für diesen Client immer das Videostreamprofil Low (Niedrig) verwenden.	Aktivieren Sie diese Option, um für die Live-Ansicht das Videostreamprofil mit niedriger Auflösung zu verwenden. Siehe *Videostromprofile*. Diese Einstellung wirkt sich auf die Videoformate H.264 und M-JPEG aus und reduziert den Bandbreitenbedarf.
Videostreams in inaktiven Tabs unterbrechen	Aktivieren Sie diese Option, um Videostreams in inaktiven Registerkarten zu unterbrechen. Dies reduziert den Bandbreitenbedarf.

PTZ (Schwenken, Neigen, Zoomen)	
Mit dem ersten Klicken Ansicht auswählen statt PTZ zu starten	Aktivieren Sie diese Option, um beim ersten Klick auf die Ansicht die Ansichtsauswahl aufzurufen. Jeder weitere Klick in der Ansicht regelt die PTZ-Steuerung.

Audio	
Push-to-talk release delay (ms) (Freigabeverzögerung für Sprechtaste (ms))	Stellen Sie die Audioübertragungszeit des Mikrofons nach Loslassen der Sprechtaste (**Push-to-talk**) in Millisekunden ein.
Für alle Duplex-Modi die Sprechtaste verwenden	Aktivieren Sie diese Option, um Push-to-Talk in den Betriebsarten Simplex, Halbduplex und Vollduplex zu verwenden.
Audio immer für Gegensprechanlage zulassen	Aktivieren Sie diese Option, um auch dann Gespräche über die Sprechanlage führen und mithören zu können, wenn keine Anrufe von den Sprechstellen eingehen.

Sofortwiedergabe	
Playback duration (s) (Wiedergabedauer (s))	Legen Sie die Wiedergabedauer zwischen 1 und 600 Sekunden fest, um zurück in die Zeitleiste zu springen und sich die Aufzeichnung wiedergeben zu lassen.

Verbundene Dienste konfigurieren

Verbundene Dienste verwalten

Die verbundenen Dienste bieten Ihnen Zugriff auf folgende Informationen:

- Webclient für AXIS Camera Station
- Geräteverwaltung
- Automatische Lizenzverwaltung
- Systemzustand überwachen

Sie müssen Ihr System registrieren und mit einer Organisation verbinden, um auf die verbundenen Dienste zu zugreifen. Weitere Informationen finden Sie unter *Registrieren Sie Ihr System bei einer Organisation, on page 125*.

Status	Die Statuskarte zeigt den Status der Verbindung zwischen dem Server und den verbundenen Diensten sowie den Namen der Organisation, mit der Sie registriert sind oder mit der Sie verbunden sind.
Verbindung trennen	Wenn Sie die Verbindung zu einem verbundenen Server trennen, ist er noch bei der Organisation registriert.

Lizenzverwaltung	Aktivieren Sie **License management (Lizenzverwaltung)**, um Ihre Lizenzen automatisch zu synchronisieren. Das bedeutet, dass das System Änderungen, die sich auf die Anzahl der Lizenzen auswirken, an AXIS License Manager übermittelt und einen neuen Lizenzstatus abruft. Schalten Sie die Option **License management (Lizenzverwaltung)** aus, um die Lizenzen manuell zu verwalten, z. B. wenn Ihr System nicht über eine Internetverbindung verfügt. Weitere Informationen finden Sie unter *Lizenzen verwalten, on page 137*.
Synchronize system (System synchronisieren)	Schalten Sie die Option **Synchronize system (System synchronisieren)** ein, um Ihre Geräte und Ansichten automatisch mit dem Webclient für AXIS Camera Station und AXIS Device Manager zu synchronisieren.

Registrieren Sie Ihr System bei einer Organisation

So registrieren Sie das System:

1. Rufen Sie **Configuration (Konfiguration)** > **Connected services (Verbundene Dienste)** > **Management (Verwaltung)** auf.
2. Klicken Sie auf die Schaltfläche **Register (Registrieren)** und befolgen Sie die angezeigten Anweisungen.

Weitere Informationen dazu, was beim Registrieren Ihres Systems zu beachten ist, finden Sie in der *Installations- und Migrationsanleitung zu AXIS Camera Station Pro*.

Einstellungen zum Aktualisieren der Firmware

Hinweis

Bei einer Verbindung zu mehreren AXIS Camera Station Pro-Servern wählen Sie zur Einstellung der Firmware-Aktualisierung einen beliebigen Server aus dem Dropdown-Menü unter **Selected server (Ausgewählter Server)** aus.

1. Gehen Sie zu **Konfiguration > Verbundene Dienste > Firmwareaktualisierungseinstellungen**.
2. Konfigurieren Sie unter **Automatic check for updates (Automatisch nach Aktualisierungen suchen)**, wie und wie häufig nach Firmware-Aktualisierungen gesucht werden soll.
3. Konfigurieren Sie unter **Upgrade (Aktualisierungsreihenfolge)** die Reihenfolge, in der die Geräte aktualisiert werden sollen.

Automatisch nach Aktualisierungen suchen	
Check for updates (Nach Aktualisierungen suchen)	Wählen Sie im Dropdown-Menü die Option **Every start-up (Bei jedem Start)** aus, um bei jedem Start nach verfügbaren Firmware-Versionen auf dem Server zu suchen. AXIS Camera Station Pro ist standardmäßig auf **Never (Nie)** eingestellt.
Check now (Jetzt prüfen)	Hiermit kann der Server nach verfügbaren Firmware-Versionen durchsucht werden.

Upgrade-Reihenfolge	
Parallel	Wählen Sie diese Option, um alle Geräte gleichzeitig zu aktualisieren. Diese Option ist schneller als **Sequential (Nacheinander)**, jedoch sind dabei alle Geräte gleichzeitig offline.
Sequentiell	Wählen Sie diese Option, um die Geräte nacheinander zu aktualisieren. Diese Option dauert länger, jedoch sind dabei nicht alle Geräte gleichzeitig offline. Wählen Sie **Cancel remaining upgrades (Verbleibende Aktualisierungen abbrechen)**, wenn die sukzessive Aktualisierung eines Geräts nicht beendet werden kann.

Automatische Firmware-Suche einschalten

Axis Secure Remote Access v2

Axis Secure Remote Access v2 ermöglicht den Zugriff auf AXIS Camera Station Pro über sichere und verschlüsselte Internetverbindungen.

Hinweis

Axis Secure Remote Access v2 ist für die AXIS Camera Station Pro Version 6.8 oder höher verfügbar.

So aktivieren Sie Axis Secure Remote Access v2:

1. Registrieren Sie Ihren Server bei einer Organisation. Siehe *Registrieren Sie Ihr System bei einer Organisation, on page 125*.
2. Melden Sie sich mit Axis Secure Remote Access v2 an. Siehe *Bei AXIS Secure Remote Access v2 anmelden, on page 10*.

So beschränken Sie den Zugriff ausschließlich auf AXIS Camera Station Pro Server:

1. Gehen Sie in My Systems zu **Organization (Organisation) > Users (Benutzer)**.
2. Wählen Sie den Benutzer aus, den Sie konfigurieren möchten.
3. Klicken Sie auf **Roles and access (Rollen und Zugriff)**.
4. Weisen Sie die Rolle **„ACS Pro Secure Remote Access" (Sicherer Fernzugriff auf ACS Pro)** zu. Diese Rolle beschränkt den Zugriff ausschließlich auf AXIS Camera Station Pro Server, ohne den Zugriff auf andere My Systems-Funktionen von Axis zu erlauben.

Nach der Registrierung können Sie die Zugriffsberechtigungen weiter verwalten, indem Sie über Axis My Systems Benutzerrollen für Organisationen zuweisen. Weitere Informationen zu AXIS Camera Station Pro Benutzerrechten finden Sie unter *Benutzerberechtigungen, on page 138*.

Cloud-Speicherung

AXIS Camera Station Cloud Storage ist ein lizenzierter Dienst, mit dem Sie Ihre Aufzeichnungen in der Cloud speichern können. Weitere Informationen finden Sie unter *AXIS Camera Station Cloud Storage - Benutzerhandbuch*.

Bevor Sie den Cloud-Speicher nutzen können, müssen Sie Ihr System in den verbundenen Diensten registrieren. Sobald Sie Ihr System registriert haben, können Sie den Cloud-Speicher für Ihre Kameras unter „My Systems" verwalten.

Server konfigurieren

Servereinstellungen

Rufen Sie **Configuration > Server > Settings (Konfiguration > Server > Einstellungen)** auf, um die Server-Einstellungen von AXIS Camera Station Pro zu konfigurieren.

Hinweis

Bei einer Verbindung zu mehreren AXIS Camera Station Pro-Servern wählen Sie zur Konfiguration der Server-Einstellungen einen beliebigen Server aus dem Dropdown-Menü **Selected server (Ausgewählter Server)** aus.

Exportieren	
Audio einschließen, wenn Aufzeichnungen zum Export hinzugefügt werden	Wählen Sie aus, ob beim Hinzufügen von Aufzeichnungen zur Exportliste auch die Audiospur miteingeschlossen werden soll.

Protokolle

Geben Sie an, wie lange Alarme, Ereignisse und Audits vorgehalten werden sollen. Geben Sie einen Wert zwischen 7 und 1000 Tagen ein.

Um Protokolle kontinuierlich in Echtzeit in eine Datei zu schreiben, damit sie von Drittanbietersystemen wie Splunk, Elastic oder einem SIEM-Tool verarbeitet werden können, wählen Sie **Write audit logs to file (Auditprotokolle in Datei schreiben)**, **Write event logs to file (Ereignisprotokolle in Datei schreiben)** oder beides.

Der Server schreibt Protokolleinträge in `C:\ProgramData\Axis Communications\AXIS Camera Station\Core\Server\Logs`. Die Dateien liegen im Klartext vor und werden aus den Systemberichten ausgeschlossen.

Datei	Beschreibung
`AcsService.exe.audit.log.export`	Einträge im Prüfprotokoll
`AcsService.exe.event.log.export`	Einträge im Ereignisprotokoll

Externe Daten

Geben Sie die Anzahl der Tage an, für die die externen Daten gespeichert werden sollen. Geben Sie einen Wert zwischen 1 und 1000 Tagen ein.

SMTP-Server

Fügen Sie SMTP-Server hinzu, um bei Systemalarmen oder Aktivierung einer Ereigniskonfigurationsregel E-Mails zu versenden.

Einen SMTP-Server hinzufügen:

1. Klicken Sie unter **SMTP servers (SMTP-Server)** auf **Add (Hinzufügen)**.
2. Konfigurieren Sie unter **Server** die Serveradresse, den Port, die Authentifizierung und das TLS-Protokoll.
3. Geben Sie unter **Sender (Absender)** die E-Mail-Adresse und den Namen ein, die in der E-Mail des Absenders angezeigt werden sollen.

Server	
Adresse	Geben Sie die-Adresse des SMTP-Servers ein.
Port	Geben Sie den Port ein. 587 ist der Standardport für SMTP-TLS-Verbindungen.
TLS verwenden	Wählen Sie diese Option, wenn der SMTP-Server TLS verwendet. Das Standardprotokoll ist TLS.
Authentifizierung durchführen	Aktivieren Sie diese Option, wenn für den Server ein Benutzername und ein Kennwort erforderlich sind. Geben Sie den Benutzernamen und das Kennwort für den Server-Zugriff ein.

Bearbeiten	Um einen SMTP-Server zu ändern, wählen Sie den Server aus und klicken Sie auf **Bearbeiten**.
Entfernen	Um einen SMTP-Server zu entfernen, wählen Sie den Server aus und klicken Sie auf **Entfernen**. Wählen Sie **Ja** in dem Dialogfenster, um den Server zu löschen.
Alle testen	Um einen SMTP-Server zu testen, wählen Sie den entsprechenden Server aus und klicken auf **Test all... (Alle testen)**. Geben Sie im Popup-Dialogfeld unter **Recipient (Empfänger)** eine E-Mail-Adresse ein, und klicken Sie auf **OK**, um eine Test-E-Mail zu versenden. Der SMTP-Server fragt testweise eine Liste von Ergebnissen und möglichen Aktionen ab.
Pfeiltasten	Wählen Sie einen Server aus, und verwenden Sie die Pfeile, um die Server-Reihenfolge in der Liste zu ändern. Das System verwendet die Server in der Reihenfolge, in der sie aufgelistet sind.

Server-Testergebnisse	
OK	Die Verbindung mit dem SMTP-Server konnte hergestellt werden. Stellen Sie sicher, dass die Empfänger die Test-E-Mail erhalten.
Unbekannter Fehler	Beim Versuch, die E-Mail zu versenden, ist ein unerwarteter Fehler aufgetreten. Prüfen Sie, dass der SMTP-Server korrekt funktioniert.
Keine Verbindung	AXIS Camera Station Pro kann nicht auf den SMTP-Server zugreifen. Stellen Sie sicher, dass der SMTP-Server ordnungsgemäß funktioniert und alle Router und Proxy-Server den Datenverkehr zwischen AXIS Camera Station Pro und SMTP-Server gestatten.
Konfigurationsfehler	TLS wurde angefordert, aber der Server unterstützt keine StartTLS, keine Authentifizierung oder keinen kompatiblen Authentifizierungsmechanismus.
TLS/SSL-Handshake-Fehler	Fehler bei der TLS/SSL-Verschlüsselung, z. B. ungültiges Serverzertifikat.
Authentifizierung erforderlich	Der Server benötigt zum Senden von E-Mails eine Authentifizierung.

Server-Testergebnisse	
Authentifizierungsfehler	Falsche Zugangsdaten.
Verbindung unterbrochen	Es wurde eine Verbindung hergestellt, die jedoch unterbrochen wurde.

Systemalarm

Ein Systemalarm wird ausgelöst bei Verbindungsabbruch zu einer Kamera, Verweigerung des Zugriffs auf einen Aufzeichnungsspeicher, unerwartetem Herunterfahren des Servers oder Aufzeichnungsfehlern. Bei Systemalarmen ist ein Versand von E-Mail-Benachrichtigungen möglich.

Hinweis

Um E-Mails versenden zu können, müssen Sie zunächst einen SMTP-Server hinzufügen.

E-Mail-Benachrichtigung bei Systemalarm senden:

1. Aktivieren Sie **Bei Systemalarm E-Mails an folgende Empfänger senden**, um die Systemalarm-E-Mail zu aktivieren.
2. Unter **Recipients (Empfänger)**:
   2.1. Wählen Sie aus, ob die Adresse in das Feld **To (An)**, **Cc (Kopie)** oder **Bcc (Blindkopie)** der E-Mail eingetragen werden soll.
   2.2. Geben Sie die E-Mail-Adresse ein.
   2.3. Klicken Sie auf **Hinzufügen**, um die E-Mail-Adresse in das Feld **Empfänger** einzufügen.

Verbindung zum Gerät	
Wenn möglich, Hostnamen statt IP-Adresse für neu hinzugefügte Geräte verwenden	Verwenden Sie nach Möglichkeit den Host-Name, um eine Verbindung zu neu hinzugefügten Geräten herzustellen. Ist kein Host-Name verfügbar, wird stattdessen die IP-Adresse verwendet.
Verwenden Sie die Hostnamen auch dann weiter, wenn Sie nicht erreichbar werden	Verwenden Sie für den Verbindungsaufbau den Hostnamen. Für die automatische Umschaltung auf einen Verbindungsaufbau über die IP-Adresse deaktivieren Sie das Kontrollkästchen. Sie können manuell auswählen, ob der Hostname oder die IP-Adresse für die Verbindung mit Geräten verwendet werden soll. Siehe *Verbindung, on page 71*.

Sprache	
Sprache des Servers ändern	Ändert den Namen der AXIS Camera Station Pro Service Control und AXIS Camera Station Secure Entry. Zum Beispiel: Systemalarme, Audit-Protokollmeldungen und externe Daten auf der Registerkarte **Data search (Datensuche)**. Die Änderung wird nach dem Neustart wirksam.

Body Worn	
Laufwerk **Ordner**	Wählen Sie das Laufwerk und den Ordner aus, in dem Sie abgelehnte Inhalte aus dem Body Worn-System empfangen möchten. Weitere Informationen finden Sie unter *Übertragung von Aufzeichnungen in einen Speicher für abgelehnte Inhalte im Benutzerhandbuch AXIS Body Worn Solution*.
Anzahl der Tage, die abgelehnte Inhalte aus dem Body Worn-System behalten werden sollen.	Dies ist die Verweildauer abgelehnter Inhalte.

Feedback	
Axis Communications die Nutzung anonymisierter Server-Daten gestatten	Wählen Sie diese Option, um uns bei der Verbesserung der Anwendung und der Benutzerfreundlichkeit zu unterstützen. Weitere Informationen zur Optionsänderung für den Client finden Sie unter *Clienteinstellungen, on page 119*.

Erweiterte Einstellungen

Die Einstellungen sollten nur auf Anweisung des Axis Supports geändert werden. Um eine erweiterte Einstellung zu ändern:

1. Die Einstellung und ihren Wert eingeben.
2. Klicken Sie auf **Hinzufügen**.

Zur Aktivierung der Debug-Protokollierung zur Fehlerbehebung wählen Sie **Enable server side debug logging (Serverseitige Fehlerprotokollierung aktivieren)**. Diese Einstellung beansprucht mehr Speicherplatz auf Ihrer Festplatte und wird von der Datei `log4net.config` im Verzeichnis **ProgramData** überschrieben.

Weitere Informationen finden Sie unter *Erweiterte Servereinstellungen in der Übersicht zur Fehlersuche der AXIS Camera Station Pro*.

Komponenten

Komponenten sind Softwaremodule, die Ihrem System weitere Funktionen hinzufügen. Auf der Komponentenseite können Sie Komponenten verwalten und deren Status anzeigen.

So sehen Sie die Liste der installierten Komponenten an:

1. Rufen Sie **Configuration > Server > Components (Konfiguration > Server > Komponenten)** auf.
2. Aktivieren Sie **Show components (Komponenten anzeigen)**.

Hinweis

Wir berücksichtigen die erweiterten Einstellungen der Komponenten. Komponenten nur anzeigen und verwalten, wenn Sie Kontakt mit dem Axis Support haben.

AXIS Camera Station Pro aktualisieren

Aktualisieren auf die neueste Version von AXIS Camera Station Pro:

1. Wechseln Sie zu **Configuration > Server > Update (Konfiguration > Server > Aktualisierung)**.
2. Klicken Sie auf **Download and install... (Herunterladen und installieren...)**.

Hinweis

- Eine einmal – manuell oder zeitgeplant – gestartete Aktualisierung kann nicht mehr abgebrochen werden.
- Geplante Aktualisierungen starten automatisch.
- Aktualisieren Sie in einem Multi-Server-System immer den lokalen Server zuletzt.
- Wenn Sie den lokalen Server aktualisieren, werden der Client und die Dienststeuerung vorübergehend ausgesetzt. Während der Aktualisierung wird keine Benutzeroberfläche und kein Fortschrittsindikator angezeigt. Lassen Sie den Servercomputer eingeschaltet, bis sowohl der Client als auch der Server neu gestartet sind.

Vorfallbericht

Bei Berechtigungserteilung zur Erstellung von Vorfallsberichten können Sie Vorfallsberichte mit Aufzeichnungen, Momentaufnahmen und Notizen zu den jeweiligen Vorfällen erstellen. Siehe *Vorfallsberichte exportieren, on page 33*.

Um die Einstellungen für Vorfallsberichte zu konfigurieren:

1. **Configuration > Server > Incident report (Konfiguration > Server > Vorfallsbericht)** aufrufen.
2. Wählen Sie unter **Location (Speicherort)** den Speicherort der Vorfallberichte aus.
3. Wählen Sie aus der Dropdown-Liste unter **Export format (Exportformat)** ein Format aus, in das Sie Ihre Aufzeichnungen exportieren möchten.
4. Um Vorfallsberichte Gruppen zuzuordnen, unter **Categories (Kategorien)** entsprechend Kategorien hinzufügen oder löschen. Als Kategorien können Ordnernamen das Exportzielorts verwendet werden, sofern diese im Ordnerverzeichnis des Servers als Variable konfiguriert sind.
   4.1. Den Namen der Kategorie in das Feld eingeben. Beispiele sind: Unfall oder Diebstahl.
   4.2. Klicken Sie auf **Hinzufügen**.
   4.3. Um eine Kategorie zu entfernen, diese wählen und **Remove (Entfernen)** anklicken.
5. Geben Sie unter **Description template (Beschreibungsvorlage)** alle Informationen ein, die bei der Erstellung Ihrer Vorfallsberichte in der Beschreibung (**Description**) angezeigt werden sollen. Zum Beispiel: Erstellt von: <Name, E-Mail-Adresse und Telefonnummer eingeben>.
6. Klicken Sie auf **Anwenden**.

Standort	
Server directory path (Server-Verzeichnispfad)	Wählen Sie diese Option, um Ihre Vorfallsberichte in einem Ordner auf dem Rechner zu speichern, und geben Sie den entsprechenden Verzeichnispfad ein. Servername, Kategorie oder Benutzername können dabei als Variablen definiert werden. Zum Beispiel: `C:\Reports\$(Server Name)\$(Category)\$(User Name)\`.
Network directory path (Netzwerk-Verzeichnispfad)	Wählen Sie diese Option, um Ihre Aufzeichnungen im Ordner eines Netzwerkspeichers zu speichern. Geben Sie den Verzeichnispfad ein, oder verwenden Sie die Zugangsdaten für den Netzwerkspeicher. Die Netzwerk-Freigabe muss vom AXIS Camera Station Pro-Server erreichbar sein. Für weitere Informationen zum Hinzufügen von Aufzeichnungsspeicher, siehe *Speicher verwalten*.

Exportformat	
ASF	Bei Auswahl dieser Option können Sie mit **Add digital signature (Digitale Signatur hinzufügen)** eine digitale Signatur hinzufügen, um Bildmanipulationen auszuschließen. Siehe dazu den Abschnitt Digitale Signatur in *Aufzeichnungen exportieren*. Sie können auch **Use password (Kennwort verwenden)** wählen, um ein Kennwort für die digitale Signatur zu verwenden.
MP4	Exportierte Aufzeichnungen enthalten kein Audio im Format G.711 oder G.726.

Geplanter Export

Wechseln Sie zu **Configuration > Server > Scheduled export (Konfiguration > Server > Geplanter Export)**, um den Export von Aufzeichnungen zeitlich zu planen.

Zum gewählten Zeitpunkt startet ein Export aller Aufzeichnungen, die nach dem vorhergehenden Export erstellt wurden. Ist der letzte Export älter als eine Woche oder kein früherer Export vorhanden, umfasst der Export nur Aufzeichnungen, die weniger als eine Woche zurückliegen. Um ältere Aufzeichnungen zu exportieren, wechseln Sie auf die Registerkarte **Recordings (Aufzeichnungen)** und exportieren diese manuell. Siehe *Aufzeichnungen exportieren*.

Hinweis

Bei einer Verbindung zu mehreren AXIS Camera Station Pro-Servern wählen Sie zur Aktivierung und Verwaltung der geplanten Exporte einen beliebigen Server aus dem Dropdown-Menü unter **Selected server (Ausgewählter Server)** aus.

Geplanter Export von Aufzeichnungen

1. Wählen Sie unter **Scheduled export (Geplanter Export)** die Option **Enable scheduled export (Geplanten Export aktivieren)**, um Aufzeichnungen geplant zu exportieren.
2. Unter **Cameras (Kameras)** wählen Sie mit den Kontrollkästchen, von welchen Kameras die Aufzeichnungen exportiert werden sollen. Das System wählt standardmäßig alle aufgelisteten Kameras aus. Deaktivieren Sie **Use all cameras (alle Kameras verwenden)**, und wählen Sie die gewünschten Kameras aus der Liste aus.
3. Konfigurieren Sie unter **Export (Exportieren)** den Speicherort der Aufzeichnungen, das Format und die Erstellung der Wiedergabeliste.
4. Wählen Sie unter **Weekly schedule (Wöchentlicher Zeitplan)** die Uhrzeit und die Tage aus, an denen die Aufzeichnungen exportiert werden sollen.
5. Klicken Sie auf **Anwenden**.

Exportieren	
Server directory path (Server-Verzeichnispfad)	Wählen Sie diese Option, um Ihre Aufzeichnungen in einem Ordner auf dem Rechner zu speichern, und geben Sie den entsprechenden Verzeichnispfad ein.
Network directory path (Netzwerk-Verzeichnispfad)	Wählen Sie diese Option, um Ihre Aufzeichnungen im Ordner eines Netzwerkspeichers zu speichern. Geben Sie den Verzeichnispfad ein, oder verwenden Sie die Zugangsdaten für den Netzwerkspeicher. Die Netzwerk-Freigabe muss vom AXIS Camera Station Pro-Server erreichbar sein. Für weitere Informationen zum Hinzufügen von Aufzeichnungsspeicher, siehe *Speicher verwalten*.

Exportieren	
Titelliste erstellen (.asx)	Wählen Sie diese Option, um eine Wiedergabeliste in dem von Windows Media Player verwendeten .asx-Format zu erstellen. Die Aufzeichnungen werden in der Reihenfolge wiedergegeben, in der sie aufgezeichnet wurden.
Exportformat	Wählen Sie ein Format aus, in das Ihre Aufzeichnungen exportiert werden sollen. **ASF** – Wählen Sie **Add digital signature (Digitale Signatur hinzufügen)**, um Bildmanipulationen durch eine digitale Signatur auszuschließen. Siehe dazu den Abschnitt Digitale Signatur in *Aufzeichnungen exportieren*. Sie können auch **Use password (Kennwort verwenden)** wählen, um ein Kennwort für die digitale Signatur zu verwenden. **MP4** – Exportierte Aufzeichnungen enthalten kein Audio im Format G.711 oder G.726.

Microsoft Windows 2008 Server

Um Aufzeichnungen von einem Server zu exportieren, der unter Microsoft Windows 2008 Server läuft, müssen Sie Desktop Experience installieren:

1. Klicken Sie auf **Start > Verwaltung > Server-Manager**, um Server-Manager zu öffnen.
2. Klicken Sie unter **Features Summary (Funktionsübersicht)** auf **Add features (Funktionen hinzufügen)**.
3. Wählen Sie **Desktop Experience**, und klicken Sie auf **Next (Weiter)**.
4. **Install (Installieren)** anklicken.

Microsoft Windows 2012 Server

Um Aufzeichnungen von einem Server zu exportieren, der unter Microsoft Windows 2012 Server läuft, müssen Sie Desktop Experience installieren:

1. Klicken Sie auf **Start > Verwaltung > Server-Manager**, um Server-Manager zu öffnen.
2. Wählen Sie **Verwalten > Rollen und Features hinzufügen**, um den Assistenten zum Hinzufügen von Rollen und Funktionen auszuführen.
3. Wählen Sie unter **Features Summary (Funktionsübersicht)** die Option **User Interfaces and Infrastructure (Benutzerschnittstellen und Infrastruktur)**.
4. Wählen Sie **Desktop Experience**, und klicken Sie auf **Next (Weiter)**.
5. **Install (Installieren)** anklicken.

WebRTC-Einstellungen

Der Webclient für AXIS Camera Station verwendet WebRTC zur Kommunikation mit dem Server.

TURN aktivieren	Diese Option aktiviert einen lokalen TURN-Server auf dem AXIS Camera Station Pro-Server. Wählen Sie **Enable TURN (TURN aktivieren)**, wenn die WebRTC-Kommunikation über einen einzelnen Port ermöglicht werden soll, was die Konfiguration der Firewall vereinfachen kann.
Prioritize TURN (TURN priorisieren)	Wählen Sie diese Option aus, wenn WebRTC nur Relaiskandidaten in Betracht ziehen soll.

Neue Verbindung

Um eine Verbindung mit einem AXIS Camera Station Pro Server herzustellen, > **Servers > New connection (Server > Neue Verbindung)** aufrufen. Siehe *Mit einem Server verbinden*.

Verbindungsstatus

Rufen Sie > **Servers > Connection status (Server > Verbindungsstatus)** auf, um eine Übersicht über den Verbindungsstatus der Server anzuzeigen.

Verwenden Sie zur Herstellung oder Trennung der Verbindung zum Server den Schieberegler vor dem Servernamen.

Statuscodes	Beschreibung	Mögliche Lösungen
Verbindung wird hergestellt	Der Client versucht, eine Verbindung zu diesem Server aufzubauen.	
Verbunden	Der Client ist über TCP mit dem Server verbunden.	
Verbunden (Axis Secure Remote Access v2)	Der Client ist über Axis Secure Remote Access v2 mit dem Server verbunden.	
Verbunden (HTTP)	Der Client ist über HTTP mit dem Server verbunden. Diese Verbindungsart ist nicht ganz so leistungsfähig wie TCP und bei einer Verbindung zu mehreren Servern langsamer.	
Wird getrennt	Der Client trennt die Verbindung zu diesem Server.	
Getrennt	Keine Verbindung zwischen Client und Server.	
Erneut verbinden	Der Client hat die Verbindung zu diesem Server unterbrochen und versucht, erneut eine Verbindung herzustellen.	
Erneute Verbindung fehlgeschlagen	Der Client kann keine neue Verbindung zu diesem Server herstellen. Er finden den Server, aber möglicherweise haben sich die Benutzerberechtigungen oder das Kennwort geändert.	• Fügen Sie den Benutzer im Dialog Benutzerberechtigung hinzu. • Prüfen Sie den Benutzernamen und das Kennwort.
Anmeldung abgebrochen	Der Benutzer hat den Anmeldevorgang abgebrochen.	
Falscher Benutzername oder falsches Kennwort	In der Spalte **Action (Aktion)** den Link anklicken und die korrekten Angaben eingeben.	
Benutzer hat keine Berechtigung auf dem Server	Der Server verwehrt die Anmeldung des Benutzers.	Fügen Sie den Benutzer im Dialog Benutzerberechtigung hinzu.

Sicherheitsüberprüfung fehlgeschlagen	Eine WCF-bezogene Sicherheitsprüfung ist fehlgeschlagen. Stellen Sie sicher, dass die UTC-Zeit des Client- und des Server-Rechners synchronisiert ist.	
Keine Verbindung mit dem Server-Computer	Unter der verwendeten Adresse keine Antwort vom Server-Computer.	• Überprüfen Sie das Netzwerk auf einwandfreie Funktion. • Prüfen Sie, ob der Server läuft.
Kein Server läuft	Der Rechner, auf dem der Server läuft, ist erreichbar, aber der Server wird nicht ausgeführt.	Starten Sie den Server.
Kommunikationsfehler	Ausfall der Verbindung zum Server. Stellen Sie sicher, dass auf den Server-Computer zugegriffen werden kann.	• Überprüfen Sie das Netzwerk auf einwandfreie Funktion. • Prüfen Sie, ob der Server läuft.
Ungültiger Hostname	Das DNS kann den Hostnamen nicht in eine IP-Adresse übersetzen.	• Die korrekte Schreibweise des Hostnamens überprüfen. • Prüfen Sie, dass der DNS über die erforderlichen Informationen verfügt.
Bereits mit demselben Server verbunden	Der Client ist bereits mit diesem Server verbunden.	Entfernen Sie den doppelten Servereintrag.
Nicht der erwartete Server	Unter dieser Adresse hat ein anderer als der erwartete Server geantwortet.	Aktualisieren Sie die Serverliste, um sich mit diesem Server zu verbinden.
Client-Version (x) ist nicht mit Server-Version (y) kompatibel	Der Client ist im Vergleich zum Server zu alt oder zu neu.	Stellen Sie sicher, dass sowohl auf dem Client- als auch dem Server-Rechner die gleiche Version von AXIS Camera Station Pro installiert ist.
Server zu beschäftigt	Keine Server-Antwort aufgrund von Leistungsproblemen.	Stellen Sie sicher, dass der Server-Rechner und das Netzwerk nicht überlastet sind.

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

Mehrere Server

Serverlisten

Sie können Ihre AXIS Camera Station Pro Server in Serverlisten organisieren. Ein Server kann mehreren Server-Listen angehören. Serverlisten können importiert, exportiert und in anderen AXIS Camera Station Pro Clients verwendet werden.

Rufen Sie > **Servers > Server lists (> Server > Serverlisten)** auf, um das Dialogfenster zu den Serverlisten zu öffnen.

Es erscheint die Standardliste **Recent connections (Letzte Verbindungen)** mit den in der letzten Sitzung verwendeten Servern. Die Einträge in der Liste **Recent connections (Letzte Verbindungen)** können nicht gelöscht werden.

	Wählen Sie die Server-Liste aus und klicken Sie auf .
+ New server list (Neue Server-Liste hinzufügen)	Klicken Sie auf diese Option, um eine neue Server-Liste hinzuzufügen, und geben Sie einen Namen für die Liste ein.
Hinzufügen	Um einer Serverliste einen Server hinzuzufügen, wählen Sie eine Server-Liste aus und klicken auf „Add" (Hinzufügen). Geben Sie erforderlichen Informationen ein.
Export Lists (Listen exportieren)	Mit dieser Option können Sie alle Server-Listen in eine .msl-Datei exportieren. Sie können die Server-Liste importieren, um sich auf den Servern anzumelden. Siehe *Mit einem Server verbinden*.
Bearbeiten	Um Server in einer Serverliste zu bearbeiten, wählen Sie einen Server aus und klicken auf **Edit (Bearbeiten)**. Sie können jeweils nur einen Server bearbeiten.
Entfernen	Um Server aus einer Serverliste zu löschen, wählen Sie die entsprechenden Server aus und klicken auf **Remove (Entfernen)**.
Server umbenennen	Doppelklicken Sie auf die Liste, und geben Sie einen neuen Listennamen ein.

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

Server in Server-Listen organisieren

Switch konfigurieren

Sollten Sie ein Gerät der Serie AXIS Camera Station S22 Appliance besitzen, besteht die Möglichkeit, das Gerät über AXIS Camera Station Pro zu konfigurieren. Rufen Sie **Configuration > Switch > Management (Konfiguration > Switch > Verwaltung)** auf und geben Sie Ihre Zugangsdaten ein, um die Switch-Verwaltungsseite im AXIS Camera Station Pro Client zu öffnen. Informationen zur Switch-Konfiguration finden Sie im Benutzerhandbuch für Geräte der Serie AXIS Camera Station S22 Appliance auf *axis.com*.

Hinweis

AXIS Camera Station Pro kann nur eine Verbindung zu https://192.168.0.1/ herstellen. Dies ist die Standard-IP-Adresse des Switches.

Lizenzen verwalten

Auf der Seite „Manage licenses" (Lizenzen verwalten) wird der aktuelle Lizenzstatus angezeigt.

Test	Bei der Installation von AXIS Camera Station Pro erhalten Sie einen 90-tägigen Testzeitraum. In dieser Zeit ist das System voll funktionsfähig, sodass Sie es konfigurieren und alle Funktionen testen können, bevor Sie Lizenzen erwerben.
Überprüfen Sie Ihre Lizenzen	Wenn die Lizenzdauer des Systems ohne automatische Erneuerung abläuft, gewährt AXIS License Manager Ihnen eine weitere 30-tägige Frist.
Lizenzen	Das System ist vollständig lizenziert und bis zum Ablauf des Gültigkeitsdatums funktionsfähig.
Changes made in the system require a license synchronization (Änderungen am System erfordern eine Lizenzsynchronisierung)	Wenn Sie Geräte zu einem lizenzierten System hinzufügen, versucht AXIS Camera Station Pro, die Änderungen mit AXIS License Manager zu synchronisieren, um den Status der Systemlizenzen erneut zu bewerten. Wenn Sie die automatische Lizenzierung nutzen, werden Sie dies möglicherweise überhaupt nicht bemerken. Wenn Sie jedoch die manuelle Lizenzierung nutzen und die Systemänderungen nicht innerhalb von 60 Tagen neu mit AXIS License Manager synchronisieren, ist das System nicht länger lizenziert.
Nicht lizenziert	Das System ist funktionsfähig, jedoch mit begrenztem Funktionsumfang. Aufzeichnungs- und Aktionsregeln bleiben weiterhin gültig und es gehen keine Aufzeichnungen verloren. Die folgenden Funktionen sind nicht verfügbar: • Livestreams • Wiedergabe von Aufzeichnungen • Sofortige Wiedergabe • Momentaufnahmen • Export von Aufzeichnungen

Sie können Ihr System auf zwei Arten lizenzieren:

Automatische Lizenzierung (Onlinesysteme) – Mit dieser Option übermittelt das System Änderungen, die sich auf die Anzahl der Lizenzen auswirken, automatisch an AXIS License Manager und ruft einen neuen Lizenzstatus ab. Diese Option erfordert eine Internetverbindung. Weitere Informationen finden Sie unter *Ein System online lizensieren., on page 138*.

Manuelle Lizenzierung (Offlinesysteme) – Mit dieser Option müssen Sie Ihre Systemdatei manuell exportieren, auf AXIS License Manager hochladen und die neue Lizenz anschließend in Ihr System importieren. Jedesmal, wenn Sie Änderungen am System vornehmen, die sich auf die Anzahl der Lizenzen auswirken, müssen Sie die manuelle Lizenzierung wiederholen. Wählen Sie diese Option, wenn Sie es vorziehen, die Lizenzen manuell zu verwalten, oder wenn Ihr System nicht über eine Internetverbindung verfügt. Weitere Informationen finden Sie unter *Ein System offline lizensieren, on page 138*.

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 Pro 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.

Die Sicherheit konfigurieren

Benutzerberechtigungen

Rufen Sie **Configuration > Security > User permissions (Konfiguration > Sicherheit > Benutzerrechte)** auf, um die in AXIS Camera Station Pro vorhandenen Benutzer und Gruppen anzusehen.

Hinweis

Administratoren von Computern, auf denen AXIS Camera Station Pro Server ausgeführt werden, erhalten automatisch Administratorrechte für AXIS Camera Station Pro. Die Zugriffsrechte der Benutzergruppe „Administratoren" können nicht geändert oder gelöscht werden.

Vor Hinzufügen eines Benutzers oder einer Benutzergruppe müssen Sie den Benutzer oder die Benutzergruppe zunächst auf dem lokalen Rechner registrieren oder sicherstellen, dass dieser/diese über ein Windows® Active Directory-Benutzerkonto verfügt. So fügen Sie Benutzer bzw. Gruppen hinzu: *Hinzufügen von Benutzern oder Gruppen*.

Ein Benutzer, der zu einer bestimmten Benutzergruppe gehört, erhält die höchste einzeln oder für Benutzergruppe vergebene Rollenberechtigung. Der Nutzer erhält die entsprechenden Zugriffsrechte sowohl als Einzelperson als auch als Zugehöriger einer Benutzergruppe. Beispiel: Ein Benutzer besitzt als Einzelperson Zugriff auf Kamera X. Außerdem ist der Benutzer Teil einer Gruppe, die Zugriff auf die Kameras Y und Z hat. Somit besitzt der Benutzer Zugriff auf die Kameras X, Y und Z.

	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 bzw. der Gruppe zugeordnete Zugriffsrolle. Mögliche Werte sind: Administrator, Bediener und Betrachter.
Details	Die auf dem lokalen Computer oder in Active Directory angezeigten detaillierten Benutzerinformationen.
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 Pro zugreifen. Um einen Benutzer zu AXIS Camera Station Pro 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)**.
- **Users (Benutzer)** rechts anklicken und **New user (Neuer Benutzer)** wählen.
- 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. Bei zu vielen Benutzern oder Benutzergruppen werden keine Suchergebnisse angezeigt. Verwenden Sie in diesem Fall die Filterfunktion.
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	Falls eine Verbindung zu mehreren AXIS Camera Station Pro-Servern besteht, wählen Sie unter **Selected server (Ausgewählter Server)** einen Server aus dem entsprechenden Dropdown-Menü aus.

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 zur Konfiguration von Systemeinstellungen 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 Pro 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 Aufzeichnungen manuell zu starten und zu stoppen.
Mechanisches PTZ	Zugriff auf mechanische PTZ-Steuerungen gewähren. Nur für Kameras mit mechanischem PTZ 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 und Auswahl von **Mechanical PTZ (Mechanischer PTZ)**.

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 Pro.
Bearbeiten	Erlaubt die Bearbeitung der Ansichten in AXIS Camera Station Pro.

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	Erlaubt dem Benutzer das Einsehen des E/A-Port-Status. Der Status des Ports kann durch den Benutzer nicht geändert werden.
Schreiben	Erlaubt dem Benutzer das Ändern des E/A-Port-Status.

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	Erlaubt die Erstellung von Momentaufnahmen in den Betriebsarten „Live-Ansicht“ und „Aufzeichnen“.
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 Alarme, 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.
Zutrittsverwaltung	Erlaubt die Zugriffsverwaltung und Zugriff auf die Einstellungen von Active Directory.

AXIS Audio Manager Pro

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

Zugriff auf Komponenteneinstellungen von AXIS Audio Manager Pro	Nur Bediener. Gestatten Sie die Konfiguration von AXIS Audio Manager Pro in AXIS Camera Station Pro und den Zugriff auf die Schnittstelle eines AXIS Audio Manager Pro-Servers.
Zugriff auf die AXIS Audio Manager Pro-Schnittstelle	Nur Betrachter. Gestatten Sie den Zugriff auf die Schnittstelle eines AXIS Audio Manager Pro-Servers.

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 die Konfiguration der Systemzustandsüberwachung der Anlage.
Auf Systemzustandsüberwachung zugreifen	Erlaubt den Zugriff auf die Systemzustandsüberwachung der Anlage.

Zertifikate

Zur Verwaltung der Einstellungen für den Zertifikatsaustausch zwischen dem AXIS Camera Station Pro Server und den Geräten rufen Sie **Configuration > Security > Certificates (Konfiguration > Sicherheit > Zertifikate)** auf.

Weitere Informationen dazu, wie Sie HTTPS- und IEEE 802.1X-Zertifikate aktivieren, löschen und anzeigen, finden Sie unter *Sicherheit, on page 70*.

AXIS Camera Station Pro kann verwendet werden als:

- **Root-Zertifizierungsstelle (Certificate Authority – CA):** Bei Verwendung von AXIS Camera Station Pro als Stamm-CA nutzt AXIS Camera Station Pro das eigene Stammzertifikat zur Ausstellung von Server-Zertifikaten, sodass keine andere Stammzertifizierungsstelle in den Prozess eingebunden ist.
- **Intermediäre Zertifizierungsstelle (Certificate Authority – CA):** In diesem Fall müssen Sie zur Ausstellung und Signierung von Server-Zertifikaten für Ihre Axis Geräte das Zertifikat einer Zertifizierungsstelle (CA-Zertifikat) und den entsprechenden privaten Schlüssel in AXIS Camera Station Pro importieren. Dieses CA-Zertifikat kann ein Stammzertifikat oder das Zwischenzertifikat einer anderen CA sein.

Hinweis

Beim Deinstallieren von AXIS Camera Station Pro werden die CA-Zertifikate der vertrauenswürdigen Root-Zertifizierungsstellen von Windows entfernt. Dies gilt nicht für importierte CA-Zertifikate, die manuell gelöscht werden müssen.

Zertifizierungsstelle (CA)

Zertifizierungsstellen ermöglichen die Aktivierung von HTTPS und IEEE 802.1X auf Geräten ohne bestehende Client/Server-Zertifikate. Von AXIS Camera Station Pro als CA ausgestellte Zertifikate können automatisch Client/Server-Zertifikate auf Geräten erstellen, signieren und installieren, die HTTPS oder IEEE 802.1X verwenden. Sie können AXIS Camera Station Pro als Root-CA verwenden oder ein CA-Zertifikat importieren und AXIS Camera Station Pro als Zwischen-CA nutzen. Bei Installation des Servers erzeugt das System eine Root-CA.

Importieren	Klicken Sie auf diese Option, um ein vorhandenes CA-Zertifikat und seinen privaten Schlüssel zu importieren. AXIS Camera Station Pro speichert sein Kennwort.
Erstellen	Klicken Sie auf diese Option, um einen neuen öffentlichen und privaten Schlüssel sowie ein selbstsigniertes CA-Zertifikat mit einer Gültigkeitsdauer von 10 Jahren zu erzeugen. Bei der Generierung einer neuen Zertifizierungsstelle werden sämtliche Komponentenzertifikate ersetzt und alle Komponenten neu gestartet.
Ansehen	Klicken Sie auf diese Option, um die Einzelheiten des CA-Zertifikats anzuzeigen.

Exportieren	Klicken Sie auf diese Option, um das CA-Zertifikat in eine Datei zu exportieren. Es gibt zwei Optionen für den Export: • **Ohne privaten Schlüssel:** Das Zertifikat wird im Format .cer oder .crt gespeichert. Verwenden Sie diese Option, wenn Sie das öffentliche Zertifikat lediglich auf anderen Systemen installieren müssen, die von AXIS Camera Station Pro signierte Zertifikate als vertrauenswürdig einstufen sollten. • **Mit privatem Schlüssel:** Das CA-Zertifikat wird im PKCS12-Format (.pfx oder .p12) gespeichert. Verwenden Sie diese Option, wenn Sie das CA-Zertifikat auf einem anderen AXIS Camera Station Pro-Server importieren müssen. Es ist nicht möglich, ein Zertifikat vom Typ .cer oder .crt wieder in AXIS Camera Station Pro zu importieren.
Anzahl der Gültigkeitsdaten für die signierten Client/Server-Zertifikate	Legen Sie die Anzahl der Gültigkeitstage für die automatisch erstellten Client/Server-Zertifikate fest. Die Höchstdauer beträgt 1095 Tage (drei Jahre). Beachten Sie, dass die CA keine Zertifikate signiert, die über ihr eigenes Ablaufdatum hinaus gültig sind.

Erstellen einer Root-CA

Beim Start von AXIS Camera Station Pro wird nach einer CA gesucht. Fehlt diese, wird automatisch eine Root-CA erzeugt. Dazu gehören ein selbstsigniertes Root-Zertifikat und ein kennwortgeschützter Privatschlüssel. AXIS Camera Station Pro speichert das Kennwort, macht es jedoch nicht sichtbar. Ein CA-Zertifikat, das von AXIS Camera Station Pro generiert wurde, ist zehn Jahre gültig.

Weitere Informationen zum manuellen Erstellen einer neuen CA zum Ersetzen der alten CA finden Sie unter *Ersetzen einer CA, on page 145*.

Bei einer Aktualisierung von Version 5.45 oder einer früheren Version, die ein manuell auf einem Gerät installiertes Zertifikat verwendet, greift AXIS Camera Station Pro automatisch auf die vorhandene Stammzertifizierungsstelle zurück und installiert ein neues Zertifikat, sobald das manuell installierte Zertifikat abläuft.

Hinweis

Wenn Sie ein CA-Zertifikat erstellen, wird es zu Windows Trusted Root-Zertifikaten hinzugefügt.

Import einer CA

Wenn Sie ein CA-Zertifikat von einer anderen CA installieren, können Sie AXIS Camera Station Pro als Zwischen-CA verwenden. Importieren Sie eine vorhandene CA, bestehend aus einem Zertifikat und einem privaten Schlüssel, damit AXIS Camera Station Pro Zertifikate im Namen dieser CA signieren kann. Bei der Datei muss es sich um eine PKCS#12-Datei handeln, das Zertifikat muss eine Basic Constraint (2.5.29.19) haben, die es als CA-Zertifikat ausweist, und es muss innerhalb seiner Gültigkeitsdauer verwendet werden. Zum Importieren einer CA als Ersatz für die vorhandene, siehe. *Ersetzen einer CA, on page 145*

Hinweis

- Falls die importierte CA kein Kennwort erfordert, erscheint jedes Mal ein entsprechender Dialog, wenn

ein Kennwort eingegeben werden muss, beispielsweise bei Verwendung von HTTPS oder IEEE auf einem Gerät oder beim Hinzufügen eines Geräts. Klicken Sie zum Fortfahren auf **OK**.

- Wenn Sie ein CA-Zertifikat importieren, wird es den Windows Trusted Root-Zertifikaten hinzugefügt.
- Wenn Sie ein CA-Zertifikat importieren, muss das Stammzertifikat bereits im Windows-Zertifikatsspeicher vorhanden sein. Fehlt das Stammzertifikat, schlägt der Import fehl und es wird eine Fehlermeldung angezeigt. AXIS Camera Station Pro verwendet weiterhin die bisherige CA.
- Nach dem Deinstallieren von AXIS Camera Station Pro müssen die importierten CA-Zertifikate manuell von den Windows-Zertifizierungsstellen für vertrauenswürdige Root-Zertifizierungen entfernt werden.

Ersetzen einer CA

CA zur Ausstellung signierter Zertifikate für Geräte mit HTTPS-Verbindung ersetzen:

1. Wechseln Sie zu **Configuration > Security > Certificates > HTTPS (Konfiguration > Sicherheit > Zertifikate > HTTPS)**.
2. Schalten Sie **Validate device certificate (Gerätezertifikat validieren)** aus.
3. Klicken Sie unter **Certificate Authority (Zertifizierungsstelle)** auf **Generate (Generieren)** oder **Import (Importieren)**.
4. Geben Sie Ihr Kennwort ein, und klicken Sie auf **OK**.
5. Wählen Sie die Anzahl der gültigen Tage der signierten Client/Server-Zertifikate.
6. **Konfiguration > Geräte > Verwaltung** aufrufen.
7. Rechtsklicken Sie die Geräte und wählen Sie **Sicherheit > HTTPS > Aktivieren/Aktualisieren**.
8. Rufen Sie **Konfiguration > Sicherheit > Zertifikate > HTTPS** auf und aktivieren Sie **Validate device certificate (Gerätezertifikat validieren)**.

Benutzerdefiniertes Zertifikat erstellen

Sie können ein benutzerdefiniertes Zertifikat erstellen, das von der AXIS Camera Station Pro-Zertifizierungsstelle signiert wurde. Sie können diese Zertifikate beispielsweise für externe HTTPS-Endpunkte verwenden. Diese Zertifikate müssen nach Ablauf manuell erneuert werden. So erstellen Sie ein benutzerdefiniertes Zertifikat:

1. Rufen Sie **Configuration (Konfiguration)** > **Security (Sicherheit)** > **Certificates (Zertifikate)** auf.
2. Klicken Sie unter **Issue custom certificate (Benutzerdefiniertes Zertifikat erstellen)** auf **Issue certificate... (Zertifikat ausstellen)**.
3. Geben Sie die Zertifikatdetails ein und klicken Sie auf **OK**.

Zertifikat ausstellen	
Allgemeiner Name (CN)	Identifiziert den Zertifikatinhaber. Beim CN handelt es sich in der Regel um den vollständig qualifizierten Domainnamen (FQDN) oder die IP-Adresse, unter der Sie das Zertifikat installieren.
Private key password (Kennwort für den privaten Schlüssel)	Kennwort zum Schutz des privaten Schlüssels.
Duration (days) (Dauer (Tage))	Die Anzahl der Tage, die das Zertifikat gültig ist.
Server authentication (Serverauthentifizierung)	Wählen Sie diese Option aus, wenn Sie das Zertifikat auf einem Server als Beleg für die Identität des Servers verwenden möchten. In der Regel werden Geräte oder andere Endpunkte, mit denen AXIS Camera Station Pro über HTTPS verbunden ist, als Servergeräte betrachtet, deren Zertifikate eine Serverauthentifizierung verwenden sollten.

Zertifikat ausstellen	
Client authentication (Client-Authentifizierung)	Wählen Sie diese Option aus, wenn Sie das Zertifikat auf einem Client als Beleg für die Identität des Clients verwenden möchten, bevor Sie eine Verbindung zu einem Server herstellen dürfen. Geräte, die beispielsweise auf ein zutrittsgesteuertes IEEE 802.1X-Netzwerk zugreifen möchten, müssen dieses Zertifikat vor dem Betreten verwenden.
Organisation (O)	Die Organisation des Zertifikatinhabers.
Country code (C) (Ländercode (C))	Der Ländercode des Zertifikatinhabers.
DNS SAN	Dynamische Namen für Server mit alternativen Namen. Alternative FQDNs für die Kontaktaufnahme mit dem Zertifikatshalter. Beim Erstellen eines Zertifikats fügt das System das CN automatisch als DNS-SAN hinzu. Sie können mehrere durch Kommas getrennte Adressen eingeben, z. B. Adresse-1.com, Adresse-2.com.
IP SAN	Alternative Namen für IP-Adresssubjekt. Alternative IP-Adressen für die Kontaktaufnahme mit dem Zertifikatinhaber. Das System fügt das CN automatisch als IP SAN hinzu, wenn es sich um eine IP-Adresse handelt. Sie können mehrere durch Kommas getrennte Adressen eingeben, z. B. 192.168.1.1,192.168.1.2

HTTPS

AXIS Camera Station Pro prüft standardmäßig die Signatur des aktiven HTTPS-Serverzertifikats auf jedem angeschlossenen Gerät und stellt keine Verbindung zu Geräten ohne geprüftes Zertifikat her. Das Serverzertifikat muss von der aktiven Zertifizierungsstelle in AXIS Camera Station Pro oder über den Windows-Zertifikatspeicher validiert werden. AXIS Camera Station Pro prüft bei Aktivierung der Option **Validate device address (Geräteadresse validieren)** außerdem, ob die Adresse im HTTPS-Zertifikat des Geräts mit der zur Kommunikation mit dem Gerät verwendeten Adresse übereinstimmt.

Kameras mit Firmware-Version 7.20 oder höher werden mit einem selbstsignierten Zertifikat ausgeliefert. Diese Zertifikate sind nicht vertrauenswürdig. Generieren oder importieren Sie stattdessen eine CA, damit AXIS Camera Station Pro neue Zertifikate für Geräte ausstellen kann, die HTTPS verwenden.

Zertifikat validieren	Aktivieren Sie dies, um die Verbindung nur für Geräte mit gültigem Zertifikat zu ermöglichen. Ohne Zertifikatsprüfung wird der Zugriff auf Geräte mit ungültigen Zertifikaten ermöglicht.
Geräteadresse validieren	Deaktivieren Sie die Option für ein stabiles Verhalten in DHCP-Netzwerken ohne Host-Namen. Aktivieren Sie diese Option, um für zusätzliche Sicherheit die Übereinstimmung der Adressen zu gewährleisten. Diese Einstellung sollte nur bei Netzwerken aktiviert werden, in denen die Geräte hauptsächlich über Hostnamen kommunizieren oder eine statische IP-Adresse besitzen.

Hinweis

- Wenn keine sichere Verbindung (HTTPS) verfügbar ist, können Sie ein neues HTTPS-Zertifikat ausstellen. Siehe *Geräte hinzufügen, on page 46*
- Zur Verwendung von HTTPS ist für Videogeräte Firmware-Version 5.70 oder höher und für Zutrittskontroll- und Audiogeräte Firmware-Version 1.25 oder höher erforderlich.

Einschränkungen

- Andere Ports als 443 (Standard-Port) werden nicht unterstützt.
- Alle Zertifikate in einem Installationspaket müssen dasselbe Kennwort besitzen.
- Zertifikatvorgänge über unverschlüsselte Kanäle wie „Basic" werden nicht unterstützt. Stellen Sie die Geräte auf „Encrypted & unencrypted" (Verschlüsselt und unverschlüsselt) oder „Encrypted only" (Nur verschlüsselt), um eine Digest-Kommunikation zu ermöglichen.
- HTTPS kann nicht für Netzwerk-Switches der Serie AXIS T85 PoE+ aktiviert werden.

IEEE 802.1X

Bei der 802.1X Authentifizierung durch AXIS Camera Station Pro ist der Anfragende ein Axis Netzwerkgerät, das sich mit dem LAN verbinden möchte. Der Authentifikator ist ein Netzwerkgerät wie z. B. ein Ethernet-Switch oder ein WLAN-Zugangspunkt. Der Authentifizierungsserver ist in der Regel ein Host, auf dem eine Software läuft, die das RADIUS- und EAP-Protokoll unterstützt.

Zur Aktivierung von IEEE 802.1X müssen Sie ein CA-Zertifikat für die IEEE 802.1X-Authentifizierung importieren. Das CA-Zertifikat zur IEEE 802.1X-Authentifizierung und das IEEE 802.1X-Client-Zertifikat werden bei der Aktivierung oder Aktualisierung von IEEE 802.1X installiert. Authentifizierungszertifikate können entweder extern, z. B. vom IEEE 802.1X-Authentifizierungsserver, oder direkt von AXIS Camera Station Pro bezogen werden. Dieses Zertifikat wird auf jedem Axis Gerät installiert und verifiziert den Authentifizierungsserver.

Hinweis

Zur Verwendung von IEEE 802.1X-Zertifikaten ist Firmware-Version 5.50 oder höher für Videogeräte und Firmware-Version 1.25 oder höher für Zutrittskontroll- und Audiogeräte erforderlich.

IEEE 802.1X konfigurieren:

1. Wechseln Sie zu **Konfiguration > Sicherheit > Zertifikate**.
2. Wählen Sie im Dropdown-Menü unter **EAPOL-Version** die gewünschte EAP-Version (Extensible Authentication Protocol) aus.
3. Wählen Sie im Dropdown-Menü unter **EAP identity (EAP-Identität)** aus, ob Sie die MAC-Adresse oder den Hostnamen des Geräts oder einen benutzerdefinierten Text verwenden möchten.
4. Geben Sie bei Auswahl von **Custom (Benutzerdefiniert)** einen beliebigen Text ein, der in **Custom** als EAP-Identität fungiert.
5. Klicken Sie auf **Import (Importieren)** und wählen Sie die CA-Zertifikatsdatei zur IEEE 802.1X-Authentifizierung aus.
6. Wählen Sie im Dropdown-Menü unter **Common name (Gemeinsamer Name)** aus, ob die **Device IP address (IP-Adresse)** oder die **Device EAP identity (EAP-Identität)** des Geräts als gemeinsamer Name in den für die einzelnen Geräte erstellten Zertifikaten verwendet werden soll, wenn AXIS Camera Station Pro als Zertifizierungsstelle fungiert.
7. **Konfiguration > Geräte > Verwaltung** aufrufen.
8. Klicken Sie mit der rechten Maustaste auf die entsprechenden Geräte und wählen Sie **Security > IEEE 802.1X > Enable/Update (Sicherheit > IEEE 802.1X > Aktivieren/Aktualisieren)**.

Einschränkungen

- Bei Geräten mit mehreren Netzwerkadaptern (z. B. drahtlose Kameras) kann IEEE 802.1X nur für den ersten Adapter, in der Regel die Kabelverbindung, aktiviert werden.
- Geräte, bei denen der Parameter `Network.Interface.I0.dot1x.Enabled` fehlt, werden nicht unterstützt. Zum Beispiel: Video-Decoder der Serie AXIS P39, AXIS T85 und AXIS T87

- Zertifikatvorgänge über unverschlüsselte Kanäle wie „Basic" werden nicht unterstützt. Stellen Sie die Geräte auf „Encrypted & unencrypted" (Verschlüsselt und unverschlüsselt) oder „Encrypted only" (Nur verschlüsselt), um eine Digest-Kommunikation zu ermöglichen.

Warnhinweis: Zertifikat läuft ab

Bei Ablauf eines Client- oder Serverzertifikats oder bereits abgelaufenem Zertifikat erscheint eine Warnmeldung. Bei bestimmten Zertifikaten wird außerdem von der Warnung ein Systemalarm ausgelöst. Dies sind im Einzelnen alle Client- und Server-Zertifikate, die von AXIS Camera Station Pro auf Geräten installierten CA-Zertifikate, von AXIS Camera Station Pro ausgestellte CA-Zertifikate sowie IEEE 802.1X-Zertifikate. Die Warnmeldungen erscheinen unter **Status** auf der Seite **Device management (Geräteverwaltung)** sowie als Symbol in der Liste **Installed certificates (Installierte Zertifikate)**.

Geben Sie unter **Certificate expiration warning (Warnung vor Zertifikatablauf)** ein, wie viele Tage vor Ablauf des Zertifikats AXIS Camera Station Pro Sie benachrichtigen soll.

Zertifikatserneuerung

Zertifikat zwischen Server und Gerät erneuern

Die von AXIS Camera Station Pro ausgestellten Geräte-, Client- oder Server-Zertifikate werden 7 Tage vor Ablauf und Erscheinen der Warnmeldung automatisch verlängert. Hierfür muss HTTPS oder IEEE 802.1X auf dem Gerät aktiviert sein. Weitere Informationen zur manuellen Verlängerung oder Aktualisierung von Zertifikaten finden Sie unter *Sicherheit, on page 70*.

Zertifikat zwischen Server und Client erneuern

Sie können ein neues Serverzertifikat auf der Registerkarte Zertifikate in der AXIS Camera Station Pro Dienststeuerung erstellen. Die entsprechende Anleitung finden Sie unter *Zertifikate, on page 235*.

Kennwort zurücksetzen

1. Wechseln Sie zu **Konfiguration > Sicherheit > Zertifikate**.
2. Schalten Sie die Option **Validate device certificate (Gerätezertifikat validieren)** ein, um sicherzustellen, dass Geräte, die CA-Zertifikate verwenden, auch erreichbar sind.
3. Klicken Sie unter **Certificate Authority (Zertifizierungsstelle)** auf **Generate (Erzeugen)**, und geben Sie Ihr Kennwort ein.
4. Klicken Sie unter **Certificate Authority (Zertifizierungsstelle)** auf **Export (Exportieren)**, um das CA-Zertifikat lokal zu speichern.
5. Wechseln Sie zu **Configuration > Devices > Management (Konfiguration > Geräte > Verwaltung)**, und aktivieren Sie HTTPS auf den ausgewählten Geräten.
6. Schalten Sie **Validate device certificate (Gerätezertifikat validieren)** ein.

Konfigurieren der Zutrittskontrolle

Wenn Sie Ihrem System einen Axis Network Door Controller hinzugefügt haben, können Sie die Hardware für die Zutrittskontrolle in AXIS Camera Station Version 6.x oder höher konfigurieren.

Die vollständige Vorgehensweise zum Einrichten eines Axis Network Door Controller in AXIS Camera Station Pro finden Sie unter *Einrichten eines Axis Network Door Controllers*.

Hinweis

Stellen Sie vor dem Start Folgendes sicher:

- Aktualisieren Sie die AXIS OS-Version des Controllers unter **Configuration (Konfiguration) > Devices (Geräte) > Management (Verwaltung)**.
- Legen Sie unter **Konfiguration > Geräte > Verwaltung** Datum und Uhrzeit für den Controller fest.
- Aktivieren Sie HTTPS auf dem Controller unter **Configuration > Devices > Management (Konfiguration > Geräte > Management)**.

Vorgehensweise zum Konfigurieren der Zutrittskontrolle

1. Informationen zum Bearbeiten der vordefinierten Identifizierungsprofile oder zum Erstellen eines neuen Identifizierungsprofils finden Sie unter *Identifizierungsprofile, on page 168*.
2. Informationen zur Verwendung eines benutzerdefinierten Setups für Kartenformate und die PIN-Länge finden Sie unter *Kartenformate und PIN, on page 170*.
3. Fügen Sie einen Zugang hinzu und wenden Sie ein Identifizierungsprofil auf den Zugang an. Siehe *Hinzufügen eines Zugangs, on page 152*.
4. Konfigurieren Sie den Zugang.
   - *Zugangsmonitor hinzufügen, on page 159*
   - *Notfall-Eingang hinzufügen, on page 161*
   - *Leser hinzufügen, on page 161*
   - *REX-Gerät hinzufügen, on page 164*
5. Fügen Sie eine Zone hinzu und fügen Sie der Zone Zugänge hinzu. Siehe *Zone hinzufügen, on page 165*.

Kompatibilität der Gerätesoftware für Tür-Steuerungen

Wichtig

Beachten Sie bei der Aktualisierung des AXIS OS auf Ihrer Tür-Steuerung die folgenden Punkte:

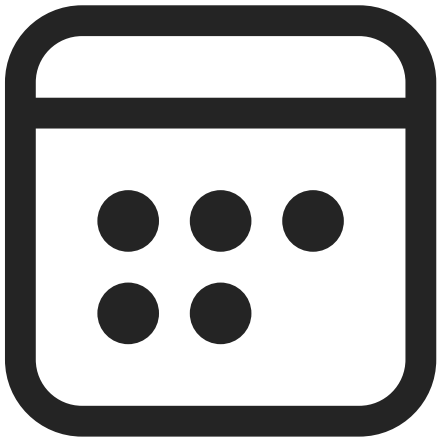
- **Unterstützte AXIS OS Versionen:** Die unten aufgeführten unterstützten AXIS OS Versionen gelten nur bei einer Aktualisierung von der empfohlenen Originalversion der AXIS Camera Station Pro und wenn das System über eine Tür verfügt. Wenn das System diese Bedingungen nicht erfüllt, müssen Sie eine Aktualisierung auf die von empfohlene AXIS OS Version für die jeweilige AXIS Camera Station Pro Version vornehmen.
- **Unterstützte AXIS OS Mindestversion:** Die älteste im System installierte AXIS OS-Version bestimmt die unterstützte AXIS OS Mindestversion, mit einer Grenze von zwei früheren Versionen. Angenommen, Sie verwenden die AXIS Camera Station Pro Version 6.5 und aktualisieren alle Geräte auf die empfohlene AXIS OS Version 12.0.86.2, dann wird die AXIS OS Version 12.0.86.2 zur unterstützte Mindestversion für Ihr System.
- **Aktualisierung über die empfohlene AXIS OS Version hinaus:** Angenommen, Sie führen eine Aktualisierung auf eine AXIS OS Version durch, die über der empfohlenen Version für eine bestimmte AXIS Camera Station Pro Version liegt. Dann können Sie jederzeit problemlos auf die von empfohlene AXIS OS Version zurückstufen, solange diese innerhalb der Unterstützungsgrenzen für die AXIS Camera Station Pro Version liegt.
- **Empfehlungen für zukünftiges AXIS OS:** Verwenden Sie immer die empfohlene AXIS OS Version für die jeweilige AXIS Camera Station Pro Version, um die Systemstabilität und vollständige Kompatibilität zu gewährleisten.
- **Änderungen nachverfolgen:** Beim Ändern der Firmware-Version von 10.12.xx auf 11.0.xx oder höher muss auf die werksseitige Standardeinstellung zurückgesetzt werden.

Die folgende Tabelle zeigt die minimale und empfohlene AXIS OS Version für jede AXIS Camera Station Pro Version:

AXIS Camera Station Version	AXIS OS Mindestversion	Empfohlene AXIS OS Version
Pro 6.15	12.5.68.1	12.8.55.1
Pro 6.14	12.5.68.1	12.8.55.1
Pro 6.13	12.5.68.1	12.6.102.1

Türen und Bereiche

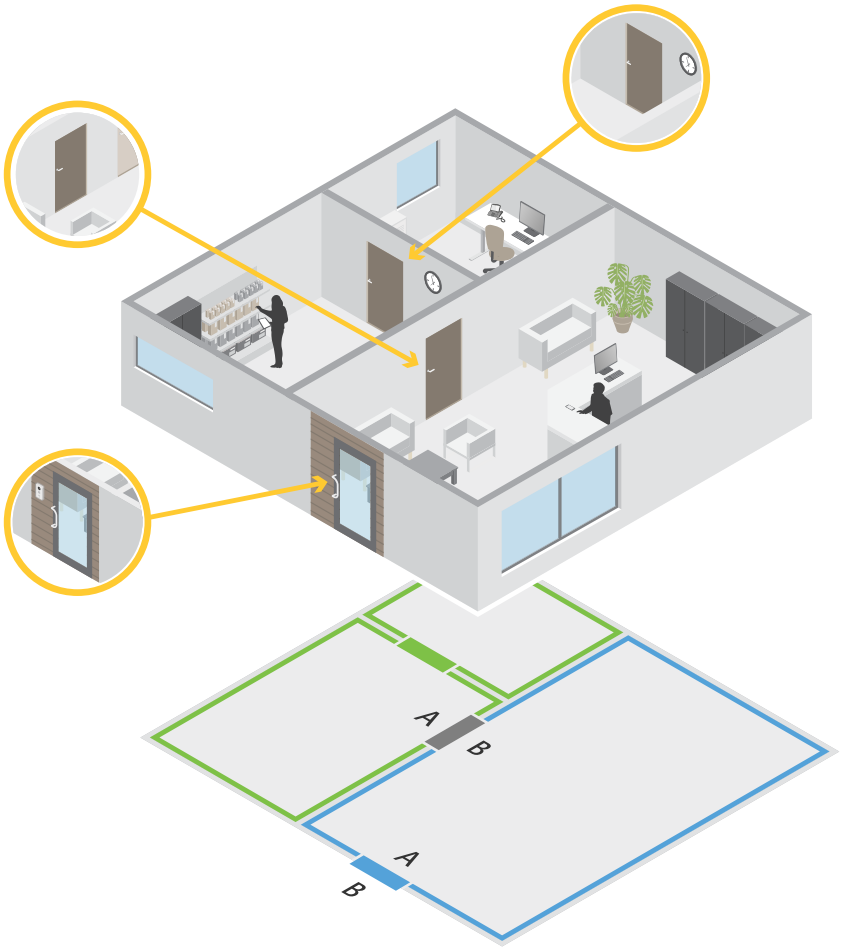
Rufen Sie **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugänge und Zonen)** auf, um eine Übersicht zu erhalten und Zugänge und Zonen zu konfigurieren.

 Manuelle Aktionen	Legen Sie den Status eines Zugangs manuell fest. Wählen Sie aus den folgenden Optionen aus: **Reset (Zurücksetzen)** (gemäß den Systemregeln), **Grant access (Zugriff gewähren)** (Zugang für 7 Sekunden entriegeln), **Unlock (Entriegeln)** (Zugang entriegelt lassen), **Verriegeln** (Zugang verriegelt lassen) oder **Sperren** (Zugang von beiden Seiten sperren).
 **Entriegelungspläne**	Sie können einen Zeitplan für die automatische Entriegelung von Zugängen zu bestimmten Zeiten festlegen. Zu allen anderen Zeiten bleiben die Zugänge verriegelt. Um festzulegen, dass die erste Person den Zugang manuell zunächst entriegeln muss, bevor der Zeitplan aktiviert wird, aktivieren Sie die Option **First person in (Nach Entriegelung durch erste Person)**.
Identifizierungsprofil	Ändern Sie das Identifizierungsprofil für Zugänge.
Pin Chart	Zeigen Sie das Pin Chart des Controllers an, das einem Zugang zugeordnet ist. Wenn Sie das Pin Chart ausdrucken möchten, klicken Sie auf **Print (Drucken)**.
Secure Channel	Schalten Sie OSDP Secure Channel für einen bestimmten Leser ein oder aus.

Türen	
Bezeichnung	Der Name des Zugangs.
Typ	Hierbei handelt es sich um die Art der Zugangskonfiguration.
Gerät	Das bezieht sich auf das am Zugang angebrachte Gerät.

IP-Adresse	Die IP-Adresse der an die Tür angeschlossenen Tür-Steuerung.
Seite A	Die Zone, in der sich Seite A des Zugangs befindet.
Seite B	Die Zone, in der sich Seite B des Zugangs befindet.
Identifizierungsprofil	Das Identifizierungsprofil, das auf den Zugang angewendet wird.
Batterie	Hierbei handelt es sich um den Status der Batterie in der Tür-Steuerung.
Status	Den Zugangs. • **Online** Der Zugang ist online und funktioniert normal. • **Leser offline:** Der Leser in der Zugangskonfiguration ist offline. • **Leserfehler:** Der Leser in der Türkonfiguration unterstützt keinen sicheren Kanal oder sicherer Kanal ist für den Leser nicht aktiviert. • **Alte Firmware:** Das Gerät nutzt eine veraltete Firmware-Version. Aktualisieren Sie die Firmware, um die optimale Funktion und den höchsten Grad an Sicherheit zu gewährleisten.
Zonen	
Bezeichnung	Der Name der Zone.
Anzahl der Zugänge	Die Anzahl der Zugänge in der Zone.
Sicherheitsgrad	Hierbei handelt es sich um die für die Zone geltende Sicherheitsstufe.

Beispiel für Zugänge und Zonen



- Es gibt zwei Zonen: eine grüne und eine blaue.
- Es gibt drei Zugänge: einen grünen, einen blauen und einen braunen.
- Beim grünen Zugang handelt es sich um einen internen Zugang in der grünen Zone.
- Der blaue Zugang ist ein Umgrenzungszugang nur für die blaue Zone.
- Der braune Zugang ist ein Umgrenzungszugang sowohl für die grüne als auch für die blaue Zone.

Hinzufügen eines Zugangs

Hinweis

- Sie können eine Tür-Steuerung mit einer Tür mit zwei Schlössern oder mit zwei Türen mit jeweils einem Schloss konfigurieren. Mehrfachsteuerungen unterstützen weitere Schlosskonfigurationen.
- Wenn einer Tür-Steuerung keine Türen zugewiesen sind und Sie eine neue Version von AXIS Camera Station Pro mit einer Tür-Steuerung mit älterer Firmware verwenden, verhindert das System das Hinzufügen einer Tür. Wenn der Tür-Steuerung jedoch bereits eine Tür hinzugefügt wurde, gestattet das System das Hinzufügen neuer Türen auf Systemcontrollern mit älterer Firmware.

Erstellen einer neuen Zugangskonfiguration zum Hinzufügen einer Tür:

1. Rufen Sie **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen)** auf.
2. Klicken Sie auf + **Add door (Zugang hinzufügen)** und wählen Sie einen Zugangstyp aus dem Aufklappmenü aus.

Türarten	
Tür	Eine herkömmliche Tür mit einem Zugangsmonitor, der Schlösser und Leser unterstützt. Erfordert eine Tür-Steuerung.
Drahtloser Zugang	Ein Zugang, der sich mit Funkschlössern und Kommunikationshubs ASSA ABLOY Aperio® konfigurieren lässt. Weitere Informationen finden Sie unter *Drahtloses Schloss hinzufügen, on page 157*.
Überwachter Zugang	Ein Zugang, der melden kann, ob er geöffnet oder geschlossen ist. Weitere Informationen finden Sie unter *Überwachten Zugang hinzufügen, on page 160*.
Vorgesehener Zugang	Ein Zugang, den Sie als Platzhalter in einem System hinzufügen können, ohne dass Sie die Hardware dafür auswählen müssen.
Etage	Ein Zugangstyp für die Aufzugssteuerung, der den Zugriff auf die Aufzugsetagen mithilfe von Kartenlesegeräten authentifiziert. Weitere Informationen finden Sie unter *Eine Etage für die Aufzugsteuerung hinzufügen BETA, on page 160*.

3. Geben Sie einen Namen für den Zugang ein und wählen Sie im Aufklappmenü **Device (Geräte)** eine Tür-Steuerung aus, die mit dem Zugang verknüpft werden soll. Der Controller ist ausgegraut, wenn Sie keine weitere Tür hinzufügen können, wenn er offline ist oder HTTPS nicht aktiviert ist.
4. Klicken Sie auf **Next (Weiter)**, um die Seite zur Zugangskonfiguration aufzurufen.
5. Wählen Sie im Drop-Down Menü **Primary lock (Primäres Schloss)** einen Relay-Port aus.
6. Um zwei Schlösser am Zugang zu konfigurieren, wählen Sie den anderen Relay-Port im Drop-Down Menü **Secondary lock (Sekundäres Schloss)** aus.
7. Wählen Sie ein Identifizierungsprofil aus. Siehe *Identifizierungsprofile, on page 168*.
8. Konfigurieren Sie die Zugangseinstellungen. Siehe *Einstellungen der Tür, on page 154*.
9. *Zugangsmonitor hinzufügen, on page 159*
10. *Notfall-Eingang hinzufügen, on page 161*
11. *Leser hinzufügen, on page 161*
12. *REX-Gerät hinzufügen, on page 164*
13. Konfigurieren Sie die Sicherheitsstufe. Siehe *Sicherheitsstufe der Tür, on page 155*.
14. **Save (Speichern)** anklicken.

Konfiguration eines Zugangs kopieren:

1. Rufen Sie **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen)** auf.
2. Klicken Sie auf + **Add door (Zugang hinzufügen)**.
3. Geben Sie einen Namen für den Zugang ein und wählen Sie im Aufklappmenü **Device (Geräte)** eine Tür-Steuerung aus, die mit dem Zugang verknüpft werden soll.
4. Klicken Sie auf **Next (Weiter)**.
5. Wählen Sie aus im Drop-Down Menü **Copy configuration (Konfiguration kopieren)** eine vorhandene Zugangskonfiguration aus. Es enthält die angeschlossenen Zugänge und der Controller ist ausgegraut, wenn er mit zwei Zugängen oder einem Zugang mit zwei Schlössern konfiguriert wurde.

6. Sie können die Einstellungen jederzeit ändern.
7. **Save (Speichern)** anklicken.

So entfernen Sie einen Zugang:

1. Rufen Sie **Configuration > Access control > Door and zones > Zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen > Zonen)** auf.
2. Wählen Sie einen Zugang in der Liste aus.
3. Klicken Sie auf **Remove (Entfernen)** und bestätigen Sie.

Hinzufügen und Konfigurieren von Zugängen und Zonen

Einstellungen der Tür

So bearbeiten Sie einen Zugang:

1. Rufen Sie **Configuration > Access control > Door and Zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen)** auf.
2. Wählen Sie den Zugang aus, den Sie bearbeiten möchten.
3. Klicken Sie auf **Edit (Bearbeiten)**.
4. Ändern Sie die Einstellungen und klicken Sie auf **Save (Speichern)**.

Zugangszeit (s)	Legen Sie die Anzahl von Sekunden fest, die der Zugang geöffnet bleibt, nachdem Zutritt gewährt wurde. Die Tür bleibt entriegelt, bis sie sich öffnet oder bis die eingestellte Zeit endet. Die Tür verriegelt sich beim Schließen selbst dann, wenn noch Zugangszeit bleibt.
Open-too-long time (sec) (Maximale Öffnungsdauer (s))	Nur gültig, wenn ein Zugangsmonitor konfiguriert ist. Legen Sie fest, wie viele Sekunden die Tür geöffnet bleibt. Wenn die Tür geöffnet ist, wenn die eingestellte Zeit endet, löst sie einen Alarm einer zu lange geöffneten Tür aus. Richten Sie eine Aktionsregel ein, die festlegt, welche Aktion ausgelöst werden soll, wenn die maximale Öffnungsdauer überschritten wird.
Lange Zutrittszeiten (Sekunden)	Legen Sie die Anzahl von Sekunden fest, die der Zugang geöffnet bleibt, nachdem Zutritt gewährt wurde. Der Wert für die lange Zutrittszeit überschreibt die bereits festgelegte Zutrittszeit für Karteninhaber, wenn diese Einstellung aktiviert ist.
Long open-too-long time (sec) (Lange maximale Öffnungsdauer (s))	Nur gültig, wenn ein Zugangsmonitor konfiguriert ist. Legen Sie fest, wie viele Sekunden die Tür geöffnet bleibt. Wenn die Tür geöffnet ist, wenn die eingestellte Zeit endet, löst sie ein Ereignis einer zu lange geöffneten Tür aus. Wenn Sie die Einstellung **Long access time (Lange Zugangszeit)** einschalten,

	überschreibt der Wert für die lange maximale Öffnungsdauer die bereits festgelegte maximale Öffnungsdauer für Karteninhaber.
Verzögerungszeit bis zum Wiederverriegeln (ms)	Legen Sie die Zeit (in Millisekunden) fest, die die Tür nach dem Öffnen oder Schließen entriegelt bleibt.
Wieder verriegeln	• **After opening: (Nach dem Öffnen:)** Nur gültig, wenn ein Zugangsmonitor hinzugefügt wurde. • **After closing: (Nach dem Schließen:)** Nur gültig, wenn ein Zugangsmonitor hinzugefügt wurde.
Zugang erzwungen	Wählen Sie, ob das System einen Systemalarm auslösen soll, wenn eine Tür gewaltsam geöffnet wurde. Erfordert einen Türpositionssensor (DPS).
Tür zu lange geöffnet	Wählen Sie, ob das System einen Systemalarm auslösen soll, wenn eine Tür zu lange offen gehalten wird.

Manuelle Aktionen

Sie können die folgenden manuellen Aktionen an Zugängen und Zonen durchführen:

Zurücksetzen – Stellt die konfigurierten Systemregeln wieder her.

Zugang gewähren – Entriegelt 7 Sekunden lang einen Zugang oder eine Zone und sperrt sie dann wieder.

Entriegeln – Hält den Zugang unverschlossen, bis Sie zurücksetzen.

Schloss – Hält den Zugang gesperrt, bis das System einem Karteninhaber den Zugriff gewährt.

Verriegelung – Niemand kommt rein oder raus, bis Sie zurücksetzen oder entsperren.

Um eine manuelle Aktion durchzuführen:

1. Rufen Sie **Configuration** > **Access control** > **Doors and zones** (Konfiguration > Zutrittskontrolle > Zugang und Zonen) auf.
2. Wählen Sie den Zugang oder die Zone aus, für die Sie eine manuelle Aktion durchführen möchten.
3. Klicken Sie auf eine der manuellen Aktionen.

Sicherheitsstufe der Tür

Sie können einer Tür die folgenden Sicherheitsfunktion hinzufügen:

Zwei-Personen-Regel – Die Zwei-Personen-Regel erfordert, dass zwei Personen gültige Zugangsdaten verwenden, um Zugang zu erhalten.

Double Swipe – Mit dem doppelten Durchziehen kann der Karteninhaber den aktuellen Status einer Tür überschreiben. Beispielsweise kann er damit einen Zugang außerhalb des regulären Zeitplans sperren und entsperren, was bequemer ist, als das Entsperren des Zugangs im System. Die Double-Swipe-Funktion wirkt sich nicht auf einen vorhandenen Zeitplan aus. Wenn etwa ein Zugang zur Schließzeit gemäß Zeitplan verriegelt werden soll und ein Mitarbeiter in die Mittagspause geht, wird der Zugang dennoch gemäß Zeitplan verriegelt.

Sie können die Sicherheitsstufe konfigurieren, während Sie eine neue Tür hinzufügen, oder Sie können die Konfiguration für eine vorhandene Tür durchführen.

So fügen Sie eine **Zwei-Personen-Regel** zu einem vorhandenen Zugang hinzu:

1. Rufen Sie **Configuration** > **Access control** > **Doors and zones** (Konfiguration > Zutrittskontrolle > Zugang und Zonen) auf.
2. Wählen Sie die Tür aus, für die Sie eine Sicherheitsstufe konfigurieren möchten.
3. Klicken Sie auf **Edit (Bearbeiten)**.
4. Klicken Sie auf **Security level (Sicherheitsstufe)**.
5. Aktivieren Sie **Zwei-Personen-Regel**.
6. Klicken Sie auf **Anwenden**.

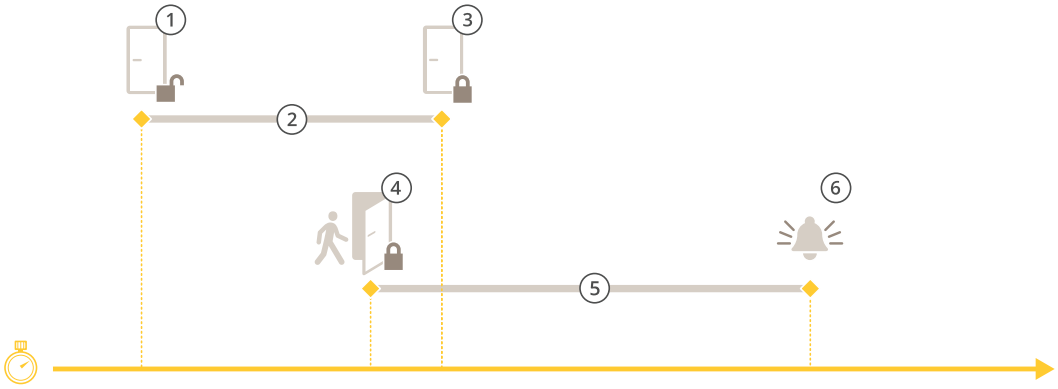
Zwei-Personen-Regel	
Side A (Seite A) und **Side B (Seite B)**	Wählen Sie aus, auf welchen Seiten der Tür die Regel verwendet werden soll.
Zeitschemata	Wählen Sie „While the rule is active" (Während die Regel aktiv ist).
Zeitüberschreitung (Sekunden)	Timeout ist die maximal zulässige Zeit zwischen dem Durchziehen der Karte oder der Verwendung eines anderen Typs gültiger Zugangsdaten.

So fügen Sie einem vorhandenen Zugang **Double Swipe** hinzu:

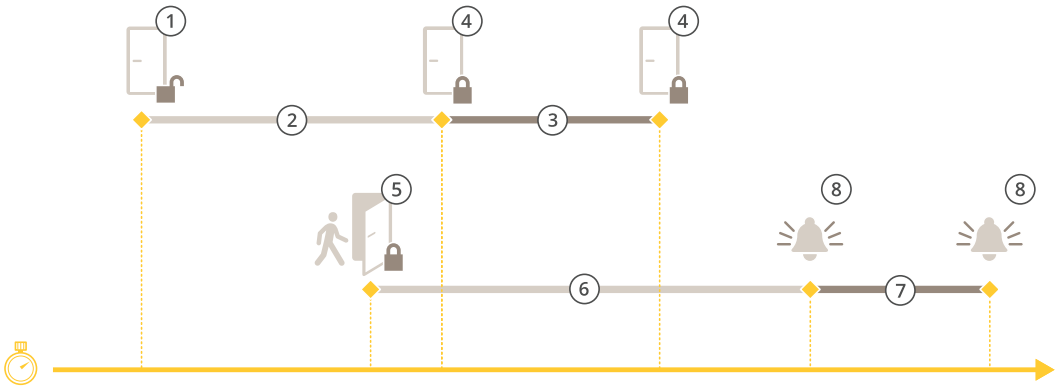
1. Rufen Sie **Configuration** > **Access control** > **Doors and zones** (Konfiguration > Zutrittskontrolle > Zugang und Zonen) auf.
2. Wählen Sie die Tür aus, für die Sie eine Sicherheitsstufe konfigurieren möchten.
3. Klicken Sie auf **Edit (Bearbeiten)**.
4. Klicken Sie auf **Security level (Sicherheitsstufe)**.
5. Aktivieren Sie **Double Swipe**.
6. Klicken Sie auf **Anwenden**.
7. Wenden Sie **Double Swipe** auf einen Karteninhaber an.
   7.1. Öffnen Sie eine Registerkarte **Access Management (Zugangsverwaltung)**.
   7.2. Klicken Sie beim zu bearbeitenden Karteninhaber auf ⋮ und dann auf **Edit (Bearbeiten)**.
   7.3. Klicken Sie **Mehr** an.
   7.4. Wählen Sie **Allow double-swipe (Double Swipe zulassen)** aus.
   7.5. Klicken Sie auf **Anwenden**.

Double Swipe	
Zeitüberschreitung (Sekunden)	Timeout ist die maximal zulässige Zeit zwischen dem Durchziehen der Karte oder der Verwendung eines anderen Typs gültiger Zugangsdaten.

Zeitoptionen



1 Zugang gewährt – Schloss entriegelt
2 Zugangszeit
3 Keine Aktion ausgeführt – Schloss verriegelt
4 Aktion ausgeführt (Tür geöffnet) – Schloss verriegelt oder bleibt entriegelt, bis die Tür geschlossen wird
5 Zu lange geöffnet
6 Zu lange geöffnet – Alarm wird ausgelöst



1 Zugang gewährt – Schloss entriegelt
2 Zugangszeit
3 2+3: Lange Zugriffszeit
4 Keine Aktion ausgeführt – Schloss verriegelt
5 Aktion ausgeführt (Tür geöffnet) – Schloss verriegelt oder bleibt entriegelt, bis die Tür geschlossen wird
6 Zu lange geöffnet
7 6+7: Lange maximale Öffnungsdauer
8 Zu lange geöffnet – Alarm wird ausgelöst

Drahtloses Schloss hinzufügen

AXIS Camera Station Pro unterstützt die Funkschlösser und Kommunikationshubs ASSA ABLOY Aperio®. Das drahtlose Schloss wird über einen Aperio-Kommunikationshub am RS485-Anschluss der Türsteuerung mit dem System verbunden. An einer Türsteuerung können Sie 16 Funkschlösser anschließen.

Hinweis

- Für die Einrichtung muss auf der Axis Türsteuerung AXIS OS Version 11.6.16.1 oder höher ausgeführt werden.
- Für die Einrichtung ist eine gültige Lizenz für AXIS Door Controller Extension erforderlich.
- Die Uhrzeit des Axis Tür-Controllers und des AXIS Camera Station Pro Servers muss synchronisiert werden.
- Vor dem Start müssen Sie die mithilfe der Aperio-Programmieranwendung, die von ASSA ABLOY unterstützt wird, Aperio-Schlösser mit dem Aperio-Hub koppeln.
- An jeden RS485-Steckverbinder kann jeweils nur ein Aperio-Hub angeschlossen werden. Multi-Drop wird nicht unterstützt.
- Funkschlösser folgen Zeitplänen für die Entsperrung nicht, wenn sie offline sind.

1. Greifen Sie auf die Türsteuerung zu.
   1.1. **Konfiguration > Geräte > Andere Geräte** aufrufen.
   1.2. Öffnen Sie die Weboberfläche der Türsteuerung, die mit dem Aperio-Kommunikationshub verbunden ist.
2. Aktivieren Sie AXIS Door Controller Extension.
   2.1. Gehen Sie auf der Weboberfläche der Türsteuerung zu **Apps**.
   2.2. Öffnen Sie das Kontextmenü von AXIS Door Controller Extension .
   2.3. Klicken Sie auf **Lizenz mit einem Schlüssel aktivieren** und wählen Sie Ihre Lizenz.
   2.4. Aktivieren Sie **AXIS Door Controller Extension**.
3. Verbinden Sie das Funkschloss über den Kommunikationshub mit der Türsteuerung.
   3.1. Gehen Sie auf der Weboberfläche der Türsteuerung zu **Access control > Wireless locks (Zugriffssteuerung > Funkschlösser)**.
   3.2. Klicken Sie auf **Connect communication hub (Kommunikationshub verbinden)**.
   3.3. Geben Sie einen Namen für den Hub ein und klicken Sie auf **Verbinden**.
   3.4. Klicken Sie auf **Funkschloss verbinden**.
   3.5. Wählen Sie die Adresse des Schlosses sowie die Funktionen für das hinzugefügte Schloss und klicken Sie auf **Save (Speichern)**.
4. Fügen Sie die Tür hinzu und konfigurieren Sie sie mit dem Funkschloss.
   4.1. In AXIS Camera Station Pro gehen Sie zur **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen)** auf.
   4.2. Klicken Sie auf **Add door (Zugang hinzufügen)**.
   4.3. Wählen Sie die mit dem Aperio-Kommunikationshub verbundenen Türsteuerung, wählen Sie **Wireless door (Drahtloser Zugang)** als **Door type (Zugangsart)**.
   4.4. Klicken Sie auf **Next (Weiter)**.
   4.5. Wählen Sie Ihr **Funkschloss**.
   4.6. Definieren Sie die Türseiten A und B und fügen Sie Sensoren hinzu. Weitere Informationen finden Sie unter *Türen und Bereiche, on page 149*.

4.7. **Save (Speichern)** anklicken.

Nach dem Anschluss des Funkschlosses werden Akkustand und Status in der Zugangsübersicht angezeigt.

Akkustand	Aktion
Gut	Keine
Niedrig	Das Schloss funktioniert wie vorgesehen. Sie sollten den Akku jedoch ersetzen, bevor der Akkustand ein kritisches Niveau erreicht.
Kritisch	Tauschen Sie den Akku aus. Das Schloss funktioniert nicht wie vorgesehen.

Sperrstatus	Aktion
Online	Keine
Verriegelungsstau	Mechanische Probleme mit dem Schloss beheben.

Zugangsmonitor hinzufügen

Ein Zugangsmonitor ist ein Zugangspositionsschalter, der den physischen Zustand eines Zugangs überwacht. Sie können Ihrem Zugang wahlweise einen Zugangsmonitor hinzufügen und konfigurieren, wie der Zugangsmonitor angeschlossen ist.

1. Rufen Sie die Seite zur Zugangskonfiguration auf. Siehe *Hinzufügen eines Zugangs, on page 152*.
2. Klicken Sie unter **Sensors (Sensoren)** auf **Add (Hinzufügen)**.
3. Wählen Sie **Door monitor sensor (Türmonitor-Sensor)**.
4. Wählen Sie den I/O-Port aus, mit dem Sie den Zugangsmonitor verbinden möchten.
5. Wählen Sie unter **Door open if (Tür geöffnet wenn)** aus, wie die Stromkreise des Türmonitors angeschlossen sind.
6. Legen Sie eine **Debounce time (Entprellzeit)** fest, um die Statusänderungen des digitalen Eingangs zu ignorieren, bevor er einen neuen stabilen Status annimmt.
7. Um ein Ereignis auszulösen, wenn die Verbindung zwischen dem Netzwerk-Tür-Controller und dem Zugangsmonitor unterbrochen wird, aktivieren Sie **Supervised input (Überwachte Eingänge)**. Siehe *Überwachte Eingänge, on page 167*.

Tür auf, wenn	
Stromkreis geöffnet	Der Schaltkreis des Zugangsmonitors ist ein Öffner-Kontakt. Der Zugangsmonitor gibt bei offenem Schaltkreis an, dass der Zugang geöffnet ist. Der Zugangsmonitor gibt bei geschlossenem Schaltkreis an, dass der Zugang geschlossen ist.
Stromkreis geschlossen	Der Schaltkreis des Zugangsmonitors ist ein Schliesser-Kontakt. Der Zugangsmonitor gibt bei offenem Schaltkreis an, dass der Zugang geschlossen ist. Der Zugangsmonitor gibt bei geschlossenem Schaltkreis an, dass der Zugang offen ist.

Überwachten Zugang hinzufügen

Ein überwachter Zugang ist ein Zugangstyp, dessen geöffneter oder geschlossener Zustand angezeigt werden kann. Dies kann z. B. eine Brandschutztür sein: Diese benötigt kein Schloss, aber Sie müssen wissen, ob sie geöffnet ist.

Ein überwachter Zugang unterscheidet sich von einem normalen Zugang mit Monitor. Ein normaler Zugang mit Monitor unterstützt Schlösser und Kartenleser, erfordert aber eine Tür-Steuerung. Ein überwachter Zugang unterstützt einen Sensor für die Türposition, benötigt aber nur ein netzwerkbasiertes E/A-Relaismodul, das mit einer Tür-Steuerung verbunden ist. Sie können bis zu fünf Sensoren für die Türposition mit einem netzwerkbasierten E/A-Relaismodul verbinden.

Hinweis

Für einen überwachten Zugang brauchen Sie das netzwerkbasierte E/A-Relaismodul AXIS A9210 mit der neuesten Firmware und die Anwendung AXIS Monitoring Door ACAP.

Überwachten Zugang einrichten:

1. Installieren Sie AXIS A9210 und aktualisieren Sie das Gerät mit der neuesten Version von AXIS OS.
2. Installieren Sie die Sensoren für die Türposition.
3. Gehen Sie in AXIS Camera Station Pro zu **Configuration (Konfiguration)** > **Access control (Zutrittskontrolle)** > **Doors and zones (Türen und Zonen)**.
4. Klicken Sie auf **Add door (Zugang hinzufügen)**.
5. Geben Sie einen Namen ein.
6. Wählen Sie unter **Type (Typ) Monitoring door (Überwachter Zugang)** aus.
7. Wählen Sie unter **Device (Gerät)** Ihr netzwerkbasiertes E/A-Relaismodul aus.
8. Klicken Sie auf **Next (Weiter)**.
9. Klicken Sie unter **Sensors (Sensoren)** auf **Add (Hinzufügen)** und wählen Sie **Door position sensor (Sensor Türposition)** aus.
10. Wählen Sie den E/A, der mit dem Sensor für die Türposition verbunden ist.
11. Klicken Sie auf **Hinzufügen**.

Eine Etage für die Aufzugsteuerung hinzufügen BETA

Eine Etage ist ein Zugangstyp, mit dem Sie den Zugriff auf Aufzugsetagen kontrollieren. Wenn Sie eine Etage hinzufügen, erstellen Sie eine Aufzugsressource, die alle Etagen für diesen Aufzug gruppiert. Auf jeder Etage werden mithilfe eines Kartenlesegeräts in der Aufzugskabine die Benutzer authentifiziert, bevor ihnen der Zugriff zu dieser Etage gewährt wird.

Bevor Sie anfangen, ist eventuell Folgendes erforderlich:

- Ein unterstützter Netzwerk-Tür-Controller, der Ihrem System hinzugefügt wurde, wie beispielsweise *A1610*, *A1710-B* oder *A1810-B*.
- *A9910 I/O-Relais-Erweiterungsmodul* für zusätzliche Relais. Anweisung zum Hinzufügen Ihres Moduls zu einem Controller finden Sie unter .

Hinweis

Diese Funktion befindet sich in der Beta-Phase und unterstützt derzeit bis zu 16 Etagen und ausschließlich Leser.

So richten Sie eine Wiederholung ein:

1. Rufen Sie **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen)** auf.
2. Klicken Sie auf **Add (Hinzufügen)** und wählen Sie **Floor (Etage)** BETA.
3. Geben Sie einen Namen für die Etage ein.
4. Wählen Sie Ihren Controller aus.

5. Wählen Sie unter **Elevator (Aufzug)** einen vorhandenen Aufzug aus oder klicken Sie auf **Create new elevator (Neuen Aufzug erstellen)**, um einen neuen hinzuzufügen, und geben Sie dann einen Namen ein.
6. Wählen Sie unter **Side A (Seite A)** die Option **Card reader (Kartenleser)** aus und konfigurieren Sie Ihr Lesegerät. **Side B (Seite B)** kann aus Sicherheitsgründen nicht konfiguriert werden.
7. Klicken Sie auf **Save and add new (Speichern und neu hinzufügen)**, um weitere Etagen zum selben Aufzug hinzuzufügen. Die Konfiguration des Aufzugs und des Lesegeräts bleibt für die nächste Etage unverändert. Bitte beachten Sie, dass diese Option nur verfügbar ist, wenn Ihr Controller über Relais verfügt.
8. Klicken Sie auf **Save (Speichern)**, wenn Sie die Etage hinzugefügt haben. Die Etagen werden mit der Namenskonvention „Aufzugname – Etagenname" angezeigt. Beispiel: „Westseite – Etage 1"

Hinweis

- Lesegeräte, die auf mehreren Etagen verwendet werden, können nur auf der ersten Etage bearbeitet werden, auf der sie hinzugefügt wurden.
- Aufzüge werden automatisch gelöscht, wenn alle zugehörigen Etagen gelöscht werden.

Notfall-Eingang hinzufügen

Sie können einen Notfalleingang hinzufügen und konfigurieren, um eine Aktion zu starten, die die Tür verriegelt oder entriegelt. Sie können auch das Anschließen des Stromkreises konfigurieren.

1. Rufen Sie die Seite zur Zugangskonfiguration auf. Siehe *Hinzufügen eines Zugangs, on page 152*.
2. Klicken Sie unter **Sensors (Sensoren)** auf **Add (Hinzufügen)**.
3. Wählen Sie **Emergency input (Notfalleingang)** aus.
4. Wählen Sie unter **Emergency state (Notfallstatus)** die Stromkreisverbindung aus.
5. Legen Sie eine **Debounce time (ms) (Entprellzeit(ms))** fest, um die Statusänderungen des digitalen Eingangs zu ignorieren, bevor er einen neuen stabilen Status annimmt.
6. Wählen Sie aus, welche **Emergency action (Notfall-Aktion)** beim Empfang des Ausnahmezustandssignal ausgelöst wird.

Ausnahmezustand	
Stromkreis geöffnet	Der Schaltkreis für den Notfall-Eingang ist ein Öffner-Kontakt. Der Notfall-Eingang sendet das Signal für den Ausnahmezustand, wenn der Schaltkreis geöffnet ist.
Stromkreis geschlossen	Der Schaltkreis für den Notfall-Eingang ist ein Schliesser-Kontakt. Der Notfall-Eingang sendet das Signal für den Ausnahmezustand, wenn der Schaltkreis geschlossen ist.

Notfall-Aktion	
Tür entriegeln	Die Tür wird entriegelt, wenn sie das Signal für den Ausnahmezustand empfängt.
Tür verriegeln	Die Tür wird verriegelt, wenn sie das Signal für den Ausnahmezustand empfängt.

Leser hinzufügen

Sie können eine Tür-Steuerung zum Verwenden von mehreren kabelgebundenen Lesern konfigurieren. Wählen Sie einen Leser für eine oder für beide Seiten eines Zugangs.

Wenn ein benutzerdefiniertes Setup von Kartenformaten oder PIN-Längen auf einen Leser angewendet wird, wird dieses in **Card formats (Kartenformate)** unter **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugänge und Zonen)** deutlich angezeigt. Siehe *Türen und Bereiche, on page 149*.

Hinweis

- Sie können auch bis zu 16 Bluetooth-Leser zu einer Tür-Steuerung hinzufügen. Weitere Informationen finden Sie unter *Bluetooth-Leser hinzufügen, on page 163*.
- Wenn Sie eine Axis Netzwerk-IP-Türsprechanlage als IP-Leser verwenden, nutzt das System die auf der Webseite des Geräts eingestellte PIN-Konfiguration.

1. Rufen Sie die Seite zur Zugangskonfiguration auf. Siehe *Hinzufügen eines Zugangs, on page 152*.
2. Klicken Sie für eine Seite des Zugangs auf **Add (Hinzufügen)**.
3. Wählen Sie **Card reader (Kartenleser)**.
4. Wählen Sie unter **Reader type (Lesertyp)** die gewünschte Option aus.
5. So verwenden Sie ein benutzerdefiniertes Setup der PIN-Länge für diesen Leser.
   5.1. Klicken Sie auf **Erweitert**.
   5.2. Aktivieren Sie **Custom PIN length (Benutzerdefinierte PIN-Länge)**.
   5.3. Legen Sie Werte für **Min PIN length (Min. PIN-Länge)**, **Max PIN length (Max. PIN-Länge)** und **End of PIN character (Ende des PIN-Zeichens)** fest.
6. So verwenden Sie ein benutzerdefiniertes Kartenformat für diesen Leser.
   6.1. Klicken Sie auf **Erweitert**.
   6.2. Aktivieren Sie **Custom card formats (Benutzerdefinierte Kartenformate)**.
   6.3. Wählen Sie die Kartenformate, die Sie für den Leser verwenden möchten. Wenn bereits ein Kartenformat mit der gleichen Bitlänge verwendet wird, müssen Sie es zuerst deaktivieren. Ein Warnsymbol wird auf dem Client angezeigt, wenn sich das Kartenformat von der konfigurierten Systemkonfiguration unterscheidet.
7. Klicken Sie auf **Hinzufügen**.
8. Um einen Leser zur anderen Türseite hinzuzufügen, dieses Verfahren erneut verwenden.

Informationen zur Installation eines AXIS-Barcodelesers finden Sie unter *AXIS Barcode Reader installieren, on page 174*.

Lesertyp	
OSDP RS485 Halbduplex	Wählen Sie für RS485-Leser **OSDP RS485 half duplex (OSDP RS485-Halbduplex-Betrieb)** und einen Leserport aus.
Wiegand	Wählen Sie für Leser, die Wiegand-Protokolle verwenden, die Option **Wiegand** und einen Leserport aus.
IP-Leser	Wählen Sie für IP-Leser die Option **IP reader (IP-Leser)** und wählen Sie im Drop-Down Menü ein Gerät aus. Die IP-Türsprechanlagen von Axis können als IP-Leser verwendet werden.

Wiegand	
LED-Steuerung	Wählen Sie entweder **Single wire (Einzelner Draht)** oder **Dual wire (R/G) (Doppeldraht (R/G))** aus. Leser mit einer dualen LED-Steuerung verwenden verschiedene Adern für die roten und grünen LEDs.

Manipulationsalarm	Wählen Sie aus, wann der Manipulationseingang des Lesers aktiv ist. • **Open circuit (Offener Stromkreis)**: Der Leser übermittelt dem Zugang das Manipulationssignal, wenn der Schaltkreis geöffnet ist. • **Closed circuit (Geschlossener Stromkreis)**: Der Leser übermittelt dem Zugang das Manipulationssignal, wenn der Schaltkreis geschlossen ist.
Tamper debounce time (Entprellzeit)	Legen Sie eine **Tamper debounce time (Entprellzeit Manipulation)** fest, um die Statusänderungen des Manipulationseingangs des Lesers zu ignorieren, bevor er einen neuen stabilen Status annimmt.
Überwachter Eingang	Um ein Ereignis auszulösen, wenn die Verbindung zwischen dem Netzwerk-Zugangscontroller und dem Leser unterbrochen wird, aktivieren Sie dies. Siehe *Überwachte Eingänge, on page 167*.

Bluetooth-Leser hinzufügen

Mit dem AXIS A4612 Network Bluetooth Reader können Sie die Beschränkungen der kabelgebundenen Tür-Steuerungen von Axis überwinden und bis zu 16 dieser Leser einer eigenen Tür zuweisen. Jeder Leser unterstützt die Verwaltung von Türschloss, Request-to-Exit-Gerät (REX) und Türpositionsschalter (Door Position Switch, DPS).

Für das Hinzufügen und die Verwendung dieser Leser sind keine zusätzlichen Lizenzen erforderlich.

So fügen Sie einen AXIS A4612 Network Bluetooth Reader zu einer Tür hinzu:

1. Stellen Sie sicher, dass der AXIS A4612 mit der Tür-Steuerung gekoppelt ist. Siehe *App AXIS Mobile Credential als Bluetooth-Zugangsdaten verwenden, on page 163*.
2. Rufen Sie die Seite zur Zugangskonfiguration auf. Siehe *Hinzufügen eines Zugangs, on page 152*.
3. Klicken Sie unter einer Seite der Tür auf **Add (Hinzufügen)** und wählen Sie dann **Card reader (Kartenleser)** aus.
4. Wählen Sie **IP reader (IP-Leser)** und anschließend den gekoppelten AXIS A4612 aus der Drop-down-Liste aus. Wenn dieser Leser für die Zugangsdaten zur Kopplung verwendet werden soll, markieren Sie ihn für die Kopplung. Klicken Sie auf **Hinzufügen**.
5. Ändern Sie auf der Registerkarte **Overview (Übersicht)** das Identifizierungsprofil. Sie können die Profile **Tap in app (In App tippen)** oder **Touch Reader (Kartenleser berühren)** verwenden, wenn Sie den AXIS A4612 nur auf einer Seite der Tür angebracht haben und auf der anderen Seite ein REX-Gerät verwenden.

App AXIS Mobile Credential als Bluetooth-Zugangsdaten verwenden

In diesem Beispiel wird gezeigt, wie Sie den Bluetooth-Kartenleser AXIS A4612 zu Ihrem System hinzufügen, damit Karteninhaber Zugänge mit der App AXIS Mobile Credential entriegeln können.

1. Installieren Sie den Bluetooth-Kartenleser und verbinden Sie ihn mit einer Tür-Steuerung.
2. Fügen Sie den Bluetooth-Kartenleser in der Web-Oberfläche der Tür-Steuerung hinzu.
   2.1. Rufen Sie die Tür-Steuerung auf und gehen Sie zu **Peripherals (Peripheriegeräte)** > **Readers (Kartenleser)**.
   2.2. Klicken Sie auf **Add reader (Kartenleser hinzufügen)**.

2.3. Geben Sie im Dialog **Add Bluetooth reader (Bluetooth-Kartenleser hinzufügen)** die erforderlichen Informationen ein.

2.4. Klicken Sie auf **Hinzufügen**.

3. Fügen Sie den Bluetooth-Kartenleser in AXIS Camera Station Pro einem Zugang hinzu.

3.1. Rufen Sie **Configuration** > **Access control** > **Doors and zones** (Konfiguration > Zutrittskontrolle > Zugang und Zonen) auf.

3.2. Wählen Sie den Zugang aus, dem der Bluetooth-Kartenleser hinzugefügt werden soll, und klicken Sie auf **Edit (Bearbeiten)**.

3.3. Klicken Sie neben dem Zugang, an dem sich der Bluetooth-Kartenleser befindet, auf **+ Add (Hinzufügen)**.

3.4. Wählen Sie **Card reader (Kartenleser)**.

3.5. Wählen Sie unter **Add IP reader (IP-Leser hinzufügen) IP-Leser** aus.

3.6. Wählen Sie unter **IP-Kartenleser** Ihren Bluetooth-Kartenleser aus.

3.7. Klicken Sie auf **Hinzufügen**.

4. Wählen Sie den zu koppelnden Bluetooth-Kartenleser aus. Dies müssen Sie für mindestens einen Bluetooth-Kartenleser in Ihrem System tun.

4.1. Wählen Sie den soeben hinzugefügten Bluetooth-Kartenleser aus.

4.2. Klicken Sie auf **Edit (Bearbeiten)**.

4.3. Wählen Sie unter **Edit bluetooth reader (Bluetooth-Kartenleser bearbeiten) Use this reader for pairing (Diesen Kartenleser zum Koppeln verwenden)** aus.

4.4. Klicken Sie auf **Anwenden**.

5. Wählen Sie als Identifizierungsprofil **Tap in app (In App tippen)** oder **Touch reader (Kartenleser berühren)** aus. Weitere Informationen finden Sie unter *Identifizierungsprofile, on page 168*.

6. Fügen Sie dem Karteninhaber die mobilen Zugangsdaten hinzu. Siehe *Zugangsdaten hinzufügen, on page 189*.

7. Koppeln Sie die mobilen Zugangsdaten mit dem gekoppelten Kartenleser.

7.1. Bringen Sie das Mobiltelefon des Karteninhabers zum Bluetooth-Kartenleser, an dem das Koppeln aktiviert sein muss.

7.2. Befolgen Sie die Anweisungen in der E-Mail an den Karteninhaber.

REX-Gerät hinzufügen

Sie können ein REX-Gerät auf einer oder auf beiden Seiten des Zugangs hinzufügen. Ein REX-Gerät kann ein PIR-Sensor, eine REX-Taste oder eine Druckstange sein.

1. Rufen Sie die Seite zur Zugangskonfiguration auf. Siehe *Hinzufügen eines Zugangs, on page 152*.
2. Klicken Sie für eine Seite des Zugangs auf **Add (Hinzufügen)**.
3. **REX device (REX-Gerät)** auswählen.
4. Wählen Sie den I/O-Port aus, mit dem Sie das REX-Gerät verbinden möchten. Wenn nur ein Port verfügbar ist, wird dieser Port automatisch ausgewählt.
5. Wählen Sie aus, welche **Action (Aktion)** beim Empfang des REX-Signals von der Tür ausgelöst werden soll.
6. Wählen Sie unter **REX active (REX aktiv)** aus, wie die Schaltkreise des Zugangsmonitors angeschlossen sind.
7. Legen Sie eine **Debounce time (ms) (Entprellzeit(ms))** fest, um die Statusänderungen des digitalen Eingangs zu ignorieren, bevor er einen neuen stabilen Status annimmt.

8. Um ein Ereignis auszulösen, wenn die Verbindung zwischen dem Netzwerk-Tür-Controller und dem REX-Gerät unterbrochen wird, aktivieren Sie **Supervised input (Überwachte Eingänge)**. Siehe *Überwachte Eingänge, on page 167*.

Aktion	
Tür entriegeln	Wählen Sie diese Option aus, um die Tür zu entriegeln, wenn sie das REX-Signal empfängt.
Keine	Wählen Sie diese Option aus, wenn Sie beim Empfang des REX-Signals keine Aktion von der Tür auslösen möchten.

REX aktiv	
Stromkreis geöffnet	Wählen Sie aus, ob der REX-Schaltkreis ein Öffner-Kontakt ist. Das REX-Gerät sendet das Signal, wenn der Schaltkreis geöffnet ist.
Stromkreis geschlossen	Wählen Sie aus, ob der REX-Schaltkreis ein Schliesser-Kontakt ist. Das REX-Gerät sendet das Signal, wenn der Schaltkreis geschlossen ist.

Zone hinzufügen

Eine Zone ist ein bestimmter physischer Bereich mit einer Gruppe von Zugängen. Sie können Zonen erstellen und den Zonen Zugänge hinzufügen. Es gibt zwei Arten von Türen:

- **Perimeter door (Umgrenzungszugang):** : Karteninhaber betreten oder verlassen die Zone durch diesen Zugang.
- **Internal door (Interner Zugang):** : Ein interner Zugang innerhalb der Zone.

Hinweis

Ein Umgrenzungszugang kann zu zwei Zonen gehören. Ein interner Zugang kann nur zu einer Zone gehören. Eine Übersicht finden Sie unter *Beispiel für Zugänge und Zonen, on page 152*.

1. Rufen Sie **Configuration > Access control > Door and zones > Zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen > Zonen)** auf.
2. Klicken Sie auf **Add zone (Zone hinzufügen)**.
3. Geben Sie einen Zonennamen ein.
4. Klicken Sie auf **Add door (Zugang hinzufügen)**.
5. Wählen Sie die Türen aus, die Sie der Zone hinzufügen möchten, und klicken Sie auf **Add (Hinzufügen)**.
6. Der Zugang ist standardmäßig ein Umgrenzungszugang. Um das zu ändern, wählen Sie im Aufklappmenü die Option **Internal door (Interner Zugang)** aus.
7. Ein Umgrenzungszugang verwendet standardmäßig die Türseite A als Eingang zur Zone. Um das zu ändern, wählen Sie im Drop-Down Menü die Option **Leave (Verlassen)** aus.
8. Um eine Tür aus der Zone zu entfernen, wählen Sie diese aus und klicken Sie auf **Remove (Entfernen)**.
9. **Save (Speichern)** anklicken.

Zum Bearbeiten einer Zone:

1. Rufen Sie **Configuration > Access control > Door and zones > Zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen > Zonen)** auf.
2. Eine Kamera aus der Liste wählen.
3. Klicken Sie auf **Edit (Bearbeiten)**.

4. Ändern Sie die Einstellungen und klicken Sie auf **Save (Speichern)**.

So entfernen Sie eine Zone:

1. Rufen Sie **Configuration > Access control > Door and zones > Zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen > Zonen)** auf.
2. Eine Kamera aus der Liste wählen.
3. Klicken Sie auf **Remove (Entfernen)**.
4. **Yes (Ja)** anklicken

Sicherheitsstufe der Zone

Sie können einer Zone die folgenden Sicherheitsfunktion hinzufügen:

Anti-Passback – Diese Funktion verhindert, dass eine Person die gleichen Zugangsdaten verwenden kann wie jemand, der bereits vor ihr einen Bereich betreten hat. Dadurch wird gewährleistet, dass eine Person den Bereich zuerst verlassen muss, bevor sie ihre Zugangsdaten erneut verwenden kann.

Hinweis

- Für die Anti-Passback-Funktion empfehlen wir den Einsatz von Zugangspositionssensoren an allen Zugängen in der Zone, damit das System registrieren kann, dass ein Benutzer den Zugang nach dem Durchziehen seiner Karte auch wirklich geöffnet hat.
- Wenn eine Tür-Steuerung offline geht, funktioniert Anti-Passback so lange, wie alle Zugänge in der Zone zu derselben Tür-Steuerung gehören. Wenn die Zugänge in der Zone jedoch zu verschiedenen Tür-Steuerungen gehören, die offline gehen, funktioniert Anti-Passback nicht mehr.

Sie können die Sicherheitsstufe konfigurieren, während Sie eine neue Zone hinzufügen, oder Sie können die Konfiguration für eine vorhandene Zone durchführen. So fügen Sie einer vorhandenen Zone eine Sicherheitsstufe hinzu:

1. Rufen Sie **Configuration** > **Access control** > **Doors and zones** (Konfiguration > Zutrittskontrolle > Zugang und Zonen) auf.
2. Wählen Sie die Zone aus, für die Sie eine Sicherheitsstufe konfigurieren möchten.
3. Klicken Sie auf **Edit (Bearbeiten)**.
4. Klicken Sie auf **Security level (Sicherheitsstufe)**.
5. Schalten Sie die Sicherheitsfunktionen ein, die Sie dem Zugang hinzufügen möchten.
6. Klicken Sie auf **Anwenden**.

Anti-Passback	
Log violation only (Soft) (Nur Verstoß protokollieren (Soft))	Verwenden Sie diese Option, um einer zweiten Person den Zutritt mit den gleichen Zugangsdaten wie die erste Person zu gestatten. Diese Option löst lediglich einen Systemalarm aus.

Deny access (Hard) (Zutritt verweigern (Hard))	Verwenden Sie diese Option, um zu verhindern, dass der zweite Benutzer mit den gleichen Zugangsdaten wie die erste Person den Zugang verwendet. Diese Option löst ebenfalls einen Systemalarm aus.
Zeitüberschreitung (Sekunden)	Die Zeitspanne, bis das System einem Benutzer erneut den Zutritt gewährt. Geben Sie **0** ein, wenn Sie keine Zeitüberschreitung verwenden möchten. Für die Zone gilt dann Anti-Passback, bis der Benutzer die Zone verlässt. Verwenden Sie für die Zeitüberschreitung den Wert **0** nur dann zusammen mit **Deny access (Hard) (Zutritt verweigern (Hard))**, wenn alle Zugänge in der Zone auf beiden Seiten über Leser verfügen.

Überwachte Eingänge

Überwachte Eingänge können bei Unterbrechung der Verbindung mit einer Tür-Steuerung ein Ereignis auslösen.

- Verbindung zwischen Tür-Controller und Türmonitor. Siehe *Zugangsmonitor hinzufügen, on page 159*.
- Verbindung zwischen dem Tür-Controller und dem Leser, der Wiegand-Protokolle verwendet. Siehe *Leser hinzufügen, on page 161*.
- Verbindung zwischen Tür-Controller und REX-Gerät. Siehe *REX-Gerät hinzufügen, on page 164*.

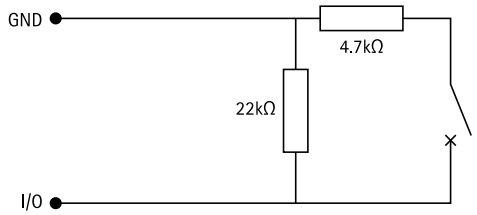
Um überwachte Eingänge zu verwenden:

1. Installieren Sie, wie im Anschlussschaltbild dargestellt, Abschlusswiderstände so nah wie möglich am Peripheriegerät.
2. Gehen Sie zur Konfigurationsseite eines Lesers, eines Zugangsmonitors oder eines REX-Geräts und aktivieren Sie **Supervised input (Überwachte Eingänge)**.
3. Wenn Sie nach dem Schaltplan für eine Parallelschaltung vorgegangen sind, wählen Sie **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Parallelschaltung mit einem parallelen Widerstand (22 KΩ) und einem seriellen Widerstand (4,7 KΩ))**.
4. Wenn Sie nach dem Schaltplan für eine Serienschaltung vorgegangen sind, wählen Sie **Serial first connection (Serienschaltung)** und im Drop-Down Menü **Resistor values (Widerstandswerte)** einen Widerstandswert.

Anschlussschaltbilder

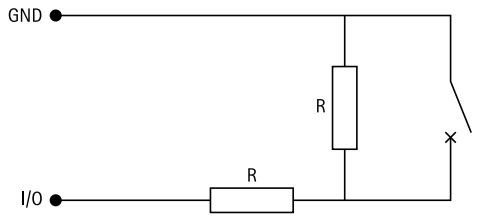
Paralleler Anschluss hat Vorrang

Die Widerstandswerte müssen 4,7 kΩ und 22 kΩ betragen.



Serielle erste Verbindung

Die Widerstandswerte müssen identisch sein und zwischen 1 und 10 kΩ liegen.



Identifizierungsprofile

Ein Identifizierungsprofil ist eine Kombination aus Identifikationsarten und Zeitplänen. Sie können ein Identifizierungsprofil auf einen oder mehrere Zugänge anwenden, um festzulegen, wie und wann ein Karteninhaber einen bestimmten Zugang nutzen kann.

Hinweis

Dynamische QR und PIN müssen zusammen verwendet werden.

Rufen Sie **Configuration > Access control > Identification profiles (Konfiguration > Zutrittskontrolle > Identifizierungsprofile)** auf, um Identifizierungsprofile zu erstellen, zu bearbeiten oder zu entfernen.

Die verfügbaren Identifizierungsprofile:

Karte – Karteninhaber müssen die Karte durch einen angeschlossenen Leser ziehen, um Zutritt zum Zugang zu erhalten.

Karte und PIN – Karteninhaber müssen die Karte durch einen angeschlossenen Leser ziehen und die PIN eingeben, um Zutritt zum Zugang zu erhalten.

PIN – Karteninhaber müssen die PIN eingeben, um Zutritt zum Zugang zu erhalten.

Karte oder PIN – Karteninhaber müssen die Karte durch einen angeschlossenen Leser ziehen oder die PIN eingeben, um Zutritt zum Zugang zu erhalten.

QR – Karteninhaber müssen für den Zugriff auf den Zugang der Kamera den QR-Code® zeigen. Sie können das QR-Identifizierungsprofil sowohl für statische als auch für dynamische QR verwenden.

Nummernschild – Karteninhaber müssen mit einem Fahrzeug mit zugelassenem Fahrzeugkennzeichen auf die Kamera zufahren.

Antippen in der App – Karteninhaber müssen den Ausweis in der AXIS Camera Station Mobile App antippen, während sie sich in Reichweite des Bluetooth-Lesers befinden.

Leser berühren – Karteninhaber müssen den Bluetooth-Leser berühren, während sie ein Mobiltelefon mit mobilen Zugangsdaten bei sich tragen.

*QR Code ist eine eingetragene Marke von Denso Wave Incorporated in Japan und anderen Ländern.

Erstellen eines Identifizierungsprofils

1. Rufen Sie **Configuration > Access control > Identification profiles (Konfiguration > Zutrittskontrolle > Identifizierungsprofile)** auf.
2. Klicken Sie auf **Create identification profile (Identifizierungsprofil erstellen)**.
3. Geben Sie einen Namen für das Identifizierungsprofil ein.
4. Wählen Sie **Include facility code for card validation (Gebäude-Zugangscode in Kartenprüfung einbeziehen)** aus, um den Gebäude-Zugangscode als eines der Felder für das Überprüfen von Anmeldedaten zu verwenden. Dieses Feld ist nur verfügbar, wenn Sie **Facility code (Gebäude-Zugangscode)** unter **Access management > Settings (Zugriffsverwaltung > Einstellungen)** eingeschaltet haben.
5. Für Seite A klicken Sie auf **+ Add (+ Hinzufügen)**, wählen Sie eine Identifikationsart und einen Zeitplan aus.

- Wenn Sie von Karteninhabern verlangen möchten, dass sie mehr als eine Identifikationsart verwenden, wählen Sie mehrere Typen in derselben Zeile aus.
- Damit Karteninhaber beide Typen nutzen können, klicken Sie erneut auf **+ Add (+ Hinzufügen)** und fügen Sie eine weitere Zeile hinzu.

6. Für Seite B klicken Sie auf **+ Add (+ Hinzufügen)**, wählen Sie eine Identifikationsart und einen Zeitplan aus.
7. Klicken Sie auf **OK**.

Einrichten von Identifizierungsprofilen

Bearbeiten eines Identifizierungsprofils

1. Rufen Sie **Configuration > Access control > Identification profiles (Konfiguration > Zutrittskontrolle > Identifizierungsprofile)** auf.
2. Wählen Sie ein Identifizierungsprofil aus und klicken Sie auf .
3. Ändern Sie den Namen des Identifizierungsprofils, indem Sie einen neuen Namen eingeben.
4. Bearbeiten Sie die Einstellungen für die Seite des Zugangs.
5. Um das Identifizierungsprofil auf der anderen Seite des Zugangs zu bearbeiten, wiederholen Sie die vorherigen Schritte.
6. Klicken Sie auf **OK**.

Identifizierungs Profil bearbeiten	
×	Gehen Sie wie folgt vor, um eine Identifikationsart und den zugehörigen Zeitplan zu entfernen.
Identifizierung	Um eine Identifikationsart zu ändern, wählen Sie aus dem Drop-Down Menü **Identification type (Identifikationsart)** eine oder mehrere Identifikationsarten aus.
Zeitschema	Um einen Zeitplan zu ändern, wählen Sie aus dem Drop-Down Menü **Schedule (Zeitplan)** einen oder mehrere Zeitpläne aus.
+ **Hinzufügen**	Fügen Sie eine Identifikationsart und den zugehörigen Zeitplan hinzu, indem Sie auf **Add (Hinzufügen)** klicken und die Identifikationsarten und Zeitpläne festlegen.

Entfernen eines Identifizierungsprofil

1. Rufen Sie **Configuration > Access control > Identification profiles (Konfiguration > Zutrittskontrolle > Identifizierungsprofile)** auf.
2. Wählen Sie ein Identifizierungsprofil aus und klicken Sie auf .

3. Wenn das Identifizierungsprofil für einen Zugang verwendet wird, wählen Sie für den Zugang ein anderes Identifizierungsprofil aus.
4. Klicken Sie auf **OK**.

Zurücksetzten eines vordefinierten Kartenformats

1. Rufen Sie **Configuration > Access Control > Card formats and PIN (Konfiguration > Zutrittskontrolle > Kartenformate und PIN)** auf.
2. Klicken Sie auf , um ein Kartenformat auf die Standardfeldzuordnung zurückzusetzen.

Kartenformate und PIN

Das Kartenformat legt fest, wie ein Leser die Daten einer Karte interpretiert. Es stehen vordefinierte Kartenformate zur Verfügung, die Sie verwenden oder bearbeiten können. Außerdem haben Sie die Möglichkeit, eigene Kartenformate zu erstellen.

Rufen Sie **Configuration > Access Control > Card formats and PIN (Konfiguration > Zutrittskontrolle > Kartenformate und PIN)** auf, um Kartenformate zu erstellen, zu bearbeiten oder zu aktivieren. Sie können auch eine PIN konfigurieren.

Die benutzerdefinierten Kartenformate können die folgenden Datenfelder enthalten, die zur Überprüfen von Anmeldedaten verwendet werden.

Kartennummer – Eine Teilmenge der binären Zugangsdaten, die als Dezimal- oder Hexadezimalzahlen codiert ist. Verwenden Sie die Kartennummer, um eine bestimmte Karte oder einen bestimmten Karteninhaber zu identifizieren.

Einrichtungscode – Eine Teilmenge der binären Zugangsdaten, die als Dezimal- oder Hexadezimalzahlen codiert ist. Verwenden Sie den Gebäude-Zugangscode, um einen bestimmten Endkunden oder Standort zu identifizieren.

PIN-Konfiguration

1. Rufen Sie **Configuration > Access Control > Card formats and PIN (Konfiguration > Zutrittskontrolle > Kartenformate und PIN)** auf.
2. Klicken Sie unter **PIN configuration (PIN-Konfiguration)** auf .
3. Legen Sie **Min PIN length (Min. PIN-Länge)**, **Max PIN length (Max. PIN-Länge)** und **End of PIN character (Ende des PIN-Zeichens)** fest.
4. Klicken Sie auf **OK**.

Erstellen eines Kartenformats

1. Rufen Sie **Configuration > Access Control > Card formats and PIN (Konfiguration > Zutrittskontrolle > Kartenformate und PIN)** auf.
2. **Add card format (Kartenformat hinzufügen)** aufrufen.
3. Geben Sie einen Namen für das Kartenformat ein.
4. Geben Sie im **Feld für die Bitlänge** eine Zahl zwischen 1 und 256 ein.
5. Wählen Sie **Invert bit order (Bit-Reihenfolge invertieren)** aus, falls Sie die Bit-Reihenfolge der vom Kartenleser empfangenen Daten umkehren möchten.
6. Wählen Sie **Invert byte order (Byte-Reihenfolge umkehren)** aus, falls Sie die Byte-Reihenfolge der vom Kartenleser empfangenen Daten umkehren möchten. Diese Option ist nur verfügbar, wenn Sie eine Bitlänge angeben, die man durch acht teilen kann.
7. Wählen Sie die Datenfelder aus und konfigurieren Sie sie so, dass sie im Kartenformat aktiv sind. Entweder **Card number (Kartennummer)** oder **Facility code (Gebäude-Zugangscode)** muss im Kartenformat aktiv sein.

8. Klicken Sie auf **OK**.
9. Um das Kartenformat zu aktivieren, aktivieren Sie das Kontrollkästchen vor dem Namen des Kartenformats.

Hinweis

- Zwei Kartenformate mit der gleichen Bitlänge können nicht gleichzeitig aktiviert sein. Wenn Sie beispielsweise zwei Kartenformate mit 32 Bit definiert haben, kann nur eines davon aktiv sein. Deaktivieren Sie das Kartenformat, um das andere zu aktivieren.
- Kartenformate können nur aktiviert oder deaktiviert werden, wenn der Netzwerk-Tür-Controller im System mit mindestens einem Leser konfiguriert wurde.
- Die vordefinierten Kartenformate können bearbeitet, aber nicht gelöscht werden. Um Änderungen an einem vordefinierten Format rückgängig zu machen, klicken Sie auf das Symbol „Zurücksetzen", um die Standardeinstellungen wiederherzustellen. Von Ihnen erstellte Kartenformate können gelöscht werden.

ⓘ	Klicken Sie auf ⓘ, um ein Beispiel für die Ausgabe nach dem Invertieren der Bit-Reihenfolge anzuzeigen.
Bereich	Legen Sie den Bitbereich der Daten für das Datenfeld fest. Der Bereich muss innerhalb der Werte liegen, die Sie für **Bit length of card reader message (Bitlänge der Kartenleser-Nachricht)** angegeben haben.
Ausgabeformat	Wählen Sie das Ausgabeformat der Daten für das Datenfeld aus. **Decimal (Dezimal)**: Dieses System ist auch als Stellenwertsystem mit der Basiszahl 10 bekannt und besteht aus den Zahlen 0–9. **Hexadecimal (Hexadezimal)**: Dieses System ist ein Stellenwertsystem mit der Basiszahl 16 und verwendet 16 eindeutige Zeichen: die Ziffern 0 bis 9 und die Buchstaben a bis f.
Bit-Reihenfolge des Teilbereichs	Wählen Sie die Bit-Reihenfolge aus. **Little endian (Little-Endian)**: Das erste Bit ist das kleinste (mit der geringsten Bedeutung). **Big endian (Big-Endian)**: Das erste Bit ist das größte (mit der größten Bedeutung).

Einrichten von Kartenformaten

Bearbeiten eines Kartenformats

1. Rufen Sie **Configuration > Access Control > Card formats and PIN (Konfiguration > Zutrittskontrolle > Kartenformate und PIN)** auf.
2. Wählen Sie ein Kartenformat aus und klicken Sie auf ✎.

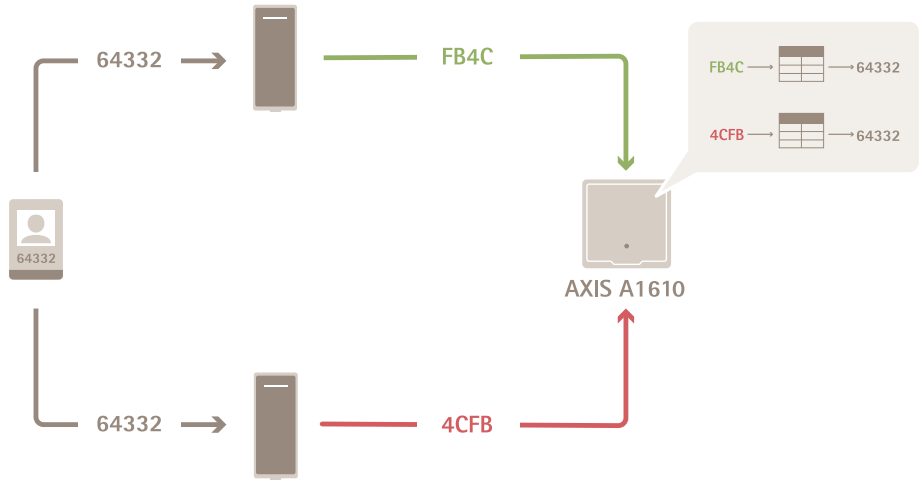
3. Wenn Sie ein vordefiniertes Kartenformat bearbeiten, können Sie nur **Invert bit order (Bit-Reihenfolge invertieren)** und **Invert byte order (Byte-Reihenfolge umkehren)** bearbeiten.
4. Klicken Sie auf **OK**.

Sie können nur die benutzerdefinierten Kartenformate entfernen. So entfernen Sie ein benutzerdefiniertes Kartenformat:

1. Rufen Sie **Configuration > Access Control > Card formats and PIN (Konfiguration > Zutrittskontrolle > Kartenformate und PIN)** auf.
2. Wählen Sie ein benutzerdefiniertes Kartenformat aus, klicken Sie auf und dann auf **Yes (Ja)**.

Einstellungen für das Kartenformat

Übersicht



- Die Kartennummer in Dezimalstellen lautet `64332`.
- Ein Leser wandelt die Kartennummer an die Hexadezimalzahl `FB4C` um. Der andere Leser wandelt sie in die Hexadezimalzahl `4CFB` um.
- Der AXIS A1610 Network Door Controller empfängt die Hexadezimalzahl `FB4C` und wandelt sie entsprechend den auf den Leser angewendeten Kartenformateinstellungen in die Dezimalzahl `64332` um.
- Der AXIS A1610 Network Door Controller empfängt die Hexadezimalzahl `4CFB`, ändert sie durch Umkehrung der Byte-Reihenfolge in `FB4C` und wandelt sie entsprechend den auf den Leser angewendeten Kartenformateinstellungen in die Dezimalzahl `64332` um.

Bit-Reihenfolge umkehren

Nach dem Umkehren der Bit-Reihenfolge werden die vom Leser empfangenen Kartendaten Bit für Bit von rechts nach links ausgelesen.

Byte-Reihenfolge umkehren

Eine Gruppe von acht Bits ist ein Byte. Nach dem Umkehren der Byte-Reihenfolge werden die vom Leser empfangenen Kartendaten Byte für Byte von rechts nach links ausgelesen.

26-Bit-Standard-Wiegand-Kartenformat

1 *Führende Parität*
2 *Einrichtungscode*
3 *Kartennummer*
4 *Angehängte Parität*

Verschlüsselte Kommunikation

OSDP mit Secure Channel

AXIS Camera Station Secure Entry unterstützt OSDP (Open Supervised Device Protocol) Secure Channel, um die Zeilenverschlüsselung zwischen Controller und Axis Lesegeräten zu ermöglichen.

So aktivieren Sie OSDP Secure Channel für ein gesamtes System:

1. Gehen Sie zu **Konfiguration > Zutrittskontrolle > Verschlüsselte Kommunikation**.
2. Geben Sie den Hauptverschlüsselungsschlüssel an und klicken Sie auf **OK**.
3. **OSDP Secure Channel** aktivieren. Diese Option ist nur verfügbar, nachdem Sie den Hauptverschlüsselungsschlüssel eingegeben haben.
4. Standardmäßig wird der OSDP Secure Channel-Schlüssel vom Hauptverschlüsselungsschlüssel generiert. So legen Sie den OSDP Secure Channel-Schlüssel manuell fest:
   4.1. Klicken **Sie unter OSDP Secure Channel** (Sicherer Kanal) auf .
   4.2. **Hauptverschlüsselungsschlüssel zum Generieren des Schlüssels für OSDP mit Secure Channel verwendenentfernen**.
   4.3. Geben Sie den OSDP Secure Channel-Schlüssel ein und klicken Sie auf **OK**.

Informationen zum Aktivieren oder Deaktivieren von OSDP Secure Channel für ein bestimmtes Lesegerät finden Sie unter *Zugänge und Zonen*.

Hinweis

Falls die Zutrittskontrolleinheit, der Host oder das Bedienfeld den OSDP-Sicherheitskanal unterstützt, empfehlen wir Ihnen, diesen auf dem Leser zu aktivieren, um die Kommunikationssicherheit zu erhöhen. Um einen sicheren Kanal zu gewährleisten, setzen Sie den DIP-Schalter Nr. 6 am Leser auf „Ein“.

Der Verschlüsselungsschlüssel wird bei der Ersteinrichtung im Klartext übertragen, daher sollten alle RS485-Verbindungen und -Geräte während dieses Vorgangs überwacht werden.

AXIS Barcode Reader

AXIS Barcode Reader ist eine Anwendung, die auf Axis Kameras installiert werden kann. Der Axis Tür-Controller nutzt den externen Peripherie-Authentifizierungsschlüssel, um den Zugriff zu gewähren und den AXIS Barcodeleser sowie den AXIS License Plate Verifier zu authentifizieren. Für einen vollständigen Workflow zum Einrichten von AXIS License Plate Verifier in AXIS Camera Station Pro, siehe .

AXIS Barcode Reader installieren

1. Laden Sie die Installationsdatei für die Anwendung von *axis.com* herunter
2. Gehen Sie zur Webseite zu Ihrer Axis IP-Türsprechanlage oder Kamera.
3. Installieren Sie die Anwendung.
4. Die Lizenz aktivieren.
5. Starten Sie die Anwendung.
6. Wir empfehlen Ihnen, folgende Kameraeinstellung für eine höhere QR-Genauigkeit zu ändern.
   6.1. Gehen Sie zu Kameraeinstellungen.
   6.2. Bewegen Sie unter **Bild > Belichtung**den Schieberegler **Kompromiss Rauschen zu Bewegungsunschärfe** in die Mitte.

AXIS Barcode Reader konfigurieren

1. Um die QR-Zugangsdaten zu ändern, gehen Sie zu **Configuration > Access control > Identification profiles (Konfiguration > Zutrittskontrolle > Identifizierungsprofile)** und klicken Sie auf . Siehe dazu *Identifizierungsprofile*.
2. Fügen Sie einen Zugang hinzu. Siehe hierzu *Zugang hinzufügen*.
3. Wählen Sie **QR** als Identifizierungsprofil für diesen Zugang. Siehe dazu *Einstellungen des Zugangs*.
4. Fügen Sie einen Barcodeleser hinzu. Siehe dazu *Leser hinzufügen*.
   4.1. Klicken Sie für eine Seite des Zugangs auf **Leser hinzufügen**.
   4.2. Wählen Sie **AXIS Barcode Reader** in der Auswahlliste **Lesertyp**. Geben Sie einen Namen ein und klicken Sie auf **OK**.

1. Um die QR-Zugangsdaten zu ändern, gehen Sie zu **Configuration > Access control > Identification profiles (Konfiguration > Zutrittskontrolle > Identifizierungsprofile)** und klicken Sie auf . Siehe dazu *Identifizierungsprofile*.
2. Fügen Sie einen Zugang hinzu. Siehe hierzu *Zugang hinzufügen*.
3. Wählen Sie **QR** als Identifizierungsprofil für diesen Zugang. Siehe dazu *Einstellungen des Zugangs*.
4. Fügen Sie einen Barcodeleser hinzu. Siehe dazu *Leser hinzufügen*.
   4.1. Klicken Sie für eine Seite des Zugangs auf **Leser hinzufügen**.
   4.2. Wählen Sie **AXIS Barcode Reader** in der Auswahlliste **Lesertyp**. Geben Sie einen Namen ein und klicken Sie auf **OK**.

Eine Verbindung mit dem Zugangscontroller erstellen

1. In AXIS Camera Station Pro:
   1.1. Gehen Sie zu **Konfiguration > Zutrittskontrolle > Verschlüsselte Kommunikation**.
   1.2. Klicken Sie unter **Authentifizierungsschlüssel für externes Peripheriegerät** auf **Authentifizierungsschlüssel anzeigen** und **Schlüssel kopieren**.
2. Gehen Sie auf der Weboberfläche des Geräts, auf dem AXIS Barcode Reader ausgeführt wird, wie folgt vor:
   2.1. Öffnen Sie die Anwendung AXIS Barcode Reader.
   2.2. Wenn das Serverzertifikat in AXIS Camera Station Pro nicht konfiguriert ist, aktivieren Sie **Ignore server certificate validation (Validierung von Serverzertifikaten ignorieren)**. Weitere Informationen dazu finden Sie unter *Zertifikate*.
   2.3. Wenn das Serverzertifikat in AXIS Camera Station Pro nicht konfiguriert ist, aktivieren Sie **Ignore server certificate validation (Validierung von Serverzertifikaten ignorieren)**. Weitere Informationen dazu finden Sie unter *Zertifikate*.

2.4. Aktivieren Sie **AXIS Camera Station Secure Entry**.

2.5. Klicken Sie auf **Hinzufügen**, geben Sie die IP-Adresse des Zugangscontrollers ein und fügen Sie den Authentifizierungsschlüssel ein.

2.6. Wählen Sie im Drop-Down Menü für den Zugang den Leser zum Lesen der Barcodes aus.

Multiserver BETA

Mit Multiserver können globale Karteninhaber und Karteninhabergruppen auf dem Hauptserver von den verbundenen Subservern aus verwendet werden.

Hinweis

- Ein System kann bis zu 64 Subserver unterstützen.
- Dafür ist AXIS Camera Station 5.47 oder höher erforderlich.
- Es ist erforderlich, dass sich der Hauptserver und die Subserver im selben Netzwerk befinden.
- Auf Haupt- und Subservern müssen Sie die Windows-Firewall so konfigurieren, dass auf dem Secure Entry Port eingehende TCP-Verbindungen zulässig sind. Der Standardport ist 55767. Eine individuelle Portkonfiguration finden Sie unter *Allgemeines, on page 218*.
- Durch das Verbinden eines Subservers mit einem Hauptserver wird dessen Leserschlüssel ersetzt, wodurch alle bestehenden Bluetooth-Zugangsdaten ungültig werden. Um dies zu vermeiden, erstellen Sie die Bluetooth-Zugangsdaten auf dem Hauptserver statt auf dem Subserver.

Vorgehensweise

1. Konfigurieren Sie einen Server als Subserver und erstellen Sie die Konfigurationsdatei. Siehe *Die Konfigurationsdatei vom Subserver erstellen, on page 175*.
2. Konfigurieren Sie einen Server als Hauptserver und importieren Sie die Konfigurationsdatei der Subserver. Siehe *Importieren der Konfigurationsdatei auf den Hauptserver, on page 175*.
3. Konfigurieren Sie globale Karteninhaber und Karteninhabergruppen auf dem Hauptserver. Siehe *Karteninhaber hinzufügen, on page 187* und *Gruppe hinzufügen, on page 192*.
4. Auf dem Subserver können Sie die globalen Karteninhaber und Karteninhabergruppen anzeigen und überwachen. Siehe *Zutrittsverwaltung, on page 187*.

Die Konfigurationsdatei vom Subserver erstellen

1. Wechseln Sie vom Subserver zu **Configuration > Access Control > Multi server**.
2. Klicken Sie auf **Subserver**.
3. Klicken Sie auf **Erstellen**. Es wird eine Konfigurationsdatei im JSON-Format erstellt.
4. Klicken Sie auf **Herunterladen** und wählen Sie einen Speicherort für die Datei aus.

Importieren der Konfigurationsdatei auf den Hauptserver

1. Wechseln Sie vom Hauptserver zu **Configuration > Access Control > Multi server**.
2. Klicken Sie auf **Hauptserver**.
3. Klicken Sie auf + **Add (Hinzufügen)** und rufen Sie die vom Subserver generierte Konfigurationsdatei auf.
4. Geben Sie den Servernamen, die IP-Adresse und die Portnummer des Subservers ein.
5. Klicken Sie auf **Import (Importieren)**, um den Subserver hinzuzufügen.
6. Der Status des Subservers zeigt `Connected` an.

Subserver sperren

Sie können einen Subserver nur sperren, bevor die Konfigurationsdatei auf einen Hauptserver importiert wird.

1. Wechseln Sie vom Hauptserver zu **Configuration > Access Control > Multi server**.
2. Klicken Sie auf **Subserver** und klicken Sie auf **Server sperren**.
   Jetzt können Sie diesen Server als Haupt- oder Subserver konfigurieren.

Subserver entfernen

Nach dem Importieren der Konfigurationsdatei eines Subservers ist der Subserver mit dem Hauptserver verbunden.

Subserver entfernen:

1. Vom Hauptserver:
   1.1. Rufen Sie **Access management > Dashboard (Zugriffsverwaltung > Dashboard)** auf.
   1.2. Ändern Sie die globalen Karteninhaber und Gruppen in lokale Karteninhaber und Gruppen.
   1.3. Rufen Sie **Configuration > Access control > Multi server (Konfiguration > Zutrittskontrolle > Multi-Server)** auf.
   1.4. Klicken Sie auf **Main server (Hauptserver)**, um die Liste der Subserver anzuzeigen.
   1.5. Wählen Sie den Subserver aus und klicken Sie auf **Löschen**.
2. Vom Subserver:
   - Rufen Sie **Configuration > Access control > Multi server (Konfiguration > Zutrittskontrolle > Multi-Server)** auf.
   - Klicken Sie auf **Sub server (Subserver)** und dann auf **Revoke server (Server sperren)**.

Active-Directory-Einstellungen[BETA]

Hinweis

Der Zugriff auf AXIS Camera Station Pro erfolgt über Microsoft Windows-Benutzerkonten sowie über die Benutzer und Gruppen in Active Directory. Die Art und Weise, wie Sie Benutzer unter Windows hinzufügen, hängt von Ihrer Version ab. Weitere Informationen finden Sie unter *support.microsoft.com*. Falls Sie ein Active Directory-Domainnnetzwerk verwenden, halten Sie bitte Rücksprache mit Ihrem Netzwerkadministrator.

Wenn Sie die Seite mit den Active Directory-Einstellungen zum ersten Mal öffnen, können Sie Microsoft Active Directory-Benutzer in Karteninhaber in AXIS Camera Station Pro importieren. Siehe *Active-Directory-Benutzer importieren, on page 176*.

Nach der ersten Konfiguration werden auf der Seite mit den Active Directory-Einstellungen die folgenden Optionen angezeigt.

- Erstellen und verwalten Sie Karteninhabergruppen basierend auf Gruppen in Active Directory.
- Richten Sie eine geplante Synchronisierung zwischen Active Directory und dem Zugriffsverwaltungssystem ein.
- Führen Sie eine manuelle Synchronisierung durch, um alle aus Active Directory importierten Karteninhaber zu aktualisieren.
- Verwalten Sie die Datenzuordnung zwischen Benutzerdaten aus Active Directory und Karteninhabereigenschaften.

Active-Directory-Benutzer importieren

So importieren Sie Active Directory-Benutzer in Karteninhaber in AXIS Camera Station Pro:

1. Rufen Sie **Configuration (Konfiguration)** > **Access control (Zutrittskontrolle)** > **Active directory settings (Active-Directory-Einstellungen)**[BETA] auf.
2. Klicken Sie auf **Set up import (Import einrichten)**.
3. Befolgen Sie die Anweisungen auf dem Bildschirm, um diese drei Hauptschritte abzuschließen:

3.1. Wählen Sie einen Benutzer aus Active Directory aus, der als Vorlage für die Datenzuordnung verwendet werden soll.

3.2. Ordnen Sie Benutzerdaten aus der Active Directory-Datenbank den Karteninhabereigenschaften zu.

3.3. Erstellen Sie im Zutrittsverwaltungssystem eine neue Karteninhabergruppe und wählen Sie aus, welche Active Directory-Gruppen importiert werden sollen.

Die importierten Benutzerdaten können nicht geändert werden. Sie können jedoch dem importierten Karteninhaber Zugangsdaten hinzufügen. Informationen dazu finden Sie unter *Zugangsdaten hinzufügen, on page 189*.

Wichtig

Wenn Sie einen Benutzer in Active Directory deaktivieren, löscht AXIS Camera Station Pro den Karteninhaber und alle zugehörigen Daten, einschließlich der Verlaufsdaten, endgültig. Diese Aktion kann nicht rückgängig gemacht werden. Um den Zugang eines Karteninhabers zu sperren, ohne dessen Daten zu verlieren, setzen Sie seine Zugangsberechtigung in AXIS Camera Station Pro aus, anstatt ihn in Active Directory zu deaktivieren.

Konfiguration von AXIS Audio Manager Pro

Sie können sich mit einem AXIS Audio Manager Pro-Server verbinden und die damit verbundenen Audiogeräte in AXIS Camera Station Pro verwenden.

Für diese Konfiguration sind AXIS Camera Station Pro 6.12 oder höher und AXIS Audio Manager Pro 5.0 oder höher erforderlich. Sowohl der AXIS Camera Station Pro- als auch der AXIS Audio Manager Pro-Server müssen im Voraus eingerichtet werden, entweder auf demselben Server oder auf verschiedenen Rechnern im selben Netzwerk.

Wichtig

Bei der Ausführung von AXIS Camera Station Pro und AXIS Audio Manager Pro auf demselben Server werden beide standardmäßig für die Verwendung von Port 443 konfiguriert. Um Verbindungsprobleme zu vermeiden, stellen Sie für eine Software einen anderen Port ein.

Sie können die Portkonfiguration in AXIS Camera Station Pro über *Allgemeines, on page 218* anpassen. Weitere Informationen zur Anpassung der Portkonfiguration in AXIS Audio Manager Pro finden Sie im *Benutzerhandbuch zu AXIS Audio Manager Pro*.

Erste Schritte mit AXIS Audio Manager Pro in AXIS Camera Station Pro:

1. Im AXIS Audio Manager Pro:
   1.1. Gehen Sie zu **System settings (Systemeinstellungen)** > **API access (API-Zugriff)**.
   1.2. Aktivieren Sie die API und geben Sie einen Benutzernamen und ein Kennwort ein.
2. In AXIS Camera Station Pro:
   2.1. Öffnen Sie **Configuration (Konfiguration)** > **AXIS Audio Manager Pro** und klicken Sie auf **Connect (Verbinden)**, um eine Verbindung zu Ihrem AXIS Audio Manager Pro-Server einzurichten.
   2.2. Geben Sie im Popup-Dialog **Server URL (URL des Servers)**, **API username (API-Benutzername)** und **API password (API-Kennwort)** Ihres AXIS Audio Manager Pro-Servers ein und klicken Sie auf **Connect (Verbinden)**.

Sobald die Verbindung hergestellt ist, haben Sie folgende Optionen:

- **Server status (Serverstatus)** des AXIS Audio Manager Pro-Servers und **Device status (Gerätestatus)** der mit diesem Server verbundenen Geräte anzeigen.
- Neue AXIS Audio Manager Pro-Registerkarte öffnen, um auf die Weboberfläche des Servers zuzugreifen.
- Neue Audiofunktionen in AXIS Camera Station Pro verwenden.

Weitere Informationen finden Sie unter *AXIS Audio Manager Pro, on page 209*.

Hinweis

Um Probleme mit Zertifikaten zu vermeiden, empfehlen wir Ihnen, ein Zertifikat bei einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) zu erstellen oder zu erwerben, es in AXIS Audio Manager Pro hochzuladen und zur Liste der vertrauenswürdigen Zertifikate des AXIS Camera Station Pro-Servers hinzuzufügen. Weitere Informationen finden Sie im *Benutzerhandbuch zu AXIS Audio Manager Pro*.

Intelligente Suche 2 konfigurieren

Mithilfe von „Intelligente Suche 2" können Sie mehrere Filter festlegen, um in den mit Axis Kameras gemachten Aufzeichnungen auf einfache Weise Personen und Fahrzeuge zu finden.

Informationen zu Anforderungen, Einschränkungen und Verwendung dieser Funktion finden Sie unter *Intelligente Suche 2, on page 37*.

1. Gehen Sie zu **Configuration > Smart search 2 (Konfiguration > Intelligente Suche 2) > Settings (Einstellungen)**.
2. Unter **Cameras (Kameras)**:
   2.1. Wählen Sie die Kameras, die Metadaten an „Intelligente Suche 2" senden sollen.
   2.2. Um für eine Kamera die Server-Klassifizierung im Hintergrund zuzulassen, wählen Sie **Allow (Zulassen)** bei der Option **Background server classification (Server-Klassifizierung im Hintergrund)**.
   Dadurch wird zwar die Server-Auslastung erhöht, aber das Benutzererlebnis verbessert.
   2.3. Klicken Sie zur Begrenzung der Anzahl der auf dem Server gespeicherten Erfassungen unter **Filter (Filtern)** ⚙ an und erstellen Sie Filter für **Area (Bereich)**,**Size and duration (Größe und Dauer)** sowie **Swaying objects (schaukelnde Objekte)**.
   Mit diesen Filtern können Sie Ausschlussbereiche, kleine Objekte oder Objekte, die nur sehr kurz erscheinen, und schwankende Objekte wie Laub ausschließen.
   Die Suchfilter der intelligenten Suche verwenden alle vorhandenen Bewegungseinstellungsfilter als Ausgangspunkt.
3. Unter **Speicher**:
   – Wählen Sie das Laufwerk und den Ordner zum Speichern der Erfassungen aus und klicken Sie auf **Anwenden**.
   – Legen Sie das Speichergrößenlimit fest und klicken Sie auf **Anwenden**. Die ältesten Erfassungen werden entfernt, wenn der Speichergrenzwert erreicht wird.
4. Wählen Sie **Include periods with missing metadata (Zeiträume mit fehlenden Metadaten einschließen)**, um nach Zeiträumen zu suchen, in denen keine Metadaten aufgezeichnet wurden, und diese anzuzeigen.
5. Aktivieren Sie die Option **Let the server classify detections when you start a search (Server Klassifizierung von Erfassungen erlauben, wenn Suche gestartet wird)**, um detailliertere Suchergebnisse zu erhalten, die auch von der Kamera nicht klassifizierte Erfassungen enthalten. Für eine schnellere Suche empfiehlt es sich, diese Option zu deaktivieren.

Klassifizierung durch den Server im Hintergrund	
	Serverklassifizierungsstatus ab der letzten Stunde, wenn die Serverklassifizierung langsam ist. Wird angezeigt, wenn weniger als 95 % der Erfassungen klassifiziert sind.
	Serverklassifizierungsstatus ab der letzten Stunde, wenn die Serverklassifizierung langsam ist. Wird angezeigt, wenn weniger als 50 % der Erfassungen klassifiziert sind.

Trigger

Sie können intelligente Suchfilter konfigurieren, die als Auslöser in Aktionsregeln verwendet werden können. So erstellen Sie einen Auslöser mit der intelligenten Suchfunktion:

1. Gehen Sie zu **Configuration (Konfiguration)** > **Smart search 2 (Intelligente Suche 2)** > **Triggers (Auslöser)**.
2. Klicken Sie auf **Create (Erstellen)**.
3. Konfigurieren Sie Ihre Filter. Weitere Informationen zu intelligenten Suchfiltern finden Sie unter *Suche mit Filtern, on page 37*.
4. Klicken Sie auf **Next (Weiter)**.
5. Passen Sie unter **Confidence (Zuverlässigkeitsstufe)** die Vertrauenswürdigkeit der Erfassungen an. Bei einer höheren Zuverlässigkeitsstufe werden unsichere Klassifizierungen ignoriert, was die Anzahl der Erfassungen reduziert.
6. Klicken Sie auf **Next (Weiter)**.
7. Geben Sie einen Namen für Ihren Auslöser ein und klicken Sie auf **Save (Speichern)**.

Hinweis

- Die Funktion Intelligente Suche 2 benötigt in der Regel einige Sekunden nach Verlassen des Kamerasichtfelds durch ein Objekt, um die Videodaten zu analysieren und zu überprüfen, was erfasst wurde. Wenn Sie beispielsweise eine Aktionsregel festgelegt haben, die bei der Erfassung eines roten Fahrzeugs ausgelöst wird, erfolgt das Auslösen der Aktion erst einige Sekunden, nachdem das Fahrzeug den Kamerabereich verlassen und die intelligente Suche ein rotes Fahrzeug erkannt hat.
- **Visual similarity (Visuelle Ähnlichkeit)** ist nicht als Option für Auslöser verfügbar, die die Funktion Intelligente Suche 2 nutzen.
- Durch das Erstellen eines Auslösers für eine Kamera kann der Server Objekterfassungen verarbeiten, auch wenn für diese Kamera die Option **Enable background processing (Verarbeitung im Hintergrund aktivieren)** deaktiviert ist.
- Bei der Option **Delayed detection periods (Zeiträume mit verzögerter Erfassung)** handelt es sich um Zeiträume mit einer hohen Verarbeitungsverzögerung, die zu einer verspäteten Auslösung von Aktionsregeln geführt haben. Treten diese häufig auf, können Sie Ihren Auslöser so anpassen, dass er weniger Kameras einschließt, und Kamerafilter wie das Überfahren/Überschreiten von Linien, Bereich, Größe und Dauer nutzen, um das Problematik zu minimieren.

Weitere Informationen zur Verwendung von Auslösern mit der Intelligenten Suche 2 in einer Aktionsregel finden Sie unter *Auslöser mit der Funktion Intelligente Suche 2 erstellen, on page 104*.

Konfigurieren Sie Überwachung des Systemzustands BETA

Hinweis

- Bei Verbindung zu mehreren AXIS Camera Station Pro Servern können Sie die Überwachung des

Systemzustands für jeden verbundenen Server konfigurieren. Wählen Sie dazu den Server aus dem Drop-Down Menü **Selected server (Ausgewählter Server)** aus.

- Wenn Sie Systeme in verschiedenen Netzwerken verwalten, stellt die Server-Überwachung in „My Systems" (Meine Systeme) die gleichen Funktionen über die Cloud bereit.

Einstellungen

Cloud-Verbindung	Wenn Sie Ihren Server bei einer Organisation registriert haben, können Sie Ihre Daten zum Systemzustand von jedem Ort aus einsehen. Wenn Sie noch nicht verbunden sind, klicken Sie **Manage (Verwalten)** an und befolgen Sie die Anweisungen auf dem Bildschirm.
Data retrieval frequency (Datenabruffrequenz)	Wählen Sie eine niedrigere Datenfrequenz aus, um Warnungen in Bezug auf alte Daten oder allgemeine Leistungsprobleme im System zu beheben. Bei einem Multisystem-Setup wird empfohlen, für ein Untersystem mindestens die gleiche Einstellung wie für das übergeordnete System zu verwenden. • **Low (Niedrig)**: Für Systeme mit über 100 Geräten. • **Medium (Mittel)**: Für Systeme mit 25 bis 100 Geräten. • **High (Hoch)**: Für Systeme mit weniger als 25 Geräten.

Benachrichtigungen

Um Benachrichtigungen per E-Mail zu senden:

1. Konfigurieren Sie einen SMTP-Server und eine E-Mail-Adresse zum Senden der Benachrichtigungen. Siehe *Servereinstellungen, on page 127*
2. Konfigurieren Sie die E-Mail-Adressen, um die Benachrichtigungen zu empfangen. Siehe *E-Mail-Empfänger konfigurieren, on page 180*.
3. Konfigurieren sie die Benachrichtigungsregeln. Siehe *Benachrichtigungsregeln konfigurieren, on page 180*.

E-Mail-Empfänger konfigurieren

1. Rufen Sie **Konfiguration > Überwachung des Systemzustands > Benachrichtigungen** auf.
2. Geben Sie unter **E-Mail-Empfänger** eine E-Mail-Adresse ein und wählen Sie **Speichern**. Wiederholen Sie diesen Vorgang, um mehrere E-Mail-Empfänger hinzuzufügen.
3. Um den SMTP-Server zu testen, klicken Sie auf **Test-E-Mail senden**. Eine Meldung zeigt, dass die Test-E-Mail gesendet wurde.

Benachrichtigungsregeln konfigurieren

Es gibt zwei standardmäßig aktivierte Benachrichtigungsregeln.

System ausgefallen – Senden Sie eine Benachrichtigung, wenn das System in einem Einzelsystem-Setup oder ein beliebiges System in einem Multisystem-Setup länger als normal ausfällt.

Gerät ausgefallen – Senden Sie eine Benachrichtigung, wenn ein in der Überwachung des Systemzustands aufgeführtes Gerät länger als normal ausfällt.

1. Rufen Sie **Konfiguration > Überwachung des Systemzustands > Benachrichtigungen** auf.

2. Schalten Sie unter **Notification rules (Benachrichtigungsregeln)** die Benachrichtigungsregeln ein oder aus.
3. Unter **Applied rules (Angewandte Regeln)** wird eine Liste der Systeme und Geräte mit der angewendeten Benachrichtigungsregel angezeigt.

Multisystem

Mit der Überwachung des Systemzustands können Sie die Zustandsdaten mehrerer sekundärer Systeme von einem Hauptsystem aus überwachen.

1. Erstellen Sie in einem sekundären System die Systemkonfiguration. Siehe *Systemkonfiguration erstellen, on page 181*.
2. Laden Sie im Hauptsystem die Systemkonfiguration hoch. Siehe *Daten von anderen Systemen abrufen, on page 181*.
3. Wiederholen Sie die vorherigen Schritte in anderen sekundären Systemen.
4. Überwachen Sie die Daten zum Gerätezustand mehrerer Systeme vom Hauptsystem aus. Siehe *Überwachung des Systemzustands [BETA], on page 199*.

Systemkonfiguration erstellen

1. Rufen Sie **Konfiguration > Überwachung des Systemzustands > Multisystem** auf.
2. Klicken Sie auf **Erstellen**.
3. Klicken Sie auf **Kopieren**, um den Upload auf das Hauptsystem zu ermöglichen.
4. Um die Details der Systemkonfiguration anzuzeigen, klicken Sie auf **Details anzeigen**.
5. Um die Systemkonfiguration neu zu erstellen, klicken Sie auf **Löschen**, um die bestehende Konfiguration zu löschen.

Nach dem Hochladen der Systemkonfiguration in das Hauptsystem werden die Hauptsysteminformationen unter **Systems with access (Systeme mit Zugriff)** angezeigt.

Daten von anderen Systemen abrufen

Nachdem Sie die Systemkonfiguration eines sekundären Systems erstellt und kopiert haben, können Sie sie in das Hauptsystem hochladen.

1. Rufen Sie im Hauptsystem **Konfiguration > Überwachung des Systemzustands > Multisystem** auf.
2. Klicken Sie auf **Paste (Einfügen)**, um die aus dem sekundären System kopierten Informationen einzufügen.
3. Überprüfen Sie die IP-Adresse des Hosts und klicken Sie auf **Hinzufügen**.
   Das sekundäre System wird unter **Available systems (Verfügbare Systeme)** angezeigt.

Analysefunktionen konfigurieren

AXIS Data Insights Dashboard

AXIS Data Insights Dashboard stellt die Analysedaten Ihrer Geräte in Grafiken und Diagrammen dar. Die Konfigurationsseite für AXIS Data Insights Dashboard zeigt alle unterstützten Anwendungen und konfigurierten

Szenarien auf den Geräten in Ihrem System an. Rufen Sie **Analytics (Analysefunktionen)** > **Data Insights Dashboard** für Folgendes auf:

- Eine Liste der Kameras und Datenquellen anzeigen, auf denen die unterstützten Anwendungen laufen.
- Eine Liste der unterstützten Anwendungen und Szenarien für jedes Gerät oder jede Datenquelle anzuzeigen. Wir unterstützen Folgendes:
  - AXIS Object Analytics: Querschnittszählung und Belegung von Bereichen
  - AXIS Audio Analytics
  - AXIS Image Health Analytics
  - AXIS People Counter
  - AXIS P8815-2 3D Counter
  - AXIS Air Quality Sensors (Luftqualitätsmonitor)

  Hinweis

  Sie können eine Datenmenge von maximal 100 MB speichern, was die Speicherdauer begrenzt. So ergibt sich zum Beispiel für einen Luftqualitätssensor, der alle 12 Datentypen überwacht, eine Speicherdauer von etwa 430 Tagen.
- Wählen Sie aus, welche Szenarien in das Dashboard integriert werden sollen.
- Gruppieren Sie Szenarien, um das Filtern von Daten im Dashboard zu aktivieren, z. B. um Kameras am selben Standort zu gruppieren.

Hinweis

Um die Daten der AXIS Object Analytics Personenzählung im Dashboard **In and Out counting (Zählen der Eintritte und Austritte)** anzuzeigen, wählen Sie die Richtung des Szenarios, indem Sie **In (Eintritte)** oder **Out (Austritte)** im Feld **Direction (Richtung)** auswählen.

- Den Status von Szenarien anzeigen.

Einschließen	Aktivieren Sie den Schalter in der Spalte **Include (Einbeziehen)**, um die Daten eines Szenarios in einem Dashboard anzuzeigen.
Tags	Wählen Sie in der Spalte **Tags (Registerkarten)** Registerkarten aus dem Drop-Down Menü aus, um sie zu einem Szenario hinzuzufügen.

So fügen Sie einen neuen Tag hinzu:

1. Öffnen Sie die Registerkarte **Tags**.
2. Geben Sie einen Namen für den Tag ein.
3. Klicken Sie auf den Pfeil.

Hinweis

- AXIS Data Insights Dashboard erfordert verschlüsselte Verbindungsprotokolle TLS Version 1.2 und höher auf Ihrem Windows-Server.
- AXIS Data Insights Dashboard hat Vorrang vor allen vorhandenen MQTT-Einstellungen auf einer Kamera, wenn:
  - Die Kamera keinen konfigurierten MQTT-Client hat.

  - Sie manuell ein Szenario für eine Kamera aktivieren, die mit einem anderen AXIS Camera Station Pro Server verbunden ist.
- Bei Verbindung mit AXIS Data Insights Dashboard ist der MQTT-Client der Kamera nur Data Insights Dashboard zugeordnet.
- Die Kameras und der AXIS Camera Station Pro Server müssen sich im selben Netzwerk befinden.
- Für optimale Leistung wird ein Server mit mindestens 16 GB RAM für die Ausführung von AXIS Data Insights Dashboard in AXIS Camera Station Pro empfohlen.
- Es können maximal 100 MB Daten gespeichert werden, was zu einer begrenzten Speicherzeit führt. Zum Beispiel:
  - Die geschätzte Belegungsdauer auf einem Parkplatz, der mit vier Kameras ausgestattet ist, von denen jede so konfiguriert ist, dass sie rund um die Uhr fünf Unterklassen von Fahrzeugen wie Autos und Fahrräder erkennt, ergibt eine Aufbewahrungszeit von 260 Tagen.
  - Die Personenzählung in einer Einzelhandelsumgebung, die mit acht Kameras ausgestattet ist und in der der Personenstrom 12 Stunden lang ununterbrochen ist, ergibt eine Aufbewahrungszeit von etwa 1270 Tagen.
  - Eine Kamera, die ein Szenario mit sechs Klassen und einem Zählfluss von 24 Stunden durchläuft, ergibt eine Aufbewahrungszeit von etwa 860 Tagen.

Weitere Informationen zum Hinzufügen eines Dashboards zu einer geteilten Ansicht finden Sie unter *AXIS Data Insights Dashboard in einer geteilten Ansicht, on page 20*.

Aktivieren von AXIS Data Insights Dashboard

Kennzeichenüberprüfung

Sie können den Status des AXIS License Plate Verifier ACAP auf Ihren Kameras und Kameragruppen anzeigen, um die Verwaltung der Kennzeichenliste auf der Seite „Kennzeichenprüfer" zu vereinfachen.

Die Registerkarte **Cameras (Kameras)** enthält eine Liste aller angeschlossenen Geräte mit installiertem AXIS License Plate Verifier:

- **Kamera**: Der Name der Kamera.
- **Version**: Die Version von AXIS License Plate Verifier, die auf der Kamera installiert ist.
- **Status**: Der aktuelle Status von AXIS License Plate Verifier.
- **Latest event (Letztes Ereignis)**: Der Zeitpunkt des letzten von der Kamera aufgezeichneten Ereignisses.
- **Allowed (Zugelassen)**: Die Anzahl der Kennzeichen, die in der Liste „Zulässig" der Kamera enthalten sind.
- **Blocked (Gesperrt)**: Die Anzahl der Kennzeichen, die in der Liste „Gesperrt" der Kamera enthalten sind.
- **Benutzerdefiniert**: Die Anzahl der Kennzeichen, die in der Liste „Benutzerdefiniert" der Kamera enthalten sind.
- **Gruppe**: Zu welcher Gruppe die Kamera gehört.

Die Registerkarte **Groups (Gruppen)** enthält eine Liste aller Kameragruppen und eine Unterliste der in jeder Gruppe enthaltenen Kameras. Auf diesem Tab haben Sie folgende Möglichkeiten:

- Klicken Sie auf **New... (Neu...)**, um eine neue Gruppe hinzuzufügen.

- Klicken Sie auf **Delete (Löschen)**, um eine vorhandene Gruppe zu löschen.
- Benennen Sie eine ausgewählte Gruppe im Feld **Group name (Gruppenname)** um.
- Klicken Sie auf **Add... (Hinzufügen...)**, um eine Kamera zu einer ausgewählten Gruppe hinzuzufügen.
- Klicken Sie auf **Remove (Entfernen)**, um eine Kamera aus einer Gruppe zu entfernen.

Sie können gemeinsame Listen für gruppierte Kameras erstellen. Weitere Informationen finden Sie unter *Fahrzeugkennzeichen-Verwaltung, on page 208*.

Konfiguration von Body Worn-Geräten

Anschließen eines Body Worn-Systems

Verbinden Sie Ihr am Körper getragenes System mit AXIS Camera Station Pro, um Aufzeichnungen und Metadaten von Body Worn-Kameras zu übertragen.

1. Gehen Sie zu **Configuration (Konfiguration) > Body worn (Am Körper getragene Geräte) > Connect a body worn system (Anschließen eines Body Worn-Systems)**.
2. Wählen Sie unter **Connection method (Verbindungsmethode)** aus, wie Sie die Verbindung herstellen möchten:
   - **Direkt verbinden**: Geben Sie die IP-Adresse und die Zugangsdaten des Body Worn Managers ein, um eine direkte Verbindung herzustellen.
   - **Verbindungsdatei generieren**: Erstellen Sie eine Konfigurationsdatei, die Sie in Ihren Body Worn Manager hochladen können.

Hinweis

Bevor Sie die Verbindungsdatei erstellen, müssen Sie das Serverzertifikat erneuern, wenn sich die IP-Adresse des Servers geändert hat oder AXIS Camera Station von einer Version vor 5.33 aktualisiert wurde. Wie Sie das Zertifikat erneuern können, erfahren Sie unter *Zertifikate, on page 143*.

Wenn Sie **Direkt verbinden:** ausgewählt haben

3. Geben Sie unter **Configure direct connection (Direkte Verbindung konfigurieren)** die **IP-Adresse**, den **Benutzernamen** und das **Kennwort** für Ihren Body Worn Manager ein.

1. Gegebenenfalls ändern Sie den **Systemnamen von AXIS Camera Station**. Dieser Name gibt an, wohin Aufzeichnungen kopiert oder übertragen werden.
2. Wenn Sie alle bestehenden Verbindungen beenden möchten, wählen Sie **End existing connections (Bestehende Verbindungen beenden)**. Anschließend müssen Sie die neue Verbindungsdatei auf jeden Controller des AXIS Body Worn Systems hochladen.
3. **Connect (Verbinden)** anklicken.

Wenn Sie **Verbindungsdatei generieren** ausgewählt haben:

4. Ändern Sie unter **Verbindungsdatei generieren** optional den **Systemnamen von AXIS Camera Station**. Dadurch sind Sie in der Lage festzustellen, wohin Aufzeichnungen kopiert oder übertragen werden.
   4.1. Wenn Sie alle bestehenden Verbindungen beenden möchten, wählen Sie **End existing connections (Bestehende Verbindungen beenden)**. Anschließend müssen Sie die neue Verbindungsdatei auf jeden Controller des AXIS Body Worn Systems hochladen.
   4.2. Klicken Sie auf **Export (Exportieren)** und speichern Sie die Verbindungsdatei.
   4.3. Laden Sie die Verbindungsdatei in Ihren Body Worn Manager hoch.

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

Ein Axis Body Worn-Systems einrichten

Aufzeichnungen einer Axis Body Worn-Kamera abspielen und exportieren

Momentaufnahmen

Exportieren Sie Momentaufnahmen automatisch aus den Lesezeichen der Body Worn-Kamera in einen Ordner, wenn die Aufzeichnungen an AXIS Camera Station Pro übertragen werden.

1. Gehen Sie zu **Configuration (Konfiguration) > Body worn (Am Körper getragene Geräte) > Snapshots (Momentaufnahmen)**.
2. Geben Sie unter **Storage location (Speicherort)** den Ordnerpfad ein, in dem Sie die Momentaufnahmen speichern möchten.
3. Klicken Sie auf **Anwenden**.
4. Aktivieren Sie **Snapshot export (Momentaufnahmen exportieren)**.

CAD-Integration

Integrieren Sie Ihr computergestütztes Einsatzleitsystem (CAD), um Aufzeichnungen von Body Worn-Kameras anhand der Einsatzdaten automatisch zu kategorisieren.

So richten Sie die Integration ein:

1. Gehen Sie zu **Configuration (Konfiguration) > Body worn (Am Körper getragene Geräte) > CAD integration (CAD-Integration)**.
2. Klicken Sie auf **Set up integration (Integration einrichten)**.
3. Wählen Sie Ihr Dateiformat (CSV oder XML) aus und klicken Sie auf **Next (Weiter)**.
4. Schalten Sie die Option **Shared network drive (Freigegebenes Netzwerklaufwerk)** ein, falls sich Ihre CAD-Datei auf einem gemeinsamen Netzlaufwerk befindet.
5. Geben Sie den Ordnerpfad der CAD-Datei, den Dateinamen (nur CSV) und das Spaltentrennzeichen ein.
6. Klicken Sie auf **Next (Weiter)**.
7. Ordnen Sie jedes Feld der Kennung zu, wie sie in Ihrer CAD-Datei erscheint:
   - **Officer name (Name des Beamten)**: Muss mit den Namen der virtuellen Kameras in AXIS Camera Station Pro übereinstimmen. Sollte der Name nicht übereinstimmen, aktualisieren Sie ihn im Body Worn Manager und nicht in AXIS Camera Station Pro.
   - **Event ID (Ereignis-ID)**: eindeutige Sendungskennung.
   - **Call category (Anrufkategorie)**: Aufzeichnungskategorie. Falls sie nicht existiert, wird sie erstellt.
   - **Dispatch time (Sendezeit)**: Startzeit im RFC-3339-Format, z. B. „2025-11-25T09:49:17+01:00".
   - **Clearance time (Abschlusszeit)**: Endzeit im RFC-3339-Format.
   - **Case number (Fallnummer)**: die mit dem Auftrag verknüpfte Fall-ID. Die Spalten muss in der Datei vorhanden sein, der Wert kann jedoch leer bleiben.
8. Klicken Sie auf **Finish (Fertigstellen)** und anschließend auf **Apply (Übernehmen)**.

9. Um Ihre Aufzeichnungen anzusehen, klicken Sie auf + und wählen Sie **CAD recordings (CAD-Aufzeichnungen)**, um alle automatisch kategorisierten Aufzeichnungen anzuzeigen. Sie können nach Zeit oder nach dem Namen des Beamten filtern.

Hinweis

Wenn neue Kategorien automatisch erstellt werden, müssen Sie deren Speicherdauern manuell festlegen.

Einschränkungen
Es kann zu Datenverlusten kommen, wenn:

- AXIS Camera Station Pro oder die Komponente wird nicht ausgeführt.
- Die Exportdateien sind größer als 1 GB.
- Die Netzwerk-Zugangsdaten müssen aktualisiert werden.

Body Worn-Einstellungen

Konfigurieren Sie Speicherorte für Aufzeichnungen von am Körper getragenen Geräten.

Aufzeichnungsspeicher
Wählen Sie einen Speicherort für Body Worn-Aufzeichnungen, der standardmäßig für neue Body Worn-System-Benutzer verwendet wird.

1. Gehen Sie zu **Configuration (Konfiguration) > Body worn (Am Körper getragene Geräte) > Body worn settings (Einstellungen für am Körper getragene Geräte)**.
2. Wählen Sie unter **Recording storage (Aufzeichnungsspeicher)** im Dropdown-Menü **Disk (Datenträger)** einen Datenträger aus.
3. Klicken Sie auf **Save (Speichern)**.

Speicher abgelehnter Aufzeichnungen
Wählen Sie aus, wo Sie abgelehnte Inhalte aus dem Body Worn-System speichern möchten.

1. Wählen Sie unter **Rejected recordings storage (Speicher für abgelehnte Aufzeichnungen)** im Dropdown-Menü **Disk (Datenträger)** einen Datenträger aus und geben Sie einen **Ordnernamen** ein.
2. Stellen Sie die Anzahl der Tage ein, für die abgelehnte Inhalte in **Anzahl der Tage, die abgelehnte Inhalte aus dem Body Worn-System behalten werden sollen** aufbewahrt werden sollen.
3. Klicken Sie auf **Save (Speichern)**.

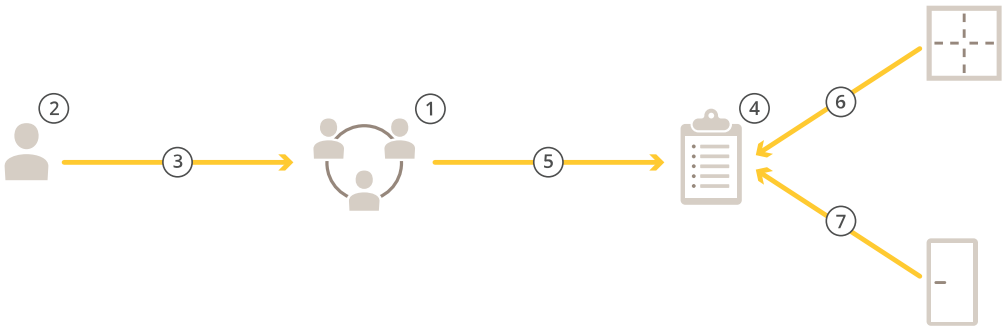
Zutrittsverwaltung

Auf der Registerkarte „Access Management (Zugriffsverwaltung)" können Sie die Karteninhaber, Gruppen und Zugangsregeln des Systems konfigurieren und verwalten.

Die vollständige Vorgehensweise zum Einrichten eines Axis Network Door Controller in AXIS Camera Station Pro finden Sie unter *Einrichten eines Axis Network Door Controllers*.

Vorgehensweise bei der Zugriffsverwaltung

Die Struktur der Zugriffsverwaltung ist flexibel. Gehen Sie anhand der Anforderungen der jeweiligen Anwendung vor. Im Folgenden finden Sie ein Beispiel für eine Vorgehensweise:



1. *Gruppe hinzufügen, on page 192*.
2. *Karteninhaber hinzufügen, on page 187*.
3. Fügen Sie Karteninhaber und Gruppen hinzu.
4. *Zugangsregel hinzufügen, on page 192*.
5. Ordnen Sie Zugangsregeln Gruppen zu.
6. Ordnen Sie Zugangsregeln Zonen zu.
7. Ordnen Sie Zugangsregeln Zugänge zu.

Karteninhaber hinzufügen

Ein Karteninhaber ist eine Person mit einer eindeutigen ID, die im System registriert ist. Konfigurieren Sie einen Karteninhaber mit Zugangsdaten, die dem System mitteilen, wer die Person ist und wann und wie der Person die Nutzung von Zugängen gewährt wird.

Sie können Benutzer auch über eine Active-Directory-Datenbank als Karteninhaber zuweisen (siehe *Active-Directory-Einstellungen*[BETA]*, on page 176*).

1. Öffnen Sie eine Registerkarte Access Management (Zugangsverwaltung).
2. Rufen Sie **Cardholder management (Karteninhaberverwaltung)** > **Cardholders (Karteninhaber)** und klicken Sie auf **+ Add (+ Hinzufügen)**.
3. Geben Sie den Vor- und Nachnamen des Karteninhabers ein. Optional können Sie weitere Angaben zum Karteninhaber machen:
   - Geben Sie unter **E-Mail** die E-Mail-Adresse des Karteninhabers ein.
   - Wählen Sie unter **Groups (Gruppen)** die Gruppen aus, denen Sie den Karteninhaber hinzufügen möchten.
   - Wählen Sie unter **Access rules (Zugangsregeln)** die Regeln aus, die Sie auf den Karteninhaber anwenden möchten.

4. Um ein Foto hinzuzufügen, klicken Sie auf **Cardholder picture (Karteninhaberfoto)** und wählen Sie eine der folgenden Optionen aus:
   - **Upload (Hochladen)**, um ein Bild von Ihrem Gerät hinzuzufügen.
   - **Capture (Fotografieren)**, um direkt mit Ihrer Kamera ein Foto aufzunehmen.

   Hinweis

   Bei dem Bild muss es sich um eine JPG-, PNG- oder GIF-Datei handeln. Bilder werden automatisch auf eine maximale Größe von 700 x 700 Pixel skaliert und in das JPG-Format umgewandelt.
5. Klicken Sie auf **Advanced (Erweitert)**, um zusätzliche Einstellungen vorzunehmen.
6. Fügen Sie Zugangsdaten für den Karteninhaber hinzu. Siehe *Zugangsdaten hinzufügen, on page 189*.
7. **Save (Speichern)** anklicken.
8. Um Ausweise für einen oder mehrere Karteninhaber zu drucken, wählen Sie den/die Karteninhaber aus und klicken Sie auf **Print Badge**[BETA] **(Ausweis drucken)**. Weitere Informationen finden Sie unter *Print badge (Ausweis drucken) [BETA], on page 198*.

Im Suchfeld können Sie einen Karteninhaber mit seinem Vor- oder Nachnamen suchen. Um nach einer Quelle zu filtern, klicken Sie auf **Filter** und wählen Sie dann **Local (Lokal)**, **Global**, **(AD)** oder **Center** aus.

Erweitert	
Lange Zugriffszeit	Wählen Sie diese Option aus, damit für den Karteninhaber eine lange Zutrittszeit und eine lange Dauer für einen zu lange geöffneten Zugang gelten sollen, wenn ein Zugangsmonitor installiert ist.
Karteninhaber suspendieren	Wählen Sie diese Option aus, um den Karteninhaber zu suspendieren. Diese Option setzt vorübergehend alle Zugangsberechtigungen des Karteninhabers aus.
Allow double-swipe (Double Swipe zulassen)	Auswählen, um einem Karteninhaber zu erlauben, den aktuellen Zustand eines Zugangs außer Kraft zu setzen. Dies kann beispielsweise dazu verwendet werden, eine Tür außerhalb des regulären Zeitplans zu entriegeln.
Vom Lockdown ausgeschlossen	Wählen Sie diese Option aus, um dem Karteninhaber während der Sperrzeit Zugang zu gewähren.
Exempt from anti-passback (Doppelnutzungsausnahme)	Sie können einem Karteninhaber jetzt eine Ausnahme von der Anti-Passback-Regel gewähren. Die Anti-Passback-Funktion verhindert, dass eine Person die gleichen Zugangsdaten verwenden kann wie jemand, der bereits vor ihr einen Bereich betreten hat. Die erste Person muss zunächst den Bereich verlassen, bevor ihre Zugangsdaten erneut verwendet werden können.
Globaler Karteninhaber	Wählen Sie diese Option aus, damit der Karteninhaber auf den Subservern angezeigt und überwacht werden kann. Diese Option ist nur für auf dem Hauptserver erstellte Karteninhaber verfügbar. Siehe *Multiserver [BETA], on page 175*.

Karteninhaber und Gruppen hinzufügen

Zugangsdaten hinzufügen

Sie können einem Karteninhaber die folgenden Arten von Zugangsdaten hinzufügen:

- *QR-Code als Zugangsdaten, on page 189*
- *PIN-Zugangsdaten, on page 190*
- *Smartphone-Zugangsdaten, on page 190*
- *Kartenzugangsdaten, on page 190*
- *Fahrzeugkennzeichen Zugangsdaten, on page 191*

Verfallsdatum	
Gültig ab	Legen Sie ein Datum und einen Zeitpunkt für die Gültigkeit der Zugangsdaten fest.
Gültig bis	Wählen Sie eine Option aus dem Drop-Down Menü.

Gültig bis	
Kein Enddatum	Die Zugangsdaten laufen niemals ab.
Datum	Wählen Sie ein Datum und eine Uhrzeit aus, an dem die Zugangsdaten ablaufen.
Von der ersten Verwendung	Wählen Sie aus, wie lange nach der ersten Verwendung die Zugangsdaten ablaufen. Wählen Sie eine Anzahl von Tagen, Monaten, Jahren oder Wiederholungen nach der ersten Verwendung aus.
Von der letzten Verwendung	Wählen Sie aus, wie lange nach der letzten Verwendung die Zugangsdaten ablaufen. Wählen Sie Tage, Monate oder Jahre nach der letzten Verwendung aus.

QR-Code als Zugangsdaten

Hinweis

Für die Verwendung von QR-Codes als Zugangsdaten ist eine Synchronisierung der Zeit auf dem Systemcontroller und der Kamera mit AXIS Barcode Reader erforderlich. Für eine perfekte Zeitsynchronisierung empfehlen wir Ihnen, für beide Geräte die gleiche Zeitquelle zu verwenden.

So fügen Sie einem Karteninhaber QR-Zugangsdaten hinzu:

1. Klicken Sie unter **Credentials (Zugangsdaten)** auf **+ Add (+ Hinzufügen)** und wählen Sie **QR-code (QR-Code)** aus.
2. Geben Sie einen Namen für die Zugangsdaten ein.
3. **Dynamic QR** ist standardmäßig aktiviert. Sie müssen Dynamic QR mit PIN-Anmeldedaten verwenden.

4. Legen Sie das Start- und Enddatum für die Zugangsdaten fest.
5. Um nach dem Speichern des Karteninhabers den QR-Code automatisch per E-Mail zu versenden, wählen Sie beim Speichern der Anmeldedaten **QR-Code an den Karteninhaber senden**.
6. Klicken Sie auf **Hinzufügen**.

PIN-Zugangsdaten

So fügen Sie einem Karteninhaber PIN-Zugangsdaten hinzu:
1. Klicken Sie unter **Credentials (Zugangsdaten)** auf **+ Add (+ Hinzufügen)** und wählen Sie **PIN** aus.
2. Geben Sie eine PIN ein.
3. Um einen stillen Alarm mit einer separaten PIN auszulösen, schalten Sie optional **Duress PIN (Zwangs-PIN)** ein und geben Sie eine Zwangs-PIN ein.
4. Legen Sie die Zugangsdaten **Valid from (Gültig ab)** und **Valid to (Gültig bis)** fest.
5. Klicken Sie auf **Hinzufügen**.

Smartphone-Zugangsdaten

Hinweis

Der Karteninhaber muss über eine E-Mail-Adresse verfügen, um die mobilen Zugangsdaten zu erhalten.

So fügen Sie einem Karteninhaber mobile Zugangsdaten hinzu:
1. Klicken Sie unter **Credentials (Zugangsdaten)** auf **+ Add (+ Hinzufügen)** und wählen Sie **Mobile credential (Mobile Zugangsdaten)** aus.
2. Geben Sie einen Namen für die Zugangsdaten ein.
3. Legen Sie das Start- und Enddatum für die Zugangsdaten fest.
4. Wählen Sie **Send the mobile credential to the cardholder after saving (Mobile Zugangsdaten nach dem Speichern an Karteninhaber senden)** aus. Der Karteninhaber erhält eine E-Mail mit Anweisungen zum Koppeln.
5. Klicken Sie auf **Hinzufügen**.

Siehe das Beispiel in *App AXIS Mobile Credential als Bluetooth-Zugangsdaten verwenden, on page 163*.

Kartenzugangsdaten

So fügen Sie einem Karteninhaber Karten-Zugangsdaten hinzu:
1. Klicken Sie unter **Credentials (Zugangsdaten)** auf **+ Add (+ Hinzufügen)** und wählen Sie **Card (Karte)** aus.
2. Um die Kartendaten manuell einzugeben, geben Sie einen Kartennamen, eine Kartennummer und eine Bitlänge ein.

Hinweis

Die Bitlänge ist nur konfigurierbar, wenn Sie ein Kartenformat mit einer bestimmten Bitlänge erstellen, die sich nicht im System befindet.

3. So rufen Sie automatisch die Kartendaten der zuletzt durch den Leser gezogenen Karte ab:
   3.1. Wählen Sie aus dem Ausklappmenü **Select reader (Leser auswählen)** einen Zugangspunkt aus.
   3.2. Ziehen Sie die Karte durch den Leser, der an diesen Zugang angeschlossen ist.
   3.3. Klicken Sie auf **Get last swiped card data from the door's reader(s) (Daten der zuletzt verwendeten Karte vom Leser des Zugangs abrufen)**.

Hinweis

Sie können den 2N-Desktop-USB-Kartenleser verwenden, um die Kartendaten abzurufen. Weitere Informationen finden Sie unter *Einrichten des 2N-Desktop-USB-Kartenlesers*.

4. Einen Einrichtungscode eingeben. Dieses Feld ist nur verfügbar, wenn Sie **Facility code (Gebäude-Zugangscode)** unter **Access management > Settings (Zugriffsverwaltung > Einstellungen)** aktiviert haben.
5. Legen Sie das Start- und Enddatum für die Zugangsdaten fest.
6. Klicken Sie auf **Hinzufügen**.

Fahrzeugkennzeichen Zugangsdaten

So fügen Sie einem Karteninhaber Fahrzeugkennzeichen-Zugangsdaten hinzu:

1. Klicken Sie unter **Credentials (Zugangsdaten)** auf **+ Add (+ Hinzufügen)** und wählen Sie **License plate (Fahrzeugkennzeichen)** aus.
2. Geben Sie einen Namen für die Zugangsdaten ein, der das Fahrzeug beschreibt.
3. Geben Sie das Fahrzeugkennzeichen für das Fahrzeug ein.
4. Legen Sie das Start- und Enddatum für die Zugangsdaten fest.
5. Klicken Sie auf **Hinzufügen**.

Fahrzeugkennzeichen als Zugangsdaten verwenden

In diesem Beispiel sehen Sie, wie Sie eine Tür-Steuerung, eine Kamera mit AXIS License Plate Verifier und ein Fahrzeugkennzeichen als Zugangsdaten verwenden, um einem Fahrer Zugang zu gewähren.

1. Fügen Sie die Tür-Steuerung und die Kamera zu AXIS Camera Station Pro hinzu. Siehe *Geräte hinzufügen, on page 6*.
2. Aktualisieren Sie die Firmware der neuen Geräte auf die neueste verfügbare Version. Siehe *Aktualisieren der Firmware, on page 68*.
3. Fügen Sie einen neuen Zugang hinzu, die mit Ihrer Tür-Steuerung verbunden ist. Siehe *Hinzufügen eines Zugangs, on page 152*.
   3.1. Fügen Sie auf **Seite A** einen Leser hinzu. Siehe *Leser hinzufügen, on page 161*.
   3.2. Wählen Sie unter **Türeinstellungen** die Option **AXIS License Plate Verifier** als **Lesertyp** und geben Sie einen Namen für den Leser ein.
   3.3. Fügen Sie optional einen Leser oder ein REX-Gerät auf **Seite B** hinzu.
   3.4. **OK** anklicken.
4. Installieren und aktivieren Sie AXIS License Plate Verifier auf Ihrer Kamera. Siehe das Benutzerhandbuch zu *AXIS License Plate Verifier*.
5. Starten Sie AXIS License Plate Verifier.
6. Konfigurieren Sie AXIS License Plate Verifier.
   6.1. Gehen Sie zu **Konfiguration > Zutrittskontrolle > Verschlüsselte Kommunikation**.
   6.2. Klicken Sie unter **Authentifizierungsschlüssel für externes Peripheriegerät** auf **Authentifizierungsschlüssel anzeigen** und **Schlüssel kopieren**.
   6.3. Öffnen Sie AXIS License Plate Verifier über die Weboberfläche der Kamera.
   6.4. Setup nicht ausführen.
   6.5. **Settings (Einstellungen)** aufrufen.
   6.6. Wählen Sie unter **Zutrittskontrolle** die Option **Sicherer Zugang** as **Typ**.
   6.7. Geben Sie in **IP address (IP-Adresse)** die IP-Adresse für die Tür-Steuerung ein.
   6.8. Fügen Sie in **Authentifizierungsschlüssel** den zuvor kopierten Authentifizierungsschlüssel ein.
   6.9. **Connect (Verbinden)** anklicken.
   6.10. Wählen Sie unter **Door controller name (Tür-Steuerung)** Ihre Tür-Steuerung aus.
   6.11. Wählen Sie unter **Lesername** den Leser aus, den Sie zuvor hinzugefügt haben.

6.12. Schalten Sie Integration ein.

7. Fügen Sie den Karteninhaber hinzu, dem Sie Zugriff gewähren möchten. Siehe *Karteninhaber hinzufügen, on page 187*
8. Fügen Sie dem neuen Karteninhaber die Zugangsdaten zum Fahrzeugkennzeichen hinzu. Siehe *Zugangsdaten hinzufügen, on page 189*
9. Fugen Sie eine Zugangsregel hinzu. Siehe *Zugangsregel hinzufügen, on page 192*.
   9.1. Einen Zeitplan hinzufügen.
   9.2. Fügen Sie den Karteninhaber hinzu, dem Sie Zugang über das Fahrzeugkennzeichen gewähren möchten.
   9.3. Fügen Sie die Tür dem AXIS License Plate Verifier hinzu.

Gruppe hinzufügen

Gruppen ermöglichen es Ihnen, Karteninhaber und deren Zugangsregeln gemeinsam und effizient zu verwalten.

1. Öffnen Sie eine Registerkarte Access Management (Zugangsverwaltung).
2. Rufen Sie **Cardholder management (Karteninhaberverwaltung)** > **Groups (Gruppen)** und klicken Sie auf **+ Add (+ Hinzufügen)**.
3. Geben Sie einen Namen und optional Initialen für die Gruppe ein.
4. Wählen Sie **Global group (Globale Gruppe)** aus, damit der Karteninhaber auf den Subservern angezeigt und überwacht werden kann. Diese Option ist nur für auf dem Hauptserver erstellte Karteninhaber verfügbar. Siehe *Multiserver BETA, on page 175*.
5. So fügen Sie der Gruppe Karteninhaber hinzu:
   5.1. **+ hinzufügen** anklicken.
   5.2. Wählen Sie die gewünschten Karteninhaber aus und klicken Sie auf **Add (Hinzufügen)**.
6. **Save (Speichern)** anklicken.
7. Um Ausweise für alle Karteninhaber einer Gruppe zu drucken, wählen Sie die Gruppe aus und klicken Sie auf **Print Badge BETA (Ausweis drucken)**. Weitere Informationen finden Sie unter *Print badge (Ausweis drucken) BETA, on page 198*.

Zugangsregel hinzufügen

Eine Zugangsregel definiert die Bedingungen, die erfüllt sein müssen, damit der Zugang gewährt wird.

Eine Zugangsregel umfasst Folgendes:

Karteninhaber und Karteninhabergruppen – Legen fest, wem der Zugang gewährt werden soll.

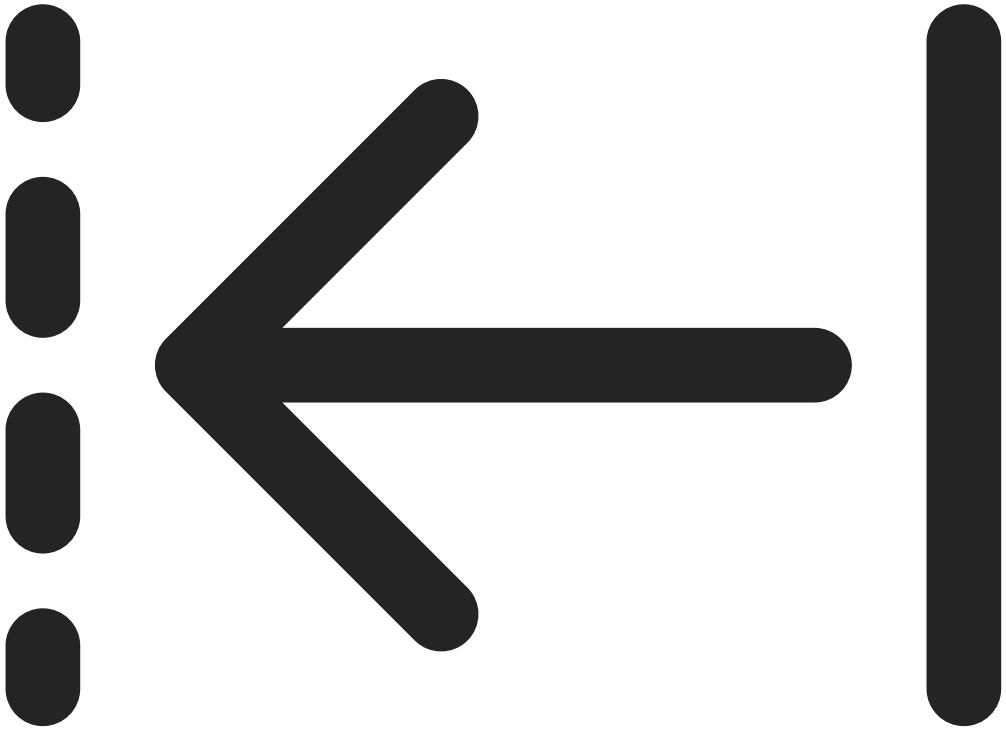
Türen und Bereiche – Geben an, wofür der Zugang gilt.

Zeitschemata – Legen fest, wann der Zugang gewährt werden soll.

So fügen Sie eine Zugangsregel hinzu:

1. Öffnen Sie eine Registerkarte Access Management (Zugangsverwaltung).
2. Wechseln Sie zu **Cardholder management (Karteninhaberverwaltung)**.

3. Klicken Sie unter **Access rule (Zugangsregel)**



auf **+ Add (+ Hinzufügen)**.

4. Geben Sie einen Namen für die Regel ein und klicken Sie auf **Next (Weiter)**.
5. Konfigurieren der Karteninhaber und Gruppen:
   5.1. Klicken Sie unter **Cardholders (Karteninhaber)** oder **Groups (Gruppen)** auf **+ Add (+ Hinzufügen)**.
   5.2. Wählen Sie Karteninhaber bzw. Gruppen und klicken Sie auf **Add (Hinzufügen)**.
   5.3. Sie können einen Karteninhaber oder eine Gruppe auch direkt auf eine Zugriffsregel ziehen und ablegen, um diese anzuwenden. Sobald Sie ein Element ziehen, werden die Zugangsregeln hervorgehoben, auf denen Sie es ablegen können. Wenn Sie mehrere Karteninhaber oder Gruppen gleichzeitig ziehen, wird deren Anzahl angezeigt.
6. Zugänge und Bereiche konfigurieren:
   6.1. Klicken Sie unter **Doors (Zugänge)** oder **Zones (Zonen)** auf **+ Add (+ Hinzufügen)**.
   6.2. Wählen Sie Zugänge bzw. Zonen und klicken Sie auf **Add (Hinzufügen)**.
7. Konfigurieren der Zeitpläne:
   7.1. Klicken Sie unter **Schedules (Zeitpläne)** auf **+ Add (+ Hinzufügen)**.
   7.2. Wählen Sie einen oder mehrere Zeitpläne aus und klicken Sie auf **Add (Hinzufügen)**.

8. **Save (Speichern)** anklicken.

Eine Regel für den Zugriff, bei der eine oder mehrere der oben beschriebenen Komponenten fehlen, ist unvollständig. Sie können alle unvollständigen Regeln für den Zugriff auf der Registerkarte **Incomplete (Unvollständig)** einsehen.

Berichte zur Systemkonfiguration exportieren

Sie können Berichte exportieren, die verschiedene Typen von Informationen über das System enthalten. AXIS Camera Station Pro exportiert den Bericht als Datei mit kommagetrennten Werten (CSV) und speichert ihn im Standard-Download-Ordner. So exportieren Sie einen Bericht:

1. Öffnen Sie eine Registerkarte Access Management (Zugangsverwaltung).
2. Rufen Sie **Reports (Berichte)** > **System configuration (Systemkonfiguration)** auf.
3. Wählen Sie die Berichte aus, die Sie exportieren möchten, und klicken Sie auf **Download**.

Detaillierter Bericht der Karteninhaber	Dieser Bericht enthält Informationen zu Karteninhabern, Zugangsdaten, Kartenüberprüfung und zur letzten Transaktion.
Bericht über den Zugang von Karteninhabern	Dieser Bericht enthält die Karteninhaberinformationen und Informationen über die Karteninhabergruppen, Zugangsregeln, Zugänge und Zonen, mit denen der Karteninhaber in Verbindung steht.
Bericht über den Gruppenzugang von Karteninhabern	Dieser Bericht enthält den Namen der Karteninhabergruppe und Informationen zu den Karteninhabern, Zugangsregeln, Zugängen und Zonen, mit denen die Karteninhabergruppe in Verbindung steht.
Bericht über Zugangsregeln	Dieser Bericht enthält den Namen der Zugangsregel und Informationen zu den Karteninhabern, Karteninhabergruppen, Zugangsregeln, Zugänge und Zonen, mit denen die Zugangsregel in Verbindung steht.
Bericht über den Zugang zu Türen	Dieser Bericht enthält den Namen des Zugangs und Informationen zu den Karteninhabern, Karteninhabergruppen, Zugangsregeln und Zonen, mit denen der Zugang in Verbindung steht.
Bericht über den Zonenzugang	Dieser Bericht enthält den Namen der Zone und Informationen zu den Karteninhabern, Karteninhabergruppen, Zugangsregeln und Zugänge, mit denen die Zone in Verbindung steht.

Berichte über Karteninhaberaktivitäten erstellen

Ein Appellbericht listet die Karteninhaber innerhalb einer bestimmten Zone auf und hilft dabei festzustellen, wer zu einem bestimmten Zeitpunkt anwesend ist.

Ein Musterungsbericht listet Karteninhaber innerhalb einer bestimmten Zone auf und hilft dabei, in Notfällen festzustellen, wer sicher ist und wer vermisst wird. Er unterstützt die Verwaltung von Gebäuden bei der Lokalisierung von Mitarbeitern und Besuchern nach Evakuierungen. Ein Sammelpunkt ist ein ausgewiesener Kartenleser, an dem sich das Personal bei Notfällen meldet und einen Bericht über die Personen am und außerhalb des Standorts erstellt. Das System kennzeichnet Karteninhaber als vermisst, bis sie sich an einem Sammelpunkt melden oder bis jemand sie manuell als sicher kennzeichnet.

Sowohl die Appell- als auch die Musterungsberichte erfordern Zonen zum Tracking der Karteninhaber.

So erstellen Sie einen Appell- oder Musterungsbericht und führen ihn aus:

1. Öffnen Sie eine Registerkarte Access Management (Zugangsverwaltung).
2. Rufen Sie **Reports (Berichte)** > **Cardholder activity (Karteninhaberaktivitäten)** auf.
3. Klicken Sie auf **+ Add (+ Hinzufügen)** und wählen Sie **Appell / Musterung**.
4. Geben Sie einen Namen für den Bericht ein.
5. Wählen Sie die Zonen aus, die in den Bericht aufgenommen werden sollen.
6. Wählen Sie die Gruppen aus, die Sie in den Bericht aufnehmen möchten.
7. Wenn Sie einen Musterungsbericht wünschen, wählen Sie **Mustering point (Sammelpunkt)** und einen Kartenleser für den Sammelpunkt.
8. Wählen Sie einen Zeitrahmen für den Bericht aus.
9. **Save (Speichern)** anklicken.
10. Wählen Sie den Bericht aus und klicken Sie auf **Run (Ausführen)**.

Status des Appellberichts	Beschreibung
Anwesend	Der Karteninhaber hat die angegebene Zone betreten und sie nicht verlassen, bevor Sie den Bericht ausgeführt haben.
Nicht anwesend	Der Karteninhaber hat die angegebene Zone verlassen und sie nicht betreten, bevor Sie den Bericht ausgeführt haben.

Status des Musterungsberichts	Beschreibung
Sicher	Der Karteninhaber hat seine Karte am Sammelpunkt benutzt.
Fehlt	Der Karteninhaber hat seine Karte am Sammelpunkt nicht benutzt.

Import und Export

Karteninhaber importieren

Über diese Option können Karteninhaber, Karteninhabergruppen, Zugangsdaten und Bilder von Karteninhabern aus einer CSV-Datei importiert werden. Stellen Sie zum Importieren von Bildern von Karteninhaber sicher, dass der Server Zugriff auf die Bilder hat.

Beim Importieren von Karteninhabern speichert das Zugangsverwaltungssystem automatisch die Systemkonfiguration inklusive sämtlicher Hardwarekonfiguration und löscht alle zuvor gespeicherten.

Sie können Benutzer auch über eine Active-Directory-Datenbank als Karteninhaber zuweisen (siehe *Active-Directory-Einstellungen[BETA], on page 176*).

Optionen importieren	
Neu	Diese Option entfernt vorhandene Karteninhaber und fügt neue Karteninhaber hinzu.
Aktualisieren	Über diese Option werden vorhandene Karteninhaber aktualisiert und neue Karteninhaber hinzugefügt.
Hinzufügen	Diese Option behält vorhandene Karteninhaber bei und fügt neue Karteninhaber hinzu. Kartennummern und Karteninhaber-IDs sind eindeutig und können nur einmal verwendet werden.

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Import and export (Import und Export)**.
2. Klicken Sie auf **Import cardholders (Karteninhaber importieren)**.
3. Wählen Sie **Neu**, **Aktualisieren** oder **Hinzufügen**.
4. Klicken Sie auf **Next (Weiter)**.
5. Klicken Sie auf **Choose a file (Wählen Sie eine Datei)** und rufen Sie die CSV-Datei auf. **Öffnen** anklicken.
6. Geben Sie ein Spaltentrennzeichen ein, wählen Sie einen eindeutigen Bezeichner aus und klicken Sie auf **Next (Weiter)**.
7. Weisen Sie jeder Spalte eine Überschrift zu.
8. Klicken Sie auf **Importieren**.

Einstellungen importieren	
Erste Zeile ist Kopfzeile	Wählen Sie aus, ob die CSV-Datei eine Spaltenüberschrift enthält.
Spaltentrennzeichen	Geben Sie ein Spaltentrennformat für die CSV-Datei ein.
Eindeutiger Bezeichner	Das System identifiziert standardmäßig einen Karteninhaber mit der **Cardholder ID (Karteninhaber-ID)**. Alternativ können Sie dazu den Vor- und Nachnamen oder die E-Mail-Adresse verwenden. Mit der eindeutigen Kennung wird der Import doppelter Personalaufzeichnungen verhindert.
Format der Kartennummer	In der Standardeinstellung ist **Allow both hexadecimal and number (Hexadezimal und Zahl zulassen)** ausgewählt.

Karteninhaber exportieren

Diese Option exportiert die Daten des Karteninhabers im System in eine CSV-Datei.

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Import and export (Import und Export)**.
2. Klicken Sie auf **Export cardholders (Karteninhaber exportieren)**.
3. Wählen Sie einen Download-Speicherort und klicken Sie auf **Save (Speichern)**.

AXIS Camera Station Pro aktualisiert die Karteninhaberfotos in `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos`, wenn die Konfiguration geändert wird.

Import rückgängig machen

Beim Import von Karteninhabern wird die Konfiguration des Systems automatisch gespeichert. Über **Undo import (Import rückgängig machen)** werden die Daten des Karteninhabers und die Hardwarekonfiguration auf die Voreinstellungen vor dem letzten Import des Karteninhabers zurückgesetzt.

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Import and export (Import und Export)**.
2. Klicken Sie auf **Undo import (Import rückgängig machen)**.
3. **Yes (Ja)** anklicken

Zugriffsverwaltungseinstellungen

So passen Sie die Karteninhaberfelder an, die im Zugriffsverwaltungsdashboard verwendet werden:

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Settings (Einstellungen)** > **Custom cardholder fields (Benutzerdefinierte Karteninhaberfelder)**.
2. **+ Add (+ Hinzufügen)** anklicken und eine Bezeichnung eingeben. Sie können bis zu 6 benutzerdefinierte Felder hinzufügen.
3. Klicken Sie auf **Hinzufügen**.

So aktivieren Sie die Verwendung eines Gebäude-Zugangscodes, um Ihr Zutrittssystem zu überprüfen:

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Settings (Einstellungen)** > **Facility code (Gebäude-Zugangscode)**.
2. Wählen Sie **Facility code on (Gebäude-Zugangscode ein)** aus.

Hinweis

Sie müssen beim Konfigurieren von Identifizierungsprofilen außerdem die Option **Include facility code for card validation (Gebäude-Zugangscode in Kartenprüfung einbeziehen)** auswählen. Siehe *Identifizierungsprofile, on page 168*.

So bearbeiten Sie eine E-Mail-Vorlage für den Versand von QR- oder mobilen Zugangsdaten:

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Settings (Einstellungen)** > **Email templates (E-Mail-Vorlagen)**.
2. Bearbeiten Sie Ihre Vorlage und klicken Sie auf **Update (Aktualisieren)**.

Ausweisvorlagen BETA

Sie können Ausweisvorlagen mit Karteninhaberinformationen, Fotos, Logos und individuellem Branding anpassen. So erstellen Sie eine neue Vorlage:

1. Rufen Sie **Access management (Zutrittsmanagement) > Settings (Einstellungen) > Badge templates (Ausweisvorlagen)** BETA auf.
2. Klicken Sie auf **Create new template (Neue Vorlage erstellen)**.
3. Geben Sie einen Namen in das Feld **Template name (Vorlagenname)** ein.
4. Wählen Sie **Use as default template for printing (Als Standardvorlage für den Druck verwenden)**, wenn Sie diese Vorlage als Standardvorlage festlegen möchten.
5. Passen Sie das Ausweisdesign an:
   - Wählen Sie bis zu fünf Textfelder aus, die auf der Vorderseite angezeigt werden sollen, einschließlich aller von Ihnen erstellten benutzerdefinierten Felder. Beim Drucken erscheinen nur ausgefüllte Felder auf dem Ausweis.

- Wählen Sie die Schriftart und Farbe für den Text aus.
- Fügen Sie eine Hintergrundfarbe oder ein Hintergrundbild hinzu.
- Laden Sie ein Logo für Ihre Organisation hoch.
- Für die Rückseite fügen Sie entweder eine Hintergrundfarbe oder ein Hintergrundbild hinzu.

6. Klicken Sie auf **Save (Speichern)**, um Ihre Änderungen zu speichern, oder auf **Save as (Speichern unter)**, um sie als neue Vorlage zu speichern.

Hinweis

Sobald eine Vorlage erstellt wurde, kann sie nicht mehr bearbeitet, sondern lediglich umbenannt werden.

Print badge (Ausweis drucken) BETA

Sie können Identifizierungsausweise für Karteninhaber mithilfe Ihrer konfigurierten Identifizierungsvorlagen drucken. Bitte beachten Sie, dass die Kartenkodierung derzeit nicht unterstützt wird. Vorbereitungen:

- Stellen Sie sicher, dass der Karteninhaber über mindestens eine Kartenberechtigung verfügt. Es ist nicht möglich, Ausweise für Karteninhaber ohne Berechtigung zu drucken.
- Sie benötigen einen Drucker, der das Kartenformat CR80 unterstützt und mit kompatiblem Druckmaterial wie dickem Karton kompatibel ist.
- Konfigurieren Sie die Druckeinstellungen Ihres Browsers:
  1. Stellen Sie die Seitengröße auf CR80 oder eine benutzerdefinierte Größe ein, die den Abmessungen Ihrer Karte entspricht.
  2. Stellen Sie das Format auf Hochformat ein.
  3. Schalten Sie die Ränder aus oder stellen Sie sie auf das Minimum ein.

Wichtig

Secure Entry (Sicherer Zugang) unterstützt Drucker mit Windows-Treibern. Die korrekte Funktion mit Druckern der Serie HID Fargo wurde überprüft. Sollten Sie einen Treiber für Ihren Drucker benötigen, wenden Sie sich an den Hersteller Ihres Druckers.

So drucken Sie Ausweise:

1. Rufen Sie **Access management (Zutrittsmanagement) > Cardholder management (Karteninhaberverwaltung) > Cardholders (Karteninhaber)** auf.
2. Wählen Sie einen oder mehrere Karteninhaber aus.
3. Klicken Sie auf **Print badge (Ausweis drucken)** BETA.
4. Klicken Sie auf **Select template (Vorlage auswählen)** und wählen Sie aus der Dropdown-Liste **Template (Vorlage)** die gewünschte Vorlage für den Ausweis aus.
5. Wenn der Karteninhaber über mehrere Kartenberechtigungen verfügt, wählen Sie eine aus dem Dropdown-Menü **Card (Karte)** aus.
6. Klicken Sie auf **Drucken**.

Hinweis

Falls Ihr Drucker keinen Duplexdruck unterstützt, drucken Sie bitte zunächst alle Vorderseiten aus, drehen Sie anschließend den Kartenstapel um und legen Sie ihn erneut in das Fach ein, um die Rückseiten zu drucken.

Überwachung des Systemzustands BETA

Über die Registerkarte „System Health Monitoring" (Überwachung des Systemzustands) können Sie die Zustandsdaten eines einzelnen oder mehrerer AXIS Camera Station Pro-Systeme im selben Netzwerk überwachen.

Wenn Sie Systeme in verschiedenen Netzwerken verwalten, stellt die Server-Überwachung in „My Systems" (Meine Systeme) die gleichen Funktionen über die Cloud bereit.

	Zeigt eine Zusammenfassung der Geräte und Systeme an, auf die Sie Zugriff haben. Siehe *Lagerbestand, on page 199*.
	Zeigt eine Speicherübersicht und die Aufzeichnungsdetails der einzelnen Kameras der überwachten Systeme an. Siehe *Speicherung, on page 200*.
	Zeigt die Protokolle der Überwachung des Systemzustands der überwachten Systeme an. Siehe *Benachrichtigungen, on page 201*.

Einschränkungen

- Sie können den Speicher für Aufzeichnungen auf AXIS S3008 Recorder nicht überwachen.
- Die Benachrichtigungseinstellungen wirken sich nur auf den lokalen Server zur Überwachung des Systemzustands aus.
- Das System kennzeichnet Aufzeichnungen mit Ausnahme von kontinuierlichen und durch Bewegung ausgelösten Aufzeichnungen mit dem Aufzeichnungstyp **None (Keine)**.

Vorgehensweise

1. *Konfigurieren Sie Überwachung des Systemzustands BETA, on page 179*
   1.1. Benachrichtigungen einrichten. Siehe *Benachrichtigungen, on page 180*.
   1.2. Multisytem richten. Siehe *Multisystem, on page 181*.
2. Überwachen Sie den Systemzustand von AXIS Camera Station Pro Systemen.
   2.1. *Lagerbestand, on page 199*
   2.2. *Speicherung, on page 200*
   2.3. *Benachrichtigungen, on page 201*

Lagerbestand

Auf der Inventarseite finden Sie eine Übersicht über die Geräte und Systeme, auf die Sie Zugriff haben.

1. Klicken Sie auf der Registerkarte **System Health Monitoring (Überwachung des Systemzustands)**BETA auf .
2. Um eine Zusammenfassung eines Systems zu erhalten, klicken Sie auf **AXIS Camera Station**.
   Die Informationen werden auf der rechten Seite angezeigt, einschließlich System- und Serverdetails.
3. Um eine Übersicht über ein Gerät anzuzeigen, klicken Sie auf das Gerät in der Liste.
   Die Informationen werden auf der rechten Seite angezeigt, einschließlich der Gerätedetails und der Speicherinformationen, wenn das Gerät eine Videoquelle enthält.
4. Um den Systembericht herunterzuladen, wählen Sie die Option **AXIS Camera Station system report (AXIS Camera Station-Systembericht)** im Drop-Down Menü **Create report (Bericht erstellen)** aus. Siehe *Systembericht, on page 213*.

5. So laden Sie einen Bericht zur Überwachung des Systemzustands herunter:
   5.1. Wählem Sie im Drop-Down Menü **Create report (Bericht erstellen)** die Option **System Health Monitoring report (Bericht zur Überwachung des Systemzustands)** aus.
   5.2. Um die Datenbank in den Bericht einzubeziehen, wählen Sie **Alle Datenbanken einbeziehen** und klicken Sie auf **Herunterladen**.
   5.3. Wenn der Bericht fertig ist, klicken Sie, um ihn zu speichern.

Speicherung

Die Speicherseite zeigt die Speicherübersicht und die Aufzeichnungsdetails der einzelnen Kameras der überwachten Systeme an. Klicken Sie auf eine Spaltenüberschrift, um nach dem Inhalt der Spalte zu sortieren.

1. Klicken Sie auf der Registerkarte **System Health Monitoring (Überwachung des Systemzustands)**BETA auf .
2. Wenn Sie Multisystem-Zustandsdaten überwachen, wählen Sie ein System aus dem Drop-Down Menü aus.

Zusammenfassung	
Status	Der Speicherstatus. Siehe *Speicher konfigurieren, on page 74*.
Standort	Pfad und Name des Speichers.
Gesamt	Die Gesamtgröße des Speicherplatzes. Diese Wert entspricht dem in Windows unter den Eigenschaften des Speicherorts als Gesamtspeicher angezeigten Wert.
Zugewiesen:	Die maximale Menge an Speicherplatz, die für die Aufzeichnungen bereitgestellt wird.
Used (Verwendet)	Der von Aufzeichnungen derzeit belegte Speicherplatz.
Letzte Aktualisierung	Zeitpunkt, an dem die Information zuletzt aktualisiert wurde.

Kamera	
Status	(leer): Normalstatus. Warnsymbol: Die Aufbewahrungszeit wird nicht eingehalten. Informationssymbol: Die Aufbewahrungszeit wird nicht eingehalten, da die Kameraaufzeichnungen zu kurz sind.
Bezeichnung	Der Kameraname.
Aufzeichnungstyp	Die für die Kamera verwendeten Aufzeichnungstypen.
Aufbewahrung einstellen	Die für die Kamera unter **Konfiguration > Speicher > Auswahl** eingestellte Aufbewahrungszeit.
Aktuelle Aufbewahrung	Die Anzahl der Tage, die die Aufzeichnungen der Kamera im Speicher aufbewahrt wurden.
Älteste Aufzeichnung	Der Zeitpunkt der ältesten Aufzeichnung der Kamera, die im Speicher aufbewahrt wird.
Neueste Aufnahme	Der Zeitpunkt der neusten Aufzeichnung der Kamera, die im Speicher aufbewahrt wird.
Standort	Der von der Kamera verwendete Speicherort.

Kamera	
Verwendeter Speicher	Der von Aufzeichnungen dieser Kamera derzeit belegte Speicherplatz.
Letzte Aktualisierung	Zeitpunkt, an dem die Information zuletzt aktualisiert wurde.

Benachrichtigungen

Die Benachrichtigungsseite zeigt die Protokolle der Überwachung des Systemzustands der überwachten Systeme an. Klicken Sie auf eine Spaltenüberschrift, um nach dem Inhalt der Spalte zu sortieren.

Klicken Sie auf der Registerkarte **System Health Monitoring (Überwachung des Systemzustands)**BETA auf .

Verlauf	
Benachrichtigung gesendet	Die Uhrzeit, zu der die Benachrichtigung gesendet wurde.
Komponente	Zeigt den Gerätenamen für Benachrichtigungen an, die durch `device down` oder `system` ausgelöst wurden, für Benachrichtigungen, die durch `system down` ausgelöst wurden.
System	Der Name des Systems, in dem das Ereignis auftritt.
Regel	Die Regel, von der die Benachrichtigung ausgelöst wurde. `System down` oder `Device down`
Erkannt	Zeitpunkt, zu dem das Problem erkannt wurde.
Aufgelöst	Zeitpunkt, zu dem das Problem gelöst wurde.

Hotkeys

Auf der Registerkarte „Hotkeys“ werden die verfügbaren Hotkeys angezeigt. Der Typ des Hotkeys hängt von der für AXIS Camera Station Pro verwendeten Steuerung ab.

- Eine Tastenkombination auf der Tastatur
- Eine Tastenkombination auf dem Funktionstastenfeld
- Eine Joystick-Taste
- Eine Jog Dial-Taste

Wenn Sie eine Kamera oder Ansicht von einem verbundenen Server löschen, werden die entsprechenden Hotkeys ebenfalls gelöscht.

Das System unterteilt die Hotkeys in die folgenden Kategorien:

- Kamera
- Geräteverwaltung
- Die Kamera aufrufen
- Die Option Ansicht aufrufen
- Navigation
- PTZ-Voreinstellungen
- Aufzeichnungen
- Sequenzen
- Geteilte Ansicht
- Tab
- Sonstige

Die Aktionen in den Kategorien „Navigate to cameras (Kameras aufrufen)“ und „Navigate to views (Ansichten aufrufen)“ müssen manuell zugewiesen werden.

Hinweis

- Bereits für eine andere Aktion verwendete Hotkeys werden beim Hinzufügen oder Bearbeiten mit Warnsymbolen gekennzeichnet. Um den Konflikt anzuzeigen, den Mauszeiger auf das Warnsymbol führen. Drücken Sie zum Abbrechen ESC . Drücken Sie ENTER, um den Hotkey zu verwenden und die den Konflikt auslösende Belegung automatisch zu entfernen.
- Bei einer Verbindung zu mehreren Servern sind in den Kategorien „Navigate to cameras“ (Kameras aufrufen) und „Navigate to views“ (Ansichten aufrufen) auch die Kameras und Ansichten der verbundenen Server aufgelistet.

Hotkey zuweisen	Wenn der Keyboard-Wert einer Aktion leer ist, klicken Sie auf diesen Wert, um dieser Aktion einen Hotkey zuzuweisen. • Um einen Hotkey über die Tastatur hinzuzufügen, drücken Sie Strg und mindestens eine weitere Taste oder eine der Funktionstasten F2–F12. • Wenn Sie einen Hotkey für eine Aktion mit dem Funktionstastenfeld definieren möchten, geben Sie eine Zahlenkombination ein und drücken Sie eine der Funktionstasten F1-F5. • Um einen Hotkey für eine Aktion mit dem Joystick oder Jog Dial hinzuzufügen, drücken Sie die Taste auf dem Joystick bzw. Jog Dial, um ihr die Aktion zuzuweisen.
Hotkey bearbeiten	Klicken Sie den Keyboard-Wert einer Aktion, um den Wert zu bearbeiten.
Hotkey entfernen	Klicken Sie den Keyboard-Wert einer Aktion, um den Wert zu löschen.
	Klicken Sie auf , um die Hotkey-Tabelle auszudrucken.
	Klicken Sie auf , um alle Hotkey-Zuweisungen auf die ursprünglichen Einstellungen zurückzusetzen.

Tasten Steuerungsgerät Videosicherheit

Hotkey-Zuordnung – Joystick	Standardaktion	AXIS TU9002	AXIS T8311
Taste 1	Die Voreinstellung 1 aufrufen	J1	J1
Taste 2	Die Voreinstellung 2 aufrufen	J2	J2
Taste 3	Die Voreinstellung 3 aufrufen	J3	J3
Taste 4	Die Voreinstellung 4 aufrufen	J4	J4
Taste 5	Mausklick links simulieren	J5	L
Taste 6	Linke rechte Taste simulieren	J6	R
Taste 7	Vorherige Zelle in geteilter Ansicht wählen	Oben links	-
Taste 8	Nächste Zelle in geteilter Ansicht wählen	Oben rechts	-
Taste 9	Zur vorherigen Aufzeichnung springen		-
Taste 10	Wiedergabe/Pause		-
Taste 11	Zur nächsten Aufzeichnung springen		-

Hotkey-Zuordnung – Joystick	Standardaktion	AXIS TU9002	AXIS T8311
Taste 12	Lesezeichen hinzufügen		-
Taste 13	Zoomring-Funktion zwischen digitalem Zoom und Wiedergabegeschwindigkeit umschalten	M1	-
Taste 14	Zwischen den Optionen Live und Aufzeichnung wechseln	M2	-
Taste 15	Bild zurück	Oben links umgeschaltet	-
Taste 16	Bild vorwärts springen	Oben rechts umgeschaltet	-

Hotkey-Zuordnung – Tastatur	Standardaktion	AXIS TU9003	AXIS T8312
A	Ansichten öffnen		
B	Zur nächsten Kamera oder Ansicht wechseln		
ALT+B	Zur vorherigen Kamera oder Ansicht wechseln	Alt+	-
TAB	Zur nächsten Registerkarte wechseln		-
ALT+TAB	Zur vorherigen Registerkarte wechseln	Alt+	-
C	-	-	
D	-	-	
E	-	-	
PLUS	Fokus weiter gefasst	+	-
MINUS	Fokus näher gefasst	-	-
F2	Hotkeys öffnen	F2	F2
F4	Offene Protokolle	F4	F4
F5	Konfiguration	F5	F5
F10	Autofokus	F10	-

Hotkey-Zuordnung – Jog	Standardaktion	AXIS T8313
Jog 1	Exportmarkierung einblenden/ausblenden	L
Jog 2	Lesezeichen hinzufügen	
Jog 3	Zur vorherigen Aufzeichnung springen	
Jog 4	Wiedergabe/Pause	
Jog 5	Zur nächsten Aufzeichnung springen	
Jog 6	Zwischen den Optionen Live und Aufzeichnung wechseln	R

Hinweis

AXIS T8311 Video Surveillance Joystick unterstützt die Joystick-Tasten 7–10 nicht.

Protokolle

Standardmäßig werden auf der Registerkarte „Logs (Protokolle)“ die Live-Protokolle einschließlich Live-Alarme, Ereignisse und Audit-Protokolle angezeigt. Sie können auch nach älteren Protokollen suchen. Konfigurieren Sie die Anzahl der Tage für die Speicherung von Protokollen unter **Configuration > Server > Settings (Konfiguration > Server > Einstellungen)**.

Zeit	Datum und Zeit der Aktion.
Typ	Der Typ der Aktion: Alarm, Ereignis und Audit.
Kategorie	Die Kategorie der Aktion.
Nachricht	Kurzbeschreibung der Aktion.
Benutzer	Der AXIS Camera Station Pro Benutzer, der die Aktion ausführt.
Computer	Der Computer (Windows-Domainname), auf dem AXIS Camera Station Pro installiert ist. Dieser Wert wird vom Client bereitgestellt und kann vom Server nicht unabhängig überprüft werden.
Windows-Benutzer	Der Windows-Benutzer, der AXIS Camera Station Pro verwaltet. Dieser Wert wird vom Client bereitgestellt und kann vom Server nicht unabhängig überprüft werden. In der Spalte „Benutzer“ wird der Benutzer, der durch die Authentifizierung angemeldet ist, angezeigt.
Server	Nur verfügbar, wenn mehrere Server verbunden werden. Der Server auf dem die Aktion vorkommt.
Komponente	Protokollerzeugende Komponente.

Protokolle suchen

1. Klicken Sie auf der Registerkarte “Protokolle“ unter **Log search (Protokollsuche)** auf **Search (Suchen)**.
2. Geben Sie in das Filterfeld die Schlüsselwörter ein. AXIS Camera Station Pro durchsucht die Protokollliste außer in **Time (Zeit)** und zeigt die Suchergebnisse an, die alle Schlüsselwörter enthalten. Unterstützte Suchoperatoren finden Sie unter *Suche optimieren, on page 44*.
3. Wählen Sie **Alarms (Alarme)**, **Audits** oder **Events (Ereignisse)** unter **Filter** aus.
4. Wählen Sie im Kalender ein Datum oder einen Datumsbereich aus.
5. Wählen Sie **Start time (Startzeit)** und **End time (Endzeit)** aus den Drop-Down Menüs aus.
6. Klicken Sie auf **Suchen**.

Alarmprotokoll

Das Alarmprotokoll zeigt Systemalarme sowie Alarme, die auf Basis von Regeln und Bewegungserkennung generiert wurden, in einer Liste an. Die Liste enthält Datum und Uhrzeit des Alarms, die Alarmkategorie sowie eine Alarmnachricht. Siehe *Alarme*.

	Klicken Sie auf einen Alarm und , um die Registerkarte „Recordings (Aufzeichnungen)“ zu öffnen und die Wiedergabe zu starten, wenn der Alarm eine Aufzeichnung enthält.
	Klicken Sie auf einen Alarm und , um das Alarmverfahren zu öffnen, wenn der Alarm ein Alarmverfahren enthält.

	Klicken Sie auf einen Alarm und , um andere Clients zu benachrichtigen, dass der Alarm bearbeitet wird.
	Klicken Sie auf einen Alarm und , um das Protokoll in eine Textdatei zu exportieren.

Ereignisprotokoll

Das Ereignisprotokoll zeigt Kamera- und Server-Ereignisse, z. B. Aufzeichnungen, Auslöser, Alarme, Fehler und Systemmeldungen in einer Liste an. Die Liste enthält Datum und Uhrzeit des Ereignisses, die Ereigniskategorie sowie eine Ereignismeldung. Wählen Sie die Ereignisse und klicken Sie auf in der Toolbar, um die Ereignisse zu exportieren und als Textdatei abspeichern.

Prüfprotokoll

Im Audit-Protokoll finden Sie alle Benutzeraktionen, wie beispielsweise manuelle Aufzeichnungen, gestartete oder gestoppte Videostreams und Aktionsregeln, sowohl von Zugängen als auch von Karteninhabern erstellte.

Wählen Sie die Audits und klicken Sie auf in der Toolbar, um die Audits zu exportieren und als Textdatei abspeichern.

Fahrzeugkennzeichen-Verwaltung

Um Fahrzeugkennzeichenlisten in AXIS Camera Station Pro zu verwalten, öffnen Sie die Registerkarte **License plate management (Kennzeichenverwaltung)**.

Auf dieser Registerkarte können Sie drei Kennzeichenlisten für einzelne Kameras oder Kameragruppen bearbeiten:

1. Wählen Sie eine Gruppe oder Kamera aus den Listen „ **Groups (Gruppen)** und **Cameras (Kameras)** aus.
2. Wählen Sie die Liste aus, die Sie bearbeiten möchten. Der Standard sieht vor, dass die drei Listen, die Sie bearbeiten können, **Allow list (Zulassungsliste)**, **Block list (Sperrliste)** bzw. **Custom list (Benutzerdefinierte Liste)** heißen.
3. Um den Namen der Liste zu bearbeiten, klicken Sie auf **Edit list name (Listennamen bearbeiten)**.
4. Geben Sie neue Fahrzeugkennzeichen in die Spalte „Kennzeichen" und eine Beschreibung (falls vorhanden) in die Spalte „Beschreibung" ein. Klicken Sie auf **Add (Hinzufügen)**, um sie in der Liste zu speichern.
5. Klicken Sie **Anwenden** an, um Ihre Änderungen zu speichern.

Um ein Kennzeichen, das Sie einer Liste hinzugefügt haben, zu bearbeiten oder zu entfernen, wählen Sie es aus und klicken Sie auf **Edit (Bearbeiten)** oder **Remove (Entfernen)**.

AXIS Audio Manager Pro

Über die Registerkarte „AXIS Audio Manager Pro" können Sie über AXIS Camera Station Pro direkt auf die Schnittstelle eines AXIS Audio Manager Pro-Servers zugreifen. Weitere Informationen zur Server-Schnittstelle finden Sie im *Benutzerhandbuch zu AXIS Audio Manager Pro*.

Die Registerkarte wird erst angezeigt, wenn Sie in AXIS Camera Station Pro eine Verbindung zu einem AXIS Audio Manager Pro-Server hergestellt haben. Weitere Informationen finden Sie unter *Konfiguration von AXIS Audio Manager Pro, on page 177*.

Wichtig

Es ist nicht möglich, per Secure Remote Access v2 auf die Schnittstelle eines AXIS Audio Manager Pro-Servers zuzugreifen.

Die Integration ermöglicht Ihnen außerdem Folgendes:

- *Erstellung von Auslösern in Audio Manager, on page 104*
- *Erstellung von Aktionen in Audio Manager, on page 114*
- Hinzufügen von Audiobereichen zu Karten. Siehe dazu *Lageplan, on page 22*.
- *Verwendung von Durchsageschnittstellen in geteilten Ansichten, on page 20*
- Festlegung von Benutzerrechten für AXIS Audio Manager Pro in AXIS Camera Station Pro. Siehe *Benutzer-/Gruppenberechtigungen, on page 140*.
- Auswahl von Audiogeräten über den AXIS Audio Manager Pro-Server als verknüpftes Audiogerät einer Kamera. Siehe *Videostreamprofile bearbeiten, on page 54*.

Alarme

Die Registerkarte Alarme ist am unteren Rand des AXIS Camera Station Pro Clients verfügbar und zeigt ausgelöste Ereignisse und Systemalarme an. Informationen zum Erstellen eines Alarms finden Sie unter *Aktionsregeln*. Informationen zum Alarmtyp "Wartung der Datenbank erforderlich", siehe *Datenbankwartung, on page 234*

Zeit	Der Zeitpunkt des Alarms.
Kategorie	Die Kategorie des ausgelösten Alarms.
Beschreibung	Eine kurze Beschreibung des Alarms.
Server	Verfügbar bei Verbindung zu mehreren Servern. AXIS Camera Station Pro Server, der den Alarm sendet.
Komponente	Alarmauslösende Komponente.
	Die Option zum Anzeigen von Alarmverfahren ist nur verfügbar, wenn der Alarm ein Alarmverfahren enthält.
	Die Option zum Aufrufen von Aufzeichnungen ist nur verfügbar, wenn der Alarm eine Aufzeichnung enthält.
	Ausgewählten Alarm bestätigen
	Entfernen Sie den Alarm. Der Alarm wird nur vorübergehend entfernt, wenn Sie den Alarm vor dem Entfernen nicht bestätigen.

Umgang mit einem spezifischen Alarm:

1. Klicken Sie auf **Alarms and Tasks (Alarme und Aufgaben)** am unteren Rand des AXIS Camera Station Pro Clients und rufen Sie die Registerkarte **Alarms (Alarme)** auf.
2. Wählen Sie für Alarme mit einer Aufzeichnung den Alarm aus und klicken Sie auf , um auf der Registerkarte **Recording alerts (Aufzeichnungsalarme)** die Aufzeichnung aufzurufen.
3. Für Alarme ohne eine Aufzeichnung öffnen Sie eine Registerkarte mit Live-Ansicht und doppelklicken Sie auf den Alarm, um die Aufzeichnung für den Zeitpunkt des Alarms auf der Registerkarte **Recording alerts (Aufzeichnungsalarme)** anzuzeigen.
4. Für Alarme mit einem Alarmverfahren wählen Sie den Alarm aus und klicken Sie auf , um das Alarmverfahren zu öffnen.
5. Um andere Clients darüber zu informieren, dass die Alarme bearbeitet wurden, wählen Sie die Alarme aus und klicken Sie auf .
6. Um die Alarme aus der Liste zu entfernen, wählen Sie die Alarme aus und klicken Sie auf .

Aufgaben

Die Registerkarte „Tasks (Aufgaben)" wird unten im AXIS Camera Station Pro-Client angezeigt.

Die folgenden Aufgaben sind benutzerspezifisch. Sie werden nur Administratoren und dem einleitenden Benutzer angezeigt.

- Systembericht
- Vorfallbericht erstellen
- Aufzeichnungen exportieren

Administratoren können alle Aufgaben aller Benutzer, einschließlich benutzerspezifischer Aufgaben, aufrufen und durchführen.

Bediener und Betrachter können:

- Alle selbst eingeleiteten Aufgaben und die nicht-benutzerspezifischen Aufgaben anderer Benutzer aufrufen.
- Eigene eingeleitete Aufgabe abbrechen oder erneut einleiten. Erneut eingeleitet können nur Aufgaben zu Vorfallsberichten und zum Exportieren von Aufzeichnungen.
- Die Resultate aller Aufgaben in der Liste aufrufen.
- Erledigte Aufgaben aus der Liste entfernen. Dies betrifft nur den lokalen Client.

Bezeichnung	Der Name der Aufgabe.
Starten	Zeitpunkt, zu dem die Aufgabe gestartet wurde.
Nachricht	Zeigt den Status oder Informationen zur Aufgabe an. Mögliche Status: • **Canceling (Wird abgebrochen)**: Bereinigen vor Abbruch der Aufgabe. • **Canceled (Abgebrochen)**: Bereinigung ist abgeschlossen und die Aufgabe wurde abgebrochen. • **Error (Fehler)**: Aufgabe wurde mit Fehlern beendet, d. h. sie schlug auf einem oder mehreren der gewählten Geräte fehl. • **Finished (Beendet)**: Aufgabe abgeschlossen. • **Finished during lost connection (Beendet während Verbindungsabbruch)**: Wird angezeigt, wenn die Aufgabe abgeschlossen wurde, während die Verbindung zum Server unterbrochen war. Der Aufgabenstatus konnte nicht ermittelt werden. • **Lost connection (Verbindung unterbrochen)**: Wird angezeigt, wenn die Verbindung zwischen Client und Server während der Ausführung der Aufgabe unterbrochen wurde. Der Aufgabenstatus konnte nicht ermittelt werden. • **Running (Wird ausgeführt)**: Aufgabe wird aktuell ausgeführt. • **Pending (Ausstehend)**: Warten auf das Beenden einer anderen Aufgabe.
Besitzer	Der Benutzer, der die Aufgabe gestartet hat.
Fortschritt	Zeigt den Fortschritt der Aufgabe an.
Server	Verfügbar bei einer Verbindung mit mehreren Servern. Zeigt den AXIS Camera Station Pro Server an, der die Aufgabe ausführt.

Eine oder mehrere Aufgaben erledigen:

1. Klicken Sie auf **Alarms and Tasks (Alarme und Aufgaben)** am unteren Rand des AXIS Camera Station Pro Clients und dann auf die Registerkarte **Tasks (Aufgaben)**.
2. Wählen Sie die Aufgaben aus und klicken Sie auf eine der Aktionen.

	Anklicken, um das Dialogfeld „Task result (Aufgabenergebnis)“ anzuzeigen.
	Anklicken, um die Aufgabe abzubrechen.
	Anklicken, um die Aufgaben aus der Liste zu löschen.
	Falls das Erstellen eines Vorfallsberichts oder das Exportieren von Aufzeichnungen fehlschlägt, durch Anklicken einen erneuten Versuch einleiten.

Aufgabenergebnis

Wenn eine Aufgabe auf mehreren Geräten ausgeführt wurde, werden die Ergebnisse für die einzelnen Geräte angezeigt. Alle fehlgeschlagenen Vorgänge sollten manuell überprüft und konfiguriert werden.

Für die meisten Aufgaben werden folgende Details aufgeführt. Für Aufgaben wie das Exportieren von Aufzeichnungen und Systemberichte auf die Aufgabe doppelklicken, um den Ordner mit den gespeicherten Dateien zu öffnen.

MAC-Adresse	Die MAC-Adresse des aktualisierten Geräts.
Adresse	Die IP-Adresse des aktualisierten Geräts.
Nachricht	Informationen zur Durchführung der Aufgabe: • **Finished (Beendet)**: Die Aufgabe wurde erfolgreich abgeschlossen. • **Error (Fehler)**: Die Aufgabe konnte auf dem Gerät nicht abgeschlossen werden. • **Canceled (Abgebrochen)**: Die Aufgabe wurde vor Fertigstellung abgebrochen.
Beschreibung	Weitere Informationen über die Aufgabe.

Je nach Art der durchgeführten Aufgabe werden die folgenden Details aufgeführt:

Neue Adresse	Die neu zugewiesene IP-Adresse des Geräts.
Aktionsregeln	Die Firmwareversion und der Produktname des Geräts.
Details	Die Seriennummer und IP-Adresse eines ersetzten Geräts und die Seriennummer und IP-Adresse des neuen Geräts.
Referenz-ID	Referenz-ID des Vorfallsberichts.

Berichte erstellen

Client-Konfigurationsdatei

Das Client-Konfigurationsblatt ist für die Fehlersuche und bei der Kontaktaufnahme mit dem Support hilfreich.

Um einen Bericht mit einer Übersicht über die Konfiguration des Client-Systems im HTML-Format anzuzeigen:

1. **Konfiguration** > **Server** > **Diagnose** aufrufen.
2. Klicken Sie auf **View client configuration sheet (Client-Konfigurationsdatei anzeigen)**.

Server-Konfigurationsdatei

Das Server-Konfigurationsblatt enthält allgemeine Informationen über Konfiguration, Kameraeinstellungen, einschließlich Aktionsregeln, Zeitpläne, Aufzeichnungsspeicher, Zusatzgeräte und Lizenzen. Dieser ist bei der Fehlerbehebung und bei der Kontaktaufnahme mit dem Support hilfreich.

Um einen Bericht mit einer Übersicht über die Konfiguration des Server-Systems im HTML-Format anzuzeigen:

1. **Konfiguration** > **Server** > **Diagnose** aufrufen.
2. Klicken Sie auf **View server configuration sheet (Server-Konfigurationsdatei anzeigen)**.

Systembericht

Der Server-Bericht ist eine .zip-Datei mit Parametern und Protokolldateien, die den Axis Customer Support bei der Analyse Ihres Systems unterstützen.

Fügen Sie immer einen Server-Bericht bei, wenn Sie sich an den Kundensupport wenden.

So erzeugen Sie den Systembericht:

1. Rufen Sie das Menü in der rechten oberen Ecke auf.
2. Klicken Sie auf **Help (Hilfe)** > **System report (Systembericht)**.
3. Bearbeiten Sie den Dateinamen, wenn Sie den automatisch generierten Dateinamen ändern möchten.
4. Klicken Sie **Durchsuchen**, um anzugeben, wo der Server-Bericht gespeichert werden soll.
5. Wählen Sie Ihre bevorzugten Einstellungen:
   - **Automatically open folder when report is ready (Automatisches Öffnen des Ordners, wenn der Bericht fertig ist)**, um ihn sofort ansehen zu können.
   - **Include all databases (Alle Datenbanken einbeziehen)**, um detaillierte Informationen über Aufzeichnungen und Systemdaten hinzuzufügen.
   - **Include screenshots of all monitors (Screenshots von allen Monitoren einbeziehen)**, um die Analyse von Systemberichten zu vereinfachen.
6. Klicken Sie auf **OK**.

Einen Systembericht erstellen

AXIS Installation Verifier

AXIS Installation Verifier startet einen Leistungstest, mit dem überprüft wird, ob sämtliche Geräte in einem System nach der Installation funktionieren. Die Ausführung des Test dauert etwa 20 Minuten.

Prüfungen	
Normal conditions (Normale Bedingungen)	Test des Daten-Streamings und des Datenspeichers anhand der aktuellen Systemeinstellungen in AXIS Camera Station Pro. Ausgang: Bestanden oder fehlgeschlagen.
Schwaches Licht	Test des Daten-Streamings und des Datenspeichers anhand von Einstellungen, die auf schlechte Lichtverhältnisse optimiert sind, beispielsweise Verstärkungseinstellungen. Ausgang: Bestanden oder fehlgeschlagen.
Stresstest	Test, bei dem das Daten-Streaming und der Datenspeicher kontinuierlich erhöht werden, bis die Belastungsgrenze des Systems erreicht ist. Ausgang: Informationen zur maximalen Systemleistung.

Hinweis

- Sie können nur Geräte testen, die AXIS Camera Application Platform 2 (ACAP 2) und höher unterstützen.
- Während des Tests befindet sich AXIS Camera Station Pro im Wartungsmodus und sämtliche Überwachungsaktivitäten sind vorübergehend nicht verfügbar.

Um den Test zu starten:

1. **Konfiguration** > **Server** > **Diagnose** aufrufen.
2. Auf **AXIS Installation Verifier öffnen ...** klicken.
3. Klicken Sie auf **Start**.
4. Wenn der Test abgeschlossen ist, klicken Sie auf **View report (Bericht ansehen)**, um den Bericht anzuzeigen, oder klicken Sie auf **Save report (Bericht speichern)**, um den Bericht zu speichern.

Anlagenliste

Exportieren Sie eine Anlagenliste für Ihr Video Management System. In der Liste werden Name, Typ, Modell, Status und Seriennummer und Modell des Folgenden aufgeführt:

- Alle verbundenen Server
- Alle verbundenen Geräte
- Das Client-Terminal, von dem Sie die Anlagenliste exportieren, wenn Sie mit mehreren Terminals verbunden sind

Anlageliste exportieren:

1. Gehen Sie zu ☰ **> Other > Asset list (Weitere > Anlagenliste)**.
2. Klicken Sie auf **Exportieren**.
3. Wählen Sie den Speicherort und klicken Sie auf **Speichern**.
4. Unter **Latest export (Neuester Export)** wird ein Link zur Datei angezeigt bzw. aktualisiert.
5. Klicken Sie auf den Link, um zum Speicherort der Datei zu gelangen.

Status der Axis Services

Um den Status der Onlinedienste von Axis einzusehen:

1. **Konfiguration** > **Server** > **Diagnose** aufrufen.
2. Klicken Sie auf **View status of Axis services (Status der Axis-Dienste anzeigen)**.

AXIS Camera Station Pro Dienststeuerung

Der Server verwendet die Dienststeuerung von AXIS Camera Station Pro zum Starten und Stoppen sowie zum Ändern der Einstellungen. Sie wird nach dem Ende der Installationsarbeiten automatisch aufgerufen. Nach einem Serverneustart wird die Dienststeuerung automatisch zwei Minuten später neu gestartet. Ein Symbol im Benachrichtigungsbereich von Windows zeigt den Status des Dienstes an.

Rechtsklicken Sie auf das Symbol und wählen Sie **Open AXIS Camera Station Service Control (Dienststeuerung der AXIS Camera Station öffnen)**, **Start Service (Dienst starten)**, **Stop Service (Dienst anhalten)**, **Restart Service (Dienst erneut starten)** oder **Exit (Schließen)** aus.

So öffnen Sie die Dienststeuerung über das Startmenü:

Rufen Sie das Menü **Start (Startmenü)** auf und wählen Sie **All Programs > Tools > Service Control (Alle Programme > Tools > Dienststeuerung)** aus.

	Wird ausgeführt
	Wird gestartet
	Beendet

Modify Settings (Einstellungen ändern)	Wählen Sie diese Option aus, um die Server-Einstellungen ändern zu können.
Auf Werkseinstellungen zurücksetzen??	Klicken Sie darauf, um alle Einstellungen auf die ursprünglichen Standardeinstellungen zurückzusetzen.
Starten	Klicken Sie darauf, um den Serverstatus zu ändern.
Anhalten	
Neu starten	Klicken Sie darauf, um einen Neustart des Servers durchzuführen.

Allgemeines

Wählen Sie in AXIS Camera Station Pro **Modify settings (Einstellungen ändern)** aus und klicken Sie auf **General (Allgemein)**, um die allgemeinen Server-Einstellungen zu ändern.

Servereinstellungen	
Servername	Der Name des Servers. Der Servername wird im Software-Client angezeigt. Der Standardservername ist der Computername. Der Name ändert sich nicht, wenn Sie den Computernamen ändern.
Web client port (Webclientport)	Der Webclient für AXIS Camera Station verwendet diesen Port.
Ports range (Portbereich)	Geben Sie den Portbereich an. Der Rest der Ports ändert sich automatisch.
Allow AXIS Camera Station Pro to add exceptions to the Windows Firewall (Ausnahmen für Windows Firewall erlauben)	Wählen Sie diese Option aus, wenn Sie zulassen möchten, dass der Windows-Firewall von AXIS Camera Station Pro automatisch Ausnahmen hinzugefügt werden, wenn ein Benutzer den Portbereich ändert.

Hinweis

- Wenn zwischen Client und Server NAT, Firewall oder Ähnliches installiert ist, konfigurieren Sie die Ports in der NAT und/oder Firewall als geöffnete Ports.
- Die Portnummern müssen im Bereich 1024–65534 liegen.

Portliste für AXIS Camera Station Pro

Die folgenden Tabellen zeigen, welche Ports und Protokolle AXIS Camera Station Pro verwendet. Für die optimale Leistung und Verwertbarkeit müssen diese ggf. in der Firewall erlaubt werden. Wir berechnen die Portnummern auf Grundlage des HTTP-Hauptports 29200.

Server zu Geräten

Port	Anzahl	Protokoll	Ein-/Ausgang	Beschreibung
HTTP- und HTTPS-Hauptports	80 und 443	TCP	Ausgehend	Wird für Videostreams und Gerätedaten verwendet.

Standardmäßiger Bonjour-Port	5353	UDP	Multicast (Eingehend und ausgehend)	Zur Erkennung von Geräten mit mDNS Discovery (Bonjour). Multicast 224.0.0.251. Ist keine Verbindung mit dem Standardport möglich, liegt dies möglicherweise daran, dass dieser von einer anderen Anwendung verwendet wird, die die Freigabe verweigert. In diesem Fall wird ein zufälliger Port verwendet. Bonjour entdeckt bei Verwendung eines zufälligen Ports keine Geräte mit verbindungslokalen Adressen.
Standardmäßiger SSDP-Port	1900	UDP	Multicast (Eingehend und ausgehend)	Zur Erkennung von Geräten mit SSDP (UPNP). Multicast 239.255.255.250.
Standardport für WS-Discovery	3702	UDP	Multicast (Eingehend und ausgehend)	WS-Discovery-Webanalyse zur Erkennung von Onvif-Geräten. Multicast 239.255.255.250.

Client zu Server

Port	Anzahl	Protokoll	Ein-/Ausgang	Kommunikation zwischen	Beschreibung
HTTP-Port für Videostream	29200	TCP	Eingehend	Server und Client	Für Video-, Audio- und Metadaten-stream verwendet (AES-Verschlüsse-lung).
Haupt-TCP-Port	29202	TCP	Eingehend	Server und Client	+2 Offset vom HTTP-Port für Videostream.

					Für verschlüsselte Anwendungsdaten verwendet (Verschlüsselung TLS 1.2).
API-Webserverport	29204	TCP	Eingehend	Server und mobile Apps	+4 Offset vom HTTP-Port für Videostream. Für Anwendungsdaten und Videostream MP4 über HTTPS verwendet.
API-Medienport	29205	TCP	Eingehend	Server und mobile Apps	+5 Offset vom HTTP-Port für Videostream. Für Videostream RTSP über HDMI verwendet.

Lokaler HTTP-Port für Proxyserver	29206	TCP	Eingehend	Interne Kommunikation auf dem Server	+6 Offset vom HTTP-Port für Videostream (ServerPortParser). +2 Versatz vom API-Webserverport (RemoteFacadeBinder). Nur intern auf dem AXIS Camera Station Pro Server-Computer zugänglich. Workaround-Port für unbekannte Ausgabe. Mobile Apps tätigen Anrufe zum SRA-Modul, das HTTPS empfängt, in HTTP konvertiert und an den lokalen HTTP-Port für Proxyserver und den API-Medienport weitersendet.
Port des Web-Proxy-Endpunkts	29207	TCP	Eingehend	Server und Komponente	+7 Offset vom HTTP-Port für Videostream. Dient der sicheren Kommunikation zwischen Komponente und Geräten.

Domänen und Ports für sicheren Fernzugriff v2

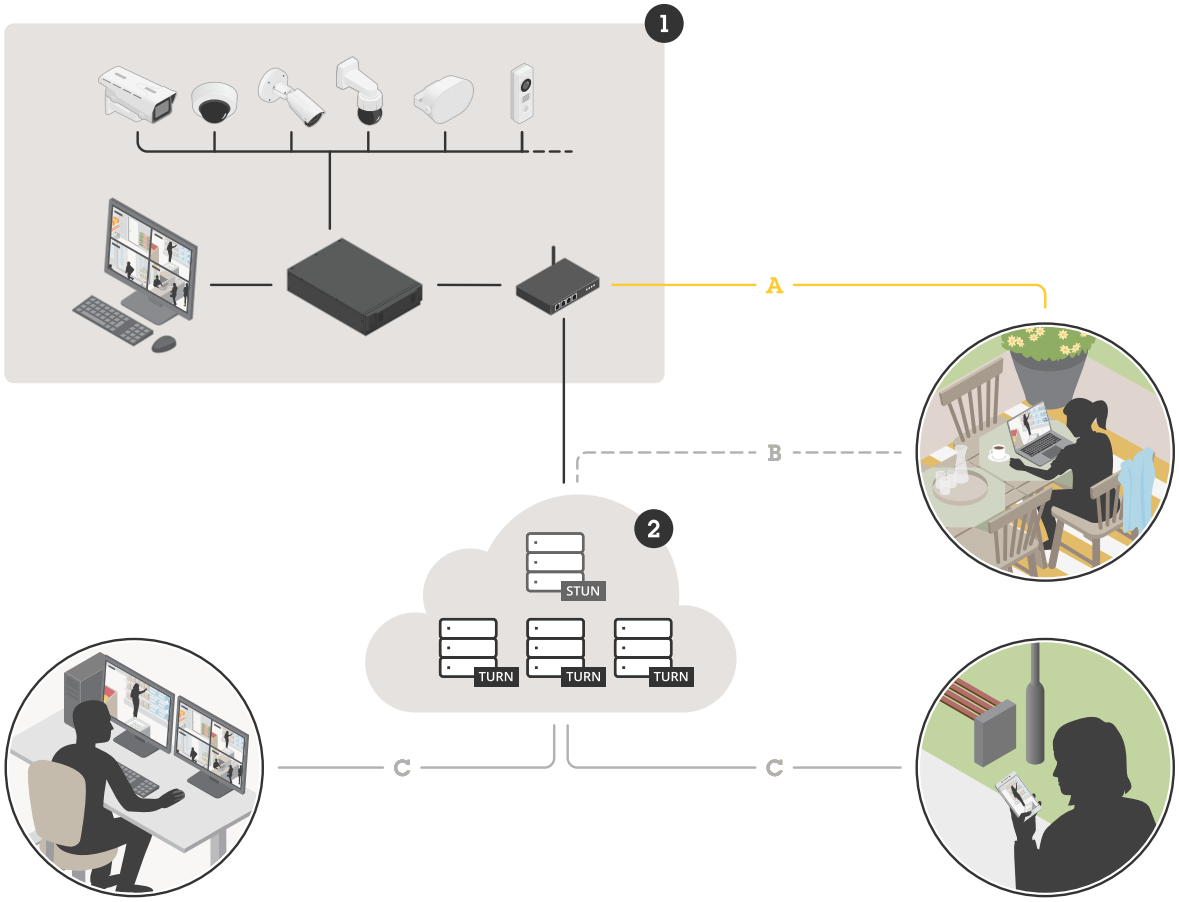


Bild: Übersicht über die Lösung für SRA v2 in AXIS Camera Station Pro

1. Überwachter Standort im lokalen Netzwerk mit lokalem Anzeige-Client
   - A – Fernverbindung (Peer-to-Peer)
   - B – Temporäre STUN/TURN-Verbindung zu den verbundenen Diensten von Axis Cloud

Name oder Typ	Adresse	Portnummer	Protokoll	Richtung
MyAxis-Anmeldung für SRA v2	https://eu.login.connect.axis.com	443	TCP	Eingehend und ausgehend
Kommunikation mit Cloud-Dienst für SRA v2	https://eu.cs.connect.axis.com	443	TCP	Eingehend und ausgehend
Kommunikation mit Cloud-Dienst-API für SRA v2	https://api.vms.axis.cloud	443	TCP	Eingehend und ausgehend
EdgeHost-Komponente	75.2.119.140	443, 8443	-	Eingehend und ausgehend
EdgeHost-Komponente	99.83.133.42	443, 8443	-	Eingehend und ausgehend
EdgeHost-Komponente	cep.connect.axis.com	443, 8443	-	Eingehend und ausgehend

2. Verbundene Dienste von Axis Cloud

– C – TURN-Fernverbindung zu den verbundenen Diensten von Axis Cloud

Name oder Typ	Adresse	Portnummer	Protokoll	Richtung
Kommunikation mit P2P-Proxy und WebRTC-Komponenten	wss://signaling.prod.webrtc.connect.axis.com	443	TCP	Eingehend und ausgehend
Kommunikation mit P2P-Proxy und WebRTC-Komponenten	https://*.turn.prod.webrtc.connect.axis.com	443, 3478, 5349, 49152-65535	TCP	Eingehend und ausgehend

Für Komponenten reserviert

Komponente	Abhören auf der Schnittstelle	Port	Anzahl	Protokoll	Ein-/Ausgang	Kommunikation zwischen	Beschreibung
Sicherer Eingang	Localhost (127.0.0.1)	Webserver-port	29214	HTTPS	Eingehend	Client (Registerkarte Zugriffsverwaltung) und Komponente	+14 Offset vom HTTP-Port für Videostream. Ältere Installationen verwendeten Port 8081.
Sicherer Eingang	Alle (0.0.0.0/INADDR_ANY)	Webserver-port	29215	HTTPS	Eingehend	Haupt- und Subserver	+15 Offset vom HTTP-Port für Videostream. Wird für die Kommunikation zwischen Haupt- und Nebenservern bei der Einrichtung von mehreren Servern verwendet.
Überwachung des Systemzustands	Alle (0.0.0.0/INADDR_ANY)	Webserver-port	29216	HTTPS	Eingehend	Client (Registerkarte System Health	+16 Offset vom HTTP-Port für Videostream.

Komponente	Abhören auf der Schnittstelle	Port	Anzahl	Protokoll	Ein-/Ausgang	Kommunikation zwischen	Beschreibung
						Monitoring) und Komponente	Wird zum Hosten von Webseiten von System health Monitoring sowie zum Teilen von Daten in mehreren Systemkonfigurationen verwendet.
Cloud-Dienst zur Überwachung des Systemzustands	localhost	Webserver-port	29217	HTTPS	Eingehend	AXIS Camera Station Pro (Webseite) und CloudService Backend (Plugin)	+17 Offset vom HTTP-Port für Videostream. Wird für den Cloud-Dienst zur Überwachung des Systemzustands verwendet, um die Überwachung des Systemzustands zu aktivieren.
Intelligente Suche 2	localhost	Webserver-port	29218	HTTPS	Eingehend	Client (Registerkarte „Smart search (Intelligente Suche)“) und Komponente	+18 Offset vom HTTP-Port für Videostream. Wird zum Hosten der API der intelligenten Suche und zum Bedienen der Clientwebseite verwendet.
VMS API-Kern	127.0.0.1, ::1	GraphQL-API	29219	GraphQL	Eingehend	VMS API und	+19 Offset vom HTTP-Port für

Komponente	Abhören auf der Schnittstelle	Port	Anzahl	Protokoll	Ein-/Ausgang	Kommunikation zwischen	Beschreibung
						GraphQL-Clients	Videostream. Wird verwendet, um ACS als GraphQL-API einem Client zur Verfügung zu stellen.
			29222				Für zukünftige Verwendung reserviert.
Webclient	localhost	Webserver-port	29223	HTTPS	Eingehend	WebClient in VMS-API/ Embeddable Client	+23 Offset vom HTTP-Port für Videostream. Backend fungiert als Proxy vor konfigurierbarer VMS-API.
Embeddable Client	localhost	Webserver-port	29224	HTTPS	Eingehend	Embeddable Client an VMS API/ WebRTC Streamer/ Signalserver	+24 Offset vom HTTP-Port für Videostream. Backend fungiert als Proxy vor VMS-API.
Konfiguration des Webclients	localhost	Webserver-port	29225	HTTPS	Eingehend	AXIS Camera Station Pro Client (Webseite)	+25 Offset vom HTTP-Port für Videostream. Wird verwendet, um die Webseite und das Backend der Webclient-konfiguration zu hosten.

Komponente	Abhören auf der Schnittstelle	Port	Anzahl	Protokoll	Ein-/Ausgang	Kommunikation zwischen	Beschreibung
Embeddable Client Konfiguration	localhost	Webserver-port	29226	HTTPS	Eingehend	AXIS Camera Station Pro Client (Webseite)	+26 Offset vom HTTP-Port für Videostream. Wird verwendet, um die Webseite und das Backend der Konfiguration des Embeddable Client zu hosten.
			29227				Für zukünftige Verwendung reserviert.
Lokaler ICE-Konfigurationsgenerator	localhost	Webserver-port	29228	HTTPS	Eingehend	Signalserver an ICE-Konfigurationsgenerator	+28 Offset vom HTTP-Port für Videostream. Teil der WebRTC-Komponente vor Ort.
Lokale WebRTC-Konfiguration	localhost	Webserver-port	29229	HTTPS	Eingehend	AXIS Camera Station Pro Client (Webseite)	+29 Offset vom HTTP-Port für Videostream. Wird verwendet, um die Webseite und das Backend der WebRTC-Konfiguration zu hosten. Teil der WebRTC-Komponente vor Ort.

Komponente	Abhören auf der Schnittstelle	Port	Anzahl	Protokoll	Ein-/Ausgang	Kommunikation zwischen	Beschreibung
Lokaler TURN Server	localhost	Coturn-Serverport	29230	UDP	Eingehend/Ausgehend	Embeddable Client/WebClient ↔ TURN-Server	+30 Offset vom HTTP-Port für Videostream. Wird für „Single-Port-WebRTC" auf On-Premise-ACS verwendet.
			29231				Für zukünftige Verwendung reserviert.
Local-IAM (IDP)	0.0.0.0	IDP_OIDC (Öffentlich)	29232	HTTPS	Eingehend	Reverse-Proxy und local-iam	+32 Offset vom HTTP-Port für Videostream. Öffentlicher Port.
Local-IAM (IDP)	0.0.0.0	MTLS (Admin)	29233	HTTPS	Eingehend	Dienste anderer Anbieter	+33 Offset vom HTTP-Port für Videostream. Administrator-Port.
Local-IAM (IDP)	127.0.0.1	TOKENIZER	29234	HTTPS	Eingehend	Dienste anderer Anbieter	+34 Offset vom HTTP-Port für Videostream. Tokenizer-Port.
WebRTC	localhost	Onboarding-API	29235	HTTPS	Eingehend	Cloud-Komponente	+35 Offset vom HTTP-Port für Videostream. Wird vom Onboarding zur Konfiguration der

Komponente	Abhören auf der Schnittstelle	Port	Anzahl	Protokoll	Ein-/Ausgang	Kommunikation zwischen	Beschreibung
							webrtc nutzenden Cloud-Verbindung verwendet. Teil der WebRTC-Komponente.
Opentelemetry	127.0.0.1	gRPC-Port	29236	gRPC	Eingehend	Dienste anderer Anbieter	+36 Offset vom HTTP-Port für Videostream.
Opentelemetry	127.0.0.1	HTTP-Port	29237	HTTPS	Eingehend	Dienste anderer Anbieter	+37 Offset vom HTTP-Port für Videostream.
Audio Manager Pro		Webserverport	29238	HTTPS	Eingehend	Drittanbieter-Integrationsdienste und -komponenten	+38 Offset vom HTTP-Port für Videostream.
			29239				Für zukünftige Verwendung reserviert.
			29240				Für zukünftige Verwendung reserviert.
Data Insights Dashboard	localhost	2dpc/3dpc Push Empfänger	29241	HTTPS	Eingehend (extern)	Empfänger von Push-Nachrichten (Post) mit Personenzählldaten von 2dpc und 3dpc. Intern: Datenbank, Makler	+41 Offset vom HTTP-Port für Videostream.

Komponente	Abhören auf der Schnittstelle	Port	Anzahl	Protokoll	Ein-/Ausgang	Kommunikation zwischen	Beschreibung
Data Insights Dashboard	0.0.0.0	Makler	29242	MQTTS	Eingehend (extern) Ausgehend (Extern)	Empfänger von Ereignismeldungen der Kamera. Überbrückung von MQTT-Maklern bei Bedarf möglich (z. B. viele mit einem nach Thema. Datenbank-"Duplizierung" und Lastausgleich für Profi-Dienste beim Einrichten einer Seite verfügbar) Intern: Empfänger	+42 Offset vom HTTP-Port für Videostream.
			29243				Für zukünftige Verwendung reserviert.
NATS Broker	127.0.0.1	NATS	29244	NATS	Eingehend	Zwischen AXIS Camera Station Pro und den Komponenten und zwischen diesen Komponenten selbst	+44 Offset vom HTTP-Port für Videostream.
Opentelemetry	127.0.0.1	HTTP-Port	29245	HTTP	Eingehend	Endpunkt überwachen, um aus dem offenen Telemetrie-Kollektor	+45 Offset vom HTTP-Port für Videostream.

Komponente	Abhören auf der Schnittstelle	Port	Anzahl	Protokoll	Ein-/Ausgang	Kommunikation zwischen	Beschreibung
						die Metriken zu erhalten	
API-Gateway	Alle (0.0.0.0/INADDR_ANY)	Vom Edge-Host verwendeter Fallback-Port für Reverse-Proxy	29248	HTTPS	Eingehend	Edge-Host und Reverse-Proxy	+48 Offset vom HTTP-Port für Videostream.
API-Gateway	Alle (0.0.0.0/INADDR_ANY)	Fallback-Port, mit ACS-Serverzertifikaten gehostet, der zur Fallback-Kommunikation für den ACS Windows-Client verwendet wird	29250	HTTPS	Eingehend	ACS-Client und API-Gateway	+50 Offset vom HTTP-Port für Videostream.

Weitere Ports

Port	Anzahl	Protokoll	Ein-/Ausgang	Kommunikation zwischen	Beschreibung
Internet HTTPS	80 und 443	TCP	Ausgehend	Client und Server an Internet	Zum Aktivieren von Lizenzen, Herunterladen von Firmware, für verbundene Dienste und weiteres verwendet.
TCP-Streamingport des Servers	29198	TCP	Eingehend	Server und Gerät	-2 Offset vom HTTP-Port für Videostream.
UDP-Port zum Aktualisieren des Status	15156	UDP	Eingehend und ausgehend	Server- und Dienststeuerung	AXIS Camera Station Pro Dienststeuerung hört den Port ab, und der Server überträgt den Status einer aktuellen Aktualisierung.

Datenbank

Datenbankdateien

Kerndatenbankdateien

AXIS Camera Station Pro speichert die Kern-Datenbankdateien unter `C:\ProgramData\AXIS Communications\AXIS Camera Station Server`.

Bei AXIS Camera Station Versionen vor 5.13 ist nur eine einzelne Datenbankdatei vorhanden: **ACS.FDB**.

Bei AXIS Camera Station Version 5.13 oder höher sind drei Datenbankdateien vorhanden:

- **ACS.FDB**: Diese Kerndatenbankdatei enthält die Systemkonfiguration wie Geräte, Ansichten, Berechtigungen, Ereignisse und Videostreamprofile.
- **ACS_LOGS.FDB**: Diese Protokolldatenbankdatei enthält Protokollreferenzen.
- **ACS_RECORDINGS.FDB**: Diese Aufzeichnungsdatenbankdatei enthält Metadaten und Verweisen auf die Aufzeichnungen, die an dem unter **Configuration > Storage (Konfiguration > Speicher)** angegebenen Speicherort gespeichert sind. AXIS Camera Station Pro erfordert, dass diese Datei die Aufzeichnungen während der Wiedergabe in der Zeitleiste wiedergeben muss.

Datenbankdateien von Komponenten

SecureEntry.db – Die Datenbankdatei AXIS Secure Entry enthält alle Daten zur Zutrittskontrolle mit Ausnahme der Fotos der Karteninhaber. Sie ist unter `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\INTERNAL\main_db` gespeichert.

smartSearch.sqlite3 – Die Datenbankdatei der intelligenten Suche enthält die Kamerakonfiguration und die gespeicherten Suchfilter. Sie ist unter `C:\ProgramData\Axis Communications\AXIS Smart Search\data` gespeichert.

Datenbankeinstellungen

Die Datenbank wird jede Nacht und vor der Aktualisierung des Systems gesichert. Wählen Sie in AXIS Camera Station Pro **Modify settings (Einstellungen ändern)** aus und klicken Sie auf **Database (Datenbank)**, um die allgemeinen Backupeinstellungen zu ändern.

Backup folder (Sicherungsordner)	Klicken Sie auf **Browse** und wählen Sie einen Ort zum Speichern der Datenbanksicherung aus. Starten Sie AXIS Camera Station Pro Server neu, um die Änderung zu übernehmen. Wenn der Pfad des Sicherungsordners falsch ist oder AXIS Camera Station Pro keinen Zugriff auf die Netzwerkfreigabe hat, wird die Sicherung unter `C:\ProgramData\Axis Communications\AXIS Camera Station Server\backup` gespeichert.
Days to keep backups (Speicherdauer der Sicherungskopie)	Hier können Sie festlegen, wie viele Tage die Backups gespeichert werden. Jeder Wert zwischen 1 und 30 ist möglich. Der Standardwert ist 14 Tage.
Fortschritt der Aktualisierung	Klicken Sie **Details anzeigen**, um sich Details zur aktuellen Datenbankaktualisierung anzeigen zu lassen. Darin sind die Ereignisse eingeschlossen, die sich seit dem letzten Neustart der Dienststeuerung von AXIS Camera Station Pro ereignet haben.

Datenbanksicherung

In der Datenbank sind Informationen zu Aufzeichnungen und andere Metadaten enthalten, die für ein einwandfreies Funktionieren des Systems erforderlich sind.

Wichtig

- In der Datenbank werden die Aufzeichnungen nicht gespeichert. Geben Sie stattdessen unter **Configuration > Storage (Konfiguration > Speicher)** einen Speicherort an. Sichern Sie die Aufzeichnungen separat.
- Server- und Datenbankeinstellungen in der Dienststeuerung der AXIS Camera Station Pro werden nicht gespeichert.

Systemsicherung

Das System speichert die Systemsicherung automatisch in dem Ordner, der auf der Registerkarte **Database (Datenbank)** angegeben ist, siehe *Datenbankeinstellungen, on page 231*. Eine Systemsicherung umfasst sowohl die grundlegenden Datenbankdateien als auch die Datenbankdateien der Komponenten, siehe *Datenbankdateien, on page 231*.

Backup-Dateien	
`System_YYYY-MM-DD-HH-mm-SSSS.zip`	Eine nachts ausgelöste Sicherungskopie.
`PreUpgrade_YYYY-MM-DD-HH-mm-SSSS.zip`	Eine Sicherung wird vor einer Datenbankaktualisierung ausgelöst.
`User_YYYY-MM-DD-HH-mm-SSSS.zip`	Eine Sicherung wird vor dem Entfernen eines Speichers ausgelöst.

In der zip-Datei finden Sie folgende Dateien:

ACS	Dieser Ordner enthält die Kern-Datenbankdateien `ACS.FDB`, `ACS_LOGS.FDB` und `ACS_RECORDINGS.FDB`.
Komponenten	Dieser Ordner ist nur verfügbar, wenn Sie eine Komponente verwenden. Dies kann beispielsweise AXIS Camera Station Secure Entry oder „Intelligente Suche“ sein. • **webrtc**: Dieser Ordner enthält WebRTC Konfigurationsdateien. • **ACMSM**: Dieser Ordner enthält die Datenbankdatei `SecureEntry.db` von AXIS Camera Station Secure Entry sowie Bilder von Karteninhabern. • **Smart Search**: Dieser Ordner enthält die Intelligente Suche Datenbankdatei `smartSearch-backup-yyyyMMddHHmmssfff.sqlite3`.
`backup_summary.json`	Diese Dateien enthalten detailliertere Informationen zur Sicherung.
`_cluster_yyyyMMddHHmmssfff.dbcbackup`	Diese Datei enthält eine logische Sicherung des PostgreSQL-Datenbankclusters, einschließlich clusterweiter Daten wie Rollen und Tablespaces.

Wartungssicherung

Geben Sie auf der Registerkarte **Database (Datenbank)** den Sicherungsordner für die Wartungssicherungen an (siehe *Datenbankeinstellungen, on page 231*). Eine Wartungssicherung umfasst die Kern-Datenbankdateien, wobei sich jede Datenbankdatei in einem separaten Ordner `PreMaintenance_YYYY-MM-DD-HH-mm-SSSS` befindet.

Sie kann auf unterschiedliche Weise ausgelöst werden:

- Automatisch bei der Aktualisierung AXIS Camera Station Pro.
- Wenn Sie die Datenbankwartung manuell über die AXIS Camera Station Pro Dienststeuerung ausführen. Siehe *Datenbankwartung, on page 234*.
- Automatisch durch die im Aufgabenplaner von Windows konfigurierte geplante Datenbankwartung. Siehe *Werkzeuge, on page 236*.

Manuelle Sicherung

Hinweis

Mit einer manuellen Sicherung können nur die Kerndatenbankdateien gesichert werden. Datenbankdateien von Komponenten, wie z. B. die Datenbankdatei der intelligenten Suche, werden nicht gesichert.

Eine manuelle Sicherungskopie kann auf zwei Arten erstellt werden:

- **Option 1:** Gehen Sie zu `C:\ProgramData\AXIS Communications\AXIS Camera Station Server` und erstellen Sie eine Kopie der Datenbankdateien. Sichern Sie dann das PostgreSQL-Datenbankcluster:
  1. Öffnen Sie ein Terminal als Administrator in dem Verzeichnis, in dem Sie die Sicherung speichern möchten.
  2. Führen Sie `"C:\Program Files\Axis Communications\AXIS Camera Station\Core\DbConsole\DbConsole.exe" backup –cluster` aus.
  3. Die Sicherung wird in einem Ordner mit dem Namen **JJJJMMTThhmmssfff** in dem Verzeichnis gespeichert, in dem Sie das Terminal geöffnet haben.
- **Option 2:** Erstellen Sie einen Systembericht mit allen enthaltenen Datenbanken und kopieren Sie die Datenbanksicherungsdateien. Stellen Sie sicher, dass die Option **Include all databases (Alle Datenbanken enthalten)** ausgewählt ist. Siehe *Systembericht, on page 213*.

Wiederherstellen einer Datenbank

Falls die Datenbank aufgrund eines Hardwarefehlers oder anderer Probleme verloren geht, kann sie von einer der gespeicherten Sicherungskopien wiederhergestellt werden. Das System bewahrt Backup-Dateien standardmäßig 14 Tage lang auf. Weitere Informationen zur Datenbanksicherung finden Sie unter *Datenbanksicherung, on page 232*.

Hinweis

In der Datenbank werden die Aufzeichnungen nicht gespeichert. Geben Sie stattdessen unter **Configuration > Storage (Konfiguration > Speicher)** einen Speicherort an. Sichern Sie die Aufzeichnungen separat.

Die Datenbank wird mit den folgenden Schritten wieder hergestellt:

1. Rufen Sie die Dienststeuerung von AXIS Camera Station Pro auf und klicken Sie auf **Stop (Anhalten)**, um den Dienst anzuhalten.
2. Gehen Sie zu den Sicherungsdateien der Datenbank. Siehe *Datenbanksicherung, on page 232*.
3. Extrahieren Sie die Dateien.
4. PostgreSQL-Datenbankcluster wiederherstellen:
   4.1. Öffnen Sie als Administrator ein Terminal in dem extrahierten Ordner.

4.2. Führen Sie `"C:\Program Files\Axis Communications\AXIS Camera Station\Core\DbConsole\DbConsole.exe" restore -backup-file _cluster_yyyyMMddHHmmssfff.dbcbackup` aus.

4.3. Klicken Sie auf **y (j)**, wenn Sie dazu aufgefordert werden, die Vertrauenswürdigkeit der Quelle der Sicherungsdatei zu bestätigen.

5. Kopieren Sie im extrahierten Ordner die folgenden Datenbankdateien unter **ACS** nach `C:\ProgramData\AXIS Communications\AXIS Camera Station Server\`.
   - **ACS.FDB** - Diese Datei muss zur Wiederherstellung der Datenbank kopiert werden.
   - **ACS_LOGS.FDB** - Diese Datei muss zur Wiederherstellung der Protokolle kopiert werden.
   - **ACS_RECORDINGS.FDB** - Diese Datei muss zur Wiederherstellung von Aufzeichnungen kopiert werden.
6. Wenn Sie AXIS Camera Station Secure Entry verwenden, befolgen Sie die Anweisungen unter `RESTORE_INSTRUCTIONS.txt`, die Sie unter `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry 2\INTERNAL\main_db` finden.
7. Wenn Sie die Intelligente Suche verwenden, kopieren Sie **smartSearch-backup-yyyyMMddHHmmssfff.sqlite3** von `smartsearch` nach `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Smart Search\data` und benennen Sie es in **smartSearch.sqlite3** um.
8. Wenn Sie den VMS-Webclient verwenden, kopieren Sie alle Dateien von `webrtc` nach `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\WebRTC`.
9. Rufen Sie erneut die Dienststeuerung von AXIS Camera Station Pro auf und klicken Sie auf **Start (Starten)**, um den Dienst zu starten.

Datenbankwartung

Führen Sie unbedingt eine Datenbankwartung aus, wenn der Alarm `Database maintenance is required` angezeigt wird oder das System unerwartet ausgeschaltet wird (zum Beispiel bei einem Stromausfall).

Zum Starten der Datenbankwartung siehe *Werkzeuge, on page 236*.

Hinweis

AXIS Camera Station Secure Entry verwendet DB Janitor, um die Datenbankdateien zu überwachen und bei Bedarf zu verkleinern. Das Zutrittssystem ist in dem seltenen Fall einer erzwungenen Verkleinerung vorübergehend nicht verfügbar.

Datenbank – bewährte Vorgehensweisen

Um Probleme zu vermeiden, merken Sie sich bitte Folgendes:

Auf Laufwerkfehler prüfen – Laufwerkfehler können die Datenbank beschädigen. Verwenden Sie ein Tool wie chkdsk (Check Disk), um die Festplatte mit der Datenbank auf beschädigte Sektoren zu durchsuchen. Führen Sie chkdsk regelmäßig aus.

Antiviren-Software und externe Sicherungskopien – Schließen Sie die Datenbank von Virenscans aus, da bestimmte Antiviren-Software die Datenbank beschädigen kann. Bei Verwendung eines externen Sicherungssystems sichern Sie die aktuelle und aktive Datenbank nicht. Erstellen Sie stattdessen eine Sicherungskopie aus den Dateien im Sicherungsordner.

Stromausfall – Ein unerwartetes Ausschalten, z. B. aufgrund eines Stromausfalls, kann die Datenbank beschädigen. Verwenden Sie bei kritischen Installationen eine USV (unterbrechungsfreie Stromversorgung).

Kein Speicherplatz – Wenn die Festplatte voll wird, kann die Datenbank beschädigt werden. Um dies zu vermeiden, den AXIS Camera Station Pro-Server auf einem eigenen Computer mit ausreichend Speicherkapazität installieren. Siehe *axis.com/products/axis-camera-station/hardware-guidelines* für Hardwareanforderungen.

Defektes RAM – Regelmäßig Windows Memory Diagnostic durchführen, um das RAM auf Fehler zu prüfen.

Zertifikate

Auf der Registerkarte **Certificates (Zertifikate)** können Sie die Serverzertifikate für AXIS Camera Station Proverwalten. Sie können Informationen über das aktuelle Serverzertifikat anzeigen, sehen, wann es abläuft, neue Serverzertifikate erstellen und importieren oder das aktuelle Zertifikat exportieren. Die Serverzertifikate sind unter C:\ProgrammDaten\Axis Communications\AXIS Camera Station Server\certs gespeichert.

Server-Zertifikat

Erstellen	Erstellen Sie ein neues, selbstsigniertes Serverzertifikat. Dieses ersetzt das zuvor vom Server verwendete Zertifikat und erfordert einen Neustart des Servers, um wirksam zu werden.
Importieren...	Importieren Sie ein Serverzertifikat aus einer Datei. Unterstützt werden die Dateiformate PEM und PFX/PKCS12. Außerdem ist die Unterstützung auf RSA mit mindestens 2048-Bit-Schlüsseln beschränkt.

Hinweis

Wenn Sie ein Zertifikat mit Zwischenzertifikaten im PEM-Format importieren, werden alle Zwischenzertifikate in der .cer-Datei erwartet. Wenn Sie Ihre eigenen Zertifikate erstellen, siehe *Zwischenzertifikate für den Import vorbereiten, on page 235*.

Aktuelles Zertifikat

Listet Informationen über das aktuelle Serverzertifikat auf, mit denen manuell überprüft werden kann, ob der Client mit dem richtigen Server verbunden ist.

Ansehen	Zeigen Sie weitere Details zum Serverzertifikat an.
Exportieren...	Exportieren Sie das Serverzertifikat als PFX-Datei.

Ein neues Serverzertifikat generieren

- Drücken Sie die Windows-Taste + S, um die AXIS Camera Station Pro Service-Steuerung zu suchen und zu öffnen.
- Klicken Sie auf der Registerkarte **Certificates (Zertifikate)** auf **Generate (Generieren)**, um ein neues Serverzertifikat zu erstellen.
- Starten Sie den Server neu, um das neue Serverzertifikat anzuwenden.

Zwischenzertifikate für den Import vorbereiten

Um ein Zertifikat mit Zwischenzertifikaten in AXIS Camera Station Pro zu importieren, kombinieren Sie das Serverzertifikat und das Zwischenzertifikat in einer Datei:

1. Öffnen Sie eines der Serverzertifikate und das Zwischenzertifikat in Notepad. Der Inhalt ist wie folgt strukturiert:
   ```
   cert.cer
   ——BEGIN CERTIFICATE——
   MIIFTDCCB....
   ——END CERTIFICATE——
   ```
2. Kopieren Sie den Inhalt des einen Zertifikats in das andere und ändern Sie die erste Zeile in combined_cert.cer:
   ```
   combined_cert.cer
   ——BEGIN CERTIFICATE——
   ```

```
MIIFTDCCB....
———END CERTIFICATE———
———BEGIN CERTIFICATE———
MIIE+zCCA+OgA.....
———END CERTIFICATE———
```

3. Speichern Sie die Datei.

Werkzeuge

In der Dienststeuerung der AXIS Camera Station Pro wählen Sie **Modify settings (Einstellungen ändern)** und klicken Sie auf **Tools**, um die Datenbanksicherung zu starten und Teilsystemberichte zu erstellen.

Datenbank-Instandhalter

- AXIS Camera Station Pro Dienststeuerung öffnen.
- Klicken Sie auf **Tools**.
- Klicken Sie unter **Database maintainer (Datenbank warten)** auf **Run (Ausführen)**.
- Die voraussichtliche Ausfallzeit wird angezeigt. Klicken Sie zum Fortfahren auf **Ja**. Sobald der Vorgang gestartet wurde, kann er nicht mehr abgebrochen werden.

Hinweis

- AXIS Camera Station Pro Server sowie alle laufenden Aufzeichnungen werden während der Wartung gestoppt. Nach der Wartung startet der Server automatisch.
- Schalten Sie den Computer während der Wartung nicht aus.
- Die Datenbankwartung erfordert Administratorrechte auf dem Windows-Computer.
- Wenn die Datenbankwartung die Datenbank nicht wiederherstellen kann, wenden Sie sich an den technischen Support von Axis.

Führen Sie unbedingt eine Datenbankwartung aus, wenn der Alarm „Database maintenance is required (Wartung der Datenbank erforderlich)“ angezeigt wird oder das System unerwartet ausgeschaltet wird (zum Beispiel bei einem Stromausfall).

Die Wartung der Datenbank lässt sich in Windows auch automatisch ausführen, indem Sie unter Geplante Aufgaben den AXIS Camera Station Pro Database Maintenance Task aktivieren. Zeitpunkt und Häufigkeit der Datenbankwartung können über den Auslöser konfiguriert werden.

Systembericht

Beim Teilsystembericht handelt es sich um eine ZIP-Datei mit Parametern und Protokolldateien, anhand derer der Axis Kundensupport Ihr System analysieren kann. Fügen Sie immer einen Server-Bericht bei, wenn Sie sich an den Kundensupport wenden. Rufen Sie im AXIS Camera Station Pro Client zu **> Help > System report (> Hilfe > Systembericht)** auf, um einen vollständigen Systembericht zu erstellen.

So erzeugen Sie einen Teilsystembericht:

1. Klicken Sie auf **Ausführen**.
2. Wählen Sie die angeforderten Informationen aus und geben Sie sie in das Dialogfeld ein.
3. Klicken Sie **Bericht erstellen**.

Systemberichtstool	
Dateiname	Geben Sie einen Dateinamen für den Server-Bericht an.
Ordner	Geben Sie an, wo der Server-Bericht gespeichert werden soll.

Systemberichtstool	
Ordner automatisch öffnen, wenn Bericht erstellt wurde	Wählen Sie diese Option aus, um den Ordner automatisch zu öffnen, nachdem der Systembericht erstellt wurde.
Datenbankdatei in Bericht einbeziehen	Datenbankdatei in Bericht einbeziehen – Die Datenbank von AXIS Camera Station Pro enthält Informationen zu Aufzeichnungen sowie Daten, die die ordnungsgemäße Funktion des Systems gewährleisten.

Netzwerkprotokollierung

- Klicken Sie auf den Link, um eine Anwendung zur Netzwerkprotokollanalyse herunterzuladen.
- Klicken Sie auf **Start (Starten)**, um die Anwendung nach der Installation direkt zu starten.

Zertifizierungsstelle zurücksetzen

- Klicken Sie auf **Reset (Zurücksetzen)**, um eine neue Zertifizierungsstelle zu erstellen und den Dienst neu zu starten.
- Sobald der Dienst neu gestartet ist, können Sie sich anmelden und bei Bedarf eine benutzerdefinierte Zertifizierungsstelle importieren.

Fehlerbehebung

Informationen zu dieser Anleitung

In dieser Anleitung finden Sie eine Sammlung von Problemen im Zusammenhang mit AXIS Camera Station Pro und Informationen zu ihrer Fehlerbehebung. Wir haben die Probleme unter einem zugehörigen Thema gespeichert, um das Gesuchte einfacher zu finden. Ein Thema kann z. B. „Audio" oder „Live-Ansicht" sein. Für jedes Problem wird eine Lösung beschrieben.

Mehr erfahren

Besuchen Sie *axis.com/support* für:

- Häufig gestellte Fragen
- Hardwareanforderungen
- Softwareaktualisierungen
- Tutorien, Schulungsmaterial und andere hilfreiche Informationen

Serverdienst neu starten

Durch das Neustarten des AXIS Camera Station Pro Serverdienstes können einige allgemeine Probleme behoben werden.

Hinweis

- Der Neustart des Serverdienstes kann eine Weile dauern, und es gibt keine Möglichkeit, den Neustart abzubrechen.
- Der Server ist nicht verfügbar, während der Serverdienst neu startet.
- Alle angeschlossenen Geräte verlieren die Verbindung zum Server, während der Serverdienst neu startet.

So starten Sie den Serverdienst neu:

1. **Konfiguration** > **Server** > **Diagnose** aufrufen.
2. Klicken Sie auf **Restart AXIS Camera Station server service...(AXIS Camera Station Serverdienst neu starten...)**.

Der AXIS Camera Station Pro Dienst

Der Dienst wird häufig neu gestartet

Der Server kann überlastet sein, was zu einer langen Aufgabenwarteschlange führt und auch die Datenbanken beschädigen kann.

- Überprüfen Sie die Ressourcenverwaltung Ihres Systems, um zu verifizieren, ob AXIS Camera Station Pro oder eine andere Anwendung eine große Menge an Ressourcen verwendet.
- Führen Sie die Datenbankwartung aus. Informationen dazu finden Sie unter *Datenbankwartung* im Benutzerhandbuch zu AXIS Camera Station Pro.

Falls alle diese Maßnahmen erfolglos bleiben, wenden Sie sich an den Axis Support. Wechseln Sie zu *Eskalationsverfahren, on page 254*.

Geräte im Video Management System

Übliche Probleme

Verbindung zur Kamera nicht möglich	
Verbindung von VMS zur Kamera nicht möglich. Die aufgelisteten Kameras wurden nicht hinzugefügt.	1. Stellen Sie sicher, dass die Kamera über eine Netzwerkverbindung verfügt, über die Stromversorgung verfügt und die Kamera aktiv ist. 2. Gehen Sie zu **Konfiguration > Geräte hinzufügen** und versuchen Sie erneut, die Kamera hinzuzufügen.

Die Installation wurde abgebrochen	
Der Benutzer hat die Installation abgebrochen. Die aufgelisteten Kameras wurden nicht hinzugefügt.	Um die Kameras hinzuzufügen, **Konfiguration > Geräte hinzufügen** aufrufen.

Kennwort konnte auf Kamera nicht festgelegt werden	
Das Kennwort konnte für die aufgelisteten Kameras nicht festgelegt werden.	1. Um das Kennwort manuell festzulegen, gehen Sie zu **Konfiguration > Geräte > Verwaltung**. 2. Klicken Sie mit der rechten Maustaste auf die Kamera und wählen Sie **Benutzerverwaltung > Kennwort einstellen**.

Gerät kann nicht hinzugefügt werden

Wenn das Gerät in einem anderen System verwendet wurde, bevor es zu AXIS Camera Station Pro hinzugefügt wurde:

- Setzen Sie das Gerät auf die Werkseinstellungen zurück.

Falls das Gerät weiterhin nicht zum Video Management System hinzugefügt werden kann, versuchen Sie, das Gerät zu AXIS Device Manager hinzufügen.

Sie können ein anderes Gerätemodell als das gewünschte hinzufügen:

- Falls das Produkt neu oder mit aktueller Firmware versehen ist, kann es sich um ein Kompatibilitätsproblem handeln. Stellen Sie sicher, dass Sie die neueste Softwareversion von AXIS Camera Station Pro verwenden.

Wenn kein anderes Gerätemodell hinzugefügt werden kann:

- Rufen Sie die Fehlerbehebung für die Kamera unter *axis.com/support/troubleshooting* auf.

Die Gerätefirmware kann nicht über AXIS Camera Station Pro aktualisiert werden

Die Kamera kann nicht über die Weboberfläche aktualisiert werden:

- Rufen Sie die Fehlerbehebung für die Kamera unter *axis.com/support/troubleshooting* auf.

Die Firmware kann nicht auf allen Geräten aktualisiert werden.

- Stellen Sie sicher, dass eine Netzwerkverbindung besteht.
- Wenn es sich nicht um ein Netzwerk-Problem handelt, wenden Sie sich an den AXIS Support. Wechseln Sie zu *Eskalationsverfahren, on page 254*.

Die Firmware für bestimmte Modelle kann nicht aktualisiert werden:

- Es kann ein Kompatibilitätsproblem sein. Wenden Sie sich an den Axis Support. Wechseln Sie zu *Eskalationsverfahren, on page 254*.

Keine Geräte ermittelt

Das Video Management System durchsucht das Netzwerk automatisch nach angeschlossenen Kameras und Video-Encodern, kann jedoch keine Kameras finden.

- Stellen Sie sicher, dass die Kamera über eine Netzwerkverbindung verfügt und die Stromversorgung angeschlossen ist.
- Wenn sich Client, Server oder Kameras in verschiedenen Netzwerken befinden, konfigurieren Sie die Proxy- und Firewalleinstellungen.
  - Wenn ein Proxyserver Client und Server voneinander trennt, müssen die Proxyeinstellungen des Clients angepasst werden. Rufen Sie *Client proxy settings (Proxyeinstellungen Client)* im Benutzerhandbuch zu AXIS Camera Station Pro auf.
  - Ändern Sie das NAT- oder Sicherheitssystem, wenn der Client und der Server durch ein NAT- oder Sicherheitssystem getrennt sind. Stellen Sie sicher, dass die in der Dienststeuerung von AXIS Camera Station angegebenen HTTP-, TCP- (Transmission Control Protocol) und Streaming-Ports im Sicherheitssystem bzw. im NAT-System zugelassen sind. Weitere Informationen zur vollständigen Portliste finden Sie unter *Portliste für AXIS Camera Station Pro, on page 218*.
  - Wenn ein Proxyserver Server und Geräte voneinander trennt, müssen die Proxyeinstellungen des Servers angepasst werden. Rufen Sie den Abschnitt „Proxyeinstellungen" unter *Allgemeines zur Dienststeuerung* im Benutzerhandbuch zu AXIS Camera Station Pro.
- Informationen zum manuellen Hinzufügen von Kameras finden Sie unter *Add devices (Geräte hinzufügen)* im Benutzerhandbuch zu AXIS Camera Station Pro.

Wiederholte Meldung "Erneute Verbindung mit Kamera in 15 Sekunden"

Mögliche Probleme:

- Ein überlastetes Netzwerk.
- Kein Zugriff auf Kamera vorhanden. Stellen Sie sicher, dass die Kamera über eine Netzwerkverbindung verfügt und die Stromversorgung angeschlossen ist.
- Probleme mit der Grafikkarte bestehen.

Mögliche Lösungen bei Problemen mit der Grafikkarte:

- Installieren Sie den neuesten Grafikkartentreiber.
- Verwenden Sie eine Grafikkarte mit mehr Videospeicher und höherer Leistung.
- Nutzen Sie die CPU für Video-Rendering.
- Ändern Sie die Video- und Audioeinstellungen, beispielsweise, indem Sie die Profileinstellungen für geringe Bandbreite optimieren.

Aufzeichnungen

Siehe *Live-Ansicht, on page 243* für weitere Informationen zu möglichen Leistungsproblemen, die Aufzeichnungen und die Wiedergabe beeinträchtigen können.

Übliche Probleme

Kontinuierliche Aufzeichnung ist nicht aktiviert	
Für die aufgelisteten Kameras ist keine kontinuierliche Aufzeichnung aktiviert.	1. Um die kontinuierliche Aufzeichnung zu aktivieren, gehen Sie zu **Configuration > Recording and events > Recording method (Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode)**. 2. Wählen Sie die entsprechende Kamera und aktivieren Sie **Kontinuierlich**.

Aufzeichnen auf dem angegebenen Laufwerk nicht möglich	
Das System kann den Aufzeichnungsspeicher nicht konfigurieren.	1. Um einen anderen Speicher zu verwenden, **Configuration > Storage > management (Konfiguration > Speicher > Verwaltung)** aufrufen. 2. Fügen Sie den Speicher hinzu und konfigurieren Sie die Speichereinstellungen für die Kameras.

Installation der Anwendung AXIS Video Content Stream fehlgeschlagen	
Diese Fehlermeldung wird angezeigt, wenn die Anwendung nicht auf einer Kamera installiert werden kann, die AXIS Video Content Stream unterstützt.	1. Um die Anwendung manuell zu installieren, gehen Sie zu **Configuration > Devices > Management (Konfiguration > Geräte > Verwaltung)**. 2. Die Kamera wählen und anklicken.

Der Aufzeichnungsvorgang startet nicht

Wenn Aufzeichnungen nach einigen Sekunden nicht gestartet oder stoppt werden, deutet dies darauf hin, dass das Laufwerk voll ist oder zu viele Stördaten vorliegen.

- Überprüfen Sie in der Serverkonfigurationsdatei unter **Recording Storage (Aufzeichnungsspeicher)**, ob ausreichend freier Speicherplatz vorhanden ist und keine Stördaten vorliegen.
- Erhöhen Sie das Speicherlimit für das Video Management System.
- Weisen Sie dem Speicher-Pool mehr Speicher zu. Rufen Sie *Speicher konfigurieren* im Benutzerhandbuch zu AXIS Camera Station Pro auf.

Aufzeichnungslücken bei kontinuierlicher Aufzeichnung

Neben den Lücken werden auch **Recording errors (Aufzeichnungsfehler)** angezeigt. Diese Lücken können verschiedene Ursachen haben wie zum Beispiel:

- Serverüberlastung
- Netzwerk-Problem
- Kameraüberlastung
- Laufwerksüberlastung

Überprüfen Sie, ob die Aufzeichnungslücken bei allen Kameras auftreten. Tritt dies nicht bei allen Kameras auf, kann es sich um eine Überlastung der Kamera handeln. Stellen Sie sich folgende Fragen, um die Ursache zu ermitteln:

- Wie oft treten die Lücken auf? Jede Stunde oder täglich?
- Wie groß sind die Lücken? Handelt es sich nur um wenige Sekunden oder um Stunden?
- Wann treten die Lücken auf?

Mögliche Lösungen:

- Überprüfen Sie im Task-Manager des Servers, ob eine der Hardwareressourcen im System übermäßig stark ausgelastet ist. Wenn das Laufwerk Anzeichen einer Überlastung aufweist, fügen Sie für mehrere Kameras zusätzliche Laufwerke hinzu.
- Verringern Sie die auf das Laufwerk geschriebene Datenmenge (Videoeinstellungen, Zipstream, Bilder pro Sekunde, Auflösung). Beachten Sie stets den von AXIS Site Designer geschätzten Durchsatz. Siehe hierzu *axis.com/support/tools/axis-site-designer*.

Weitere Informationen finden Sie unter *Live-Ansicht und Wiedergabeleistung, on page 243*.

Exportierte Aufzeichnungen können nicht wiedergegeben werden

Überprüfen Sie das Dateiformat, falls Sie ihre exportierten Aufzeichnungen mit Windows Media Player nicht wiedergeben können. Um Ihre exportierten Aufnahmen abzuspielen, verwenden Sie Windows Media Player (.asf) oder AXIS File Player (.asf, .mp4, .mkv).

Weitere Informationen dazu finden Sie unter *Exportierte Aufzeichnungen wiedergeben* und überprüfen im Benutzerhandbuch zu AXIS Camera Station Pro.

Hinweis

AXIS File Player öffnet automatisch alle Aufzeichnungen, die sich im selben Ordner wie der Player befinden.

Aufzeichnungen verschwinden

Aufzeichnungen werden vom System nur für eine festgelegte Anzahl von Tagen aufbewahrt. Um die Anzahl der Tage zu ändern, **Konfiguration > Speicher > Auswahl** aufrufen.

Wenn der Speicher voll wird, werden Aufzeichnungen vor Ablauf der angegebenen Anzahl der Tage gelöscht. Versuchen Sie Folgendes, um einen vollen Speicher zu vermeiden:

- Fügen Sie mehr Speicherplatz hinzu. **Konfiguration > Speicher > Verwaltung** aufrufen.
- Ändern Sie den AXIS Camera Station Pro zugewiesenen Speicherplatz. **Konfiguration > Speicher > Verwaltung** aufrufen.
- Die Aufzeichnungsdateien verkleinern, zum Beispiel durch Anpassung der Auflösung oder der Bildrate. Gehen Sie zu **Konfiguration > Geräte > Videostreamprofile**.
  - Verwenden Sie das H.264-Videoformat für die Aufzeichnung, da das M-JPEG-Format viel mehr Speicherplatz erfordert.
  - Verwenden Sie Zipstream, um die Aufzeichnungsgröße zusätzlich zu verringern.

Probleme mit der ausfallsicheren Aufzeichnung

Nach Wiederherstellen der Verbindung erfolgt auf dem Server keine ausfallsichere Aufzeichnung.

Ursache	Lösung
Die Bandbreite für das Übertragen von Aufzeichnungen zwischen Kamera und Server reicht nicht aus.	Verbessern der Bandbreite
Während der Unterbrechung wurden von der Kamera keine Aufzeichnungen auf der SD-Karte gespeichert.	• Überprüfen Sie den Server-Bericht der Kamera. Siehe *axis.com/support/troubleshooting*. • Stellen Sie sicher, dass die SD-Karte einwandfrei funktioniert und Aufzeichnungen enthält.
Die Kamerazeit wurde durch das Trennen verändert.	• Stellen Sie sicher, dass das NTP für zukünftige Aufzeichnungen synchronisiert wird. • Synchronisieren Sie die Kamerazeit mit der Server-Zeit oder richten Sie auf der Kamera den gleichen NTP-Server ein wie auf dem Server.

Ausfallsichere Aufzeichnung in AXIS Camera Station Pro funktioniert in den folgenden Szenarien nicht:

- Kontrolliertes Herunterfahren der Server.
- Kurze Verbindungsunterbrechungen von weniger als 10 Sekunden.

Live-Ansicht

Live-Ansicht und Wiedergabeleistung

Dieser Abschnitt beschreibt mögliche Lösungen, wenn auf Ihrem AXIS Camera Station Pro Client Bildratenverluste oder grafische Probleme auftreten.

Client-Hardware	
Stellen Sie sicher, dass der Treiber der Grafikkarte oder der des Netzwerks-Adapters aktuell ist.	1. Öffnen Sie das DirectX Diagnostic Tool (auf dem Computer als Suchbegriff dxdiag eingeben). 2. Überprüfen Sie die Website des Herstellers auf aktuelle Treiber für das jeweilige Betriebssystem. 3. Überprüfen Sie, ob Client und Server auf demselben Computer ausgeführt werden. 4. Führen Sie nach Möglichkeit den Client auf einem eigens dafür eingerichteten Rechner aus.
Überprüfen Sie die Anzahl der Monitore.	Wenn Sie eine interne Grafikkarte verwenden, sollten Sie maximal zwei Monitore pro Karte verwenden. 1. Öffnen Sie das DirectX Diagnostic Tool (auf dem Computer als Suchbegriff dxdiag eingeben). 2. Stellen Sie sicher, dass die dedizierte Grafikkarte von AXIS Camera Station Pro unterstützt wird. Hinweis Der Client kann nicht auf einer virtuellen Maschine ausgeführt werden.

Verbundene Geräte	
Zu viele Clientverbindungen gleichzeitig	Stellen Sie anhand Ihres typischen Anwendungsfall sicher, dass das System die Anforderungen erfüllt, und befolgen Sie die Hardwarerichtlinien. Weitere Informationen finden Sie in den *Anforderungen an den Server AXIS Camera Station Pro Installations- und Migrationsleitfaden*.
Die Kamera ist mit einem anderen Video Management System verbunden als AXIS Camera Station Pro	Trennen Sie die Kamera vom anderen Client und verbinden Sie die Kamera als Standardeinstellung mit AXIS Camera Station Pro.
Eine Kamera verwendet viele verschiedene Videostreams (insbesondere mit hoher Auflösung)	Kann sich insbesondere bei Kameras der Baureihe M als problematisch erweisen. • Ändern Sie den Videostream auf dasselbe Streamingprofil oder auf eine niedrigere Auflösung. Siehe *Streamingprofile* im AXIS Camera Station Pro Benutzerhandbuch. • Ändern Sie den Videostream auf dasselbe Streamingprofil oder auf eine niedrigere Auflösung. Siehe *Streamingprofile* im AXIS Camera Station Pro Benutzerhandbuch.
Serverüberlastung	
Ungewöhnlich hohe Auslastung von CPU/RAM zur Zeit des Problems	Stellen Sie sicher, dass gleichzeitig keine andere Anwendung mit hohem Bedarf an CPU/RAM-Leistung ausgeführt wird.
Netzwerk-Problem	
Ungewöhnlich hoher Bandbreitenbedarf zur Zeit des Problems	Stellen Sie sicher, dass keine andere Anwendung mit hohem Bedarf an Bandbreite gleichzeitig ausgeführt wird.
Ausreichende Bandbreite / Entferntes oder lokales Netzwerk	• Überprüfen Sie die Netzwerk-Topologie. • Führen Sie eine Statusüberprüfung für alle zwischen Kameras, Server und Client verwendeten Netzwerk-Geräte durch, z. B. Switches, Router, Netzwerk-Adapter und Netzwerkkabel).

Kein Video in der Live-Ansicht

In der Live-Ansicht wird kein Video von einer bekannten Kamera angezeigt.

- Schalten Sie die Hardware-Dekodierung aus. Die Hardware-Dekodierung ist standardmäßig aktiviert. Weitere Informationen zur Hardware-Dekodierung finden Sie unter *Streaming* im Benutzerhandbuch zu AXIS Camera Station Pro.

Weitere mögliche Lösungen:

- Wenn Sie die Live-Ansicht nicht über die Weboberfläche anzeigen können oder die Weboberfläche nicht funktioniert, sollten Sie eine Fehlerbehebung für die Kamera durchführen. Gehen Sie zu *axis.com/support/troubleshooting*.
- Erstellen Sie einen Server-Bericht für die Kamera, indem Sie auf *axis.com/support/troubleshooting* gehen.
- Wenn eine Antiviren-Software installiert ist, kann sie Livestreams eventuell blockieren.
- AXIS Camera Station Pro Ordner und Prozesse zulassen, (siehe *Häufig gestellte Fragen (FAQ)*).

- Stellen Sie sicher, dass die Firewall Verbindungen über bestimmte Ports nicht blockiert. Siehe hierzu *Allgemeines zur Dienststeuerung* im Benutzerhandbuch zu AXIS Camera Station Pro.
- Stellen Sie sicher, dass für unterstützte Versionen des Betriebssystems Windows Server Desktop Experience installiert wurde. Siehe *geplantes Exportieren* im AXIS Camera Station Pro Benutzerhandbuch.
- Stellen Sie sicher, dass der Videostream bei geringerer Auflösung angezeigt werden kann.

Falls alle diese Maßnahmen erfolglos bleiben, melden Sie das Problem dem Axis Support über *Eskalationsverfahren, on page 254*.

Speicherung

Zugriff auf Netzwerk-Speicher nicht möglich

Wenn die Anmeldung bei der Dienststeuerung von AXIS Camera Station Pro über das lokale Systemkonto erfolgt, kann kein Netzwerk-Speicher mit freigegebenen Ordnern von anderen Computern hinzugefügt werden.

So ändern Sie das Anmeldekonto:

1. Öffnen Sie die **Windows-Systemsteuerung**.
2. Suchen Sie nach „Services (Dienste)".
3. Klicken Sie auf **View local services (Lokale Dienste anzeigen)**.
4. AXIS Camera Station Pro rechtsklicken und **Properties (Eigenschaften)** auswählen.
5. Rufen Sie die Registerkarte **Log on (Anmelden)** auf.
6. Ändern Sie die Einstellung von **Lokales Systemkonto** in **Dieses Konto**.
7. Wählen Sie einen Benutzer mit Zugriff auf Windows Active Directory aus.

Netzwerk-Freigabe nicht verfügbar

Stellen Sie sicher, dass Computer und Server, auf denen die Video Management Software ausgeführt wird, zur selben Domain gehören wie der Netzwerk-Speicher.

Wiederherstellen einer Verbindung zu einem Netzwerk-Speicher mit neuem Benutzernamen und neuem Kennwort nicht möglich

Wenn die Netzwerk-Freigabe Authentifizierung erfordert, erst alle aktuellen Verbindungen der Netzwerk-Freigabe beenden, danach Benutzername und Kennwort ändern.

Um den Benutzernamen und das Kennwort einer Netzwerk-Freigabe zu ändern und eine neue Verbindung aufzubauen:

1. Alle aktuellen Verbindungen der Netzwerk-Freigabe beenden.
2. Ändern Sie Benutzernamen und Kennwort.
3. Gehen Sie zu **Konfiguration > Speicher > Verwaltung** und stellen Sie die Verbindung zum Netzwerk-Speicher mit dem neuen Benutzernamen und dem neuen Kennwort wieder her.

Bewegungserkennung

Übliche Probleme

Installation der Anwendung AXIS Video Motion Detection fehlgeschlagen	
AXIS Video Motion Detection 2 oder 4 kann nicht installiert werden. Die Kamera verwendet für die Bewegungsaufzeichnung die integrierte Bewegungserkennung.	Informationen zur manuellen Installation der Anwendung finden Sie unter *Kameraanwendung installieren* im Benutzerhandbuch zu AXIS Camera Station Pro.

Abrufen der aktuellen Bewegungserkennung fehlgeschlagen	
Das Video Management System kann die Parameter der Bewegungserkennung nicht von der Kamera abrufen. Die Kamera verwendet für die Bewegungsaufzeichnung die integrierte Bewegungserkennung.	Informationen zur manuellen Installation der Anwendung finden Sie unter *Kameraanwendung installieren* im Benutzerhandbuch zu AXIS Camera Station Pro.

Bewegungserkennung nicht konfiguriert	
Die Bewegungserkennung kann in den aufgelisteten Kameras nicht konfiguriert werden.	1. Um die Bewegungserkennung manuell zu konfigurieren, **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode** aufrufen. 2. Wählen Sie die entsprechende Kamera und klicken Sie auf **Bewegungseinstellungen**, um die Bewegungserkennung zu konfigurieren.

Bewegungserkennung ist nicht aktiviert	
Für die aufgelisteten Kameras ist die Bewegungsaufzeichnung nicht aktiviert.	1. **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode** aufrufen. 2. Die Kamera auswählen und **Motion detection (Bewegungserkennung)** aktivieren, um die Aufzeichnung der Bewegungserkennung einzuschalten.

Die Bewegungserkennung erkennt zu viele oder zu wenige sich bewegende Objekte

In diesem Abschnitt werden mögliche Lösungen beschrieben, wenn Sie in Ihren Aufzeichnungen mit der videobasierten Bewegungserkennung mehr oder weniger Erfassungen erwartet haben.

Ändern der Bewegungseinstellungen

Mit den Bewegungseinstellungen kann der Bereich angepasst werden, in dem Objektbewegungen erkannt werden.

1. **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode** aufrufen.
2. Die Kamera wählen und **Bewegungserkennung** anklicken.
3. Wählen Sie die Einstellungen entsprechend der Firmware der Kamera.

AXIS Video Motion Detection 2 und 4	Sie können den ausgewählten Bereich konfigurieren. Siehe *Bearbeiten von AXIS Video Motion Detection 2 und 4* im Benutzerhandbuch zu AXIS Camera Station Pro.
Integrierte Bewegungserkennung	Sie können die Einschluss- und Ausschlussfenster konfigurieren. Siehe *Bearbeiten der integrierten Bewegungserkennung* im Benutzerhandbuch zu AXIS Camera Station Pro.

Anpassen der Triggerzeitspanne

Die Auslöserzeitspanne ist ein Intervall zwischen zwei aufeinanderfolgenden Auslösern. Diese Einstellung wird verwendet, um die Anzahl von aufeinanderfolgenden Aufzeichnungen zu verringern. Die Aufzeichnung wird

fortgesetzt, wenn innerhalb dieses Intervalls ein weiterer Trigger erfolgt. Wenn ein weiterer Trigger erfolgt, wird die Triggerzeitspanne an diesem Zeitpunkt zurückgesetzt.

So ändern Sie die Triggerzeitspanne:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode** aufrufen.
2. Die Kamera wählen.
3. Unter **Advanced (Erweitert)** können Sie mit der Option **Trigger period (Auslöseperiode)** die Auslöseperiode in Sekunden einstellen.

Aktionsregeln

Unerwartete Ereignisse durch E/A-Auslöser

Wenn etwa um 01.15 Uhr unerwartete I/O-Ereignisse gemeldet werden, ersetzen Sie Ihre vorhandenen I/O-Trigger durch Geräteereignis-Trigger.

Audio

Live-Ansicht ohne Audio

Wenn in der Live-Ansicht kein Audio vorhanden ist, gehen Sie wie folgt vor:

- Vergewissern Sie sich, ob die Kamera Audio unterstützt.
- Vergewissern Sie sich, dass im Computer eine Soundkarte vorhanden ist.
- Vergewissern Sie sich, dass das verwendete Profil für Audio konfiguriert wurde.
- Sicherstellen, dass der Benutzer Zugriffsrechte auf die Audiofunktionen hat.

Profile für Audio konfigurieren

1. Gehen Sie zu **Konfiguration > Geräte > Videostreamprofile**.
2. Die Kamera wählen.
3. Wählen Sie in den Videoprofileinstellungen unter **Format MPEG-4** oder **H.264**.
4. Wählen Sie unter **Audio** im Drop-Down Menü **Microphone (Mikrofon)** ein Mikrofon aus.
5. Wählen Sie im Drop-Down-Menü **Use microphone for (Mikrofon verwenden für)** aus, wann Audio verwendet werden soll.
6. Wählen Sie gegebenenfalls im Drop-Down-Menü **Speaker (Lautsprecher)** einen Lautsprecher aus.
7. Klicken Sie auf **OK**.

Zugriffsrechte der Benutzer überprüfen und ändern

Hinweis

Um folgende Schritte durchführen zu können, müssen Sie über Administratorrechte für AXIS Camera Station Pro verfügen.

1. Gehen Sie zu **Configuration > Security > User permissions (Konfiguration > Sicherheit > Benutzerrechte)**.
2. Wählen Sie einen Benutzer oder eine Benutzergruppe aus.
3. Wählen Sie für ein bestimmtes Gerät **Audio listen (Audio – Hören)** oder **Audio speak (Audio – Sprechen)** aus.
4. Klicken Sie auf **Anwenden**.

Kein Ton in Sequenzen

Audio kann in Videostreamprofilen ein- oder ausgeschaltet werden. Weitere Informationen finden Sie unter *Videostreamprofile* im Benutzerhandbuch zu AXIS Camera Station Pro.

Kein Ton bei der Wiedergabe

Die Wiedergabe mit Ton erfordert, dass Sie im für die Aufzeichnung verwendeten Profil Audio aktivieren.

Hinweis

Audio kann nicht zusammen mit M-JPEG-Video verwendet werden. Wählen Sie ein anderes Videoformat aus.

So verwenden Sie Audio in Aufzeichnungen:

1. Rufen Sie **Configuration > Devices > Stream profiles (Konfiguration > Geräte > Videostreamprofile)** auf, um das Videoformat für das Videoprofil einzustellen, das Sie verwenden möchten.
2. **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode** aufrufen.
3. Die Kamera wählen.
4. Wählen Sie aus dem Drop-Down Menü **Profile (Profil)** das konfigurierte Profil aus.
5. Klicken Sie auf **Anwenden**.

Von Regeln getriggerte Aufzeichnungen

So aktivieren Sie Audio in einer vorhandenen Regel:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Wählen Sie die Regel aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf **Next (Weiter)**, um **Actions (Aktionen)** aufzurufen.
4. Wählen Sie die Aktion **Record (Aufzeichnen)** aus und klicken Sie auf **Edit (Bearbeiten)**.
5. Wählen Sie ein Profil für Audio aus.
6. Klicken Sie zum Speichern auf **Fertigstellen**.

Anmeldung

Keine Anmeldung am Server oder Verbindung zum Server möglich

In diesem Bereich werden Anmelde- und Verbindungsprobleme beschrieben, die beim Verbindungsaufbau zu einem Einzelserver auftreten. Beim Anmelden an mehreren Servern wird der Client gestartet und der Verbindungsstatus wird in der Statusleiste angezeigt. Weitere Informationen zum Verbindungsstatus werden unter *Verbindungsstatus* im Benutzerhandbuch zu AXIS Camera Station Pro angezeigt.

Benutzername oder Kennwort sind nicht korrekt	Die Kombination aus Benutzername und Kennwort ist für die Anmeldung am angegebenen Server ungültig.	• Überprüfen Sie die Schreibweise oder verwenden Sie ein anderes Konto. • Stellen Sie sicher, dass der Benutzer Zugriffsrechte auf den AXIS Camera Station Pro-Server hat. • Die Uhren auf AXIS Camera Station Pro Server und Client müssen synchronisiert werden. Bei Domainbenutzern muss die Systemzeit des Domainservers mit der von Server und Client synchronisiert werden. • Ein Benutzer, der nicht dem Server hinzugefügt wurde, jedoch Mitglied der lokalen Administratorgruppe auf dem Server ist, muss den Client als Administrator ausführen. • Informationen zu Benutzerrechten finden Sie unter *Benutzerrechte konfigurieren* im Benutzerhandbuch zu AXIS Camera Station Pro.
Der Benutzer hat nicht die Berechtigung zur Anmeldung am Server	Der Benutzer kann AXIS Camera Station Pro auf dem angegebenen Server nicht verwenden.	Fügen Sie den Benutzer im Dialog Benutzerberechtigung hinzu.
Nachrichtensicherheit konnte nicht überprüft werden	Beim Aufbau der sicheren Verbindung zum Server ist ein Fehler aufgetreten. Wahrscheinlich sind die Uhrzeit auf Client oder Server nicht angemessen synchronisiert.	Die UTC-Systemzeiten von Server und Client müssen angemessen synchronisiert werden. Passen Sie die Uhrzeiten auf Client und Server so an, dass sie nicht mehr als 3 Stunden voneinander abweichen.
Keine Verbindung zum Server	Der Client kann keine Verbindung zum Server herstellen.	• Stellen Sie sicher, dass der Server-Computer eine Verbindung mit dem Netzwerk herstellen kann. • Stellen Sie sicher, dass der Server-Computer läuft. • Stellen Sie sicher, dass die Firewall richtig konfiguriert wurde. • Überprüfen Sie die Schreibweise der Server-Adresse. • Überprüfen Sie die Proxyeinstellungen des Clients.
Keine Antwort vom Server	Der Client kann Kontakt zum Server-Computer herstellen, aber es wird kein AXIS Camera Station Pro Server ausgeführt.	Stellen Sie sicher, dass eine Verbindung zum richtigen Computer hergestellt wird und dass der AXIS Camera Station Pro Server ausgeführt wird.
Client kann keine Verbindung zum Server aufbauen	Der Client kann keine Verbindung zum Server aufbauen und eine Fehlermeldung wird angezeigt.	Stellen Sie sicher, dass das Netzwerk richtig konfiguriert wurde: • Überprüfen Sie, ob das Betriebssystem unterstützt wird. Eine vollständige Liste der

		unterstützen Betriebssysteme finden Sie im *Freigabehinweis*. • Überprüfen Sie über die Dienststeuerung, ob AXIS Camera Station Pro Server ausgeführt wird, oder starten Sie den Server, falls erforderlich. • Sicherstellen, dass Client und Server mit dem selben Netzwerk verbunden sind. – Andernfalls den Client über die externe IP-Adresse des Servers verbinden. • Überprüfen Sie, ob ein Proxyserver zwischen Server und Client geschaltet ist. – Konfigurieren Sie den Proxyserver in der Dienststeuerung. – Konfigurieren Sie die Clientproxyeinstellung auf der Anmeldeseite. Wählen Sie **Change proxy settings (Einstellungen des Proxyservers ändern)** aus. – Konfigurieren Sie die Clientproxyeinstellungen in den Internetoptionen von Windows und wählen Sie unter **Change Proxy settings (Einstellungen des Proxyservers ändern)** die Standardeinstellung.
Verbindung zum Server kann nicht hergestellt werden	Beim Verbindungsaufbau zum Server ist ein unbekannter Fehler aufgetreten.	• Stellen Sie sicher, dass Adresse und Port des AXIS Camera Station Pro Servers korrekt sind. • Stellen Sie sicher, dass keine NAT-, Firewall- oder Antiviren-Software die Verbindung zum Server blockiert. Weitere Informationen finden Sie unter *Domains und Ports für Secure Remote Access v2*. • Verwenden Sie die AXIS Camera Station Pro Dienststeuerung, um sicherzustellen, dass der Server ausgeführt wird. – Öffnen Sie die AXIS Camera Station Pro Dienststeuerung, siehe *AXIS Camera Station Dienststeuerung* im AXIS Camera Station Pro Benutzerhandbuch. – Zeigen Sie den Serverstatus auf der Registerkarte **General (Allgemein)** an. Beim Status **Stopped (Angehalten)** klicken Sie auf **Start (Starten)**, um den Server zu starten.
Server kann nicht gefunden werden	Der Client kann die eingegebene Adresse nicht zu einer IP-Adresse auflösen.	• Stellen Sie sicher, dass der Server-Computer eine Verbindung mit dem Netzwerk herstellen kann.

		• Stellen Sie sicher, dass Adresse und Port des AXIS Camera Station Pro Servers korrekt sind. • Stellen Sie sicher, dass keine NAT-, Firewall- oder Antiviren-Software die Verbindung zum Server blockiert.
Server- und Clientversion sind unterschiedlich	Auf dem Client wird eine neuere AXIS Camera Station Pro Version ausgeführt als auf dem Server.	Aktualisieren Sie den Server auf die gleiche Version, die auf dem Client ausgeführt wird.
	Auf dem Server wird eine neuere AXIS Camera Station Pro Version ausgeführt als auf dem Client.	Aktualisieren Sie den Client auf die gleiche Version, die auf dem Server ausgeführt wird.
Verbindung zum Server kann nicht hergestellt werden Server ist zu stark ausgelastet.	Keine Serverantwort aufgrund von Leistungsproblemen.	Stellen Sie sicher, dass der Server-Computer und das Netzwerk nicht überlastet sind.
Der lokale AXIS Camera Station Pro Server wird nicht ausgeführt.	Sie verwenden **This computer (Diesen Computer)**, um eine Verbindung herzustellen, aber der installierte AXIS Camera Station Pro Server wird nicht ausgeführt.	Verwenden Sie die Dienststeuerung, um AXIS Camera Station Pro zu starten oder wählen Sie einen Remote-Server für die Anmeldung.
Auf diesem Computer ist kein AXIS Camera Station Pro Server installiert.	Sie verwenden **This computer (Dieser Computer)**, um eine Verbindung herzustellen, aber auf diesem Computer ist kein Server installiert.	AXIS Camera Station Pro Server installieren oder einen anderen Server wählen.
Ausgewählte Server-Liste ist leer	Die zur Anmeldung ausgewählte Serverliste war leer.	Um der Server-Liste Server hinzuzufügen, klicken Sie auf **Edit (Bearbeiten)** neben der Server-Listenauswahl.

Lizenzen

Probleme mit der Lizenzregistrierung

Falls die automatische Registrierung fehlschlägt, versuchen Sie Folgendes:

- Stellen Sie sicher, dass das System bei einer Organisation registriert ist.
- Rufen Sie **Configuration (Konfiguration)** auf, um sicherzustellen, dass **Automatic licensing (Automatische Lizenzierung)** aktiviert ist. Weitere Informationen finden Sie unter „*Lizenzen verwalten*" im AXIS Camera Station Pro Benutzerhandbuch.
- Stellen Sie sicher, dass die Server-Zeit aktuell ist.

Weitere Informationen finden Sie unter *Installations- und Migrationsanleitung zu AXIS Camera Station Pro*.

Benutzer

Domainbenutzer können nicht gefunden werden

Wenn die Suche nach dem Domänenbenutzer fehlschlägt, ändern Sie das Dienstanmeldekonto:

1. Öffnen Sie die **Windows-Systemsteuerung**.

2. Suchen Sie nach „Services (Dienste)".
3. Klicken Sie auf **View local services (Lokale Dienste anzeigen)**.
4. AXIS Camera Station Pro rechtsklicken und **Properties (Eigenschaften)** auswählen.
5. Die Registerkarte **Anmelden** anklicken.
6. Ändern Sie die Einstellung von **Lokales Systemkonto** in **Dieses Konto**.
7. Wählen Sie einen Benutzer mit Zugriff auf Windows Active Directory aus.

Zertifikatfehler

AXIS Camera Station Pro kann erst mit dem Gerät kommunizieren, nachdem der Zertifikatfehler behoben wurde.

Mögliche Fehler		
Zertifikat nicht gefunden	Das Zertifikat wurde vom Gerät entfernt.	Wenn Sie den Grund kennen, klicken Sie auf **Repair (Reparieren)**. Sollten Sie einen unberechtigten Zugriff vermuten, untersuchen Sie die Situation, bevor Sie das Zertifikat wiederherstellen. Klicken Sie auf **Advanced (Erweitert)**, um die Zertifikatdetails anzuzeigen. Mögliche Gründe für das Entfernen des Zertifikats: • Das Gerät wurde auf werksseitige Standardeinstellung zurückgesetzt. • Die sichere HTTPS-Kommunikation wurde deaktiviert. • Eine unbefugte Person hat auf das Gerät zugegriffen und es modifiziert.
Nicht vertrautes Zertifikat	Das Gerätezertifikat wurde außerhalb von AXIS Camera Station Pro geändert. Dies kann darauf hinweisen, dass eine unbefugte Person auf das Gerät zugegriffen und es modifiziert hat.	Wenn Sie den Grund kennen, klicken Sie auf **Trust This Device (Diesem Gerät vertrauen)**. Sollte dies nicht der Fall sein, untersuchen Sie die Situation, bevor Sie dem Zertifikat vertrauen. Klicken Sie auf **Advanced (Erweitert)**, um die Zertifikatdetails anzuzeigen.

Fehlendes Kennwort für Zertifizierungsstelle

Wenn Sie eine Zertifizierungsstelle in AXIS Camera Station Pro ohne ein gespeichertes Kennwort haben, wird der folgende Alarm angezeigt.

You need to provide a passphrase for the Certificate Authority certificate. (Sie müssen ein Kennwort für das CA-Zertifikat angeben.) Weitere Informationen hierzu finden Sie im Benutzerhandbuch.

Dieses Problem kann auf drei verschiedene Arten behoben werden:

- HTTPS auf einem Gerät aktivieren
- Ein vorhandene Zertifizierungsstelle importieren
- Neue Zertifizierungsstelle erstellen

HTTPS auf einem Gerät aktivieren:

1. **Konfiguration > Geräte > Verwaltung** aufrufen.
2. Klicken Sie in der Liste mit der rechten Maustaste auf ein Gerät und wählen Sie **Security > HTTPS > Enable/Update (Sicherheit > HTTPS > Aktivieren/Aktualisieren)** aus.
3. Klicken Sie zur Bestätigung auf **Ja**.
4. Geben Sie das Kennwort der Zertifizierungsstelle ein.
5. Klicken Sie auf **OK**.

So importieren Sie eine vorhandene Zertifizierungsstelle:

1. Wechseln Sie zu **Configuration (Konfiguration) > Security (Sicherheit) > Certificates (Zertifikate) > Devices (Geräte)**.
2. Schalten Sie unter HTTPS die Option **Validate device certificate (Gerätezertifikat validieren)** aus.
3. Klicken Sie unter **Certificate authority (Zertifizierungsstelle)** auf **Import (Importieren)**.
4. Geben Sie Ihr Kennwort ein, und klicken Sie auf **OK**.
5. Wählen Sie die Anzahl der gültigen Tage der signierten Client/Server-Zertifikate.
6. **Konfiguration > Geräte > Verwaltung** aufrufen.
7. Rechtsklicken Sie die Geräte und wählen Sie **Sicherheit > HTTPS > Aktivieren/Aktualisieren**.
8. Rufen Sie **Configuration (Konfiguration) > Security (Sicherheit) > Certificates (Zertifikate) > Devices (Geräte)** auf und schalten Sie **Validate device certificate (Gerätezertifikat validieren)** ein.

Hinweis

AXIS Camera Station Pro Die Geräteverbindung mit wird unterbrochen und einige Systemkomponenten werden neu gestartet.

So lassen Sie AXIS Camera Station Pro eine neue Zertifizierungsstelle generieren:

1. Wechseln Sie zu **Configuration (Konfiguration) > Security (Sicherheit) > Certificates (Zertifikate) > Devices (Geräte)**.
2. Schalten Sie unter HTTPS die Option **Validate device certificate (Gerätezertifikat validieren)** aus.
3. Klicken Sie unter **Certificate authority (Zertifizierungsstelle)** auf **Generate (Generieren)**.
4. Geben Sie Ihr Kennwort ein, und klicken Sie auf **OK**.
5. Wählen Sie die Anzahl der gültigen Tage der signierten Client/Server-Zertifikate.
6. **Konfiguration > Geräte > Verwaltung** aufrufen.
7. Rechtsklicken Sie die Geräte und wählen Sie **Sicherheit > HTTPS > Aktivieren/Aktualisieren**.
8. Rufen Sie **Configuration (Konfiguration) > Security (Sicherheit) > Certificates (Zertifikate) > Devices (Geräte)** auf und schalten Sie **Validate device certificate (Gerätezertifikat validieren)** ein.

Hinweis

AXIS Camera Station Pro Die Geräteverbindung mit wird unterbrochen und einige Systemkomponenten werden neu gestartet.

Zeitsynchronisierung

Windows Time-Dienst wird nicht ausgeführt

Der Dienst Windows Time und der NTP-Server sind nicht synchronisiert. Dies kann daran liegt, dass der Windows Time-Dienst den NTP-Server nicht erreichen kann.

- Stellen Sie sicher, dass der NTP-Server online ist.
- Stellen Sie sicher, dass die Firewalleinstellungen korrekt sind.
- Stellen Sie sicher, dass das Gerät sich in einem Netzwerk befindet, das den NTP-Server erreichen kann.

Wenden Sie sich an Ihren Systemadministrator, wenn Sie Hilfe benötigen.

Erfasste Zeitdifferenz auf einem Gerät

Das Gerät ist nicht mit der Server-Zeit synchronisiert. Die Aufzeichnung wird mit einem Zeitstempel versehen. Der Zeitpunkt, zu dem der Server die Aufzeichnung erhalten hat, ist nicht der Zeitpunkt, zu dem das Gerät sie aufgezeichnet hat.

1. Wechseln Sie zu **Configuration > Devices > Time synchronization (Konfiguration > Geräte > Zeitsynchronisierung)** und überprüfen Sie den Serverzeitversatz.
2. Wenn der Serverzeitversatz mehr als 2 Sekunden beträgt:
   2.1. **Enable time synchronization (Zeitsynchronisierung aktivieren)** wählen.
   2.2. Stellen Sie sicher, dass das Gerät den angegebenen NTP-Server erreichen kann.
   2.3. Laden Sie das Gerät unter **Konfiguration > Geräte > Management** neu.
3. Wenn der Serverzeitversatz kleiner als 2 Sekunden ist, sendet das Gerät möglicherweise nicht genügend Daten für eine Zeitsynchronisierung.
   3.1. **Alarm senden löschen, wenn die Zeitunterschied zwischen Server und Gerät größer als 2 Sekunden** ist, um Alarme zu deaktivieren.

Wenden Sie sich an den AXIS Support.

Technischer Support

Der technische Support steht Benutzern mit einer lizenzierten Version von AXIS Camera Station Pro zur Verfügung. Den technischen Support erreichen Sie über **> Help > Online Support (Hilfe > Onlinehilfe)** oder *axis.com/support*

Es wird empfohlen, dass Sie den Systembericht und die Screenshots Ihrer Supportanfrage anhängen.

Rufen Sie zum Erstellen eines Server-Berichts **> Help > System report (Hilfe > Systembericht)** auf.

Eskalationsverfahren

Wenden Sie sich bei Problemen, die mit dieser Anleitung nicht behoben werden können, an den *Axis Online Helpdesk*. Damit unser Support-Team Ihr Problem nachvollziehen und lösen kann, werden folgende Angaben benötigt:

- Eine klare Beschreibung, unter welchen Umständen das Problem auftritt und wie es reproduziert werden kann.
- Uhrzeit sowie Name oder IP-Adresse der Kamera, bei der das Problem auftritt.
- AXIS Camera Station Pro Systembericht, der direkt nach dem Auftreten des Problems erstellt wurde. Der Systembericht muss durch den Client oder Server erstellt worden sein, auf dem das Problem aufgetreten ist.
- Optionale Screenshots oder Aufzeichnungen von allen Monitoren, die das Problem anzeigen. Aktivieren Sie bei der Anfertigung der Screenshots oder der Aufzeichnung die Debug-Overlay-Funktion.
- Fügen Sie bei Bedarf die Datenbankdateien bei. Verzichten Sie auf diese Dateien, um das Hochladen zu beschleunigen.

Bei einigen Problemen sind zusätzliche Informationen erforderlich, die das Support-Team bei Bedarf anfordert.

Hinweis

Übermitteln Sie Dateien ab einer Größe von 100 MB, z. B. Dateien zum Netzwerk-Trace oder zur Datenbank, über einen sicheren, vertrauenswürdigen File-Sharing-Dienst.

Weitere Informationen	
Debug-Level-Protokollierung	Um weitere Informationen zu erhalten, ist gelegentlich eine Untersuchung auf Fehlerprotokollebene erforderlich. Dies geschieht nur auf Anweisung eines Axis Support-Mitarbeiters. Eine entsprechende Anleitung finden Sie im *Axis Online-Helpdesk*.
Debug-Overlay der Live-Ansicht	Manchmal ist es von Vorteil, Screenshots der Overlay-Informationen oder ein Video mit den geänderten Werte innerhalb der Zeitspanne, die von Interesse ist, bereitzustellen. So fügen Sie Overlay-Informationen hinzu: • Drücken Sie Ctrl + i einmal, um sich Overlay-Informationen in der Live-Ansicht anzeigen zu lassen. • Drücken Sie Ctrl + i zweimal, um Debug-Informationen hinzuzufügen. • Drücken Sie Strg + i dreimal, um das Overlay auszublenden.
Netzwerk-Trace	Falls auf Anweisung des Supporttechnikers erforderlich, erzeugen Sie beim Erstellen des Systemberichts Netzwerk-Traces. Falls das Problem reproduzierbar ist, erzeugen Sie die Netzwerk-Traces während dem Auftreten des Problems. Dazu zählen: • Ein Netzwerk-Trace von 60 Sekunden auf der Kamera (nur anwendbar auf Kameras mit Firmware ab Version 5.20). Verwenden Sie den folgenden VAPIX-Befehl, um bei Bedarf die Anmeldung, die IP-Adresse und die Dauer (in Sekunden) zu ändern: `http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=60` • Ein Netzwerk-Trace von 10 bis 30 Sekunden auf dem Server, das die Kommunikation zwischen Server und Kamera dokumentiert.
Datenbankdateien	Für Fälle, die von uns eine Untersuchung oder manuelle Reparatur der Datenbank erfordern. Wählen Sie **Include database in the report (Dem Bericht die Datenbankdatei hinzufügen)** aus, bevor Sie den Systembericht erstellen.

Weitere Informationen	
Schnappschüsse	Verwenden Sie Screenshots, wenn es sich um ein Problem mit der Live-Ansicht handelt, das mit der Benutzeroberfläche zu tun hat. Dies ist beispielsweise hilfreich, wenn es sich um die Anzeige einer Zeitleiste für Aufzeichnungen handelt oder wenn sich etwas schwer beschreiben lässt.
Bildschirmaufzeichnungen	Verwenden Sie Bildschirmaufzeichnungen, wenn sich das Problem nur schwer mit Worten beschreiben lässt. Ein Beispiel hierfür ist, wenn zum Reproduzieren des Problems viele Interaktionen mit der Benutzeroberfläche erforderlich sind.

T10196821_de

2026-04 (M29.5)

© 2023 – 2026 Axis Communications AB