

AXIS Camera Station Pro

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 Tracks „Active“, „Long-Term Support“ (LTS) und „Product Specific Support“ (PSS)* kompatibel. Weitere Informationen finden Sie in den Versionshinweisen zu AXIS Camera Station Pro oder im *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 von 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-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

Gehen Sie zur *Download-Seite von AXIS Camera Station Pro*, um das Programm herunterzuladen, zu aktualisieren oder 90 Tage lang kostenfrei zu testen.

- **Kostenfreie 90-Tage-Testversion mit vollem Funktionsumfang:** Testen Sie AXIS Camera Station Pro 90 Tage lang kostenfrei. Keine Lizenz erforderlich.
- **Unabhängige Offline-Aktualisierung Ihres Clients:** Aktualisiert den Client, also den Teil von AXIS Camera Station Pro, mit dem Sie direkt interagieren. Verwenden Sie diese Option, wenn Sie nur den Client und nicht den Server aktualisieren müssen.
- **Offline-Aktualisierung Ihres Clients und Servers:** Ein komprimiertes Aktualisierungspaket für Client und Server. Entpacken Sie die ZIP-Datei nach dem Herunterladen, um Zugriff auf die MSI- und CAB-Dateien zu erhalten, und führen Sie anschließend die MSI-Datei aus, um die Aktualisierung zu starten.
- **Online-Aktualisierung Ihres Clients und Servers:** Die Aktualisierung wird automatisch heruntergeladen, entpackt und installiert. Führen Sie die .exe-Datei aus und folgen Sie den Anweisungen auf dem Bildschirm. Stellen Sie sicher, dass Ihr Computer während der gesamten Installation mit dem Internet verbunden bleibt.
- **Mobile App für iOS:** Die Mobile App von AXIS Camera Station Pro für iPhones und iPads. Im App Store erhältlich.
- **Mobile App für Android:** Die Mobile App von AXIS Camera Station Pro für Android-Smartphones und -Tablets. Erhältlich bei Google Play.

Lernvideos

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

Systemmerkmale

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

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

- *Mit einem Server verbinden, on page 9*
- *Geräte konfigurieren, on page 48*
- *Speicher konfigurieren, on page 76*
- *Aufzeichnung und Ereignisse konfigurieren, on page 82*
- *Verbundene Dienste konfigurieren, on page 126*
- *Server konfigurieren, on page 129*
- *Die Sicherheit konfigurieren, on page 140*

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

- *Mit einem Server verbinden, on page 9*
- *Client konfigurieren, on page 121*
- *Live-Ansicht, on page 13*
- *Aufzeichnungswiedergabe, on page 27*
- *Aufzeichnungen exportieren, on page 30*

Schnellstart

Diese Anleitung hilft Ihnen bei der schnellen Inbetriebnahme Ihres Systems.

Vorbereitungen:

- Konfigurieren Sie das Netzwerk für Ihre Installation. Siehe *Netzwerkkonfiguration*.
- Konfigurieren Sie bei Bedarf die Server-Ports. Siehe *Server-Port-Konfiguration*.
- Stellen Sie sicher, dass Ihr System geschützt ist. 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 licenses (Lizenzen verwalten)** aufzurufen, auf der Sie den Server für ein Unternehmen registrieren können. Siehe *Verbundene Dienste verwalten, on page 126* und *Lizenzen verwalten, on page 138* 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

Wenn Sie AXIS Camera Station Pro zum ersten Mal aufrufen, wird die Seite **Add devices (Geräte hinzufügen)** geöffnet, auf der das Netzwerk nach Geräten durchsucht wird, die hinzugefügt werden sollen. 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. Klicken Sie auf **Close (Schließen)**, um die Konfiguration zu überspringen und später fortzufahren. So fahren Sie jetzt mit der Konfiguration fort:
 - 3.1. Wählen Sie **Quick configuration (Schnellkonfiguration)** oder **Site Designer configuration (Site Designer Konfiguration)**. Weitere Informationen, siehe *AXIS Site Designer-Projekte importieren, on page 52*.
 - 3.2. Wählen Sie **Add image overlay for date, time, and text (Overlay für Datum, Uhrzeit und Text hinzufügen)**, um Overlays zu allen Axis Kameras hinzuzufügen, die noch keine haben.
 - 3.3. Klicken Sie auf **Next (Weiter)**.

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

Konfigurieren des Aufzeichnungsverfahrens

1. Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode aufrufen.
2. Eine Kamera wählen
3. Aktivieren Sie **Motion detection (Bewegungserkennung)** oder **Continuous (Kontinuierlich)** oder beides.
4. Klicken Sie auf **Anwenden**.

Live-Video ansehen

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

Weitere Informationen, siehe *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, siehe *Aufzeichnungen, on page 27*.

Aufzeichnungen exportieren

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

Weitere Informationen, siehe *Aufzeichnungen exportieren, on page 30*.

Aufzeichnungen mit AXIS File Player wiedergeben und überprüfen

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

Hinweis

- Eine digitale Signatur unterscheidet sich von signiertem Video. Anhand eines signierten Videos können Sie eine Aufzeichnung bis zu der Kamera zurückverfolgen, von der sie stammt, und so sicherstellen, dass

sie nicht manipuliert wurde. Weitere Informationen dazu finden Sie unter *Signierte Videos* und in der Bedienungsanleitung der Kamera.

- Wenn gespeicherte Dateien keine Verbindung zu einer Datenbank der AXIS Camera Station haben (nicht indizierte Dateien), müssen Sie sie konvertieren, damit sie im AXIS File Player wiedergegeben werden können. Wenden Sie sich an den technischen Support von Axis, wenn Sie Hilfe bei der Konvertierung Ihrer Dateien benötigen.

Netzwerkkonfiguration

Konfigurieren Sie die Proxy- oder Firewall-Einstellungen, bevor Sie AXIS Camera Station Pro verwenden, falls sich Client, Server und die angeschlossenen Netzwerkgeräte in unterschiedlichen Netzwerken befinden.

Client-Proxyeinstellungen

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

Proxyeinstellungen des Servers

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

NAT und Firewall

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

Weitere Informationen, siehe *Portliste für AXIS Camera Station Pro*, on page 219.

Server-Port-Konfiguration

Der AXIS Camera Station Pro-Server nutzt die Ports 29202 (TCP) und 29204 (HTTPS) für die Kommunikation zwischen Server und 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 Pro ohne Axis Secure Remote Access v2 oder andere Axis Cloud-Dienste nutzen möchten.

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

Hinweise zur Systemsicherheit

Um unbefugten Zugriff zu Kameras und Aufzeichnungen zu verhindern:

- Verwenden Sie für alle Netzwerk-Geräte (Kameras, Video-Encoder und Zusatzgeräte) starke Kennwörter.
- Installiert AXIS Camera Station 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.

Mit einem Server verbinden

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

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

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

Remote-Server – Siehe *Mit einem Remote-Server verbinden, on page 9*.

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

Hinweis

- Bei der ersten Verbindung mit einem Server überprüft der Client die Zertifikats-ID des Servers. Um sicherzustellen, dass Sie eine Verbindung zum richtigen Server herstellen, vergleichen Sie die Zertifikats-ID mit der in der Dienststeuerung von AXIS Camera Station Pro angezeigten ID. Weitere Informationen, siehe *Allgemeine Servereinstellungen, on page 219*.
- Client und Server müssen dieselbe Version nutzen. Wenn bei der Verbindung zu einem lokalen System oder einem System mit Portzuordnung eine Versionsabweichung festgestellt wird, kann der Client die korrekte, mit dem Server übereinstimmende Version herunterladen und anschließend zu dieser wechseln.
- Damit sich ein Client mit mehreren Servern verbinden kann, muss jeder Server über dieselbe Version verfügen. Standardmäßig verwendet die Client-Verknüpfung die neueste Version.

Server-Liste	Um eine Verbindung mit einem Server aus einer Serverliste herzustellen, wählen Sie einen aus dem Auswahllisten Server list (Serverliste) aus. Klicken Sie  , um Server-Listen zu bearbeiten. Siehe <i>Serverlisten</i> .
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 <i>Serverlisten</i> .
Gespeicherte Kennwörter löschen	Um die gespeicherten Benutzernamen und Kennwörter für alle 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 Auswahllisten **Remote-Server** oder geben Sie die IP-Adresse oder DNS-Adresse in das Feld ein. Falls der Server nicht angeführt wird, klicken Sie auf , um die Liste aller verfügbaren Remote-Server zu aktualisieren. Wenn der Server so konfiguriert ist, dass er Clients auf einem anderen Port als dem Standardport 29202 zulässt, geben Sie die IP-Adresse gefolgt von der Portnummer ein, z. B.: 192.168.0.5:46001.
3. Einen der folgenden Schritte durchführen:
 - Wählen Sie **Log in as current user** (Als aktueller Benutzer anmelden), um sich als der aktuelle Windows®-Benutzer anzumelden.
 - Leeren Sie das Feld **Als aktueller Benutzer anmelden** und klicken Sie auf **Anmelden**. Wählen Sie **Other user (Anderer Benutzer)** und geben Sie einen anderen Benutzernamen und Kennwort ein, um sich mit anderen Zugangsdaten anzumelden.

Bei AXIS Secure Remote Access 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 Tag jedes Monats um Mitternacht zurückgesetzt.

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. Besuchen Sie axis.com/products/axis-camera-station/overview und laden Sie die AXIS Camera Station Mobile App herunter.
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 Mobile App von 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-Client

Registerkarten

 Live-Ansicht	Live-Video von verbundenen Kameras anzeigen. Siehe <i>Live-Ansicht</i> .
 Aufzeichnungen	Aufzeichnungen suchen, wiedergeben und exportieren. Siehe <i>Aufzeichnungen</i> .
 Intelligente Suche 1	Ereignisse in Videoaufzeichnungen schnell finden. Siehe <i>Intelligente Suche 1</i> .
 Datensuche	Nach Daten von einer externen Quelle oder einem externen System aus suchen und das genaue Geschehen bei einem Ereignis nachverfolgen. Siehe <i>Datensuche</i> , on page 45.
 Konfiguration	Verbundene Geräte verwalten und Client- bzw. Server-Einstellungen konfigurieren. Siehe <i>Konfiguration</i> .
 Hotkeys	Tastenkombinationen anzeigen und konfigurieren. Siehe <i>Hotkeys</i> .
 Protokolle	Protokolle zu Alarmen, Ereignissen und Audits. Siehe <i>Protokolle</i> .
 Zugriffsverwaltung	Karteninhaber, Gruppen, Zutrittspunkte, Zonen und Zugangsregeln des Systems konfigurieren und verwalten. Siehe <i>Zugriffsverwaltung</i> , on page 188.
 Intelligente Suche 2	Mithilfe von erweiterten Filtern Fahrzeuge und Personen anhand von Merkmalen finden. Siehe <i>Intelligente Suche 2</i> , on page 39.
 Systemzustand überwachen	Überwachen Sie die Zustandsdaten über ein einzelnes oder über mehrere AXIS Camera Station Pro-Systeme. Siehe <i>Überwachung des Systemzustands</i> ^{BETA} , on page 200.
 Warnmeldungen zur Live-Ansicht	Automatisches Wechseln zum Tab "Live-Ansicht" der Kamera oder Ansicht, wenn die Aktion "Live-Ansicht" ausgelöst wird. Siehe <i>Live-Ansichtsaktion erstellen</i> .
 Warnmeldungen aufzeichnen	Wählen Sie einen Alarm in dem Tab "Alarmer" oder "Protokolle" und klicken Sie auf  Zu Aufzeichnungen wechseln , um den Tab "Aufzeichnungsalarme" zu öffnen. Siehe <i>Alarmer</i> und <i>Protokolle</i> .

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 <i>Server konfigurieren</i> .

Aktionen	Aufzeichnung manuell starten oder anhalten und den Status der I/O-Ports ändern. Siehe <i>Manuell aufzeichnen</i> und <i>E/A-Ports überwachen</i> .
Hilfe	Hilfe- und Supportoptionen anzeigen. Wechseln Sie zu Help (Hilfe) > About (Über) , um zu sehen, welche Version von AXIS Camera Station Pro Client Sie verwenden.
Abmelden	Bei Server abmelden und Verbindung trennen.
Exit	Beenden und schließen Sie den AXIS Camera Station Pro Client.

Titelleiste

 oder F1	Hilfe öffnen.
	In den Vollbildmodus wechseln.
 oder ESC	Den Vollbildmodus beenden.

Statusleiste

- Das Warnsymbol weist auf eine Zeitabweichung zwischen Client und Server hin. Achten Sie unbedingt darauf, dass die Zeit synchronisiert wurde, um Probleme mit der Zeitleiste zu vermeiden.
- Die Server-Verbindungsstatus zeigt die Anzahl der verbundenen Server. Siehe *Verbindungsstatus*.
- Der Lizenzstatus zeigt die Anzahl von unlicenzierten Geräten. Siehe *Lizenzen verwalten*.
- Die Nutzungsübersicht für Secure Remote Access v2 zeigt an, wie viel Datenvolumen Sie diesen Monat verbraucht haben.
- **Update für AXIS Camera Station Pro verfügbar** bedeutet, dass eine neue Version verfügbar ist. Diese Anzeige ist nur sichtbar, wenn Sie als Administrator angemeldet sind. Siehe *AXIS Camera Station Pro aktualisieren, on page 132*.

Alarmer und Aufgaben

- Auf den Registerkarten „Alarmer und Aufgaben“ werden ausgelöste Ereignisse und Alarmer des Systems angezeigt. Siehe *Alarmer und Aufgaben*.

Live-Ansicht

Die Live-Ansicht gibt das Videobild verbundener Kameras in Echtzeit wieder. Bei der Verbindung mit mehreren AXIS Camera Station Pro-Servern werden alle Ansichten und Kameras nach 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 Audibereiche mit Durchsageschnittstellen in der Live-Ansicht einrichten und hinzufügen. Weitere Informationen finden Sie unter *Verwendung von Durchsageschnittstellen in geteilten Ansichten, on page 21*

Alle Benutzer können auf „Ansichten“ zugreifen. Weitere Informationen zu Benutzerzugriffsrechten siehe *Benutzerberechtigungen, on page 140*.

Informationen zur Konfiguration der Live-Ansicht finden Sie unter *Clienteneinstellungen*.

Mehrere Monitore

So öffnen Sie eine Ansicht auf einem anderen Bildschirm:

1. Öffnen Sie eine Registerkarte **Live view (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 view (Live-Ansicht)**.
2. Wählen Sie eine oder mehrere Kameras, Ansichten oder Sequenzen.
3. Klicken Sie mit der rechten Maustaste auf Ihre Auswahl und wählen Sie **Show on AXIS T8705 (Auf AXIS T8705 anzeigen)** oder **Show on AXIS D1110 (Auf AXIS D1110 anzeigen)**, abhängig davon, welchen Video-Decoder 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. Zur Bearbeitung der Kameraeinstellungen siehe <i>Kameraeinstellungen bearbeiten</i>
	Eine Ansicht entfernen. Sie müssen die Berechtigung haben, die Ansicht und alle sekundären Ansichten zu bearbeiten, um sie zu entfernen. Zum Entfernen von Kameras aus AXIS Camera Station Pro siehe <i>Kameras, on page 55</i> .
	Als Administrator können Sie die Ansicht sperren, um zu verhindern, dass Bediener sie 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 Ordner, der unter Configuration (Konfiguration) > Client > Settings (Einstellungen) angegeben ist. Hinweis AXIS Camera Station Pro verwendet normalerweise den Videostream, wenn Sie Momentaufnahmen machen, sodass Sie eine Momentaufnahme mit der Auflösung des Videostreams erhalten. 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. Das kann zu Bildern mit geringerer Auflösung führen, insbesondere in Ansichten mit mehreren Kameras, bei denen jedes Bild auf dem Bildschirm kleiner erscheint.
Momentaufnahme der Exportliste hinzufügen	Um 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 verfügbar, für die über die Weboberfläche der Kamera digitales PTZ eingerichtet wurde. 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 Musrad ein- und auszoomen. Alternativ können Sie zum Heranzoomen Strg + (+) und zum Herauszoomen Strg + (-) drücken.
In dem Bereichs zoomen	Um einen Bereich heranzuzoomen, ziehen Sie ein Rechteck um den zu vergrößern Bereich. Verwenden Sie zum Auszoomen das Musrad. 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 im Bild auf die Stelle, auf die Sie die Kamera ausrichten möchten. Um 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 Pfeilrichtung zu schwenken. Um 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. Das Dialogfeld wird 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 (Fortlaufend): Verschieben Sie den Fokus mit Nearer (Näher) oder Further (Weiter) und klicken Sie auf Stop (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 Focus recall zone (Fokusabrufzone) .
Objektverfolgung ein/aus	Um die Objektverfolgung für eine Axis PTZ-Kamera mit AXIS PTZ Autotracking ein- oder auszuschalten, klicken Sie mit der rechten Maustaste auf das Bild und wählen Sie Autotracking on/off (Objektverfolgung 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 <i>PTZ-Voreinstellungen</i> .
Voreinstellung hinzufügen	Um eine Voreinstellung hinzuzufügen, ziehen Sie die Bildansicht an die gewünschte Position, klicken Sie mit der rechten Maustaste und wählen Sie Presets (Voreinstellungen) > Add preset (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 auf wiederholbare, 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: 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).
Videostreamprofil	Um das Videostreamprofil festzulegen, klicken Sie mit der rechten Maustaste auf ein Bild und wählen Sie Videostreamprofil. Siehe <i>Videostreamprofile</i>.



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

Digitale Voreinstellungen hinzufügen



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

PTZ-Steuerung

Hinweis

Als Administrator können Sie mechanisches PTZ für Benutzer deaktivieren. Siehe *Benutzerberechtigungen*.

Aufzeichnung und unmittelbares Antworten in der Live-Ansicht

	Um die Registerkarte „Recordings“ (Aufzeichnungen) zu öffnen, 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 Mauszeiger 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.

Informationen zur Konfiguration von Einstellungen für die manuelle Aufzeichnungen wie Auflösung, Komprimierung und Bildrate finden Sie unter *Aufzeichnungsmethode*. Für weitere Informationen über Aufzeichnungen und Wiedergabe siehe *Aufzeichnungswiedergabe*.

Hinweis

Als Administrator können Sie die Funktion zur manuellen Aufzeichnung 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 *Videostreamprofile*, on page 56.

 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 <i>Streaming</i> , on page 124.

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 einer 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 Audibereich anderer Server zu Ihrer geteilten Ansicht hinzufügen.

Geteilte Ansicht hinzufügen:

1. Klicken Sie auf der Registerkarte **Live view (Live-Ansicht)** auf .
2. **Neue Geteilte Ansicht** wählen.
3. Geben Sie einen Namen für die Fensteraufteilung ein.
4. Wählen Sie im Auswahlménú unter **Template (Vorlage)** eine Anordnung aus.
5. Ziehen Sie Kameras oder Ansichten per Ziehen und Ablegen aus dem Seitenbereich in das Raster oder doppelklicken Sie auf diese, um sie dem ersten freien Bereich hinzuzufügen.
6. Klicken Sie auf **Save view (Ansicht speichern)**.

Um eine Kamera oder Ansicht im Raster zu bearbeiten, wählen Sie diese aus. Unter **Select item to configure (Element zur Konfiguration auswählen)** haben Sie folgende Möglichkeiten:

- Klicken Sie auf **Remove (Entfernen)**, um ein Element aus der Tabelle zu entfernen.
- Wählen Sie im Auswahlménú **PTZ preset (PTZ-Voreinstellung)**.

Zum Hinzufügen eines Hotspots:

- Wählen Sie ein Bild aus und klicken Sie im Bereich **Hotspot** auf **Set hotspot (Hotspot festlegen)**.

Zur automatischen Anzeige ausgelöste Videostreams im Hotspot:

- Wählen Sie **Dynamic hotspot content (Inhalte dynamischer Hotspot)** aus und konfigurieren Sie die Einstellungen. Weitere Informationen finden Sie unter *Dynamischer Hotspot, on page 18*.

Zur Festlegung des Videostreamprofils für eine Kamera:

- Klicken Sie die Kamera in der Rasteransicht mit der rechten Maustaste an und wählen Sie **Stream profile (Videostreamprofil)** aus. Siehe *Videostreamprofile, on page 56*.

Dynamischer Hotspot

Verwenden Sie dynamische Hotspots, um mehrere Ereignisse gleichzeitig zu überwachen. Wenn Aktionsregeln ausgelöst werden, erscheinen die entsprechenden Videostreams automatisch im Hotspot. Wird beispielsweise an drei verschiedenen Eingängen eine Bewegung erkannt, erscheinen alle drei Kameraansichten gleichzeitig.

Der Hotspot passt sein Raster an die Anzahl der aktiven Ansichten an. Jede Ansicht zeigt einen Countdown-Timer an und wird ausgeblendet, sobald der Countdown abgelaufen ist.

Hinweis

Bei Kameras, die durch zustandsabhängige Live-Ansichtsaktionen ausgelöst werden, beginnt der Countdown, sobald die Aktion nicht mehr aktiv ist. Bei anderen Kameras und Ansichten beginnt der Countdown sofort.

Dynamischen Hotspot erstellen

Zum Hinzufügen einer neuen Ansicht mit einem dynamischen Hotspot:

1. Klicken Sie auf der Registerkarte **Live view (Live-Ansicht)** auf **+**.
2. Klicken Sie auf **Add hotspot (Hotspot hinzufügen)**.
3. Wählen Sie die Option **Dynamic hotspot content (Inhalte dynamischer Hotspot)** aus.
4. Konfigurieren Sie die Einstellungen:
 - **Number of split view cells (Anzahl der Zellen in der geteilten Ansicht):** Die Anzahl der Zellen im Raster, auch wenn keine Ansichten aktiv sind. Bereich: 1 bis 144.
 - **Countdown in seconds (Countdown in Sekunden):** Anzeigedauer der ausgelösten Ansichten. Setzen Sie den Wert auf 0, damit die Ansichten bis zum manuellen Schließen angezeigt werden. Bereich: 0 bis 999.
 - **Seconds remaining when countdown appears in view (Verbleibende Anzeigedauer, bei der Countdown eingeblendet wird):** Legt fest, ab wann der Countdown-Timer auf dem Bildschirm erscheint. Setzen Sie den Wert auf 0, um ihn immer anzuzeigen. Die Anzeige des Timers erhöht die genutzten Systemressourcen. Bereich: 0 bis 999.
 - **Mute audio on incoming views (Audio bei neu eingeblendeten Ansichten stummschalten):** Neue Streams werden stummgeschaltet. Sie können die Stummschaltung einzeln aufheben.
 - **Allow adding views with click on view (Hinzufügen von Ansichten per Anklicken erlauben):** Sie können dem Hotspot zusätzlich zu den ausgelösten Ansichten manuell weitere Ansichten hinzufügen, indem Sie diese anklicken.
 - **Allow adding views with hotkey (Hinzufügen von Ansichten per Tastenkombination erlauben):** Sie können Tastenkombinationen verwenden, um dem Hotspot zu den ausgelösten Ansichten zusätzlich die mit den Tastenkombinationen verknüpften Ansichten hinzuzufügen.
5. Klicken Sie auf **Save view (Ansicht speichern)**.

Zum Hinzufügen eines dynamischen Hotspots zu einer bestehenden Ansicht:

1. Klicken Sie in der **Live view (Live-Ansicht)** auf **Edit view (Ansicht bearbeiten)**.
2. Klicken Sie auf **Add hotspot (Hotspot hinzufügen)**.
3. Wählen Sie **Dynamic hotspot (Dynamischer Hotspot)** aus.
4. Fahren Sie mit der Konfiguration wie in Schritt 4 oben beschrieben fort.
5. Klicken Sie auf **Save view (Ansicht speichern)**.

Hinweis

Sie können einen bestehenden Hotspot in einen dynamischen Hotspot umwandeln, indem Sie den Hotspot auf der Registerkarte **Live view (Live-Ansicht)** bearbeiten.

Ansichten steuern und verwalten

Jede Zelle in einem dynamischen Hotspot umfasst Folgendes:

- **Countdown-Anzeige:** Zeigt die verbleibende Zeit bis zum Ausblenden der Ansicht an.
- **Pause-Schaltfläche:** Zu Anhalten des Countdowns, um eine Ansicht länger anzuzeigen.
- **Schaltfläche zum Schließen:** Zum sofortigen Schließen einer Ansicht im Hotspot.
- **Blinkanzeige:** Der Countdown-Rahmen blinkt, wenn eine Ansicht erneut ausgelöst wird.

Diese Steuerelemente werden ausgeblendet, wenn Sie eine Zelle zur Einzelansicht vergrößern oder in den Wiedergabemodus wechseln. Klicken Sie doppelt auf eine beliebige Zelle, um sie in der Vollbildansicht anzuzeigen. Im Vollbildmodus wird der Countdown automatisch angehalten. Der dynamische Hotspot wird im Hintergrund weiterhin aktualisiert und zeigt Ihnen bei der Rückkehr zur Rasteransicht die aktiven Ansichten an.

Hinweis

Wenn Sie in den Wiedergabemodus wechseln, werden die Streams der Kamera angehalten und nicht mehr aktualisiert. Wechseln Sie zurück zur Live-Ansicht, um den normalen Betrieb fortzusetzen.

Zugangsdashboard in der geteilten Ansicht

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

1. Fügen Sie einen Zugang hinzu. Siehe *Fügen Sie einen Zugang hinzu, on page 154*.
2. Informationen dazu, wie Sie ein Zugangsdashboard einer geteilten Ansicht hinzufügen, finden Sie unter *Geteilte Ansicht, on page 18*.

Dashboard	Öffnen Sie die Registerkarte Dashboard, um Details zum Zugang und den Schlossstatus zu sehen. Auf dem Dashboard sehen Sie folgende Informationen: • Zutrittskontrollereignisse mit Einzelheiten zum Karteninhaber und Fotos, z. B. wenn ein Karteninhaber eine Karte durch einen Leser zieht. • Alarmer 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 Transactions (Transaktionen) verfügbar zu machen.
Zugriff	Klicken Sie auf Zutritt , um manuell Zugang zu gewähren. Daraufhin wird der Zugang entriegelt, als wäre eine Zutrittsberechtigung vorgewiesen worden. Der Zugang wird nach einer festgelegten Zeit automatisch wieder verriegelt.
Verriegeln	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 .



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

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 183*.
2. Klicken Sie auf der Registerkarte **Live view (Live-Ansicht)** auf .
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 Daten zum Szenario für Linienüberquerungen aus AXIS Object Analytics 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 178*.

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 vom AXIS Audio Manager Pro-Server über den Lautsprecher wiederzugeben.

Sequenziell

In der sequenziellen Anzeige werden die Ansichten automatisch gewechselt.

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. Klicken Sie auf der Registerkarte **Live view (Live-Ansicht)** auf **+**.
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 sie angezeigt werden sollen.
6. Klicken Sie auf eine Ansicht, um deren Einstellungen zu bearbeiten.
7. Klicken Sie auf **Save view (Ansicht speichern)**.

PTZ-Voreinstellung	Bei Kameras mit PTZ-Funktionen wählen Sie aus, in welche PTZ-Voreinstellung die Kamera geht, wenn diese Ansicht aktiv ist.
Verweildauer	Die Dauer in Sekunden, für die eine Ansicht erscheint, bevor zur nächsten gewechselt wird. Diese kann für jede Ansicht einzeln festgelegt werden.

Hinweis

- Sie können eine Sequenzansicht nicht zu einer anderen Sequenzansicht hinzufügen.
- Eine Komponentenansicht kann nicht direkt über einen Remote-Server hinzugefügt werden. Das lässt sich umgehen, indem Sie die Komponentenansicht zunächst in eine einzelne geteilte Ansicht einfügen und diese geteilte Ansicht dann über den Remote-Server hinzufügen.
- Die Wiedergabe mit der Zeitleiste kann sich ungewöhnlich verhalten. In der Wiedergabe werden alle Kameras nacheinander angezeigt, aber es ist jeweils nur eine aktiv.

Verwendung des Sequenzanzeigebalkens

Bei der Anzeige einer Sequenz können Sie diese mit einem Balken am unteren Rand des Anzeigefensters manuell steuern:

- Mit **[>]** und **[<]** springen Sie zur nächsten bzw. vorherigen Ansicht.
- **Hold (Halten)** und **Continue (Weiter)** erlauben das Anhalten und Fortsetzen der Sequenz.
- Ein Countdown zeigt an, wie viele Sekunden bis zum nächsten automatischen Wechsel verbleiben.
- Per Rechtsklick auf die Sequenz kann der Balken ausgeblendet werden.
- Wenn die Sequenz auf der Registerkarte **Recording (Aufzeichnung)** geöffnet ist, wird automatisch die Einstellung **Hold (Halten)** verwendet und Sie können nur manuell mit den Schaltflächen zur nächsten oder vorherigen Ansicht wechseln.

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, Audibereiche, Sequenzen, Webseiten, andere Lagepläne und Zutrittspunkte 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. Klicken Sie auf der Registerkarte **Live view (Live-Ansicht)** auf .
2. **Neuer Lageplan** wählen.
3. Geben Sie einen Namen für den Lageplan ein.
4. Klicken Sie auf **Bild wählen** und suchen Sie Lageplandatei. Die Datei darf nicht größer als 20 MB sein. Die folgenden Formate werden unterstützt: BMP, JPG, PNG und GIF.
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 dessen 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.
8. Klicken Sie auf **Save view (Ansicht speichern)**.

Hinweis

- Einige Einstellungen für Symbole und Lageplanbeschriftungen können gruppenweise bearbeitet werden.
- Alle Geräte, auf die Ihr Benutzerkonto keinen Zugriff hat, werden bei der Bearbeitung aus dem Lageplan entfernt.
- Eine Komponentenansicht kann nicht direkt über einen Remote-Server hinzugefügt werden. Das lässt sich umgehen, indem Sie die Komponentenansicht zunächst in eine einzelne geteilte Ansicht einfügen und diese geteilte Ansicht dann über den Remote-Server zu Ihrem Lageplan hinzufügen.

Symboleinstellungen

Klicken Sie auf ein Symbol im Lageplan, um die Symboleinstellungen zu bearbeiten.

	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.
Überwachungsbereich	Diese Option ist nur für unterstützte Geräte verfügbar. 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) , um den Überwachungsbereich blinken zu lassen, wenn eine Aufzeichnung durch die Bewegungserkennung oder andere Aktionsregeln ausgelöst wird. Informationen zur globalen Deaktivierung der Blinkfunktion für die Überwachungsbereiche aller Geräte finden Sie unter <i>Clienteneinstellungen</i> , on page 121.
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.
Aufzeichnungsindikatoren anzeigen	Mit dieser Option legen Sie fest, welche Aufzeichnungsindikatoren auf dem Symbol sichtbar sind. Aktivieren Sie die Option Small indicators (Kleine Indikatoren) , um eine kompakte Version der Indikatoren anzuzeigen. Mit den einzelnen Schaltern können Sie die Indikatoren für Recording (Aufzeichnung) , Motion detected (Bewegung erkannt) , Object detected (Objekt erkannt) und Action rule active (Aktionsregel aktiv) ein- oder ausblenden. Diese Einstellung wird auf dem Server gespeichert, sodass alle Clients dieselbe Konfiguration verwenden.

Etikett	Für Etiketten sind Einstellungen wie Text, Größe, Drehung und Farbe verfügbar. Außerdem haben Sie die Möglichkeit, die Beschriftung eines Etiketts zu unterstreichen und kursiv zu setzen.
Entfernen	Um ein Symbol vom Lageplan zu entfernen,  anklicken.

Auf dem Lageplan navigieren

Zoomen und auf dem Lageplan bewegen

- Zoomen und auf dem Lageplan bewegen können Sie sich mit der Maus, der Tastatur oder einem Joystick. Touch-Funktionen werden derzeit nicht unterstützt.

Maus

- Drehen Sie das Mousrad, um heran- bzw. herauszuzoomen.
- Wenn Sie einen Bereich des Lageplans herangezoomt haben, können Sie sich durch Ziehen auf diesem bewegen.

Tastatur

- Drücken Sie zum Heranzoomen Strg + [+] und zum Herauszoomen Strg + [-].
- Mit Strg + Pfeiltasten können Sie sich auf dem Lageplan bewegen.

Joystick

- Drehen Sie den Joystick-Kopf zum Heran- bzw. Herauszoomen.
- Neigen Sie den Joystick in die gewünschte Richtung, um sich auf dem Lageplan zu bewegen.

Schnappschuss aufnehmen

- Klicken Sie mit der rechten Maustaste auf den Lageplan, um das Kontextmenü zu öffnen. Sie können einen Schnappschuss des Lageplans auf Ihrer Festplatte speichern oder zur Registerkarte **Export (Exportieren)** hinzufügen. Der Schnappschuss nimmt den Lageplan so auf, wie er in diesem Moment erscheint, einschließlich aller aktuellen Kamerastatusangaben und Indikatorzustände.

Webseite

Die Webseitenansicht zeigt den Inhalt einer Internetseite. Sie haben die Möglichkeit, eine Webseite einer geteilten Ansicht oder einer Sequenz hinzuzufügen.

Hinzufügen einer Webseite:

1. Klicken Sie auf der Registerkarte **Live view (Live-Ansicht)** auf .
2. Wählen Sie **New web page (Neue Webseite)**.
3. Einen Namen für die Webseite eingeben.
4. Geben Sie die URL der Webseite ein.
5. Klicken Sie auf **OK**.



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

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

Auf der Registerkarte **Recordings (Aufzeichnungen)** können Sie Aufzeichnungen suchen, wiedergeben und exportieren. Die Registerkarte besteht aus einer Hauptansicht und zwei Bereichen, in denen Sie Ansichten, Bilder, Wiedergabewerkzeuge und Kameras verbundener Server finden, die jeweils nach Servernamen gruppiert sind. Siehe *Live-Ansicht*.

In der Hauptansicht haben Sie die gleichen Bildoptionen wie in der Live-Ansicht. Weitere Informationen finden Sie unter *Bilderverwaltung in der Live-Ansicht, on page 14*.

Informationen zur Änderung der Aufzeichnungsmethode und von 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, passen Sie die Aufbewahrungszeit unter **Configuration (Konfiguration) > Storage (Speicher) > Selection (Auswahl)** an.

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

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. Bewegen Sie den Schieber auf der Zeitleiste, um einen Überblick über den Inhalt zu erhalten und zu bestimmten Zeitpunkten zu springen.

- Eine rote Linie kennzeichnet eine Aufzeichnung, die durch eine Bewegung ausgelöst wurde.
- Eine blaue Linie kennzeichnet eine Aufzeichnung, die durch eine Aktionsregel ausgelöst wurde.

Aufzeichnungen finden

	Klicken Sie, um ein Datum und eine Uhrzeit in der Zeitleiste auszuwählen.
	Filtern Sie die Aufzeichnungstypen, die in der Zeitleiste angezeigt werden sollen.
	Verwenden Sie diese Option, um gespeicherte Lesezeichen zu finden. Siehe <i>Lesezeichen</i> .
	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 Kamerabeanutzer im AXIS Body Worn Assistant hinzugefügt hat.
 Intelligente Suche 1	Mit „Intelligente Suche 1“ können Sie Aufzeichnungen suchen. Siehe <i>Intelligente Suche 1</i> .

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, um heran- oder herauszuzoomen. Um einen bestimmten Bereich heranzuzoomen, bewegen Sie den Cursor zu diesem, bevor Sie scrollen.

Lesezeichen

Hinweis

- Sie können eine gesperrte Aufnahme nur löschen, wenn Sie sie manuell entsperren.
- Gesperrte Aufnahmen werden bei Entfernen der entsprechenden Kamera aus dem System gelöscht.

	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 oder sperren bzw. entsperren Sie die Aufzeichnung.
	Lesezeichen entfernen. Um mehrere Lesezeichen zu entfernen, halten Sie Strg oder die Umschalttaste, wählen Sie die zu entfernenden Lesezeichen aus und klicken Sie auf Remove (Entfernen) .
Löschen von Aufzeichnungen verhindern	Wählen Sie diese Option, um die Aufzeichnung zu sperren. Deaktivieren Sie die Option zum 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.  anklicken.
4. Einen Namen und eine Beschreibung für das Lesezeichen eingeben. Verwenden Sie Stichwörter, damit das Lesezeichen leicht zu finden ist.
5. Wählen Sie **Löschen von Aufzeichnungen verhindern**, um die Aufzeichnung zu sperren.

Hinweis

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

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

Ereigniskategorien

Weisen Sie Aufzeichnungen Kategorien zu, um die Suche bestimmter Typen von Ereignissen zu erleichtern. Bevor Sie beginnen, vergewissern Sie sich bitte, dass Sie über die erforderlichen Benutzerrechte verfügen. Siehe *Benutzer-/Gruppenberechtigungen, on page 142*.

Ereigniskategorien zuweisen

1. Suchen Sie auf der Registerkarte **Recordings (Aufzeichnungen)** die Aufzeichnung, der Sie eine Kategorie 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, siehe *Ereigniskategorien konfigurieren, on page 92*.

Aufzeichnungen exportieren

Auf der Registerkarte **Export (Exportieren)** können Sie Aufzeichnungen auf ein lokales Speichergerät oder einen Netzwerkspeicher exportieren. Außerdem finden Sie dort auch Informationen und eine Vorschau der Aufzeichnung. Sie können mehrere Dateien gleichzeitig exportieren. Unterstützte Formate sind .asf, .mp4 und .mkv.

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 33*.

Eine Aufzeichnung 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.  anklicken, 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 Exportaufgabe erscheint auf der Registerkarte **Tasks (Aufgaben)**.

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 Datei mit der Wiedergabeliste im .asx-Format, wenn Sie **Create playlist(.asx) (Wiedergabeliste erstellen (.asx))** auswählen.



Aufzeichnungen exportieren

Registerkarte Recordings (Aufzeichnungen)	
	Zur Auswahl mehrerer Aufzeichnungen klicken Sie auf  und versetzen Sie die Auswahlmarkierungen auf die gewünschten Anfangs- und Endpunkte.
	Um Aufzeichnungen innerhalb der Auswahlmarkierungen zu exportieren, klicken Sie auf  .
Aufzeichnungen hinzufügen	Zum Hinzufügen einer einzelnen Aufzeichnung klicken Sie mit der rechten Maustaste auf eine Aufzeichnung und wählen Sie Export (Exportieren) > Add recordings (Aufzeichnungen 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	Zum Löschen einer Aufzeichnung aus der Exportliste klicken Sie mit der rechten Maustaste auf eine Aufzeichnung und wählen Sie Export (Exportieren) > Remove recordings (Aufzeichnungen löschen) .
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 <i>Aufzeichnungen vor dem Export bearbeiten</i> , on page 33.
	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 Sie auf  .

Registerkarte Export	
Zum Export wechseln	Um bei geöffneter Registerkarte Incident report (Vorfallsbericht) zur Registerkarte Export zurückzukehren, klicken Sie auf Switch to export (Zum Export wechseln) .
Bevorzugtes Videostreamprofil	Wählen Sie im Feld Preferred stream profile (Bevorzugtes Videostreamprofil) das Videostreamprofil aus.
Vorschau	Zur Vorschau und zur Wiedergabe einer Aufzeichnung, diese in der exportierten Liste anklicken. Sie können nur dann eine Vorschau mehrerer Aufzeichnungen anzeigen, wenn diese von derselben Kamera stammen.
Speichern	Zum Speichern der Exportliste als Datei klicken Sie auf Save (Speichern) .
Load (Laden)	Wenn Sie eine zuvor gespeicherte Exportliste einschließen möchten, klicken Sie auf Load (Laden) .
Name of export (Exportname)	Geben Sie einen benutzerdefinierten Namen für den exportierten Ordner bzw. die Dateien ein oder lassen Sie das Feld, um die Standard-Namenskonvention in AXIS Camera Station Pro anzuwenden.
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 einen Schnappschuss hinzuzufügen, ziehen Sie die Zeitleiste in der Vorschau zu einem bestimmten Punkt, klicken Sie mit der rechten Maustaste auf die Vorschau und wählen Sie Add snapshot (Schnappschuss hinzufügen) .

Erweiterte Einstellungen	
Notizen beifügen	Wählen Sie Include notes (Notizen beifügen) , um die Notizen zu einer Aufzeichnung als .txt-Datei im Exportordner beizufügen und als Lesezeichen im AXIS File Player zu speichern.
Include AXIS File Player (AXIS File Player beifügen)	Klicken Sie auf Include AXIS File Player (AXIS File Player beifügen) , um den AXIS File Player zu den exportierten Aufzeichnungen hinzuzufügen.
Create playlist(.asx) (Wiedergabeliste erstellen (.asx))	Erstellen Sie eine Wiedergabeliste im .asx-Format für Windows Media Player, indem Sie Create playlist(.asx) (Wiedergabeliste erstellen (.asx)) auswählen. Die Aufzeichnungen werden in der Reihenfolge wiedergegeben, in der sie aufgezeichnet wurden.

Erweiterte Einstellungen	
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 <i>Exportierte Aufzeichnungen wiedergeben und überprüfen, on page 35</i> .
Export zu Zip-Datei	Zum Export der Daten in eine ZIP-Datei wählen Sie Export to Zip file (In ZIP-Datei exportieren) und geben Sie bei Bedarf ein Kennwort ein.
Exportformat	Wählen Sie im Auswahlménü Export format (Exportformat) ein Format aus, in das Sie Ihre Aufzeichnungen exportieren möchten. Bei Auswahl des MP4-Formats wird Audio im Format G.711 oder G.726 aus den exportierten Aufzeichnungen ausgeschlossen.
Edited video encoding (Bearbeitete Videocodierung)	Wenn ein Video bearbeitet wurde, können Sie das Videocodierungsformat unter Edited video encoding (Bearbeitete Videocodierung) auf <i>Automatic</i> , <i>H.264</i> oder <i>M-JPEG</i> festlegen. Bei der Einstellung <i>Automatic</i> werden M-JPEG für das M-JPEG-Format und H.264 für alle anderen Formate verwendet.

Benutzerrechte für das Exportieren

Um Aufzeichnungen zu exportieren oder Vorfalberichte zu erstellen, benötigen Sie die erforderlichen

Berechtigungen. Sie können eine Berechtigung für eine oder beide Operationen 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 140*.

Aufzeichnungen vor dem Export bearbeiten

Ein sich bewegendes Objekt weichzeichnen

1. Auf der Registerkarte **Export** oder **Incident report (Vorfalbericht)** 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 (Optionen für Umgrenzungsfelder) > Size (Größe)**, um die Größe anzupassen.
5. Verschieben Sie das Begrenzungsfeld und platzieren Sie es über dem Objekt.
6. Wechseln Sie zu **Bounding box options (Optionen für Umgrenzungsfelder) > Fill (Füllen)** 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 einen Endpunkt festzulegen, klicken Sie mit der rechten Maustaste auf die Rautenform im letzten Keyframe und wählen Sie **Set end (Ende festlegen)**. Dadurch werden die Schlüsselbilder nach dem Endpunkt entfernt.

Hinweis

Dem Video können mehrere Umgrenzungsrahmen hinzugefügt werden. Wenn sich Umgrenzungsfelder überlappen, erfolgt die Füllung des Überlappungsbereichs in der folgenden Reihenfolge: schwarz, verpixelt, dann 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 bewegendes Objekt vor anonymisierten Hintergrund anzeigen

1. Erstellen Sie ein Umgrenzungsfeld. Siehe *Ein sich bewegendes Objekt weichzeichnen, on page 33*.
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. Auf die ausgewählten Umgrenzungsfelder wird die Fülloption Clear (Klar) und auf die nicht ausgewählten die Fülloption Pixelated (Verpixelt) angewendet.
------------------------------	--

Umgrenzungsrahmen erstellen

Um Umgrenzungsfelder aus Analysedaten zu generieren, stellen Sie sicher, dass die Analysefunktionen der Kamera eingeschaltet sind. Siehe *Videostreamprofile, on page 56*.

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 bewegendes Objekt vollständig umschließen. Passen Sie bei Bedarf die Größe 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 *Installation von Kamera-Anwendungen*.



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 den AXIS File Player, um die digitale Signatur zu überprüfen und die Aufzeichnung auf Änderungen 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 den AXIS File Player. Die exportierten Aufzeichnungen werden automatisch wiedergegeben.
3. Klicken Sie im AXIS File Player auf , um die Notizen zur Aufzeichnung anzuzeigen.
4. Zur Überprüfung der digitalen Signatur von Aufzeichnungen, die mit der Option **Add digital signature (Digitale Signatur hinzufügen)** exportiert wurden:
 - 4.1. Gehen Sie zu **Tools (Werkzeuge) > Verify digital signature (Digitale Signatur überprüfen)**.
 - 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 **Incident report (Vorfallsbericht)** können Sie Vorfallsberichte auf ein lokales Speichergerät oder einen Netzwerkspeicher exportieren. Sie können Aufzeichnungen, Momentaufnahmen und Notizen in Ihre Vorfallsberichte einbinden.

Vor Exportbeginn sicherstellen, dass die entsprechende Berechtigung gegeben ist. Siehe *Benutzerrechte für das Exportieren, on page 33*.



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 30*.
3. Klicken Sie auf **Switch to incident report (Zu Vorfallsbericht wechseln)**, um die Registerkarte **Incident report (Vorfallsbericht)** zu öffnen.
4. Auf **Create report (Bericht erstellen)** klicken.
5. Wählen Sie einen Ordner aus, in dem der Vorfallsbericht gespeichert werden soll.

6. Klicken Sie auf **OK**. Die Aufgabe zum Export des Vorfallberichts erscheint auf der Registerkarte **Tasks (Aufgaben)**.

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 <i>Aufzeichnungen vor dem Export bearbeiten, on page 33</i> .
	Zur Bearbeitung von Aufzeichnungshinweisen wählen Sie eine Aufzeichnung aus und klicken auf  .
	Sie entfernen eine Aufzeichnung aus der Exportliste, indem Sie die gewünschte Aufzeichnung auswählen und auf  klicken.
Zu Vorfallbericht wechseln	Um von der geöffneten Registerkarte Export (Exportieren zur Registerkarte Incident report (Vorfallbericht) zu wechseln, klicken Sie auf Switch to incident report (Zu Vorfallbericht wechseln).
Bevorzugtes Videostreamprofil	Wählen Sie in der Auswahlliste Preferred stream profile (Bevorzugtes Videostreamprofil) das Videostreamprofil aus.
Vorschau	Zur Vorschau und Wiedergabe einer Aufzeichnung klicken Sie diese in der Exportliste an. Sie können nur dann eine Vorschau mehrerer Aufzeichnungen anzeigen, wenn diese von derselben Kamera stammen.
Speichern	Um den Vorfallbericht als Datei zu speichern, klicken Sie auf Save (Speichern).
Load (Laden)	Zum Laden eines zuvor gespeicherten Vorfallberichts, klicken Sie auf Load (Laden).
Beschreibung	Das Feld Description (Beschreibung) wird automatisch mit vordefinierten Daten aus der Beschreibungsvorlage gefüllt. Hier können Sie auch

	ergänzende Informationen hinzufügen, die in den Vorfallbericht eingeschlossen werden sollen.
Kategorie	Wählen Sie eine Kategorie aus, zu der der Bericht gehört.
Referenz-ID	Es wird automatisch eine Reference ID (Referenz-ID) generiert. Diese können Sie bei Bedarf manuell ändern. Die ID identifiziert den Vorfallbericht eindeutig.
Notizen beifügen	Wählen Sie Include notes (Notizen beifügen) , um die Notizen zu einer Aufzeichnung als .txt-Datei im Exportordner beizufügen und als Lesezeichen im AXIS File Player zu speichern.
Edited video encoding (Bearbeitete Videocodierung)	Wenn ein Video bearbeitet wurde, können Sie das Videocodierungsformat unter Edited video encoding (Bearbeitete Videocodierung) auf <i>Automatic</i> , <i>H.264</i> oder <i>M-JPEG</i> festlegen. Bei der Einstellung <i>Automatic</i> werden M-JPEG für das M-JPEG-Format und H.264 für alle anderen 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 einen Schnappschuss hinzuzufügen, ziehen Sie die Zeitleiste in der Vorschau zu einem bestimmten Zeitpunkt, klicken Sie mit der rechten Maustaste auf die Vorschau und wählen Sie Add snapshot (Schnappschuss hinzufügen) aus.

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 Auswahlliste **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 auf das Bild der Kamera-Live-Ansicht.
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

Mit „Intelligente Suche 1“ können Sie die Teile einer Aufzeichnung suchen, in denen in einem definierten Bereich eine Bewegung stattgefunden hat.

Um die Suchgeschwindigkeit zu erhöhen, wählen Sie **Include analytics data (Analysedaten einbeziehen)** in den Einstellungen für das Videostreamprofil. Siehe *Videostreamprofile*.

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. Den ausgewählten Bereich anpassen. 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 **Short-lived objects filter (Filter für kurz erscheinende Objekte)** und den **Small objects filter (Filter für kleine Objekte)**, um unerwünschte Ergebnisse herauszufiltern.
5. Wählen Sie den Datums- und Zeitbereich für die Suche aus. Wählen Sie mithilfe der Umschalttaste einen Datumsbereich aus.
6. Klicken Sie auf **Suchen**.

Die Suchergebnisse werden auf der Registerkarte **Ergebnisse** angezeigt. Sie können die Aufzeichnungen exportieren, indem Sie ein oder mehrere Ergebnisse mit der rechten Maustaste anklicken.

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.



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

Intelligente Suche 1

Intelligente Suche 2

Nutzen Sie „Intelligente Suche 2“, um sich bewegende Personen und Fahrzeuge in den Aufzeichnungen 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 *Installation von Kamera-Anwendungen*, on page 70.
- Zeitsynchronisierung zwischen AXIS Camera Station Pro Server und Kameras.

Wenn Sie „Intelligente Suche 2“ für eine Axis Kamera einschalten, beginnt AXIS Camera Station Pro mit der Erfassung von Metadaten dieser Kamera und nutzt diese zur Klassifizierung von Objekten in der Szene. Das ermöglicht Ihnen die Nutzung von Filtern, um bestimmte Inhalte zu finden.

Hinweis

- Es wird empfohlen, die kontinuierliche Aufzeichnung zu verwenden, da die bewegungsgesteuerte Aufzeichnung zu Erkennungsereignissen ohne Videomaterial führen kann.
- Verwenden Sie das H.264-Format, wenn Sie eine Vorschau von Aufzeichnungen im Suchergebnis anzeigen möchten.
- Achten Sie darauf, dass die Lichtverhältnisse den Spezifikationen der Kamera entsprechen, um eine optimale Farbklassifizierung zu gewährleisten. Nach Erfordernis zusätzliche Lichtquellen einsetzen.

Vorgehensweise

1. *Intelligente Suche 2 konfigurieren*, on page 179
2. Zeitsynchronisierung zwischen AXIS Camera Station Pro Server und Kameras konfigurieren. Siehe *Zeitsynchronisierung*, on page 75.
3. Erstellen Sie einen Filter oder laden Sie einen vorhandenen Filter. Siehe *Suche mit Filtern*, on page 39.
4. Suchergebnisse verwalten. Siehe *Ergebnisse der intelligenten Suche*, on page 44.

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 eine oder mehrere der folgenden Maßnahmen, um sie zu beschleunigen:

- Schalten Sie die Klassifizierung durch den Server im Hintergrund für wichtige oder häufig genutzte Kameras ein.
- Wenden Sie Eingangsfiler auf Kameras an, um irrelevante Erfassungen zu reduzieren.
- Verkürzung der Suchdauer.
- Reduzieren Sie die Anzahl der Kameras bei der Suche.
- Definieren Sie einen Bereich sowie eine Objektrichtung, Größe und Dauer, um die Datenmenge einzugrenzen.

Kameras	Um die Suche nach Kamera einzuschränken, klicken Sie auf Kameras (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 Search (Suchen). Hinweis Die Ähnlichkeitssuche erstellt abstrakte Darstellungen aus niedrig aufgelösten Bildausschnitten von Personen 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 erkannt werden.
Freitextsuche	Mit der Freitextsuche können Sie in natürlicher Sprache (nur Englisch) beschreiben, wonach Sie in den Aufzeichnungen suchen. Siehe <i>Freitextsuche, on page 42</i> .
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 (Linienüberquerung) , wählen Sie eine Kamera und aktivieren Sie Filter by line crossing on this camera (Auf dieser Kamera nach Linienüberquerung filtern) , um nach Linienüberquerungsereignissen zu filtern. Passen Sie

	die Linie im Bild an und fügen Sie bei Bedarf Punkte hinzu bzw. entfernen Sie diese.
Größe	Klicken Sie auf Size (Größe) , wählen Sie die Kamera und aktivieren Sie Filter by size on this camera (Auf dieser Kamera nach Größe filtern) , um nach der Größe zu filtern. Passen Sie die Mindesthöhe und -breite als Prozentwert des Gesamtbildes ein.
Dauer	Klicken Sie auf Duration (Dauer) , wählen Sie die Kamera und aktivieren Sie Filter by duration on this camera (Auf dieser Kamera nach Dauer filtern) , um nach der Dauer zu filtern. Passen Sie die Minstdauer 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 Radargeräte 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 natürlicher 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 Axis das Modell aktualisiert.
 - 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.

So suchen Sie:

1. Öffnen Sie die Registerkarte **Intelligente Suche 2**.
2. Klicken Sie auf **Objektmerkmale**.
3. Klicken Sie **Free text (Freitext)** an.
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 mit einigen wenigen Schlüsseldescriptoren. 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 über keine Fachkenntnisse im Bereich Videosicherheit verfügt. Zum Beispiel:

Eingabeaufforderung	Kommentar
Ein gelber Pickup parkt neben einem Baum	In etwa richtig
Ein fahrerloses Fahrzeug, Fahrzeugkennzeichen: CHY67F, Fahrzeugtyp: Pickup, Farbe: Gelb, Standort: neben einer großen 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 nutzt ein Modell zur Verarbeitung natürlicher Sprache sowie eine angepasste Liste unzulässiger Suchkategorien und Wörter zur Überprüfung sämtlicher Suchanfragen.

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 geben, das unserem Team zur Überprüfung übermittelt wird.

Hinweis

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

Ergebnisse der intelligenten Suche

	Um Erkennungen zu gruppieren, die wahrscheinlich zum selben Ereignis gehören, fassen Sie diese in Zeitintervallen zusammen. Wählen Sie im Dropdown-Menü  ein Intervall aus.
Neuste zuerst 	„Intelligente Suche 2“ zeigt die Suchergebnisse in absteigender Reihenfolge an, wobei die letzten Erfassungen 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 Auswahl einer hohen Zuverlässigkeitsstufe werden unsichere Klassifizierungen herausgefiltert.
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 einen Bildausschnitt 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. Für Radar lässt sich die Klassifizierung durch den Server im Hintergrund nicht einschalten.
- Das Verhalten der Objektklassifizierung ist bei Wärmebildkameras unvorhersehbar.
- Bei jeder Änderung einer PTZ-Voreinstellung werden für einen kurzen Zeitraum nach einer 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 ein Gerät, das Daten zu Ereignissen erzeugt. Weitere Informationen, siehe *Externe Datenquellen, on page 74*. Zum Beispiel:

- 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 Speicherdauer externer Daten in AXIS Camera Station Pro zu ändern, gehen Sie zu **Configuration (Konfiguration) > Server > Settings (Einstellungen) > External data (Externe Daten)**.

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 **Search options (Suchoptionen)**  und wenden Sie bei Bedarf weitere Filter an. Die verfügbaren Filter sind vom Typ der Datenquelle abhängig.
5. Geben Sie Schlüsselwörter in das Suchfeld ein. Siehe *Suche optimieren, on page 46*.
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	Verwenden Sie diese Option, um Daten einzubeziehen, die ausschließlich von dieser Komponente stammen. Mit der Zutrittskontrolle können Sie nach Zugängen und Zonen, Karteninhabern und Ereignistypen filtern.
Third party (Andere Quellen)	Verwenden Sie diese Option, um Daten von anderen Quellen als den konfigurierten Komponenten einzubeziehen.

Abhängig von der Datenquelle können Sie unterschiedliche Elemente in Ihrem Suchergebnis erhalten. Zum Beispiel:

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-Zugangsscontrollers 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. Beispiel: Fahrzeug.

Klicken Sie auf **Download search result (Suchergebnis herunterladen)**, um die Suchergebnisse in eine PDF- oder Textdatei zu exportieren. Sie können die Spalten anders anordnen und die Spaltenbreiten anpassen, um das Tabellenlayout in der PDF-Ausgabe zu optimieren. 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 „Max speed“ (Höchstgeschwindigkeit). • Eine Suche nach [Average speed] < = 28 liefert Ergebnisse mit einem Wert bis maximal 28 in der Spalte „Average speed“ (Durchschnittsgeschwindigkeit).
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 liefert nur Ergebnisse, die mit „ABC123“ in der Spalte „Cardholder“ (Karteninhaber) übereinstimmen.

Konfiguration

Auf der Registerkarte „Configuration“ (Konfiguration) können Sie verbundene Geräte verwalten und die Einstellungen für Client und Server konfigurieren. Klicken Sie auf  und wählen Sie **Configuration (Konfiguration)** aus, um die Registerkarte **Configuration (Konfiguration)** zu öffnen.

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.
- einen Video-Encoder mit einem oder mehreren Videoports.
- ein Zusatzgerät, das keine Kamera ist, wie ein E/A-Audiogerät, ein Netzwerklautsprecher oder eine Tür-Steuerung.
- ein Türkontrollsystem.

Hier können Sie folgendes:

- Kameras und Geräte ohne Videofunktionen hinzufügen. Siehe *Geräte hinzufügen*.
- Einstellungen angeschlossener Kameras bearbeiten. Siehe *Kameras*.
- Einstellungen für Geräte ohne Kamera bearbeiten. Siehe *Andere Geräte*.
- Die Auflösung, das Format und weiteren Einstellungen für Videostreamprofile bearbeiten. Siehe *Videostreamprofile*.
- 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 74*.

Geräte hinzufügen

Hinweis

- Das System erkennt Ansichtsbereiche als individuelle Kameras. Ansichtsbereiche 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 Ihre Geräte, Videostreams oder vorab aufgezeichneten Videos.
 - *Geräte ermitteln, on page 50*
 - *Videostreams finden, on page 50*
 - *Auffinden von vorab aufgezeichneten Videos, on page 51*
2. *Hinzufügen von Geräten, Videostreams oder vorab aufgezeichneten Videos, on page 51*

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...)	Der 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.
Geben Sie das Kennwort ein	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 auf Generate (Erzeugen), um ein Kennwort erzeugen zu lassen. Es wird empfohlen, eine Kopie des erzeugten Kennworts zu speichern. - Legen Sie mit Set password fest, ob das Kennwort für alle Geräte verwendet werden soll. - Wenn für das Gerät eine Kennwortrichtlinie gilt, zeigt ein Indikator für die Kennwortrichtlinie an, ob Ihr Kennwort die Anforderungen erfüllt. Weitere Informationen finden Sie unter <i>Benutzerverwaltung, on page 68</i>.
Nicht unterstütztes Modell	AXIS Camera Station Pro unterstützt das Gerätemodell nicht.

Firmware veraltet	Die Firmware des Geräts ist veraltet. Aktualisieren Sie die Firmware, bevor Sie das Gerät hinzufügen.
Fehlerhaftes Gerät	Die von AXIS Camera Station Pro abgerufenen Geräteparameter sind beschädigt.
Neigungsausrichtung einstellen	Klicken Sie auf den Link und wählen Sie die Neigungsausrichtung: Decke, Wand oder Tisch, je nach Montage der Kamera. Einige Kameramodelle erfordern die Einstellung der Neigungsausrichtung.
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. Gehen Sie zu **Configuration (Konfiguration) > Devices (Geräte) > Add devices (Geräte hinzufügen)**.
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. Wenn Sie den voreingestellten Port 80 ändern möchten, geben Sie den Portbereich ein. 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>:<port>/<path>`
Zum Beispiel: `http://<address>:80/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`
- `https://<address>:<port>/<path>`
Zum Beispiel: `https://<address>:443/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`

1. Gehen Sie zu **Configuration (Konfiguration) > Devices (Geräte) > Add devices (Geräte hinzufügen)**.
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:

- 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, siehe *Bildkonfiguration, on page 60*.
 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. Gehen Sie zu **Configuration (Konfiguration) > Devices (Geräte) > Add devices (Geräte hinzufügen)**.
3. Wählen Sie die Geräte, Videostreams oder vorab aufgezeichneten Videos aus. Klicken Sie auf **Hinzufügen**.
4. Klicken Sie auf **Close (Schließen)**, um die Konfiguration zu überspringen und später fortzufahren. So fahren Sie mit der Konfiguration fort:
 - 4.1. Wählen Sie **Quick configuration (Schnellkonfiguration)**, um die Grundeinstellungen vorzunehmen. Wenn Sie ein AXIS Site Designer-Projekt importieren, wählen Sie **Site Designer configuration (Site Designer-Konfiguration)**. Weitere Informationen, siehe *AXIS Site Designer-Projekte importieren*.
 - 4.2. Wählen Sie **Add image overlay for date, time, and text (Overlay für Datum, Uhrzeit und Text hinzufügen)**, um Overlays zu Axis Kameras hinzuzufügen, die noch keine haben.
 - 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 **Retention time (Aufbewahrungszeit)** und den **Recording storage (Aufzeichnungsspeicher)** aus und klicken Sie auf **Finish (Fertigstellen)**, um die Konfiguration zu übernehmen.

AXIS 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 Setup-Datei auf das Projekt zugreifen.

Zum Import eines AXIS Site Designer-Projekts in AXIS Camera Station Pro:

1. Generieren Sie einen Zugangscode oder laden Sie eine Projektdatei herunter:
 - 1.1. Melden Sie sich auf <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 generieren)**, wenn Ihr AXIS Camera Station Pro-Server über eine Internetverbindung verfügt, oder klicken Sie auf **Download settings file (Setup-Datei herunterladen)**, falls keine Internetverbindung besteht.
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. Um stattdessen die heruntergeladene Setup-Datei zu verwenden, wählen Sie **Choose file (Datei auswählen)**.
6. Klicken Sie auf **Import (importieren)**. AXIS Camera Station Pro versucht, das Projekt anhand der IP-Adresse oder des Produktnamens mit den ausgewählten Geräten abzugleichen. Schlägt der Abgleich fehl, wählen Sie die Geräte aus dem Auswahlmenü aus.
7. Klicken Sie auf **Next (Weiter)**.
8. Wählen Sie Ihre bevorzugte **Aufzeichnungsmethode** aus. Diese Einstellungen gelten für Kameras, die nicht der Projektkonfiguration entsprechen.
9. Klicken Sie auf **Next (Weiter)**.
10. Wählen Sie Ihre **Retention time (Aufbewahrungszeit)** und den **Recording storage (Aufzeichnungsspeicher)** aus und klicken Sie auf **Finish (Fertigstellen)**, um die Konfiguration zu übernehmen.

AXIS Camera Station Pro importiert die folgenden Einstellungen aus dem AXIS 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	✓	✓

	Encoder, Video-Decoder, Türsteuerungen, Radarmelder und Lautsprecher	Kameras, Gegensprechanlagen und F/FA-Serien
Kontinuierliche Aufzeichnung: Zeitplan- und Aufzeichnungsprofil einschließlich Bildrate, Auflösung, 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 ein nur Aufzeichnungsprofil definiert haben oder es im AXIS Site Designer-Projekt zwei identische Aufzeichnungsprofile gibt, setzt AXIS Camera Station Pro das Profil auf „Medium“ (Mittel).
- Wenn Sie beide Aufzeichnungsprofile im AXIS Site Designer-Projekt definiert haben, setzt AXIS Camera Station Pro das Profil für die kontinuierliche Aufzeichnung auf „Medium“ (Mittel) und für die bewegungsgesteuerte Aufzeichnung auf „High“ (Hoch).
- AXIS Camera Station Pro optimiert das Seitenverhältnis, weshalb die Auflösung vom AXIS Site Designer-Projekt abweichen 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.
- AXIS Camera Station Pro wendet keine Audioeinstellungen auf Türkontrollsysteme an, auch wenn die Einstellungen in AXIS Site Designer abweichen. Bei Türkontrollsystemen ist Audio immer eingeschaltet, was jedoch nur für die Live-Ansicht gilt.



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

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 50*.

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
- Export von Aufzeichnungen
- 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 Netzwerkkamera 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 Ihrer Lizenz ab.

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. Klicken Sie auf **Help (Hilfe)**, um Informationen dazu zu erhalten, wo Sie die Einstellung finden. Der Ort ist von Kameramodell und Firmware abhängig.

Ein Gerät ersetzen

Sie können ein Gerät ersetzen, die vorhandenen Einstellungen und Aufzeichnungen aber behalten. Dazu muss die Anzahl der konfigurierten Videostreams auf der neuen Kamera mit der auf 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. Falls das ersetzte Gerät den Cloud-Speicher genutzt hat, starten Sie den Dienst auf Ihrem AXIS Camera Station Pro-Server neu. Aktivieren Sie anschließend unter „My Systems“ den Cloud-Speicher für das Gerät. Siehe *Einschalten des Cloud-Speichers für Ihre einzelnen Kameras*.

8. Überprüfen Sie die Konfiguration des neuen Geräts, um die Richtigkeit der Einstellungen und die ordnungsgemäße Funktion sicherzustellen. 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

Gehen Sie zu **Configuration (Konfiguration) > Devices (Geräte) > Cameras (Kameras)**, um die Liste aller zum 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. Mit diesem Vorgang werden außerdem alle Aufzeichnungen gelöscht, die mit den gelöschten Kameras verknüpft sind, einschließlich der gesperrten Aufnahmen.

Kameraeinstellungen bearbeiten

Um Kameraeinstellungen zu bearbeiten:

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

Aktiviert	Deaktivieren Sie die Option Enabled (Aktiviert) , um die Aufzeichnung und Anzeige des Videostreams zu verhindern. 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

Gehen Sie zu **Configuration (Konfiguration) > Devices (Geräte) > Other devices (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. Siehe *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.

Videostreamprofile

Ein Videostreamprofil ist eine Gruppe von Einstellungen, die sich auf den Videostream auswirken, z. B. Auflösung, Videoformat, Bildrate und Komprimierung. Gehen Sie zu **Configuration (Konfiguration) > Devices (Geräte) > Stream profiles (Videostreamprofile)**, um die Seite **Stream profiles (Videostreamprofile)** 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 in der Live-Ansicht und bei Aufzeichnungen standardmäßig auf **Automatic (Automatisch)** eingestellt. Das Videostreamprofil wechselt automatisch auf **High (Hoch)**, **Medium (Mittel)** oder **Low (Niedrig)**, je nach der verfügbaren Größe für den Videostream.

Videostreamprofile in der Kamera

AXIS Camera Station Pro fügt der Kamera automatisch Videostreamprofile hinzu, damit Sie Aufzeichnungsregeln direkt in der Kamera konfigurieren können. Die Profile werden in der Weboberfläche der Kamera unter **Stream profiles (Videostreamprofile)** angezeigt und ihr Name besteht aus der Kamerabezeichnung und der Profilstufe, zum Beispiel „Camera 1_ACS_Pro_High“.

Die Profile werden in der Kamera im Rahmen der folgenden Vorgänge hinzugefügt oder aktualisiert:

- Eine Kamera wird zu AXIS Camera Station Pro hinzugefügt.
- Die Videostreamprofile in AXIS Camera Station Pro werden geändert.
- Die nächtliche Aktualisierung läuft.

Wenn eine Kamera aus AXIS Camera Station Pro entfernt wird, werden die von AXIS Camera Station Pro erstellten Videostreamprofile in der Kamera gelöscht.

Hinweis

Videostreamprofile mit JPEG- oder MPEG-4-Format werden nicht in der Kamera hinzugefügt.

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. Nur für Geräte anderer Hersteller verfügbar. - 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 benötigt weniger Bandbreite und Speicher als M-JPEG. Einige Kameras unterstützen außerdem H.265 , das eine etwas bessere Komprimierung bietet, jedoch mehr Rechenleistung benötigt. 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 finden Sie auf <i>AV1-Produktseite</i> . Auf der <i>Seite mit dem kompatiblen Kameras</i> können Sie prüfen, ob Ihre Kamera AV1 unterstützt.
Bildrate	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 Quellschleife 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). Dieses Profil nutzt hochentwickeltere Komprimierungswerkzeuge, um die Speichernutzung gegenüber der standardmäßigen Zipstream-Option weiter zu reduzieren. Darüber hinaus kann die Bitrate auch bei Szenen mit viel Bewegung weiter reduziert werden. • Das asf-Format unterstützt die von dieser Funktion verwendeten B-Frames nicht. • Diese Funktion wirkt sich nicht auf Videos aus, die mit Recordern der Serie AXIS S30 aufgezeichnet wurden. • 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 <i>Audio von Zusatzgeräten verwenden</i> .
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 <i>Audio von Zusatzgeräten verwenden</i> .
Mikrofon verwenden für:	Aktivieren von Audio über Mikrofon 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 mit einer Kamera verknüpft Audiogerät auswählen. Weitere Informationen finden Sie unter *Konfiguration von AXIS Audio Manager Pro, on page 178*.

Erweitert

Analysedaten einbeziehen	Um während des Videostreamings Daten für die intelligente Suche zu erfassen, Include analytics data (Analysedaten einbeziehen) wählen. Diese Option ist nur für Axis Geräte verfügbar, die Analysedaten unterstützen. Die Datenerfassung für <i>Intelligente Suche 1</i> kann zu Verzögerungen im Live-Videostreaming führen.
Verwenden Sie FFmpeg	Aktivieren Sie Use FFmpeg, um die Kompatibilität mit Geräten anderer Hersteller zu verbessern, indem Sie Use FFmpeg (FFmpeg verwenden) auswählen. Nur für Geräte anderer Hersteller verfügbar.
Objektindikatoren für PTZ-Autotracking anzeigen	Um die Objektindikatoren anzuzeigen, die von einer PTZ-Kamera in der Live-Ansicht erkannt werden, wählen Sie die Option Show PTZ autotracking object indicators (Objektindikatoren für PTZ-Autotracking anzeigen) aus und stellen Sie die Pufferzeit des Videostreams auf 2000 Millisekunden ein. Nur für PTZ-Kameras von Axis mit AXIS PTZ Autotracking verfügbar. Für einen vollständigen Workflow zum Einrichten von AXIS PTZ Autotracking in AXIS Camera Station Pro siehe <i>AXIS PTZ Autotracking einrichten</i> .
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 <code>overlays=off&color=0</code> ein, um die Overlays dieser Kamera auszublenden. Die benutzerdefinierten Einstellungen überschreiben alle vorhandenen Einstellungen. Verwenden Sie keine vertraulichen Informationen in den benutzerdefinierten Einstellungen.

Wählen Sie die zu konfigurierende Kamera aus, um die **Profileinstellungen anzupassen**, z. B. Auflösung, Bildrate, Komprimierung, Videoformat und Audio. 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. Weitere Informationen zur Bandbreitennutzung siehe *Streaming*.

Audio von Zusatzgeräten verwenden

Audio von anderen Geräten, bei denen es sich nicht um eine Kamera handelt, oder Zusatzgeräten kann mit den Videobildern einer Netzwerk-Kamera oder eines Video-Encoders für Live-Ansichten und Aufzeichnungen kombiniert 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 *Videostreamprofile*.
3. Aktivieren Sie Audio für die Live-Ansicht bzw. Aufzeichnung. Siehe *Videostreamprofile*.

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

Änderungen der Bildkonfiguration werden sofort wirksam.

Die Bildeinstellungen konfigurieren:

1. Gehen Sie zu **Configuration (Konfiguration) > Devices (Geräte) > Image configuration (Bildkonfiguration)**. AXIS Camera Station Pro zeigt einer Liste aller Kameras an.
2. Wählen Sie eine Kamera aus, um ihren Videostream in Echtzeit unter der Liste anzuzeigen. Verwenden Sie das Feld **Suchwort eingeben**, um eine bestimmte Kamera in der Liste zu finden.
3. Die Bildeinstellungen konfigurieren:

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. Der Weißabgleich dient dazu, die Farben im Bild unabhängig von der Farbtemperatur der Lichtquelle einheitlich wiederzugeben. 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 Sie diese Option, wenn eine helle Lichtquelle wie eine Glühbirne dazu führt, dass andere Bereiche des Bilds zu dunkel erscheinen.

Dynamischer Kontrast (Wide Dynamic Range) – Aktivieren Sie diese Option, um bei einem starken Kontrast zwischen hellen und dunklen Bildbereichen die Belichtung zu verbessern. Verwenden Sie den Schieberegler, um die Stufe einzustellen. Deaktivieren Sie die Option bei dunklen Lichtbedingungen.

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.

Zur Konfiguration benutzerspezifischer Entzerrungseinstellungen:

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 (Pan, tilt, zoom, PTZ) ist die Fähigkeit der Kamera zu schwenken (Bewegung nach links und rechts), zu neigen (Bewegung nach oben und unten) sowie heran- und herauszuzoomen.

Gehen Sie zu **Configuration (Konfiguration) > Devices (Geräte) > PTZ presets (PTZ-Voreinstellungen)**. AXIS Camera Station Pro zeigt eine Liste der Kameras an, die PTZ unterstützen. 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.
- Unbewegliche Kameras mit eingeschaltetem digitalem PTZ.
- ONVIF-Kameras, die PTZ-Voreinstellungen unterstützen.

Die digitale PTZ-Funktion kann über die integrierte Konfigurationsseite der Kamera eingeschaltet werden. Weitere Informationen finden Sie im Benutzerhandbuch der Kamera. Gehen Sie zum Öffnen der Konfigurationsseite zur Geräteverwaltung, wählen Sie die Kamera aus und klicken Sie auf den Link in der Spalte **Address (Adresse)**.

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. PTZ-Bewegungen sind in der Live-Ansicht erkennbar und werden aufgezeichnet.

- Wenn eine PTZ-Voreinstellung in AXIS Camera Station Pro konfiguriert ist, können Sie den vollständigen Videostream der Kamera anzeigen. PTZ-Bewegungen sind in der Live-Ansicht weder sichtbar, noch werden sie aufgezeichnet.

Hinweis

PTZ ist nicht möglich, solange die Steuerungswarteschlange der Kamera aktiv ist. Informationen zur Steuerungswarteschlange sowie zu Ihrer Aktivierung bzw. 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 Mause, 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 diese aus und klicken Sie auf **Remove (Entfernen)**. Dadurch wird die Voreinstellung sowohl aus AXIS Camera Station Pro als auch aus 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 **Configuration (Konfiguration) > Devices (Geräte) > Management (Verwaltung)**, um die Seite **Manage devices (Geräte verwalten)** zu öffnen.

Wenn Sie in *Einstellungen zum Aktualisieren der Firmware, on page 127* die automatische Überprüfung auf neue Firmware-Versionen eingerichtet haben, wird ein Link angezeigt, sobald 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 132* die automatische Überprüfung auf neue Firmware-Versionen eingerichtet haben, wird ein Link angezeigt, sobald eine neue Firmware-Version für AXIS Camera Station Pro verfügbar ist. Klicken Sie auf den Link, um die neue Version zu installieren.

AXIS Camera Station Pro zeigt eine Liste aller hinzugefügten Geräte an. 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. Die Reihenfolge der Spalten können Sie ändern, indem Sie die Kopfzeile einer Spalte anklicken und an eine andere Position ziehen.

Die folgenden Informationen wird in der Geräteliste angezeigt:

- **Name:** Wenn das Gerät ein Video-Encoder mit mehreren angeschlossenen Kameras oder eine Netzwerk-Kamera mit mehreren Ansichtsbereichen ist, wird der Gerätenamen oder eine Liste aller zugeordneten Kameranamen angezeigt.
- **MAC address (MAC-Adresse):** Die MAC-Adresse des Geräts.
- **Status:** Der Status des Geräts.
 - **OK:** Der Standardstatus einer hergestellten Geräteverbindung.
 - **Maintenance (Wartungsarbeiten):** Das Gerät wird derzeit gewartet und ist vorübergehend nicht zugänglich.
 - **Not accessible (Nicht erreichbar):** Es kann keine Verbindung zum Gerät hergestellt werden.
 - **Not accessible over set hostname (Über den festgelegten Host-Namen nicht erreichbar):** Über den angegebenen Host-Namen kann keine Verbindung zum Gerät hergestellt werden.
 - **Server not accessible (Server nicht erreichbar):** Zu dem Server, mit dem das Gerät verbunden ist, kann keine Verbindung hergestellt werden.

- **Enter password (Kennwort eingeben):** Das Gerät ist erst nach Eingabe gültiger Zugangsdaten erreichbar. Auf den Link klicken, um gültige Benutzeranmeldeinformationen bereitzustellen. Sofern das Gerät verschlüsselte Verbindungen unterstützt, wird das Kennwort verschlüsselt versendet.
- **Set password (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 (Erzeugen)**, um automatisch ein Kennwort mit der für das Gerät zulässigen Länge erzeugen zu lassen. Es wird empfohlen, eine Kopie des erzeugten Kennworts zu speichern.
 - Optional kann dieses Kennwort für alle Geräte mit dem Status `Set password` verwendet werden.
 - Wählen Sie bei Geräten, die dieses Protokoll unterstützen, **Enable HTTPS (HTTPS aktivieren)**, um es zu aktivieren.
- **Password type: unencrypted (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):** Auf dem Gerät liegt ein Problem mit dem Zertifikat vor.
- **Certificate about to expire (Zertifikat läuft ab):** Mindestens eines der Zertifikate auf dem Gerät läuft demnächst ab.
- **Certificate has expired (Zertifikat abgelaufen):** Mindestens eines der Zertifikate auf dem Gerät ist abgelaufen.
- **HTTPS certificate not trusted (HTTPS-Zertifikat nicht vertrauenswürdig):** Das HTTPS-Zertifikat auf dem Gerät wird von AXIS Camera Station Pro nicht als vertrauenswürdig eingestuft. Klicken Sie auf den Link, um ein neues HTTPS-Zertifikat auszustellen.
- **HTTP failed (HTTP-Verbindung fehlgeschlagen):** Es kann keine HTTP-Verbindung zum Gerät hergestellt werden.
- **HTTPS failed (HTTPS-Verbindung 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).
- **Address (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 74*.
- **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 74*.
- **Manufacturer (Hersteller):** Der Hersteller des Geräts.
- **Model (Modell):** Das Gerätemodell.
- **Firmware:** Die Firmwareversion, die das Gerät aktuell verwendet.
- **DHCP:** Zeigt an, ob das Gerät über DHCP mit dem Server verbunden ist.
- **HTTPS:** Der HTTPS-Status des Geräts. Zum HTTPS-Status siehe *Sicherheit, on page 72*.
- **IEEE 802.1X:** Der IEEE 802.1X-Status des Geräts. Zum IEEE 802.1X-Status siehe *Sicherheit, on page 72*.
- **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 und Systemzeit.

Hinweis

- Um den unbefugten Zugriff zu verhindern, sollten Sie nach der Wiederherstellung eines Geräts immer das Kennwort ändern.
- 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 Pro-Server 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 *Installation von Kamera-Anwendungen*.
- Wenn Sie Einstellungen auf der Konfigurationsseite eines Geräts geändert haben, laden Sie die Geräte neu.
- Geräte konfigurieren. Siehe *Geräte konfigurieren*.
- Benutzerverwaltung. Siehe *Benutzerverwaltung*.
- Zertifikate verwalten. Siehe *Sicherheit, on page 72*.
- Gerätedaten sammeln. Siehe *Gerätedaten sammeln*.
- Aktivieren Sie dieses Kontrollkästchen, um eine IP-Adresse oder einen Host-Namen zu verwenden. Siehe *Verbindung, on page 73*.
- Geräte mit Tags versehen. Siehe *Tags*.
- Anmeldeinformationen für Gerät eingeben. Klicken Sie mit der rechten Maustaste auf das Gerät und wählen Sie **Advanced (Erweitert) > Enter device credentials (Anmeldeinformationen für Gerät eingeben)** aus, um das Kennwort für das Gerät einzugeben.
- Auf der Registerkarte Konfiguration des Geräts das Gerät konfigurieren. Siehe *Registerkarte Gerätekonfiguration, on page 74*.

Zuweisen einer IP-Adresse

AXIS Camera Station Pro kann mehreren Geräten eine IP-Adresse zuweisen. Sie haben die Möglichkeit, neue IP-Adressen automatisch von einem DHCP-Server zu beziehen oder sie aus einem Adressbereich zuzuweisen.

IP-Adressen zuweisen

1. Gehen Sie zu **Konfiguration > Geräte > Management**, um die Geräte auszuwählen, 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 ein Gerät zur Zuweisung einer IP-Adresse auswählen, klicken Sie **Advanced (Erweitert)**, um die Seite **Assign IP address (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.
 - Im Bereich **Current IP address (Aktuelle IP-Adresse)** werden die aktuelle IP-Adresse, die Subnetzmaske und der Standard-Router angezeigt.
 - Bearbeiten Sie die Optionen im Bereich **New IP address (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 74*.

- Informationen zur Gerätekonfiguration finden Sie unter *Konfigurationsmethoden*.
- Informationen zur Erstellung einer Konfigurationsdatei finden Sie unter *Konfigurationsdatei erstellen*.
- Informationen zu den kopierbaren Einstellungen finden Sie unter *Konfigurationseinstellungen*.

Konfigurationsmethoden

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

Konfiguration des gewählten Gerätes verwenden

Hinweis

Diese Methode steht nur für ein einzelnes Gerät zur Verfügung und übernimmt einige oder alle der dort bereits vorhandenen Einstellungen.

1. **Configuration > Devices > Management** (Konfiguration > Geräte > Verwaltung) aufrufen.
2. Klicken Sie mit der rechten Maustaste auf ein Gerät und wählen Sie **Configure Devices (Geräte konfigurieren) > Configure (Konfigurieren)**.

3. Wählen Sie die Einstellungen, die Sie übernehmen möchten. Siehe *Konfigurationseinstellungen, on page 67*.
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. **Configuration > Devices > Management** (Konfiguration > Geräte > Verwaltung) aufrufen.
2. Klicken Sie mit der rechten Maustaste auf die Geräte und wählen Sie **Configure Devices (Geräte konfigurieren) > Configure (Konfigurieren)**. 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. Wählen Sie die Einstellungen, die Sie übernehmen möchten. Siehe *Konfigurationseinstellungen, on page 67*.
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 existieren.

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

Hinweis

Diese Methode darf nur von erfahrenen Nutzern verwendet werden.

1. **Configuration > Devices > Management** (Konfiguration > Geräte > Verwaltung) aufrufen.
2. Klicken Sie mit der rechten Maustaste auf die Geräte und wählen Sie **Configure Devices (Geräte konfigurieren) > Configure (Konfigurieren)**.
3. **Konfigurationsdatei** anklicken, um die Konfigurationsdatei aufzurufen. Informationen zur Erstellungen einer Konfigurationsdatei finden Sie unter *Konfigurationsdatei erstellen, on page 66*.
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 Sie dann auf andere Geräte anwenden. Informationen zur Verwendung von Konfigurationsdateien finden Sie unter *Konfigurationsmethoden*.

Die angezeigten Einstellungen sind die Einstellungen des Geräts, die über das AXIS Device Management erreichbar sind. Um eine bestimmte Einstellung zu finden, verwenden Sie das Feld **Suchwort eingeben**.

Eine Konfigurationsdatei erstellen:

1. **Configuration > Devices > Management** (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 Einstellungen, die das Verhalten eines Geräts steuern. Allgemeine Informationen und Parameter finden Sie im Benutzerhandbuch des Produkts auf www.axis.com

Hinweis

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

In einige Textfelder können Variablen eingefügt werden. Die Variablen werden durch Text ersetzt, bevor sie auf ein Gerät angewendet werden. Um eine Variable einzufügen, das Textfeld rechtsklicken und Folgendes wählen:

- **Insert device serial number variable (Variable zum Einfügen der Geräteseriennummer):** Diese Variable wird durch die Seriennummer des Geräts ersetzt, auf das die Konfigurationsdatei angewendet wird.
- **Insert device name variable (Variable zum Einfügen des Gerätenamens):** Diese Variable wird durch den Namen des Geräts ersetzt, das beim Anwenden der Konfigurationsdatei verwendet wird. Der Gerätename ist auf der Seite **Device management (Geräteverwaltung)** in der Spalte **Name** aufgeführt. Um ein Gerät umzubenennen, gehen Sie zur Seite **Cameras (Kameras)** oder **Other devices (Andere Geräte)**.
- **Insert server name variable (Variable zum Einfügen des Server-Namens):** Diese Variable wird durch den Namen des Servers ersetzt, der beim Anwenden der Konfigurationsdatei verwendet wird. Der Server-Name ist auf der Seite **Device management (Geräteverwaltung)** in der Spalte **Server** aufgeführt. Um einen Server umzubenennen, gehen Sie zur Dienststeuerung von AXIS Camera Station Pro.
- **Insert server time zone variable (Variable zum Einfügen der Server-Zeitzone):** Diese Variable wird durch die POSIX-Zeitzone des Servers ersetzt, der beim Anwenden der Konfigurationsdatei verwendet wird. Diese Option 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

- **Stream profiles (Videostreamprofil):** Ein Videostreamprofil ist eine vorprogrammierte Live-Ansichtskonfigurationsprofil für die Videocodierung sowie für Bild- und Toneinstellungen. Videostreamprofile können durch Kopieren auf andere Geräte übertragen werden.
- **Motion detection windows (Bewegungserkennungsfenster):** 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

Die Benutzerverwaltung erfolgt unter **Configuration (Konfiguration) > Devices (Geräte) > Management (Verwaltung)**.

Wenn Sie ein Kennwort einrichten oder Benutzer von mehreren Geräten entfernen, werden Benutzer, die nicht mehr auf allen Geräten verfügbar sind, mit  markiert. Alle Benutzer werden nur einmal angezeigt, selbst wenn sie auf verschiedenen Geräten unterschiedliche Rollen innehaben.

Hinweis

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

Kennwortrichtlinie

Bei einigen Geräten müssen Kennwörter bestimmte Kriterien erfüllen. Wenn für ein oder mehrere ausgewählte Geräte eine Kennwortrichtlinie gilt, wird der Indikator für die Kennwortstärke durch einen Indikator für die Kennwortrichtlinie ersetzt, der angibt, ob Ihr Kennwort der geltenden Richtlinie entspricht.

- Wenn keine Richtlinie gilt oder es sich um ein ONVIF-Gerät handelt, wird wie gewohnt der Indikator für die Kennwortstärke angezeigt.
- Wenn Sie mehrere Geräte mit unterschiedlichen Richtlinien ausgewählt haben, muss das Kennwort allen diesen Richtlinien entsprechen.
- Wenn das Kennwort die Anforderungen nicht erfüllt, wird **Non-compliant (Nicht konform)** angezeigt. Bewegen Sie den Mauszeiger über das Info-Symbol, um die geltenden Anforderungen anzuzeigen:

Längenrichtlinie – Das Kennwort muss mindestens 15 Zeichen lang sein.

Komplexitätsrichtlinie – Das Kennwort muss mindestens 12 Zeichen lang sein und einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten.

Beide Richtlinien – Sowohl die Anforderungen an die Länge als auch an die Komplexität müssen erfüllt werden.

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
- Ziffern 0-9
- Leerzeichen, Komma (,), Punkt (.), Doppelpunkt (:), Semikolon (;)
- !, ", #, \$, %, &, ', (, +, *, -, ., /, <, >, =, ?, [, \, ^, _`, {, |, ~, @,], }

Zum Festlegen eines Kennworts für Benutzer auf gewählten Geräten:

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 (Erzeugen)**, um ein starkes Kennwort erzeugen zu lassen.
5. Klicken Sie auf **OK**.

Hinweis

Wenn Sie die Option **Use this password for all devices without a factory default password (Kennwort für alle Geräte ohne werkseitiges Standardkennwort verwenden)** auswählen, gilt das Kennwort für alle Geräte mit dem Status **Set password (Kennwort festlegen)**. Sollte die Länge des Kennworts die von bestimmten Geräten unterstützte Höchstlänge überschreiten, werden Sie hierüber vor dem Öffnen des Dialogfelds informiert und können bei Bedarf ohne diese Geräte fortfahren.

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. Eine Liste zulässiger Zeichen finden Sie im Abschnitt **Set password (Kennwort festlegen)** oben.
4. Wählen Sie die Benutzerrechte in der Auswahlliste **Role (Rolle)** aus:
 - **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. **Enable PTZ control (PTZ-Steuerung aktivieren)**: Aktivieren Sie dieses Kontrollkästchen, um den Benutzer zum Schwenken, Neigen und Zoomen in der Live-Ansicht zu berechtigen.
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 in der Auswahlliste **User (Benutzer)** den Benutzer aus, den Sie entfernen möchten.
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 Sucheingabefeld **Type to search (Suchwort eingeben)**, um Benutzer in der Liste zu suchen.

Aktualisieren der Firmware

Als Firmware gilt jene Software, die die Funktionalität Ihres Axis Produkts bestimmt. Durch die fortlaufende Aktualisierung Ihrer Firmware stellen Sie sicher, dass Ihr Gerät stets über die neuesten Funktionen und Optimierungen verfügt.

Neue Firmware kann über AXIS Camera Station Pro heruntergeladen oder aus einer Datei auf einer Festplatte oder Speicherkarte importiert werden. Zum Download verfügbare Firmware-Versionen sind mit dem Vermerk **(Download)** nach der Versionsnummer gekennzeichnet. 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.
- **Factory default (Werkseitige Standardeinstellung):** Aktualisieren Sie auf die ausgewählte Firmware-Version und setzen Sie alle Einstellungen auf die werkseitige Standardeinstellung 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 **Invalid devices (Ungültige Geräte)** angezeigt. **Continue (Fortfahren)** anklicken, um die Geräte, die nicht konfiguriert werden können, zu überspringen.
4. Während der Aktualisierung der Firmware ist das Gerät nicht zugänglich. Klicken Sie zum Fortfahren auf **Ja**. Wenn Sie diese Meldung nicht erneut anzeigen möchten, wählen Sie **Do not show this dialog again (Diesen Dialog nicht mehr anzeigen)** aus und klicken Sie auf **Yes (Ja)**.
5. Das Dialogfeld **Upgrade firmware (Firmware aktualisieren)** führt das Gerätemodell, die Anzahl der Geräte jedes Modells, die vorhandene Firmware-Version, die verfügbaren Firmware-Versionen für die Aktualisierung und den Upgrade-Typ an. 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 zu aktualisierenden Geräte, die gewünschten Firmware-Versionen und den Upgrade-Typ aus.
 - 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*.



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

Installation von Kamera-Anwendungen

Eine Kamera-Anwendung ist eine Software, die in Netzwerk-Video-Produkte von Axis hochgeladen und dort installiert werden kann. Die Anwendungen erweitern den Funktionsumfang des Geräts, z. B. Erfassungs-, Erkennungs-, Objektverfolgungs- 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 Nutzung der Anwendung eine Lizenz erforderlich ist, können Sie die Lizenzschlüsseldatei entweder gleichzeitig mit der Anwendung oder später auf der Konfigurationsseite des Geräts installieren.

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-Version 6.50 oder neuer installieren. In den Versionshinweisen des Produkts 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-Version 5.60 oder neuer installieren.

AXIS Video Content Stream – Diese Anwendung ermöglicht Axis Kameras das Senden von Daten zur Bewegungsverfolgung an AXIS Camera Station Pro. Sie kann auf Kameras mit Firmware der Versionen 5.50 bis 9.59 installiert werden. AXIS Video Content Stream erfordert AXIS Camera Station Pro.

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

Um Kameraanwendungen zu installieren:

1. **Configuration > Devices > Management** (Konfiguration > Geräte > Verwaltung) aufrufen.
2. Wählen Sie die Kameras, auf denen Sie die Anwendungen installieren möchten. Klicken Sie  oder rechtsklicken und **Kamera-Anwendung installieren** wählen.
3. Wählen Sie die Kamera-Anwendung aus, die Sie 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

Bei einem Downgrade oder Überschreiben der Anwendung werden deren Einstellungen auf den Geräten zurückgesetzt.

5. Wenn eine Anwendung eine Lizenz erfordert, erscheint das Dialogfenster **Install licenses (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

Zur Installation von AXIS Video Motion Detection 2, AXIS Video Motion Detection 4 oder AXIS Video Content Stream ist keine Lizenz erforderlich.

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 IEEE 802.1X aktivieren, signiert die Zertifizierungsstelle (CA) von AXIS Camera Station Pro Zertifikate für Clients und Server und verteilt sie automatisch an Geräte. Die CA ignoriert vorinstallierte Zertifikate. Weitere Informationen zur Konfiguration von Zertifikaten finden Sie unter *Zertifikate, on page 145*.

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. **Configuration > Devices > Management** (Konfiguration > Geräte > Verwaltung) aufrufen.
2. Rechtsklicken Sie die Geräte:
 - Wählen Sie **Security (Sicherheit) > HTTPS > Enable/Update (Aktivieren/Aktualisieren)**, um HTTPS zu aktivieren oder die HTTPS-Einstellungen für die Geräte zu aktualisieren.
 - Wählen Sie **Security (Sicherheit) > IEEE 802.1X > Enable/Update (Aktivieren/Aktualisieren)**, um IEEE 802.1X zu aktivieren oder die IEEE 802.1X-Einstellungen für die Geräte zu aktualisieren.
 - Wählen Sie **Security (Sicherheit) > HTTPS > Disable (Deaktivieren)**, um HTTPS für Geräte zu deaktivieren.
 - Wählen Sie **Security (Sicherheit) > IEEE 802.1X > Disable (Deaktivieren)**, um IEEE 802.1X für die Geräte zu 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. Beim Löschen wird das Zertifikat 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 für die Verbindung mit dem Gerät.
	Aus	AXIS Camera Station Pro verwendet HTTP für die Verbindung mit dem Gerät.
	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. Sie erlaubt es Ihnen, eine .zip-Datei mit einem Datensammelbericht für einen bestimmten Speicherort auf den gewählten Geräten zu erstellen.

Gerätedaten erfassen:

1. **Configuration > Devices > Management** (Konfiguration > Geräte > Verwaltung) aufrufen.
2. Die Geräte rechtsklicken und **Gerätedaten erfassen** wählen.
3. Im Bereich **Data source on selected devices (Datenquelle für ausgewählte Geräte)**:
 - Klicken Sie **Voreinstellung** und wählen Sie einen aus dem Aufklappmenü der meist genutzten Befehle.

Hinweis

Einige Voreinstellungen werden nicht von allen Geräten unterstützt. Z. B. funktioniert der PTZ-Status nicht bei Audiogeräten.

- Klicken Sie **Benutzerdefiniert** und geben Sie den Pfad zur Datensammlung auf den gewählten Servern an.
4. Geben Sie im Bereich **Save as (Speichern als)** 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 von IP-Adresse oder Host-Name:

1. **Configuration > Devices > Management** (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 Porteeinstellungen wählen Sie **Edit (Bearbeiten)** aus.

Tags

Tags helfen Ihnen bei der Organisation Ihrer Geräte auf der Seite **Device management (Geräteverwaltung)**. Ein Gerät kann mehrere Tags besitzen.

Sie können Geräte nach Modell, Einsatzort oder anderen Kriterien mit einem Tag kennzeichnen. Wenn Sie beispielsweise Geräte nach Modell mit einem Tag kennzeichnen, können Sie alle Kameras dieses Modells schnell finden und aktualisieren.

Geräte mit einem Tag versehen:

1. **Configuration > Devices > Management** (Konfiguration > Geräte > Verwaltung) aufrufen.
2. Ein Gerät rechtsklicken und **Geräte mit Tags versehen** wählen.
3. Gehen Sie zu **Use existing tag (Vorhandenes Tag verwenden)** und wählen Sie ein Tag aus oder gehen Sie zu **Create a new tag (Neues Tag erstellen)** und geben Sie einen Namen für das Tag 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. Wählen Sie im Ordner **Tags** ein Tag. Es werden alle Geräte mit diesem Tag angezeigt.
3. Wählen Sie die Geräte aus, klicken Sie mit der rechten Maustaste und wählen Sie **Untag devices** (Tag für Geräte entfernen).
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 **Device tags (Geräte-Tags)**:
 - 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.
 - Klicken Sie auf , um die Seite **Device tags (Geräte-Tags)** anzuheften.
 - Klicken Sie auf ein 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. **Configuration > Devices > Management** (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. Das Gerät wird neu geladen, um die Änderungen in AXIS Camera Station Pro zu übernehmen.

Einschränkungen

- Die automatische Authentifizierung für Geräte von Drittanbietern wird nicht unterstützt.
- Für Geräte anderer Hersteller kann kein Support garantiert werden.
- Aktive Videostreams aus der Registerkarte mit der Gerätekonfiguration erhöhen die Server-Last und können die Leistung des Server-Computers beeinträchtigen.

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 45.

Gehen Sie zu **Configuration (Konfiguration) > Devices (Geräte) > External data sources (Externe Datenquellen)**, 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 eine externe Datenquelle mit einer Ansicht konfiguriert wurde, werden die von der Datenquelle erzeugten Daten in der Zeitleiste der Ansicht auf der Registerkarte **Data search (Datensuche)** automatisch mit Lesezeichen versehen. So verbinden Sie eine externe Quelle 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 zu **Configuration (Konfiguration) > Devices (Geräte) > Time synchronization (Zeitsynchronisierung)**, um die Seite **Time synchronization (Zeitsynchronisierung)** zu öffnen.

AXIS Camera Station Pro zeigt eine Liste aller hinzugefügten Geräte an. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie die Spalten aus, die angezeigt werden sollen. Die Reihenfolge der Spalten können Sie ändern, indem Sie die Kopfzeile einer Spalte anklicken und an eine andere Position ziehen.

Die folgenden Informationen wird in der Geräteliste angezeigt:

- **Name:** Wenn das Gerät ein Video-Encoder mit mehreren angeschlossenen Kameras oder eine Netzwerk-Kamera mit mehreren Ansichtsbereichen ist, wird der Gerätenamen oder eine Liste aller zugeordneten Kameranamen angezeigt.
- **Address (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 74*.
- **MAC address (MAC-Adresse):** Die MAC-Adresse des Geräts.
- **Model (Modell):** Das Gerätemodell.
- **Enabled (Aktiviert):** Zeigt an, ob die Zeitsynchronisierung eingeschaltet ist.
- **NTP source (NTP-Quelle):** Die für das Gerät konfigurierte NTP-Quelle.
 - **Static (Statisch):** Die NTP-Server des Geräts werden manuell unter **Primary NTP server (Primärer NTP-Server)** und **Secondary NTP server (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.

- **Primary NTP server (Primärer NTP-Server):** Der für das Gerät konfigurierte primäre NTP-Server. Nur verfügbar, wenn **Statisch** ausgewählt ist.
- **Secondary NTP server (Sekundärer NTP-Server):** Die für das Gerät konfigurierte sekundäre NTP-Server-Konfiguration. Nur verfügbar für AXIS Geräte, die sekundäres NTP unterstützen und wenn **Statisch** ausgewählt ist.
- **Server time offset (Serverzeitversatz):** Der Zeitunterschied zwischen Gerät und Server.
- **UTC time (UTC-Zeit):** Die koordinierte Weltzeit (UTC) auf dem Gerät.
- **Synched (Synchronisiert):** Zeigt an, ob die Einstellungen zur Zeitsynchronisation angewendet wurden. Nur für Geräte mit Firmware 9.1 oder höher verfügbar.
- **Time to next sync (Zeit 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 (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 **Static (Statisch)** ausgewählt haben, konfigurieren Sie den primären und sekundären NTP-Server.
5. Klicken Sie auf **Anwenden**.

Send alarm when the time difference between server and device is more than 2 seconds (Bei einer Zeitdifferenz zwischen Server und Gerät über 2 Sekunden Alarm senden)	Aktivieren Sie diese Option, um bei einer Zeitdifferenz zwischen Server und Gerät von mehr als 2 Sekunden einen Alarm ausgeben zu lassen.
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 **Configuration (Konfiguration) > Storage (Speicher) > Management (Verwaltung)**, um die Seite **Manage storage (Speicherverwaltung)** zu öffnen. Hier erhalten Sie eine Übersicht über den lokalen Speicher und den Netzwerk-Speicher in AXIS Camera Station Pro.

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 • Storage full (Speicher voll): Der Speicher ist voll. Das System überschreibt die ältesten freigegebenen Aufzeichnungen. • Unavailable (Nicht verfügbar): Die Speicherinformationen sind zurzeit nicht verfügbar. Dies kann der Fall sein, wenn ein Netzwerk-Speicher entfernt oder getrennt wurde. • Intruding data (Stördaten): 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. • No permissions (Keine Berechtigungen): Der Benutzer hat keine Lese- oder Schreibberechtigung für den Speicher. • Low space (Wenig freier Speicher): 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. • Insufficient capacity (Unzureichende Speicherkapazität): 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. Falls eine der physischen Festplatten des RAID-Systems ausfällt, ist Redundanz gegeben. • Degraded (Verringert): Eine der physischen Festplatten des RAID-Systems ist defekt. Die Aufzeichnung und die Wiedergabe von gespeicherten Aufzeichnungen sind weiterhin möglich. Es ist jedoch keine Redundanz gegeben. 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). • Syncing (Synchronisierung): Die RAID-Festplatten werden synchronisiert. Die Aufzeichnung und die Wiedergabe von gespeicherten Aufzeichnungen sind weiterhin möglich. Es ist jedoch keine Redundanz gegeben, falls 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. • Failure (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) . Siehe <i>Speicher verwalten, on page 78</i> .
Free (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 **Configuration (Konfiguration) > Storage (Speicher) > Management (Verwaltung)**, um die Seite **Manage storage (Speicherverwaltung)** zu öffnen. Hier können Sie den Ordner angeben, in dem die Aufzeichnungen gespeichert werden sollen. Um zu verhindern, dass der Speicher voll wird, legen Sie den Speicherplatz, den AXIS Camera Station Pro maximal nutzen darf, als Prozentsatz der Gesamtspeicherkapazität fest. 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 Speicherort im Auswahlmenü aus.
4. Zum Hinzufügen eines freigegebenen Netzwerklaufwerks wählen Sie **Shared network drive (Freigegebenes Netzwerklaufwerk)** und geben Sie dessen Pfad 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 den jeweiligen Speicher aus der Speicherliste aus und klicken Sie auf **Remove (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 Ordernamen 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 erforderliche Mindestgröße eines Speichers, der zu AXIS Camera Station Pro hinzugefügt wird, beträgt 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 Speicherplatz freizugeben.

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 gesammelt 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 Daten)** zugreifen zu können, benötigen Sie Zugriff auf den Server. AXIS Camera Station Pro organisiert die Daten zunächst nach Servern und anschließend nach den mit diesem Server verbundenen Geräten.

Sie können eine verlorene Aufzeichnung oder ein verlorenes Protokoll suchen oder die Inhalte 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. Gehen Sie nach Abschluss der Aufgabe zu **Alarms and Tasks (Alarme und Aufgaben) > Tasks (Aufgaben)** 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 **Configuration (Konfiguration) > Storage (Speicher) > Selection (Auswahl)**, um die Seite **Select storage (Speicher auswählen)** zu öffnen. Auf der Seite wird eine Liste aller Kameras in AXIS Camera Station Pro angezeigt. Hier können Sie festlegen, wie viele Tage die Aufzeichnungen bestimmter Kameras gespeichert werden sollen. Bei Auswahl dieser Option werden die Speicherinformationen unter **Recording storage (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 Gerätenamen 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 <i>Registerkarte Gerätekonfiguration, on page 74</i> .
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.
SD card playback (Wiedergabe von SD-Karte)	Hier wird angezeigt, ob die Konfiguration der Kamera die direkte Wiedergabe von Aufzeichnungen von ihrer SD-Karte in AXIS Camera Station Pro ohne Zwischenablage auf dem Server erlaubt.
Failover-Aufzeichnung	Hier wird angezeigt, ob die Kamera die ausfallsichere Aufzeichnung nutzt.
Copy to ACS Pro (Zu ACS Pro kopieren)	Hier wird angezeigt, ob die Aufzeichnungen von der SD-Karte zu AXIS Camera Station Pro kopiert werden.
Ausweichoption-Aufzeichnung	Hier wird angezeigt, ob die Kamera die Fallback-Aufzeichnung nutzt.
Server	Der Server, auf dem der lokale Speicher oder der Netzwerk-Speicher angelegt ist.

Die Speichereinstellungen für die einzelnen Kameras wurden beim Hinzufügen der Kameras zu AXIS Camera Station Pro 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. Wählen Sie unter **SD card storage (SD-Kartenspeicher)** nach Bedarf die Optionen **Playback of SD card recordings (Aufzeichnungen von SD-Karte wiedergeben)**, **Failover recording (Ausfallsichere Aufzeichnung)** und **Copy SD card recordings to ACS Pro server (SD-Kartenaufzeichnungen auf ACS-Server kopieren)** aus.
5. Klicken Sie auf **Anwenden**.

Aufzeichnungsspeicher Hinweis • Um eine SD-Karte als Aufzeichnungsspeicher nutzen zu können, muss das Gerät VAPIX unterstützen und eine SD-Karte von Axis verwendet werden. • Die SD-Kartenfunktionen unterstützen das M-JPEG-Format nicht. • Aufzeichnungen auf der SD-Karte werden von AXIS Camera Station Pro nicht gelöscht. Die Speicherdauer wird durch die entsprechende Einstellung für die SD-Karte in der Kamera festgelegt.	
Store to (Speichern auf)	Wählen Sie aus dem Auswahlmenü den Speicherort für Aufzeichnungen aus. Verfügbare Optionen sind der lokale Speicher und Netzwerk-Freigaben.
Aufbewahrungszeit	• Unlimited (Unbegrenzt): Aufzeichnungen werden so lange gespeichert, bis der Speicher voll ist. • Limited (Begrenzt): Legen Sie die maximale Speicherdauer für Aufzeichnungen in Tagen fest. 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.

SD-Kartenspeicher	
Playback SD card recordings (Aufzeichnungen von SD-Karte wiedergeben)	Aktivieren Sie diese Option, um Aufzeichnungen in AXIS Camera Station Pro ohne Zwischenablage auf dem Server direkt von der SD-Karte der Kamera wiederzugeben. In der Zeitleiste angezeigte Aufzeichnungen auf der SD-Karte können außerdem exportiert werden. Diese Funktion erfordert AXIS OS 5.60 oder höher.
Failover-Aufzeichnung	Wählen Sie diese Option aus, um Aufzeichnungen auf der SD-Karte der Kamera zu speichern, wenn die Verbindung zu AXIS Camera Station Pro unterbrochen wird. Diese Funktion ist nur für Kameras mit SD-Speicherkarte und Firmware-Version 5.20 oder höher verfügbar.
SD-Kartenaufzeichnungen auf ACS-Server kopieren	Wählen Sie diese Option, um alle Aufzeichnungen auf der SD-Karte der Kamera auf den Server zu kopieren. Verwenden Sie die Option Schedule (Zeitplan) , um den Zeitpunkt für das Kopieren der Aufzeichnungen festzulegen. Die Standardeinstellung für den Zeitplan ist Always (Immer) .

Aufzeichnung und Ereignisse konfigurieren

Beim Hinzufügen von Kameras zu AXIS Camera Station Pro konfiguriert das System automatisch die bewegungsgesteuerte oder kontinuierliche Aufzeichnung. Sie können die Aufzeichnungsmethode später an Ihre Bedürfnisse anpassen. Siehe *Aufzeichnungsmethode*, on page 88.

Bewegungsaufzeichnung

Die Bewegungserkennung wird von allen Netzwerkkameras und Video-Encodern von Axis unterstützt. Die nur bei einer Bewegung ausgelöste Aufzeichnung 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 zum Beispiel festlegen, was passiert, wenn die Kamera zu viele oder zu 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 im Auswahllisten unter **Profile (Profil)** ein Profil aus. Standardmäßig ist das Profil **High (Hoch)** ausgewählt.
6. Wählen Sie einen Zeitplan oder klicken Sie auf **New schedule... (Neuer Zeitplan...)**, um einen neuen benutzerdefinierten Zeitplan zu erstellen.
7. Legen Sie Zeitwerte für Vor- und Nachpuffer sowie die Auslösedauer fest.
8. Klicken Sie auf **Anwenden**.

Hinweis

Die Bewegungsaufzeichnung kann über Aktionsregeln konfiguriert werden. Achten Sie vor der Nutzung von Aktionsregeln darauf, dass **Motion detection (Bewegungserkennung)** unter **Recording method (Aufzeichnungsmethode)** deaktiviert ist.

Profil	Verwenden Sie eine niedrigere Auflösung, um die Aufzeichnungsgröße zu verringern. Zur Bearbeitung der Profileinstellungen siehe <i>Videostreamprofile</i> .
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)	Legt den zeitlichen Mindestabstand zwischen zwei Auslösern fest, um die Anzahl aufeinanderfolgender Aufzeichnungen zu reduzieren. Tritt innerhalb dieses Intervalls ein weiterer Auslöser ein, wird die Aufzeichnung fortgesetzt und die Auslösedauer neu gestartet.
Benachrichtigungen	Wenn die Kamera eine Bewegung erkennt, wird eine Benachrichtigung gesendet. Wird die Option Mobile App aktiviert, sendet diese eine Push-Benachrichtigung an die AXIS Camera Station Mobile App. Bei Auswahl der Option Server alarm (Serveralarm) wird in AXIS Camera Station Pro ein Alarm ausgelöst.



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

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, die Funktion in Verbindung mit der Bewegungserkennung oder der kontinuierlichen Aufzeichnung zu nutzen, damit 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**.
- Objekterkennungseignisse 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 eine Einstellung für Profile (Profil) . Hoch (High) ist die standardmäßige Profileinstellung. Verwenden Sie eine niedrigere Auflösung, um die Aufzeichnungsgröße zu verringern. Zur Bearbeitung der Profileinstellungen siehe <i>Videostreamprofile</i> .
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 <i>Ereigniskategorien, on page 29</i> .
Vorpufer:	Legen Sie die Anzahl der Sekunden vor der Erkennung des Objekts fest, die in eine Aufnahme einbezogen werden sollen.
Nachpufer:	Legen Sie die Anzahl der Sekunden nach der Erkennung des Objekts fest, die in eine Aufnahme einbezogen werden sollen.
Trigger period (Auslösedauer)	Legen Sie ein Mindestintervall zwischen aufeinanderfolgenden Auslösern fest, um übermäßig viele aufeinanderfolgende Einzelaufzeichnungen zu vermeiden. Tritt innerhalb dieses Intervalls ein weiterer Auslöser ein, wird die Aufzeichnung fortgesetzt und der Auslösezeitraum neu gestartet.
Benachrichtigungen	Sendet Ihnen eine Benachrichtigung, sobald AXIS Object Analytics ein Objekt erfasst. Wird die Option Mobile App aktiviert, sendet diese eine Push-Benachrichtigung an die AXIS Camera Station Mobile App. Server alarm (Serveralarm) löst einen Alarm in AXIS Camera Station Pro aus.

Kontinuierliche und geplante Aufzeichnung

Bei der kontinuierlichen Aufzeichnung werden Bilder fortlaufend gespeichert, weswegen sie mehr Speicherplatz als andere Aufzeichnungsoptionen benötigt. Um die Dateigröße zu reduzieren, sollten Sie stattdessen 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)**.
4. Nehmen Sie Ihre Einstellungen vor. Weitere Informationen finden Sie in der Tabelle unten.
5. Klicken Sie auf **Anwenden**.

Profil	Wählen Sie im Auswahlménú die Option Profile (Profil) . Die Standardeinstellung für das Profil ist High (Hoch) . Verwenden Sie eine niedrigere Auflösung, um die Aufzeichnungsgröße zu verringern. Zur Bearbeitung der Profileinstellungen siehe <i>Videostreamprofile</i> .
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, um eine maximale Bitratengrenze zur Beschränkung des Speicherbedarfs festzulegen. 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 <i>Durchschnittliche Bitrate einstellen, on page 88</i>).

Manuelle Aufzeichnung

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 im Auswahlménú die Option Profile (Profil) . Die Standardeinstellung für das Profil ist High (Hoch) . Verwenden Sie eine niedrigere Auflösung, um die Aufzeichnungsgröße zu verringern. Zur Bearbeitung der Profileinstellungen siehe <i>Videostreamprofile</i> .
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)	Diese Option fügt bei jedem Start einer manuellen Aufzeichnung Details zu dieser als Lesezeichen ein. Lesezeichen helfen Ihnen dabei, bestimmte Aufzeichnungen später leichter wiederzufinden und zu identifizieren. Diese Einstellung ist nur für Bediener und Administratoren verfügbar und standardmäßig deaktiviert.
Dauer maximal	Legen Sie die maximale Länge einer Aufzeichnung ohne Vorpuffer- und Nachpufferzeiten fest. Für eine unbegrenzte Dauer stellen Sie 0 ein.

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

Durch Regeln ausgelöste 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

Verwenden Sie die ausfallsichere Aufzeichnung, um Aufzeichnungen bei einem Ausfall der Verbindung zu AXIS Camera Station Pro auf der SD-Karte der Kamera zu speichern.

AXIS Camera Station Pro wählt die Methode der Ausfallsicherung automatisch anhand der Firmware-Version der Kamera aus:

- **Firmware-Version 11.11.42 oder höher:** Die ausfallsichere Aufzeichnung beginnt, sobald die Kamera den Kontakt zum Server verliert.
- **Ältere Firmware-Versionen:** Die ausfallsichere Aufzeichnung beginnt nur bei einem unerwarteten Verbindungsabbruch. Geplante Server-Neustarts lösen die ausfallsichere Aufzeichnung nicht aus.

Informationen zur Konfiguration der ausfallsicheren Aufzeichnung finden Sie unter *Das anzuschließende Geräte wählen, on page 80*.

Hinweis

- Wenn vor einer Aktualisierung die Option **Failover recording (Ausfallsichere Aufzeichnung)** aktiviert war, wird die Option **Copy SD card recordings to ACS Pro server (SD-Kartenaufzeichnungen auf ACS-Server kopieren)** automatisch aktiviert.
- Die Aufzeichnungen auf der SD-Karte werden von AXIS Camera Station Pro nicht gelöscht. Die Speicherdauer wird durch die in der Kamera eingestellte Aufbewahrungsdauer für die SD-Karte vorgegeben.
- Die Aktivierung der ausfallsicheren Aufzeichnung setzt alle bestehenden Einstellungen zur Ausfallsicherung für diese Kamera auf anderen Servern außer Kraft.
- Die ausfallsichere Aufzeichnung kann jeweils nur für einen AXIS Camera Station Pro-Server pro Kameraansicht aktiv sein.

Sobald die Verbindung bei aktivierter Option **Copy SD card recordings to ACS Pro server (SD-Kartenaufzeichnungen auf ACS-Server kopieren)** wiederhergestellt ist, werden die Aufzeichnungen auf den Server kopiert und in der Zeitleiste dunkelgrau markiert. Die Kamera verwendet einen 20-sekündigen Vor- und Nachpuffer, daher kann es dennoch zu kurzen Aufzeichnungslücken von etwa 1 bis 4 Sekunden kommen.

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.



SD-Karte für Failover-Aufzeichnung verwenden

Ausweichoption–Aufzeichnung

Sie können auf einem Gerät, das als Aufzeichnungsspeicher AXIS S3008 Recorder verwendet, Fallback–Aufzeichnung aktivieren. Nach der Aktivierung startet das Gerät automatisch die kontinuierliche Aufzeichnung, sobald die Verbindung zwischen AXIS Camera Station Pro und dem Recorder abbricht. Das Gerät verwendet für Fallback–Aufzeichnungen das Videostreamprofil „Medium“ (Mittel).

Hinweis

- Diese Funktion erfordert AXIS Camera Station 5.36 oder höher, AXIS S3008 Recorder Firmware 10.4 oder höher sowie Axis Geräte–Firmware 5.50 oder höher.
- Falls zum Startzeitpunkt der Fallback–Aufzeichnung bereits eine kontinuierliche Aufzeichnung läuft, beginnt eine neue kontinuierliche Aufzeichnung. Das System erstellt Duplikate des Videostreams auf dem Rekorder.

Fallback–Aufzeichnung aktivieren:

1. Stellen Sie sicher, dass Sie den AXIS S3008 Recorder sowie die erforderlichen Geräte hinzugefügt und den Recorder 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 bewegungsgesteuerte oder kontinuierliche Aufzeichnung.

Ein Häkchen zeigt an, welche Aufzeichnungsmethode ein Gerät verwendet. Zum Anpassen der Profileinstellungen für Video und Audio, siehe *Videostreamprofile*.

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. Auf dem Bildschirm **Recording method (Aufzeichnungsmethode)** können Sie eine Aufzeichnungsmethode ein- oder ausschalten.

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 Ziel-Bitrate erreichen und eine angemessene Videoqualität auf Grundlage des angegebenen Speichers erreichen.

Hinweis

- Diese Option ist nur für die kontinuierliche Aufzeichnung verfügbar. Die Kameras müssen die durchschnittliche Bitrate unterstützen und die Firmware-Version 9.40 oder höher nutzen.
 - Die Einstellungen der durchschnittlichen Bitrate beeinflussen die Qualität des ausgewählten Videostreamprofils.
1. Gehen Sie zu **Configuration (Konfiguration) > Storage (Speicher) > Selection (Auswahl)** und stellen Sie sicher, dass eine begrenzte Aufbewahrungszeit für die Kamera eingestellt 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. Sie garantiert nur, dass die Aufzeichnungen den angegebenen Speicherplatz nicht überschreiten, aber nicht, dass ausreichend Platz für die Aufzeichnungen 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

AXIS Video Motion Detection 2 und 4 sind Kamera-Anwendungen für Produkte, die 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 *Installation von Kamera-Anwendungen*.

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

- **Area of interest (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).
- **Area to exclude (Ausschlussbereich):** Ein Ausschlussbereich ist ein Bereich innerhalb des ausgewählten Bereichs, in dem sich bewegende Objekte ignoriert werden sollen.
- **Ignore filters (Ignorier-Filter):** Filter, die erstellt werden, um sich bewegende Objekte zu ignorieren, die von der Anwendung erkannt werden. 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.
 - **Short-lived objects filter (Filter für nur kurz erscheinende Objekte):** Dieser Filter ignoriert Objekte, die nur für kurze Zeit in einem Bild auftauchen. Das sind 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 Anwendung gemessen. Der Filter verzögert Alarmer und löst diese nicht aus, wenn das Objekt das Bild innerhalb der angegebenen Zeit verlässt.
 - **Small objects filter (Filter für kleine Objekte):** Dieser Filter ignoriert kleine Objekte, wie beispielsweise 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.
 - **Swaying objects filter (Filter für schaukelnde Objekte):** Dieser Filter ignoriert Objekte, die sich nur über eine kurze Distanz hin- und herbewegen wie etwa Zweige und Fahnen im Wind sowie deren Schatten. Die Distanz wird als Prozentwert des Gesamtbildes angegeben. 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

Diese Einstellungen werden direkt auf die Kamera angewendet.

1. **Konfiguration > Aufzeichnung und Ereignisse > Aufzeichnungsmethode aufrufen.**
2. Wählen Sie eine Kamera mit AXIS Video Motion Detection 2 oder 4 und klicken Sie auf **Motion Settings (Bewegungseinstellungen)**.
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 mehrere Ein- und Ausschlussbereiche verwenden und einen Ausschlussbereich innerhalb eines Einschlussbereichs festlegen, um bestimmte Bewegungen zu ignorieren.

So können Sie einen Einschlussbereich hinzufügen und bearbeiten:

Hinweis

Diese Einstellungen werden direkt auf die Kamera angewendet.

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 Bearbeitungsbereich anzuzeigen, wählen Sie die Option **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 (Empfindlichkeit)** an.
8. Zur Verwendung der Voreinstellungen wählen Sie **Low (Niedrig)**, **Moderate (Mittel)**, **High (Hoch)** oder **Very High (Sehr hoch)** aus. **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 lösen Objekte eine Bewegungserkennung über einen langen Zeitraum aus. 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 auf dem Bildschirm **Edit Motion Detection (Bewegungserkennung bearbeiten)** im Bereich **Window (Fenster)** 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 die Suche von Aufzeichnungen eines bestimmten Typs. So erstellen Sie eine Ereigniskategorie:

1. Rufen Sie **Configuration (Konfiguration) > Recording and events (Aufzeichnung und Ereignisse) > Event categories (Ereigniskategorien)** auf.
2. Klicken Sie auf **New (Neu)**.
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 überschreitet. Die benutzerdefinierte Aufbewahrungszeit der Ereigniskategorie gilt nur, wenn sie länger ist als der Standard.

Weitere Informationen, siehe *Ereigniskategorien*, on page 29.

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 Sie den Server im Auswahlménü **Selected server (Ausgewählter Server)** auswählen.
- 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 zur Konfiguration der I/O-Ports finden Sie im Benutzerhandbuch oder in 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)**. Passen Sie sie bei Bedarf an.
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, den dieser aufweisen soll, wenn sich AXIS Camera Station Pro mit dem Gerät verbindet. Wählen Sie **On startup set to (Beim Start festlegen auf)** und wählen Sie den Anfangszustand im Auswahlmenü **State (Status)** aus.

Edit (Bearbeiten):	Um einen Port zu bearbeiten, wählen Sie den Port aus und klicken Sie auf Edit (Bearbeiten) . Aktualisieren Sie die Port-Informationen im Dialogfenster und klicken Sie auf OK .
Entfernen	Um einen Port zu entfernen, wählen Sie den Port aus und klicken Sie auf Remove (Entfernen) .
E/A-Ports neu laden	Wenn I/O-Ports über die Setup-Seite 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 mit mehreren AXIS Camera Station Pro-Servern können zur Überwachung der E/A-Ports jeden verbundenen Server im Auswahlmenü **Selected Server (Ausgewählter Server)** auswählen.

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. Einige dieser Aktionen erfordern eine zusätzliche Konfiguration des Geräts.

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 diesen und klicken Sie auf **OK**. Weitere Informationen finden Sie unter *Auslöser hinzufügen*.
6. Wählen Sie unter **Actions (Aktionen)** die Option **Add... (Hinzufügen...)** und dann den Typ der Aktion aus, konfigurieren Sie diese und klicken Sie auf **OK**. Weitere Informationen finden Sie unter *Aktionen hinzufügen*.
7. Klicken Sie auf **Anwenden**.
 - Die Regel wird automatisch aktiviert, wenn Sie sie speichern.

Edit (Bearbeiten):	Um eine vorhandene Regel zu bearbeiten, wählen Sie die Regel aus und klicken Sie auf Edit (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, wobei eine Regel mehrere Auslöser haben kann. 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)**. Wenn Sie diese Einstellung in Verbindung mit Impulsauslösern verwenden, stellen Sie eine längere Auslösedauer ein. 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 95*.

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 96*.

Systemereignis und Fehler – Der Auslöser Systemereignis und Fehler wird aktiviert, wenn Aufnahmefehler auftreten, ein Speicher voll ist, die Verbindung eines Netzwerk-Speichers ausfällt oder die Verbindung zu einem oder mehreren Geräten unterbrochen wird. Siehe *Systemereignis- und Fehler-Auslöser erstellen, on page 96*.

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 97*. Es wird empfohlen, 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 98*.

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 103*.

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 104*.

HTTPS (extern) – Der Auslöser HTTPS extern ermöglicht es externen Anwendungen, über eine HTTPS-Verbindung Ereignisse in AXIS Camera Station Pro auszulösen. Siehe *Externen HTTPS-Auslöser erstellen, on page 105*.

Bewegungserkennungsauslöser erstellen

Der Auslöser Bewegungserkennung wird aktiviert, wenn die gewählte Kamera innerhalb eines bestimmten Bereichs eine Bewegung erkennt. Da die Erkennung in der Kamera erfolgt, trägt sie nicht zur Rechenlast von AXIS Camera Station Pro bei.

Hinweis

Verwenden Sie keine Auslöser für die Bewegungserkennung zum Start von Aufzeichnungen, wenn die bewegungsbedingte Aufzeichnung bereits in der Kamera aktiviert ist. Schalten Sie die Bewegungsaufzeichnung aus, bevor Sie Bewegungserkennungsauslöser 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. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Hinzufügen** und wählen Sie **Bewegungserkennung** aus.
4. Klicken Sie auf **OK**.
5. Im Dialogfeld:
 - 5.1. Wählen Sie die Kamera aus, die Bewegungen erkennen soll.
 - 5.2. Legen Sie ein Mindestintervall zwischen aufeinanderfolgenden Auslösern fest, um übermäßig viele aufeinanderfolgende Einzelaufzeichnungen zu vermeiden. 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. Klicken Sie auf **New (Neu)**.
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, Fehler bei der Verbindung zu einem Netzwerkspeicher oder der Verbindungsabbruch zu einem oder mehreren Geräten.

Systemereignis- und Fehler-Auslöser erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Klicken Sie auf **New (Neu)**.
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 Verbindungsabbruch zum Netzwerkdatenträger) , um den Auslöser zu bei Problemen mit dem Zugriff 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 Verbindungsproblemen mit 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. Mit Select all (Alle auswählen) und Deselect all (Alle abwählen) können sie alle Kameras auswählen bzw. die Auswahl aufheben.

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*.
- Es wird empfohlen, nach Möglichkeit Geräteereignisse anstelle von Ein-/Ausgängen als Auslöser zu verwenden. Weitere Informationen, siehe *Geräte-Ereignisauslöser erstellen, on page 98*.

Auslöser Eingang/Ausgang erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Klicken Sie auf **New (Neu)**.
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)	Legen Sie ein Mindestintervall zwischen zwei aufeinanderfolgenden Auslösern fest, um übermäßig viele aufeinanderfolgende Einzelaufzeichnungen zu vermeiden. 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. Nutzen Sie diese Option, 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. Klicken Sie auf **New (Neu)**.
3. **Hinzufügen** anklicken und **Gerät ereignis** 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 angezeigten Geräte-Ereignisauslösers im Zeitverlauf. Ein Ereignis kann einen Status haben oder nicht. Eine Treppenfunktion zeigt ein Ereignis mit einem Status (statusbehaftet) an. Eine gerade Linie mit Impulsen zeigt ein Ereignis ohne Status an.
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)	Legen Sie ein Mindestintervall zwischen zwei aufeinanderfolgenden Auslösern fest, um übermäßig viele aufeinanderfolgende Einzelaufzeichnungen zu vermeiden. 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	Verworfen Alarme
	Verworfen Ereignisse
	Alarm
Lüfter	Status
Globale Szenenänderung	Bilddienst
Hardwarefehler	Speicherfehler
	Lüfter Fehler
Heizung	Status
Eingangsanschlüsse	Virtueller Eingang
	Digitaler Eingangs-Port

	Manueller Auslöser
	Überwacher Eingangs-Port
	Digitaler Ausgangsanschluss
	Externer Eingang
Licht	Status
Lichtstatus geändert	Status
Medien	Profil geändert
	Konfiguration geändert
Überwachen	Heartbeat
Bewegungsbereichsmelder	Bewegung
Netzwerk	Kein Netz
	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 <Kanalname>
PTZ-Voreinstellungen	PTZ-Voreinstellung auf Kanal <Kanalname> 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	Pulse (Impuls):
	Intervall
	Geplantes Ereignis
Status	Aktiv
Speicher	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
	Digitaler Eingang
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 befindet sich im Betriebsbereitschaftszustand. Das Axis-Produkt erkennt beispielsweise den Systemstatus und sendet nach dem Systemstart eine Benachrichtigung an den Administrator. Wählen Sie Yes (Ja) aus, um die Aktionsregel auszulösen, wenn sich das Produkt im Bereitschaftszustand befindet. Die Regel wird nur ausgelöst, nachdem alle erforderlichen Dienste wie das Ereignissystem gestartet wurden.
Tür	
Zugang erzwungen	Der Zugang wurde erzwungen.
Manipulation der Zugangsinstallation erkannt	Wenn das System die folgenden Zustände erkennt: • Gerätegehäuse offen oder geschlossen. • Gerätebewegung. • Angeschlossener Kartenleser von der Wand entfernt. • Manipulation am angeschlossenen Zugangsmonitor, Kartenleser oder REX-Gerät. 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 das Blinken der Status-LED 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	Die Netzwerkverbindung wird unterbrochen. Gilt nur für Geräteereignisse, nicht für Ereignisse, die von AXIS Camera Station Pro verwendet werden.
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 oder an Wochenenden. 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 Bearbeiten einer Aktionsschaltfläche für eine Kamera 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 angezeigte Beschriftungstext. Bewegen Sie den Mauszeiger über die Schaltfläche, um den Tooltip anzuzeigen.

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

Wechselschaltflächen – Hierüber lassen sich Aktionen manuell starten und stoppen. Die Schaltfläche hat zwei Status: Betätigung und Nichtbetätigung. Klicken Sie zum Umschalten zwischen den beiden Schaltzuständen auf die Schaltfläche. Standardmäßig wird die Aktion beim Umschalten der Wechselschaltfläche in den eingeschalteten Zustand gestartet, kann jedoch auch umgekehrt beim Umschalten in den ausgeschalteten Zustand gestartet werden.

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 Impulseinstellung „As long as any trigger is active“ (Solange irgendein Trigger aktiv ist).

Aktionsschaltflächenauslöser erstellen:

1. Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln aufrufen.

2. Klicken Sie auf **New (Neu)**.
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. Drücken Sie Alt und die Zugriffstaste, um die Aktionsschaltfläche zu aktivieren. Wenn Sie z. B. eine Aktionsschaltfläche mit A_BC benennen, wird der Name der Aktionsschaltfläche in der Live-Ansicht auf ABC geändert. Drücken Sie Alt + B, um die Aktionsschaltfläche 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 Wechselschaltfläche müssen Sie **Trigger on toggle (Auslösung bei Einschalten)** oder **Trigger on untoggle (Auslösung bei Ausschalten)** auswählen.
 - 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 aktiviert diesen Auslöser bei Eingang von Türsignalen, die im AXIS Entry Manager konfiguriert wurden. 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. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Hinzufügen** und wählen Sie das **EREIGNIS AXIS Entry Manager** aus.
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

Der Auslöser HTTPS extern ermöglicht es externen Anwendungen, über eine HTTPS-Verbindung Ereignisse in AXIS Camera Station Pro auszulösen. Dieser Auslöser unterstützt nur HTTPS-Kommunikation und erfordert einen gültigen AXIS Camera Station Pro Benutzernamen einschließlich Domainnamen und Kennwort für 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* unter *Allgemeine Servereinstellungen*.
- 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. Sehen Sie sich die Beispiel-URL an, die dieselbe Serveradresse verwendet, über die sich der Client angemeldet hat. 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 eignen 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. Klicken Sie auf **New (Neu)**.
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 180*.
 - 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**.

Auslöser in AXIS Audio Manager erstellen

So erstellen Sie einen Auslöser im AXIS Audio Manager:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Klicken Sie auf **New (Neu)**.
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 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 jeweiligen Aktionen werden bei Aktivierung der Regel ausgelöst.

Es stehen folgende Aktionen zur Verfügung:

Aufzeichnen – Eine Aufzeichnung mit der gewählten Kamera wird gestartet. Siehe *Aufzeichnungssaktion erstellen*.

Alarm auslösen – Ein Alarm wird an alle verbundenen AXIS Camera Station Pro-Clients gesendet. Siehe *Die Aktionen "Alarm auslösen" erstellen*.

Ausgang einstellen – Der Status eines Ausgangsanschlusses wird eingestellt. Verwenden Sie diese Funktion, um ein mit dem Ausgangsanschluss verbundenes Gerät anzusteuern, z. B. zum Einschalten einer Leuchte oder Verriegeln einer Tür. Siehe *Ausgangsaktionen erstellen*.

Send email (E-Mail senden) – Eine E-Mail wird an einen oder mehrere Empfänger versendet. Siehe *Erstellen einer E-Mail-Senden-Aktion*.

Live-Ansicht – Die Live-Ansicht einer bestimmten Kamera, eine Ansicht oder eine voreingestellte Position wird in allen verbundenen AXIS Camera Station Pro-Clients geöffnet. Live-Ansichtsaktionen können auch dazu verwendet werden, minimierte geöffnete Clients aus der Taskleiste wieder einzublenden oder im Vordergrund vor anderen geöffneten Anwendungen anzuzeigen. Siehe *Live-Ansichtsaktion erstellen*.

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

Sirene und Licht – Auf einem kompatiblen Gerät wird entsprechend einem vorkonfigurierten Profil ein Sirenen- und Lichtmuster ausgelöst. Siehe *Sirenen- und Lichtaktionen erstellen, on page 113*.

Virtuelle Ein- und Ausgänge – Ein bestimmter virtueller Eingangsanschluss wird an einem Gerät ausgelöst. Siehe *Aktionen für virtuelle Ein-/Ausgänge erstellen, on page 113*.

AXIS Entry Manager – Zutritt wird gewährt bzw. eine Tür, die mit einer von AXIS Entry Manager konfigurierten Tür-Steuerung verbunden ist, wird ent- oder verriegelt. Siehe *Axis Entry Manager-Aktionen erstellen, on page 113*.

Benachrichtigung mit mobiler App senden – Eine individuelle Nachricht wird an die mobile App von AXIS Camera Station gesendet. Siehe *Erstellen von Aktionen zum Versenden von Benachrichtigungen an die mobile App, on page 114*.

Regeln aktivieren oder deaktivieren – Andere Aktionsregeln werden (de)aktiviert. Siehe *Aktion erstellen, die andere Aktionsregeln ein- oder ausschaltet, on page 114*.

Senden an Video-Decoder – Eine Ansicht wird an einen Video-Decoder gesendet, um diese für eine bestimmte Zeit auf einem Bildschirm anzuzeigen. Siehe *Eine Aktion erstellen, die eine Ansicht an einen Video-Decoder sendet, on page 115*.

Zutrittskontrolle – Diese Aktion umfasst Zugangs- und Zonenaktionen in AXIS Camera Station Secure Entry. Siehe *Zugangskontroll-Aktion erstellen, on page 115*.

Aufzeichnungsaktion erstellen

Die Aktion "Aufzeichnen" startet eine Aufzeichnung über die gewählte Kamera. Aufzeichnungen können auf der Registerkarte **Recordings (Aufzeichnungen)** aufgerufen und wiedergegeben werden.

Aufzeichnungsaktion erstellen:

1. Geben Sie einen Speicherort für die Aufzeichnung an und gehen Sie zu **Configuration (Konfiguration) > Storage (Speicher) > Selection (Auswahl)**.
2. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
3. Klicken Sie auf **New (Neu)**.
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 (Ereigniseinstellungen)** gegebenenfalls eine Ereigniskategorie für die Aufzeichnung aus.
10. Klicken Sie auf **OK**.

Videoeinstellung	
Profil	Wählen Sie im Dropdown-Menü unter Profile (Profil) ein Profil aus. Zur Bearbeitung der Profileinstellungen siehe <i>Videostreamprofile</i> .
Vorpuffer:	Legen Sie die Anzahl der Sekunden vor der erkannten Bewegung fest, die in eine Aufnahme einbezogen werden sollen.
Nachpuffer:	Legen Sie die Aufnahmedauer in Sekunden fest, die nach Ende der Aktion in die Aufzeichnung eingeschlossen werden soll.

Die Aktionen "Alarm auslösen" erstellen

Alarmauslösende Aktionen senden einen Alarm an alle mit AXIS Camera Station Pro verbundenen Clients. Der Alarm wird auf der Registerkarte **Alarms (Alarme)** sowie als Benachrichtigung in der Taskleiste angezeigt. Sie können eine Datei mit Alarmvorgängen anhängen. Der Alarmvorgang wird über den Tab **Alarme** und **Protokolle** aufgerufen.

Die Aktionen "Alarm auslösen" erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Add (Hinzufügen)** und konfigurieren Sie einen Auslöser. 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. Konfigurieren Sie den Alarmvorgang unter **Alarm procedure (Alarmvorgang)**.
 - 7.1. Wählen Sie **On alarm show alarm procedure (Alarmvorgang bei Alarm anzeigen)**.
 - 7.2. Klicken Sie auf **Upload (Hochladen)** und suchen Sie die Datei.
 - 7.3. Klicken Sie auf **Preview (Vorschau)**, um eine Vorschau der Datei anzuzeigen.
 - 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 eine Anzeigedauer von 1 und 600 Sekunden für eingeblendete Benachrichtigungen fest.

Ausgangsaktionen erstellen

Die Ausgangsaktion legt den Status eines Ausgangsports fest. Mit dieser Option können Sie das mit dem Ausgangsport verbundene Gerät steuern, um z. B. eine Leuchte einzuschalten oder einen Zutrittspunkt zu verriegeln.

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. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Add (Hinzufügen)** und konfigurieren Sie einen Auslöser. 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 sind von der Portkonfiguration abhängig.
8. Wählen Sie **Pulse (Impuls)**, um die Dauer festzulegen, für die 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 in den neuen Zustand zu versetzen, wählen Sie Keep the state for a fixed time (Für bestimmte Zeit setzen) 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. Sie können Schnappschüsse von Kameras an die E-Mail anhängen.

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. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Add (Hinzufügen)** und konfigurieren Sie einen Auslöser. 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)** E-Mail-Adressen 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 **Hinzufügen**.
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 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. Klicken Sie auf Select all (Alle auswählen) , um alle Kameras auswählen, oder Deselect all (Alle abwählen) , um die Auswahl aufzuheben.
Send one email for each event (Eine E-Mail pro Ereignis versenden)	Wählen Sie die Option Send one email for each event (Für jedes Ereignis eine E-Mail senden) , wenn Sie verhindern möchten, dass für ein Ereignis mehrere E-Mails gesendet werden.
Don't send another email for (Keine weitere E-Mail senden für)	Wählen Sie die Option Don't send another email for (Keine weitere E-Mail senden für) aus und stellen Sie über das Auswahlmenü die Mindestzeit zwischen den E-Mails ein, wenn Sie verhindern möchten, dass E-Mails zu häufig nacheinander versendet werden.

Live-Ansichtsaktion erstellen

Die Live-Ansichtsaktion ruft eine bestimmte Kamera, Ansicht oder voreingestellte Position auf der Registerkarte **Live view (Live-Ansicht)** aller verbundenen AXIS Camera Station Pro-Clients auf. Wird in der Live-Ansicht auf der Registerkarte **Live view (Live-Ansicht)** eine geteilte Ansicht mit einem Hotspot angezeigt, erscheint die in der Live-Ansichtsaktion ausgewählte Kamera im Hotspot. Weitere Informationen zu Hotspots finden Sie unter *Geteilte Ansicht*.

Live-Ansichtsaktionen können auch dazu verwendet werden, um minimierte geöffnete AXIS Camera Station Pro-Clients aus der Taskleiste wieder einzublenden oder im Vordergrund vor anderen geöffneten Anwendungen anzuzeigen.

Aktion "Live-Ansicht" erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Add (Hinzufügen)** und konfigurieren Sie einen Auslöser. Klicken Sie auf **Next (Weiter)**.
Siehe *Auslöser hinzufügen*.
4. **Hinzufügen** anklicken und **Live-Ansicht** wählen.
5. Klicken Sie auf **OK**.
6. Legen Sie unter **Live view actions (Live-Ansichtsaktionen)** fest, 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 minimierte geöffnete AXIS Camera Station Pro-Clients bei Beginn der Aktion aus der Taskleiste wieder einzublenden oder im Vordergrund vor anderen geöffneten Anwendungen anzuzeigen.
9. Klicken Sie auf **OK**.

Direktübertragungsaktionen	
Ansehen	Gehen Sie zu View (Ansicht) und wählen Sie anschließend eine Ansicht aus dem Auswahlménü aus.
Kamera	Gehen Sie zu Camera (Kamera) und wählen Sie dann eine Kamera aus dem Auswahlménü aus. Bei einer Kamera mit PTZ-Voreinstellung gehen Sie zu Go to preset (Zur Voreinstellung wechseln) und wählen Sie zum Öffnen einer voreingestellten Position einen Bereich aus dem Auswahlménü aus.
Keine Aktion	Wählen Sie No action (Keine Aktion) , wenn Sie keine Ansicht öffnen möchten.

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-Ménü aus. Ist der Hotspot bei Auslösung der Aktion in der Live-Ansicht zu sehen, wird die Kameraansicht im Hotspot angezeigt.

Beispiel:

In diesem Beispiel werden zwei Live-Ansichtsaktionen in derselben Aktionsregel verwendet.

- Erstellen Sie eine Live-Ansichtsaktion zur Anzeige der Hotspot-Ansicht auf der Registerkarte **Live alert (Live-Warnung)**.
 - Wählen Sie unter **Live view actions (Live-Ansichtsaktionen)** die Option **View (Ansicht)**.
 - Wählen Sie die Option **Hotspot view (Hotspot-Ansicht)** aus.
 - Wählen Sie unter **Anzeigen in** die Registerkarte **Live-Alarm**.
 - Wählen Sie **Anwendung bei Trigger in den Vordergrund ziehen**.
- Erstellen Sie eine weitere Live-Ansichtsaktion, um die Hotspot-Ansicht aufzurufen und die Kameraansicht im Hotspot anzuzeigen.
 - Wählen Sie unter **Live view actions (Live-Ansichtsaktionen)** die Option **Camera (Kamera)** und dann eine Kameraansicht.
 - Wählen Sie unter **Show in (Anzeigen in)** die Option **Hotspot in view (Hotspot in Ansicht)** aus.
 - 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. Sie haben zum Beispiel die Möglichkeit, HTTP-Meldungen zum Ein- oder Ausschalten einer Funktion in der Kamera oder zum Öffnen und Schließen bzw. Ver- und Entriegeln eines mit einer Tür-Steuerung verbundenen Zutrittspunkts zu verwenden.

Unterstützte Methoden: GET, POST und PUT.

Hinweis

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

Aktion "HTTP-Meldung" erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Add (Hinzufügen)** und konfigurieren Sie einen Auslöser. 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	Die Verwendung dieser Option wird empfohlen, 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 Auswahlménú Method (Methode) eine HTTP-Methode aus.
Inhaltstyp	Wählen Sie für die Methoden POST und PUT unter Content type (Inhaltstyp) den entsprechenden Inhaltstyp aus dem Dropdown-Ménú aus.
Textkörper	Geben Sie für die Methoden POST und PUT unter Body (Textkörper) den Anforderungstext ein.
Trigger data (Auslösedaten)	Es besteht auch die Möglichkeit, ebenfalls vordefinierte Auslösedaten aus dem Dropdown-Ménú einzufügen.

Trigger data (Auslösedaten)	
Type (Typ):	Auslöser, der die Aktionsregel aktiviert hat.
Source ID (Quell-ID)	Gibt die Quelle an, die zum Auslösen der Aktionsregel führte. Dabei handelt es sich oft um eine Kamera oder ein anderes Gerät. Nicht alle Quellen verfügen über eine ID.
Source Name (Quellname)	Der Name der Quelle, die zum Auslösen der Aktionsregel führte. Dabei handelt es sich oft um eine

Trigger data (Auslösedaten)	
	Kamera oder ein anderes Gerät. Nicht alle Quellen verfügen über eine ID.
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 Eingangsanschluss eines Geräts zu aktivieren. Jeder Port eines Geräts kann für eine Aktion verwendet werden.

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Add (Hinzufügen)** und konfigurieren Sie einen Auslöser. 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 aktivieren 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. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Add (Hinzufügen)** und konfigurieren Sie einen Auslöser. 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 Tür-Steuerung 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. Klicken Sie auf **New (Neu)**.

3. Klicken Sie auf **Add (Hinzufügen)** und konfigurieren Sie einen Auslöser. 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 den Zutrittspunkt, auf den diese angewendet werden soll.
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. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Add (Hinzufügen)** und konfigurieren Sie einen Auslöser. 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)** die Nachricht ein, die in der mobilen App angezeigt werden soll.
7. Konfigurieren Sie unter **Click notification and go to (Benachrichtigung anklicken und aufrufen)**, was beim Anklicken/Antippen der Benachrichtigung angezeigt werden soll.
8. Klicken Sie auf **OK**.

Click notification and go to (Benachrichtigung anklicken und aufrufen)	
Kamera	Wählen Sie die Kameraansicht aus, die bei Anklicken/Antippen der Benachrichtigung angezeigt werden soll.
Standard	Wählen Sie Default (Standard) , um beim Anklicken/Antippen der Benachrichtigung die Startseite der mobilen App öffnen zu lassen.

Aktion erstellen, die andere Aktionsregeln ein- oder ausschaltet

Verwenden Sie diese Aktion beispielsweise, um die Bewegungserkennung in einem Büro auszuschalten, wenn ein Mitarbeiter seine Zugangskarte durchzieht.

Aktion zur Aktivierung oder Deaktivierung von Aktionsregeln erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Add (Hinzufügen)** und konfigurieren Sie einen Auslöser. 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 **Return to the previous state when the trigger is no longer active** (**Zurück zum vorherigen Status, wenn der Auslöser nicht mehr aktiv ist**), wenn die ausgewählte Aktionsregel bei nicht aktivem Auslöser nicht geändert werden soll. Im Beispiel oben heißt das, dass sich die Bewegungserkennung wieder einschaltet, wenn der Mitarbeiter seine Zutrittskarte aus dem Kartenleser entnimmt.
10. Klicken Sie auf **OK**.

Aktion „Lesezeichen erstellen“

Eine Aktion zum Erstellen eines Lesezeichens fügt einer Aufzeichnung in dem Moment, in dem die Aktionsregel ausgelöst wird, ein Lesezeichen hinzu.

So erstellen Sie eine Aktion „Lesezeichen erstellen“:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Add (Hinzufügen)** und konfigurieren Sie einen Auslöser. 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.

Zur Erstellung einer Aktion für das Senden an den Video-Decoder:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Add (Hinzufügen)** und konfigurieren Sie einen Auslöser. 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 gewünschte Anzeigedauer der Ansicht in Sekunden ein.
9. Klicken Sie auf **OK**.

Zugangskontroll-Aktion erstellen

Die Zugangskontroll-Aktion kann die folgenden Aktionen in AXIS Camera Station Secure Entry veranlassen:

- **Zugangsaktionen:** Zugang gewähren; ausgewählte Zugänge verriegeln, entriegeln, zurücksetzen oder blockieren.
- **Zonenaktionen:** Ausgewählte Zugänge in ausgewählten Zonen verriegeln, entriegeln, zurücksetzen oder blockieren.
- **Aktionen für Zutrittsregeln:** Zutrittsregeln aktivieren oder deaktivieren.

Hinweis

Die Zutrittskontroll-Aktion ist nur für AXIS Camera Station Secure Entry verfügbar.

Zur Erstellung einer Zutrittskontroll-Aktion:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Add (Hinzufügen)** und konfigurieren Sie einen Auslöser. 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. Zugangsregeln aktivieren oder deaktivieren:
 - 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.

Aktionen in AXIS Audio Manager erstellen

Eine Aktion kann in AXIS Audio Manager zur Steuerung der Audiowiedergabe- und der Lautstärkeeinstellungen für verbundene Audiogeräte genutzt werden.

Zur Erstellung einer AXIS Audio Manager-Aktion:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Klicken Sie auf **New (Neu)**.
3. Klicken Sie auf **Add (Hinzufügen)** und konfigurieren Sie einen Auslöser. 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**.

AXIS Audio Manager-Aktionen	
Audiodatei abspielen	Wählen Sie die Option Play audio file (Audiodatei abspielen) , um eine ausgewählte Audiodatei wiederzugeben. Sie können außerdem Wiedergabeparameter wie die Anzahl der Wiederholungen, die Priorität und das visuelle Profil konfigurieren.
Wiedergabe der Audiodatei beenden	Wählen Sie Stop audio file (Audiodatei anhalten) , um die Audiowiedergabe anzuhalten.
Ziel aktivieren/deaktivieren	Wählen Sie Enable or disable target (Ziel aktivieren oder deaktivieren) , um Geräte einzuschalten oder auszuschalten.
Stummschalten	Wählen Sie Mute volume (Stummschalten) aus, um den Lautstärkeregler stummzuschalten.
Lautstärke festlegen	Wählen Sie Set volume (Lautstärke festlegen) , um die Lautstärke eines Lautstärkereglers einzustellen. Der Wert kann positiv oder negativ sein.
Lautstärke anpassen	Wählen Sie Offset volume (Lautstärke anpassen) , um die Lautstärke relativ zum aktuellen Pegel anzupassen. Geben Sie einen positiven Wert ein, um sie zu erhöhen, oder einen negativen Wert, um sie zu verringern.

Zeitschemata

Die Seite „Schedules“ (Zeitpläne) enthält alle Zeitpläne, die Sie auf Aufzeichnungen, Aktionsregeln und Komponenten wie AXIS Secure Entry anwenden können. Einige Zeitpläne werden während der Installation automatisch von AXIS Site Designer erstellt.

Mit dieser Funktion 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.
- **Type (Typ):** Zeigt an, ob es sich bei dem Zeitplan um einen Tages- oder Wochenplan handelt.
- **In use (Wird verwendet):** Zeigt an, ob eine Komponente, eine Aufzeichnungsregel oder eine Aktionsregel derzeit den Zeitplan verwendet.
- **Override schedules (Überschreibungszeitpläne):** Listet auf, welche Überschreibungszeitpläne für diesen Zeitplan gelten.

Die Registerkarte **Override schedules (Überschreibungszeitpläne)** ist die Hauptansicht für die Verwaltung Ihrer Überschreibungszeitpläne sowie die Anzeige der Tages- und Wochenzeitpläne, für die die Überschreibungszeitpläne gelten.

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 Auswahlménü **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**. Vergewissern Sie sich vor dem Löschen, dass der Zeitplan nicht gerade verwendet wird.

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 **Add dates (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

Dieses 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 48*.
- Konfigurieren Sie den Netzwerk-Tür-Controller. Siehe *Fügen Sie einen Zugang hinzu, on page 154*.

Aktionsregel erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln** aufrufen.
2. Klicken Sie auf **New (Neu)**.
3. Fügen Sie das Ereignis einer aufgebrochenen Tür als Auslöser hinzu:
 - 3.1. **Hinzufügen** anklicken und **Geräteereignis** 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: „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) einen 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.

Videoeinstellungen	
Profil	Wählen Sie im Auswahllistenfeld 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

Dieses 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 eine Axis Netzwerk-Tür-Steuerung und fügen Sie Karteninhaber hinzu. Siehe *Konfigurieren Sie die Zutrittskontrolle, on page 150* und *Zugriffsverwaltung, on page 188*.
- Installieren Sie ein Axis Netzwerk-Audiogerät und verbinden Sie es mit einer Kamera. Siehe *Videostreamprofile, on page 56*.
- 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 92*.

Aktionsregel erstellen:

1. **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln aufrufen.**
2. Klicken Sie auf **New (Neu)**.
3. Fügen Sie das Geräteereignis als Auslöser hinzu:
 - 3.1. **Hinzufügen** anklicken und **Geräteereignis** wählen.
 - 3.2. Klicken Sie auf **OK**.
 - 3.3. Konfigurieren Sie unter **Configure device event trigger (Geräte-Ereignisauslöser konfigurieren)** den gewünschten Ereignisseinstellungen.
 - 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 Auswahlménü **Output port (Ausgangsanschluss)** den Ausgangsanschluss des E/A-Moduls aus, das mit dem Aufzug verbunden ist.
 - 6.4. Wählen Sie im Dropdown-Ménü 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 stellen Sie die Dauer auf 60 Sekunden ein.
 - 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.
Kartenummer	Wählen Sie Card number (Kartenummer) aus und geben Sie die Kartenummer der betreffenden Person ein.

Client konfigurieren

Konfiguration > Client aufrufen, um:

- Clientspezifische Einstellungen wie Design und Sprache zu bearbeiten. Siehe *Clienteinstellungen, on page 121*.
- Benutzerspezifische Einstellungen wie Benachrichtigungen und Startoptionen zu bearbeiten. Siehe *Benutzereinstellungen, on page 122*.
- Clientspezifische Einstellungen zur Streaming-Leistung wie Videoskalierung und Hardware-Decodierung anzupassen. Siehe *Streaming, on page 124*.

Clienteinstellungen

Diese Einstellungen greifen für alle AXIS Camera Station Pro Benutzer auf dem Computer. Gehen Sie zu **Configuration (Konfiguration) > Client > Client settings (Client-Einstellungen)**.

Design	
System, Light (Hell), Dark (Dunkel)	Das Design für den Client wählen. System ist das Standarddesign für neue Installationen. Bei Auswahl der Option System richtet sich das Design nach dem Design Ihres Windows-Systems.

Allgemeines	
Anwendung beim Start von Windows ausführen	Aktivieren Sie diese Option, um AXIS Camera Station Pro beim Start von Windows automatisch ausführen zu lassen.

Live-Ansicht	
Kameranamen in Live-Ansichten anzeigen	Mit dieser Option können Sie die Kameranamen in der Live-Ansicht anzeigen.
	Aktivieren Sie die Option Show recording indicators in live views and maps (Aufzeichnungsindikatoren in Live-Ansichten und auf Lageplänen anzeigen) , um Indikatoren für Aufzeichnungen anzeigen zu lassen, die durch die Bewegungserkennung oder eine Aktionsregel ausgelöst wurden.
	Aktivieren Sie die Option Show event indicators in live views and maps (Ereignisindikatoren in Live-Ansichten und auf Lageplänen anzeigen) , um Indikatoren für Aufzeichnungen anzeigen zu lassen, die durch die Bewegungserkennung oder eine Aktionsregel ausgelöst wurden.

Lagepläne	
Allow flashing coverage areas for all maps (Blinkende Erfassungsbereiche für alle Lagepläne zulassen)	Aktivieren bzw. deaktivieren Sie diese Einstellung, um festzulegen, ob die Erfassungsbereiche auf allen Lageplänen blinken sollen. Diese globale Einstellung hat keine Auswirkungen auf die lokalen Lageplaneinstellungen. Siehe <i>Lageplan</i> , on page 23.

Sprache	
Mit dieser Option können Sie die Sprache des AXIS Camera Station Pro-Clients ändern. Starten Sie den Client neu, damit die Änderung wirksam wird.	

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 Änderung dieser Einstellung für den Server finden Sie unter <i>Servereinstellungen</i> , on page 129.

Benutzereinstellungen

Diese Einstellungen gelten für den angemeldeten AXIS Camera Station Pro-Benutzer. Gehen Sie zu **Configuration (Konfiguration) > Security (Sicherheit) > User permissions (Benutzerrechte)**.

Navigationssystem	
Strukturansicht der Navigation	Standardmäßig eingeschaltet. Zeigt Ansichten, Kameras oder beides im Navigationsbereich an.
Show in navigation (In Navigation anzeigen)	Wählen Sie aus, was im Auswahlmenü angezeigt werden soll: Ansichten, Kameras oder beides.
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 beim Hinzufügen oder Abschließen einer Aufgabe in der Windows-Taskleiste eine Benachrichtigung anzuzeigen.
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 drückt.

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 Ordner zum Speichern der 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 bzw. Bild- und Kameraansichten zu starten wie beim letzten Beenden.
Zuletzt verwendete Monitore speichern	Aktivieren Sie diese Seite, um AXIS Camera Station Pro auf demselben Monitor zu starten wie beim letzten Beenden.

Hinweis

- Bild- und Kameraansichten werden pro Registerkarte gespeichert. Das System stellt diese nur wieder her, wann sich der Client wieder mit demselben Server verbindet.
- 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, um beim Auslösen eines Alarms keinen Ton wiedergeben zu lassen.
Signalton	Wählen Sie diese Option aus, um beim Auslösen eines Alarms einen Signalton ausgeben zu lassen.
Sound file (Audiodatei)	Wählen Sie die Datei aus und klicken Sie auf Browse (Durchsuchen) , wenn beim Auslösen eines Alarms eine benutzerdefinierte Audiodatei wiedergegeben werden soll. Alle Dateiformate, die mit dem Windows Media Player kompatibel sind, werden unterstützt.
Wiedergabe	Klicken Sie auf diese Option, um den Signalton zu testen.

Akustisches Signal bei eingehendem Anruf	
Kein Ton	Wählen Sie diese Option, um bei einem eingehenden Anruf keinen Ton wiedergeben zu lassen.
Signalton	Wählen Sie diese Option aus, um bei einem eingehenden Anruf einen Signalton ausgeben zu lassen.
Sound file (Audiodatei)	Wählen Sie die Option aus und klicken Sie auf Browse (Durchsuchen) , wenn bei einem eingehenden Anruf eine benutzerdefinierte Audiodatei wiedergegeben werden soll. Alle Dateiformate, die mit dem Windows Media Player kompatibel sind, werden unterstützt.
Wiedergabe	Klicken Sie auf diese Option, um den Signalton zu testen.

Merkmale	
Intelligente Suche 1 anzeigen	Wird standardmäßig angezeigt. Deaktivieren Sie diese Option, um „Intelligente Suche 1“ auszublenden.

Warnungsdialoge anzeigen	
Warnung vor ungültigem Zertifikat	Aktivieren Sie diese Option, um bei Erkennung eines ungültigen Zertifikats eine Warnung anzeigen zu lassen.

Streaming

Gehen Sie zu **Configuration (Konfiguration) > Client > Streaming**, um die Streaming-Optionen zu konfigurieren.

Videoskalierung	
Automatisch skalieren	Wählen Sie diese Option, um das Videobild bei gleichem Seitenverhältnis an die verfügbare Anzeigefläche anzupassen.
Videobereich ausfüllen (Ränder werden evtl. abgeschnitten)	Wählen Sie diese Option, um den verfügbaren Platz mit dem Videobild auszufüllen. Wenn das Seitenverhältnis des verfügbaren Anzeigebereichs von dem des Videobilds abweicht, passt das System das Videobild entsprechend an.

Hardware-Decodierung									
Modus	• Automatic (Automatisch): Die Grafikkarte wird zur Decodierung von Streams mit einer Auflösung über 3840 x 2160p bei 25 Bildern pro Sekunde (auch als 4K oder UHD bekannt) verwendet. • On (Ein) Die Grafikkarte wird zur Decodierung von Streams mit einer Auflösung über 1920 x 1080p bei 25 Bildern pro Sekunde (auch als 1080p oder HD bekannt) verwendet. • Off (Aus): AXIS Camera Station Pro nutzt den Hauptprozessor (CPU) zur Videodecodierung.								
Grafikkarte	Wählen Sie eine Grafikkarte aus dem Dropdown-Menü aus. <table border="1"> <thead> <tr> <th>Unterstützte Grafikkarten</th><th>Decoder-Technologie</th></tr> </thead> <tbody> <tr> <td>NVIDIA</td><td>PureVideo</td></tr> <tr> <td>AMD</td><td>Unified Video Decoder (UVD)</td></tr> <tr> <td>Intel</td><td>Intel Quick Sync Video (QSV)</td></tr> </tbody> </table>	Unterstützte Grafikkarten	Decoder-Technologie	NVIDIA	PureVideo	AMD	Unified Video Decoder (UVD)	Intel	Intel Quick Sync Video (QSV)
Unterstützte Grafikkarten	Decoder-Technologie								
NVIDIA	PureVideo								
AMD	Unified Video Decoder (UVD)								
Intel	Intel Quick Sync Video (QSV)								

Hinweis

- Bei der Hardware-Decodierung wird Ihre Grafikkarte zur Videodecodierung verwendet. Bei einer leistungsfähigen Grafikkarte kann die Hardware-Decodierung die Systemleistung verbessern und die CPU-Auslastung senken, was besonders für das Videostreaming mit hoher Auflösung gilt. Die Hardware-Decodierung unterstützt ausschließlich H.264- und AV1-Streams.
- Bei Kameras mit einer Auflösung unter 1080p ist auch bei aktivierter Funktion keine Hardware-Decodierung möglich.
- Falls Ihre Grafikkarte keine 4K-Decodierung unterstützt, erfolgt die Hardware-Decodierung auch bei aktivierter Funktion ausschließlich bei Streams mit einer Auflösung von 1080p.
- Für die Hardware-Decodierung wird nur eine Grafikkarte verwendet, selbst wenn ein System über mehrere Grafikkarten verfügt.

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 <i>Videostreamprofile</i> . Diese Einstellung wirkt sich auf die Videoformate H.264 und M-JPEG aus und reduziert die benötigte Bandbreite.
Videostreams in inaktiven Tabs unterbrechen	Aktivieren Sie diese Option, um Videostreams in inaktiven Registerkarten zu unterbrechen. Dadurch wird die benötigte Bandbreite reduziert.

PTZ (Schwenken, Neigen, Zoomen)	
Mit dem ersten Klicken Ansicht auswählen statt PTZ zu starten	Aktivieren Sie diese Option, damit die Ansicht mit dem ersten Anklicken ausgewählt wird. Bei einem weiteren Anklicken wird die PTZ-Steuerung gestartet.

Audio	
Push-to-talk release delay (ms) (Freigabeverzögerung für Sprechaste (ms))	Diese Einstellung legt fest, für welche Dauer in Millisekunden nach dem Loslassen der Sprechaste noch Audio vom Mikrofon übertragen wird.
Für alle Duplex-Modi die Sprechaste 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 ohne aktiven Anruf über das Türkontrollsystem (Gegensprechanlage) hören und sprechen zu können.

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 erlauben Ihnen Zugriff auf:

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

Sie müssen Ihr System registrieren und mit einer Organisation verbinden, um auf diese Dienste zu zugreifen. Weitere Informationen, siehe *Registrieren Sie Ihr System bei einer Organisation, on page 127*.

Status	Die Statuskarte zeigt den Status der Verbindung zwischen Ihrem Server und den verbundenen Diensten an sowie den Namen der Organisation, bei der Sie registriert sind.
Verbindung trennen	Wenn Sie die Verbindung zu einem Server trennen, bleibt er weiterhin bei der Organisation registriert.
Lizenzverwaltung	Aktivieren Sie License management (Lizenzverwaltung) , um Ihre Lizenzen automatisch zu synchronisieren. Das System übermittelt Lizenzänderungen an den AXIS License Manager und ruft den aktualisierten Lizenzstatus ab. Deaktivieren Sie die Option License management (Lizenzverwaltung) , um Lizenzen manuell zu verwalten, z. B. wenn Ihr System nicht über eine Internetverbindung verfügt. Weitere Informationen zur Verwaltung von Lizenzen finden Sie unter „Lizenzen verwalten“. Weitere Informationen, siehe <i>Lizenzen verwalten, on page 138</i> .
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 zur Registrierung Ihres Systems finden Sie in *AXIS Camera Station Pro – Installations- und Migrationsanleitung*.

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 die Option Every start-up (Bei jedem Start) aus, um bei jedem Start des Servers nach verfügbaren Firmware-Updates suchen zu lassen. 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 eine verschlüsselte Internetverbindung.

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 127*.
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 Zugriffsberechtigungen verwalten, indem Sie in „Axis My Systems“ Benutzerrollen für Organisationen zuweisen. Weitere Informationen zu den Zugriffsberechtigungen in AXIS Camera Station Pro finden Sie unter *Benutzerberechtigungen, on page 140*.

Cloud-Speicherung

AXIS Camera Station Cloud Storage ist ein lizenzierter Dienst zur Speicherung Ihrer Aufzeichnungen in der Cloud. Weitere Informationen finden Sie unter *AXIS Camera Station Cloud Storage – Benutzerhandbuch*.

Wichtig

AXIS Camera Station Cloud Storage wird nur von AXIS Camera Station Pro Version 6.18 oder früher unterstützt. Wir empfehlen Ihnen, Ihre Aufzeichnungen vor der Aktualisierung auf einen lokalen Speicher zu exportieren. Bei einer Aktualisierung Pro auf eine höhere Version als 6.18 funktioniert Ihr Cloud-Speicherdienst nicht mehr und Sie verlieren alle derzeit in der Cloud gespeicherten Daten. Sicherheitsupdates für Version 6.18 werden so lange fortgesetzt, bis die Unterstützung für den Cloud-Speicher in einer späteren Version wiederhergestellt ist.

Bevor Sie den Cloud-Speicher nutzen können, müssen Sie Ihr System bei den verbundenen Diensten registrieren. Nach der Registrierung können Sie den Cloud-Speicher für Ihre Kameras unter „My Systems“ verwalten.

Server konfigurieren

Servereinstellungen

Gehen Sie zu **Configuration (Konfiguration) > Server > Components (Komponenten)**.

Hinweis

Bei einer Verbindung zu mehreren AXIS Camera Station Pro-Servern wählen Sie zur Konfiguration der Server-Einstellungen einen beliebigen Server aus dem Auswahllisten **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 Alarm-, Ereignis- und Prüfprotokolle vorgehalten werden sollen. Geben Sie einen Wert zwischen 7 und 1000 Tagen ein.	
Um Protokolle zur Nutzung in Drittanbietersystemen wie Splunk, Elastic oder einem SIEM-Tool kontinuierlich in Echtzeit in eine Datei zu schreiben, wählen Sie Write audit logs to file (Prüfprotokolle in Datei schreiben) , Write event logs to file (Ereignisprotokolle in Datei schreiben) oder beides.	
Der Server schreibt Protokolleinträge in <code>C:\ProgramData\Axis Communications\AXIS Camera Station\Core\Server\Logs</code> . Die Dateien enthalten nur Text und werden in Systemberichten nicht berücksichtigt.	
Datei	Beschreibung
<code>AcsService.exe.audit.log.export</code>	Einträge im Prüfprotokoll
<code>AcsService.exe.event.log.export</code>	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 Auslösung einer Aktionsregel 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 für den Absender angezeigt werden sollen.

Server	
Adresse	Geben Sie die-Adresse des SMTP-Servers ein.
Anschluss	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	Legen Sie fest, ob für den Server-Zugriff ein Benutzername und Kennwort erforderlich sein sollen, und geben Sie anschließend Ihre Zugangsdaten ein.

Edit (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 im Dialogfenster Yes (Ja) , 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 Dialogfenster 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 legen Sie mit den Pfeilen eine Reihenfolge fest. Das System kontaktiert die Server in der angegebenen Reihenfolge.

Server-Testergebnisse	
OK	Es konnte eine Verbindung zum SMTP-Server hergestellt werden. Vergewissern Sie sich, dass die Empfänger die Test-E-Mail erhalten haben.
Unbekannter Fehler	Beim Senden der E-Mail 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. Vergewissern Sie sich, dass der SMTP-Server funktioniert und die Router und Proxy-Server den Datenverkehr zwischen AXIS Camera Station Pro und SMTP-Server gestatten.
Konfigurationsfehler	Es erfolgte eine TLS-Anfrage, aber der Server unterstützt keine StartTLS bzw. keine Authentifizierung oder verfügt über keinen kompatiblen Authentifizierungsmechanismus.
TLS/SSL-Handshake-Fehler	Bei der TLS/SSL-Aushandlung ist ein Fehler aufgetreten, zum Beispiel aufgrund eines ungültigen Serverzertifikats.

Server-Testergebnisse	
Authentifizierung erforderlich	Der Server benötigt zum Senden von E-Mails eine Authentifizierung.
Authentifizierungsfehler	Die Zugangsdaten sind falsch.
Verbindung unterbrochen	Es wurde eine Verbindung hergestellt, die jedoch unterbrochen wurde.

Systemalarm

Ein Alarm wird ausgelöst, wenn die Verbindung zu einer Kamera ausfällt, der Zugriff zum Speichern einer Aufzeichnung verweigert wird, der Server unerwartet heruntergefahren wird oder Fehler bei der Aufzeichnung auftreten. Sie können das Versenden von E-Mail-Benachrichtigungen bei einem Alarm veranlassen.

Hinweis

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

E-Mail-Benachrichtigung bei Systemalarm senden:

1. Wählen Sie die Option **Send email on system alarm to the following recipients (Bei Systemalarm E-Mails an folgende Empfänger senden)**, um die E-Mail-Benachrichtigungsfunktion für Systemalarme 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 **Add (Hinzufügen)**, um die E-Mail-Adresse im Feld **Recipients (Empfänger)** zu speichern.

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. Um stattdessen automatisch die IP-Adresse zu verwenden, deaktivieren Sie das Kontrollkästchen. Sie können manuell auswählen, ob der Hostname oder die IP-Adresse für die Verbindung mit Geräten verwendet werden soll. Siehe <i>Verbindung, on page 73</i> .

Sprache	
Sprache des Servers ändern	Mit dieser Option ändern Sie die Sprache der Dienststeuerung von AXIS Camera Station Pro und von AXIS Camera Station Secure Entry. Diese Einstellung gilt zum Beispiel für Systemalarme, Audit-Protokollmeldungen und externe Daten auf der Registerkarte Data search (Datensuche) . Starten Sie den Server neu, damit die Änderung wirksam wird.

Body Worn	
Laufwerk Ordner	Wählen Sie das Laufwerk und den Ordner aus, in dem Sie abgelehnte Inhalte aus dem Body Worn-System speichern möchten. Weitere Informationen finden Sie unter <i>Übertragung von Aufzeichnungen in einen Speicher für abgelehnte Inhalte im Benutzerhandbuch AXIS Body Worn Solution</i> .
Anzahl der Tage, die abgelehnte Inhalte aus dem Body Worn-System behalten werden sollen.	Mit dieser Option legen Sie die Anzahl der Tage fest, für die abgelehnte Inhalte aus dem Body Worn-System gespeichert werden sollen.

Feedback	
Axis Communications die Nutzung anonymisierter Server-Daten gestatten	Mit dieser Option gestatten Sie Axis die Nutzung anonymisierter Daten zur Verbesserung der Anwendung und ihrer Benutzung. Weitere Informationen zur Änderung dieser Client-Einstellung finden Sie unter <i>Clienteneinstellungen, on page 121</i> .

Erweiterte Einstellungen

Ändern Sie diese Einstellungen nur bei ausdrücklicher Anweisung vom Axis-Support. 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)**. Bei Aktivierung dieser Einstellung wird mehr Speicherplatz benötigt. Die Datei `log4net.config` im Verzeichnis **ProgramData (Programmdaten)** hat Vorrang vor dieser Konfiguration.

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 Seite **Components (Komponenten)** 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. Halten Sie vor der Anzeige und Verwaltung von Komponenten bitte zuerst Rücksprache mit dem Axis Support.

AXIS Camera Station Pro aktualisieren

Zur Aktualisierung 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

- Sobald eine Aktualisierung manuell oder per Zeitplan gestartet wurde, kann sie 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 beendet. Der Aktualisierungsfortschritt wird nicht angezeigt. Lassen Sie den Servercomputer eingeschaltet, bis sowohl der Client als auch der Server neu gestartet sind.

Vorfallbericht

Wenn Sie die Berechtigungen für Vorfallberichte einschalten, können Sie Vorfallberichte erstellen, die Aufzeichnungen, Schnappschüsse und Notizen einschließen. Siehe *Vorfälleberichte exportieren, on page 35*.

Um die Einstellungen für Vorfälleberichte zu konfigurieren:

1. **Configuration > Server > Incident report (Konfiguration > Server > Vorfällebericht)** aufrufen.
2. Wählen Sie unter **Location (Speicherort)** den Speicherort der Vorfallberichte aus.
3. Wählen Sie aus dem Auswahllisten **Export format (Exportformat)** das Format aus, in das Sie Ihre Aufzeichnungen exportieren möchten.
4. Um Vorfälleberichte Gruppen zuzuordnen, unter **Categories (Kategorien)** entsprechend Kategorien hinzufügen oder löschen. Bei der Konfiguration als Variable im Server-Verzeichnispfad bilden die Kategorien im Exportziel die Ordernamen.
 - 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 Vorfälleberichte in der Beschreibung (**Description**) angezeigt werden sollen. Zum Beispiel: „Reported by: [name, email, phone number]“ (Gemeldet von: [Name, E-Mail-Adresse, Telefonnummer]).
6. Klicken Sie auf **Anwenden**.

Standort	
Server directory path (Server-Verzeichnispfad)	Geben Sie den Verzeichnispfad zur Speicherung Ihrer Vorfälleberichte in einem Ordner auf dem Rechner . 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. Weitere Informationen zum Hinzufügen von Aufzeichnungsspeicher siehe <i>Speicher verwalten</i> .

Exportformat	
ASF	Wählen Sie Add digital signature (Digitale Signatur hinzufügen) , um Manipulationen an Bildern zu verhindern. Siehe dazu den Abschnitt <i>Digitale Signatur in Aufzeichnungen exportieren</i> . 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

Gehen Sie zu **Configuration (Konfiguration) > Server > Scheduled export (Geplanter Export)**, um einen Zeitplan für den Export von Aufzeichnungen festzulegen.

AXIS Camera Station Pro exportiert dann zum geplanten Zeitpunkt alle Aufzeichnungen, die seit dem letzten Export angefallen sind. Wenn der letzte Export länger als eine Woche zurückliegt oder wenn kein vorheriger Export erfolgte, werden nur Aufzeichnungen aus der vergangenen Woche berücksichtigt. 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 Verwaltung der geplanten Exporte einen beliebigen Server aus dem Auswahllisten **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)** aus.
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. Weitere Informationen zum Hinzufügen von Aufzeichnungsspeicher siehe <i>Speicher verwalten</i> .

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 dem Sie Ihre Aufzeichnungen exportieren möchten. ASF: Wählen Sie Add digital signature (Digitale Signatur hinzufügen), um Manipulationen an Bildern zu verhindern. Siehe dazu den Abschnitt <i>Digitale Signatur in Aufzeichnungen exportieren</i>. 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 2012 Server

Um Aufzeichnungen von einem Server mit Microsoft Windows Server 2012 zu exportieren, installieren Sie Desktop Experience:

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	Aktiviert einen lokalen TURN-Server auf dem AXIS Camera Station Pro-Server, sodass die WebRTC-Kommunikation über einen einzigen Port erfolgen kann. Das kann die Konfiguration der Firewall vereinfachen.
Prioritize TURN (TURN priorisieren)	Wählen Sie diese Option, damit WebRTC ausschließlich Relay-Kandidaten berücksichtigt.

Neue Verbindung

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

Verbindungsstatus

Gehen Sie zu  > Server > Connection status (Verbindungsstatus), um den Verbindungsstatus aller Server anzuzeigen.

Verwenden Sie den Schieber neben dem Servernamen, um die Verbindung zu einem Server herzustellen oder zu trennen.

Statuscode	Beschreibung	Mögliche Lösungen
Verbindung wird hergestellt	Der Client versucht Verbindungsaufbau zu diesem Server.	
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	Der Client ist nicht mit diesem Server verbunden.	
Erneut verbinden	Der Client hat die Verbindung zu diesem Server verloren und versucht, erneut eine Verbindung herzustellen.	
Erneute Verbindung fehlgeschlagen	Der Server wird gefunden, aber möglicherweise haben sich die Benutzerberechtigungen oder das Kennwort geändert.	- Fügen Sie den Benutzer im Dialog User permission (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 User permission (Benutzerberechtigung) hinzu.
Sicherheitsüberprüfung fehlgeschlagen	Eine WCF-bezogene Sicherheitsprüfung ist fehlgeschlagen.	Synchronisieren Sie die UTC-Zeit von Client- und Server-Computer.

Keine Verbindung mit dem Server-Computer	Der Server hat unter der angegebenen Adresse nicht geantwortet.	• Prüfen Sie, dass das Netzwerk richtig funktioniert. • Überprüfen Sie, dass der Server ausgeführt wird.
Kein Server läuft	Der Computer, 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. • Überprüfen Sie, dass der Server ausgeführt wird.
Ungültiger Hostname	Das DNS kann den Hostnamen nicht in eine IP-Adresse übersetzen.	• Überprüfen Sie, ob der Hostname richtig geschrieben ist. • Stellen Sie sicher, dass der DNS den Hostnamen auflösen kann.
Bereits mit demselben Server verbunden	Der Client ist bereits mit diesem Server verbunden.	Entfernen Sie den doppelten Servereintrag.
Nicht der erwartete Server	An dieser Adresse hat ein anderer Server als erwartet geantwortet.	Aktualisieren Sie den Server-Computer mit dem korrekten Server.
Client-Version (x) ist nicht mit Server-Version (y) kompatibel	Der Client ist im Vergleich zum Server zu alt oder zu neu.	Installieren Sie auf dem Client- und dem Server-Computer jeweils dieselbe Version von AXIS Camera Station Pro.
Server zu beschäftigt	Keine Server-Antwort aufgrund von Leistungsproblemen.	Stellen Sie sicher, dass der Server 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 Serverlisten angehören. Sie können Serverlisten importieren, exportieren und in anderen AXIS Camera Station Pro-Clients verwenden.

Gehen Sie zu  > Servers (Server) > Server lists (Serverlisten).

Standardmäßig erscheint die Liste **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 Serverliste aus und klicken Sie auf  , um diese zu löschen.
 New server list (Neue Serverliste)	Klicken Sie auf diese Option, um eine neue Serverliste hinzuzufügen und zu benennen.
Hinzufügen	Um einer Serverliste einen Server hinzuzufügen, wählen Sie eine Serverliste 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 Serverlisten importieren, um eine Verbindung zu den Servern herzustellen. Siehe <i>Mit einem Server verbinden</i> .
Edit (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 einen Server aus einer Serverliste zu entfernen, wählen Sie ihn aus und klicken Sie auf Remove (Entfernen) .
Liste umbenennen	Doppelklicken Sie auf die Liste und geben Sie einen neuen Namen ein.



Server in Server-Listen organisieren

Switch konfigurieren

Ein Gerät der Serie AXIS Camera Station S22 Appliance können Sie über AXIS Camera Station Pro konfigurieren. Gehen Sie zu **Configuration (Konfiguration) > Switch > Management (Verwaltung)** und geben Sie Ihre Zugangsdaten ein, um die Switch-Verwaltungsseite 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. Während dieses Zeitraums ist das System voll funktionsfähig. Sie können es konfigurieren und alle Funktionen testen, bevor Sie Lizenzen erwerben.
Überprüfen Sie Ihre Lizenzen	Wenn die Lizenz des Systems ohne automatische Erneuerung abläuft, gewährt AXIS License Manager eine weitere 30-tägige Nachfrist.
Lizenzen	Das System ist bis zum Ablauf des Gültigkeitsdatums vollständig lizenziert.
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 zu aktualisieren. Wenn Sie die automatische Lizenzierung nutzen, werden Sie dies möglicherweise überhaupt nicht bemerken. Wenn Sie die manuelle Lizenzierung nutzen und nicht innerhalb von 60 Tagen eine Neusynchronisierung durchführen, wird das System als nicht lizenziert eingestuft.
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 mehr verfügbar: • Livestreams • Wiedergabe von Aufzeichnungen • Sofortige Wiedergabe • Schnappschüsse • Export von Aufzeichnungen

Sie haben zwei Optionen zur Lizenzierung Ihres Systems:

Automatische Lizenzierung (Onlinesysteme) – Ihr System übermittelt 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, siehe *Ein System online lizenzieren*, on page 139.

Manuelle Lizenzierung (Offlinesysteme) – Diese Option erlaubt Ihnen den manuellen Export Ihrer Systemdatei sowie das anschließende Hochladen zum AXIS License Manager und den Import der neuen Lizenz. Bei sämtlichen Änderungen am System, die sich auf die Anzahl der Lizenzen auswirken, müssen Sie diesen Vorgang 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, siehe *Ein System offline lizenzieren*, on page 140.

Ein System online lizenzieren.

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 lizenzieren

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 (Konfiguration) > Security (Sicherheit) > User permissions (Benutzerrechte)** auf, um die Benutzer und Gruppen in AXIS Camera Station Pro anzuzeigen.

Hinweis

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

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

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

	Gibt an, ob es sich um einen Einzelbenutzer handelt.
	Gibt an, ob es sich um eine Benutzergruppe handelt.

Bezeichnung	Der auf dem lokalen Computer oder in Active Directory angezeigte Benutzername.
Domäne	Domain, zu der der Benutzer oder die Benutzergruppe gehört.
Rolle	Die dem Benutzer oder der Benutzergruppe zugewiesene Zugriffsrolle. Mögliche Werte: Administrator, Operator (Bediener) und Viewer (Betrachter).
Details	Detaillierte Benutzerinformationen wie diese auf dem lokalen Rechner oder in Active Directory erscheinen.
Server	Server, zu der der Benutzer oder die Benutzergruppe gehört.

Hinzufügen von Benutzern oder Gruppen

Benutzer von Microsoft Windows® und Active Directory sowie Benutzergruppen können auf AXIS Camera Station 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)**.
- Klicken Sie mit der rechten Maustaste auf **Users (Benutzer)** und wählen Sie **New User (Neuer Benutzer)**.
- Geben Sie im Popup-Dialog die Daten des neuen Benutzers ein und deaktivieren Sie **User must change password at next login (Benutzer muss bei der nächsten Anmeldung das Passwort ändern)**.
- Klicken Sie auf **Create (Erstellen)**.

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

Hinzufügen von Benutzern oder Gruppen

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

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

Konfigurieren eines Benutzers oder einer Gruppe

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

Benutzer oder Benutzergruppe entfernen

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

Benutzer-/Gruppenberechtigungen

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

Administrator – Vollständiger Zugriff auf das gesamte System, einschließlich Zugriff auf Live-Videos und Video-Aufzeichnungen sämtlicher Kameras, alle I/O-Ports und Ansichten. Diese Rolle ist erforderlich, um Zutritt zur Systemkonfiguration zu haben.

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

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

Kameras

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

Zugriff	Gewährt dem Benutzer Zugriff auf die Kamera und alle Kamerafunktionen.
Video	Gewährt dem Benutzer Zugriff auf das Live-Video der Kamera.
Audio – Wiedergeben	Gewährt dem Benutzer Zugriff auf das Abhören der Kamera.
Audio – Sprechen	Gewährt dem Benutzer Zugriff auf das Sprechen über die Kamera.
Manuelle Aufzeichnung	Erlaubt das manuelle Starten und Beenden von Aufzeichnungen.

Mechanisches PTZ	Zugriff auf mechanische PTZ-Steuerungen gewähren. Nur für Kameras mit mechanischer PTZ-Steuerung verfügbar.
PZT-Priorität	Legen Sie die PTZ-Priorität fest. Eine niedrigere Zahl steht für eine höhere Priorität. Ist keine Priorität zugewiesen, beträgt die Einstellung 0. Ein Administrator hat die höchste Priorität. Wenn ein Rolle mit höherer Priorität eine PTZ-Kamera ansteuert, können andere Rollen dieselbe Kamera 10 Sekunden lang (Standardkonfiguration) nicht ansteuern. Nur für Kameras mit mechanischem PTZ-Antrieb und Auswahl von Mechanical PTZ (Mechanischer PTZ) verfügbar.

Ansichten

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

Zugriff	Gewährt Zugriff auf die Ansichten in AXIS Camera Station Pro.
Edit (Bearbeiten):	Ermöglicht die Bearbeitung von Ansichten unter 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	Ermöglicht die Ansicht des Zustands des I/O-Ports, ohne diesen zu ändern.
Schreiben	Ermöglicht die Änderung des Zustands des I/O-Ports.

System

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

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

Schnappschuss aufnehmen	Ermöglicht das Aufnehmen von Schnappschüssen in der Live-Ansicht und im Aufzeichnungsmodus.
Aufzeichnungen exportieren	Das Exportieren von Aufzeichnungen zulassen.
Vorfallsberichte erstellen	Das Erstellen von Vorfallsberichten zulassen.
Prevent access to recordings older than (Zugriff auf Aufzeichnungen verhindern, wenn älter als)	Verhindert den Zugriff auf Aufzeichnungen, die älter sind als die angegebene Minutenzahl. Benutzer können diese Aufzeichnungen bei der Suche nicht finden.

Zugriff auf Alarmer, Aufgaben und Protokolle	Erlaubt den Erhalt von Alarbenachrichtigungen und den Zugriff auf die Funktionsleiste Alarms and tasks (Alarmer und Aufgaben) sowie die Registerkarte Logs (Protokolle) .
Access data search (Zugriff auf die Datensuche)	Ermöglicht die Suche nach Daten, um nachzuverfolgen, was zum Zeitpunkt eines Ereignisses passiert ist.
Ereignisse zu Kategorien hinzufügen	Ermöglicht das Hinzufügen von Kategorien zu Ereignissen auf der Registerkarte Recordings (Aufzeichnungen) .
Kategorien von Ereignissen entfernen	Ermöglicht das Entfernen von Kategorien aus Ereignissen auf der Registerkarte Recordings (Aufzeichnungen) .

Zutrittskontrolle

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

Konfiguration der Zutrittskontrolle	Erlaubt die Konfiguration von Türen und Zonen, Identifikationsprofilen, Kartenformaten und PIN, verschlüsselter Kommunikation und Multi-Server.
Zugriffsverwaltung	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	Erlaubt die Konfiguration von AXIS Audio Manager Pro in AXIS Camera Station Pro und den Zugriff auf die Schnittstelle eines AXIS Audio Manager Pro-Servers. Nur für Bediener verfügbar.
Zugriff auf die AXIS Audio Manager Pro-Schnittstelle	Erlaubt den Zugriff auf die Schnittstelle eines AXIS Audio Manager Pro-Servers. Nur für Betrachter verfügbar.

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

Systemzustand überwachen

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

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

Zertifikate

Zur Verwaltung der Zertifikateinstellungen für den AXIS Camera Station Pro-Server und die verbundenen Geräte gehen Sie zu **Configuration (Konfiguration) > Security (Sicherheit) > Certificates (Zertifikate)**.

Weitere Informationen zum Aktivieren, Löschen und Anzeigen von HTTPS- und IEEE 802.1X-Zertifikaten finden Sie unter *Sicherheit, on page 72*.

AXIS Camera Station Pro kann verwendet werden als:

- **Stammzertifizierungsstelle (Stamm-CA):** AXIS Camera Station Pro verwendet zur Ausstellung von Serverzertifikaten ein eigenes Stammzertifikat, ohne dass eine andere Stamm-CA beteiligt ist.
- **Zwischenzertifizierungsstelle:** Importieren Sie ein CA-Zertifikat und dessen privaten Schlüssel in AXIS Camera Station Pro, um Serverzertifikate für Axis Geräte zu signieren und auszustellen. Dabei kann es sich um ein Stammzertifikat oder ein Zertifikat einer Zwischen-CA handeln.

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 dessen privaten Schlüssel zu importieren. AXIS Camera Station Pro speichert das Kennwort für das Zertifikat.
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 die 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: • Without the private key (Ohne privaten Schlüssel): Speichert das Zertifikat im Format .cer oder .crt. 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. • With the private key (Mit privatem Schlüssel): Speichert die CA im PKCS#12-Format (.pfx oder .p12). 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). Die CA signiert keine Zertifikate, die über ihr eigenes Ablaufdatum hinaus gültig sind.

Erstellen einer Root-CA

Beim Start von AXIS Camera Station Pro wird nach einer CA gesucht. Wird keine Zertifizierungsstelle gefunden, generiert es automatisch eine Stamm-CA. 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 147*.

Bei einer Aktualisierung von Version 5.45 oder einer früheren Version mit einem manuell auf einem Gerät installierten Zertifikat greift AXIS Camera Station Pro automatisch auf die vorhandene Stamm-CA zurück und installiert ein neues Zertifikat, sobald das manuell installierte 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 147*.

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 auf **OK**, um fortzufahren.

- 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. Deaktivieren Sie die Option **Validate device certificate** (Gerätezertifikat prüfen).
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. **Configuration > Devices > Management** (Konfiguration > Geräte > Verwaltung) aufrufen.
7. Rechtsklicken Sie die Geräte und wählen Sie **Sicherheit > HTTPS > Aktivieren/Aktualisieren**.
8. Gehen Sie zu **Configuration (Konfiguration) > Security (Sicherheit) > Certificates (Zertifikate) > HTTPS** und aktivieren Sie **Validate device certificate** (Gerätezertifikat prüfen).

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 zum Identitätsnachweis verwenden. 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 zum Identitätsnachweis vor dem Herstellen einer Server-Verbindung verwenden. 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 validiert standardmäßig das HTTPS-Serverzertifikat auf allen verbundenen Geräten und stellt keine Verbindung zu Geräten ohne validiertes 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 werden als nicht vertrauenswürdig eingestuft. 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 diese Option, um nur eine Verbindung zu Geräten mit einem gültigen Zertifikat zuzulassen. Ohne Validierung des Zertifikats können sich Geräte mit ungültigen Zertifikaten verbinden.
Geräteadresse validieren	Deaktivieren Sie diese Option, um ein stabileres Verhalten in DHCP-Netzwerken zu erzielen, in denen keine Host-Namen verwendet werden. Aktivieren Sie diese Option, um für zusätzliche Sicherheit die Übereinstimmung der Adressen zu gewährleisten. Es wird empfohlen, diese Einstellung nur in Netzwerken zu aktivieren, in denen Geräte hauptsächlich Host-Namen verwenden oder über statische IP-Adressen verfügen.

Hinweis

- Wenn keine sichere Verbindung (HTTPS) verfügbar ist, können Sie ein neues HTTPS-Zertifikat ausstellen. Siehe *Geräte hinzufügen, on page 48*
- Um HTTPS verwenden zu können, ist auf Videogeräten Firmware 5.70 oder höher erforderlich und Firmware 1.25 oder höher für Zugriffskontrolle und Audiogeräte.

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 bezogen, z. B. vom IEEE 802.1X-Authentifizierungsserver, oder direkt in AXIS Camera Station Pro erzeugt werden. Dieses Zertifikat wird auf jedem Axis Gerät installiert, um den Authentifizierungsserver zu überprüfen.

Hinweis

Um IEEE 802.1X-Zertifikate zu verwenden, ist Firmware 5.50 oder höher erforderlich für Videogeräte und Firmware 1.25 oder höher für Zugriffskontrolle und Audiogeräte.

IEEE 802.1X konfigurieren:

1. Wechseln Sie zu **Konfiguration > Sicherheit > Zertifikate**.
2. Wählen Sie im Auswahlnenü **EAPOL Version (EAPOL-Version)** die zu verwendende EAP-Version (Extensible Authentication Protocol) aus.
3. Wählen Sie im Auswahlnenü **EAP identity (EAP-Identität)** aus, ob Sie die MAC-Adresse des Geräts, den Host-Namen des Geräts oder einen benutzerdefinierten Text verwenden möchten.
4. Geben Sie bei Auswahl von **Custom (Benutzerdefiniert)** den Text ein, der als EAP-Identität verwendet werden soll.
5. Klicken Sie auf **Import (Importieren)** und wählen Sie die CA-Zertifikatsdatei zur IEEE 802.1X-Authentifizierung aus.
6. Wählen Sie im Auswahlnenü **Common name (Allgemeiner Name)** die Option **Device IP address (Geräte-IP-Adresse)** oder **Device EAP identity (Geräte-EAP-Identität)** als allgemeinen Namen für die für jedes Gerät erstellten Zertifikate aus.
7. **Configuration > Devices > Management** (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. Das gilt für 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 (Warnhinweis: Zertifikat läuft ab)** ein, wie viele Tage vor Ablauf des Zertifikats AXIS Camera Station Pro Sie benachrichtigen soll.

Zertifikatserneuerung

Zertifikat zwischen Server und Gerät erneuern

Von AXIS Camera Station Pro ausgestellte Client- und Server-Zertifikate werden 7 Tage vor Ablauf und Anzeige der Warnmeldung automatisch verlängert. Dazu muss für das Gerät HTTPS oder IEEE 802.1X aktiviert sein. Weitere Informationen zur manuellen Verlängerung oder Aktualisierung von Zertifikaten finden Sie unter *Sicherheit, on page 72*.

Zertifikat zwischen Server und Client erneuern

Sie können ein neues Serverzertifikat auf der Registerkarte **Certificates (Zertifikate)** in der Dienststeuerung von AXIS Camera Station Pro erstellen. Die entsprechende Anleitung finden Sie unter *Zertifikate, on page 232*.

Kennwort zurücksetzen

1. Wechseln Sie zu **Konfiguration > Sicherheit > Zertifikate**.
2. Deaktivieren Sie die Option **Validate device certificate (Gerätezertifikat prüfen)**, um den Zugriff auf Geräte mit CA-Zertifikat weiterhin zu ermöglichen.
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. Aktivieren Sie die Option **Validate device certificate (Gerätezertifikat prüfen)**.

Konfigurieren Sie die 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 der 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 170*.
2. Informationen zur Verwendung eines benutzerdefinierten Setups für Kartenformate und die PIN-Länge finden Sie unter *Kartenformate und PIN, on page 172*.
3. Fügen Sie einen Zugang hinzu und wenden Sie ein Identifizierungsprofil auf den Zugang an. Siehe *Fügen Sie einen Zugang hinzu, on page 154*.
4. Konfigurieren Sie den Zugang:
 - *Türpositionssensor hinzufügen, on page 161*
 - *Notfallsensor hinzufügen, on page 163*
 - *Leser hinzufügen, on page 164*
 - *REX-Gerät hinzufügen, on page 166*
5. Fügen Sie eine Zone hinzu und fügen Sie der Zone Zugänge hinzu. Siehe *Zone hinzufügen, on page 167*.

Kompatibilität der Gerätesoftware für Tür-Steuerungen

Wichtig

Beachten Sie bei einer Aktualisierung von AXIS OS auf Ihrer Tür-Steuerung Folgendes:

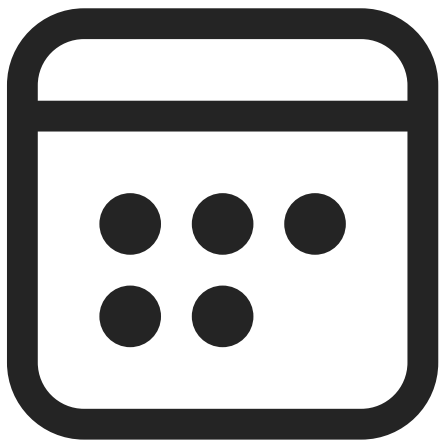
- **Unterstützte Versionen von AXIS OS:** Die unten aufgeführten unterstützten Versionen von AXIS OS gelten nur bei einer Aktualisierung von der empfohlenen AXIS Camera Station Pro-Originalversion und bei einer Systemkonfiguration mit Zutrittspunkt. Wenn das System diese Bedingungen nicht erfüllt, müssen Sie eine Aktualisierung auf die von empfohlene AXIS OS Version für die jeweilige AXIS Camera Station Pro-Version vornehmen.
- **Unterstützte Mindestversion von AXIS OS:** Die älteste im System installierte Version von AXIS OS bestimmt die unterstützte Mindestversion von AXIS OS, wobei diese maximal zwei Versionen älter sein darf. Angenommen, Sie verwenden AXIS Camera Station Pro Version 6.5 und aktualisieren alle Geräte auf die empfohlene AXIS OS-Version 12.0.86.2. Dann ist AXIS OS-Version 12.0.86.2 die Mindestversion, die von Ihrem System unterstützt wird.
- **Aktualisierung auf eine neuere als die empfohlene AXIS OS-Version:** Angenommen, Sie aktualisieren AXIS OS auf eine höhere Version als die für eine bestimmte AXIS Camera Station Pro-Version empfohlene. Dann können Sie Ihr System jederzeit problemlos auf die empfohlene AXIS OS-Version zurücksetzen, solange diese innerhalb der Unterstützungsgrenzen für die AXIS Camera Station Pro-Version liegt.
- **Zukünftige empfohlene AXIS OS-Versionen:** Verwenden Sie immer die empfohlene AXIS OS-Version für die jeweilige AXIS Camera Station Pro-Version, um die Systemstabilität und vollständige Kompatibilität zu gewährleisten.
- **Track-Wechsel:** Der Wechsel der Firmware-Tracks zwischen 10.12.xx und 11.0.xx oder höher erfordert das Zurücksetzen auf die werksseitige Standardeinstellung.

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 6.17	12.6.102.1	12.9.65.3
Pro 6.16	12.6.102.1	12.9.65.3
Pro 6.15	12.5.68.1	12.8.55.1

Türen und Bereiche

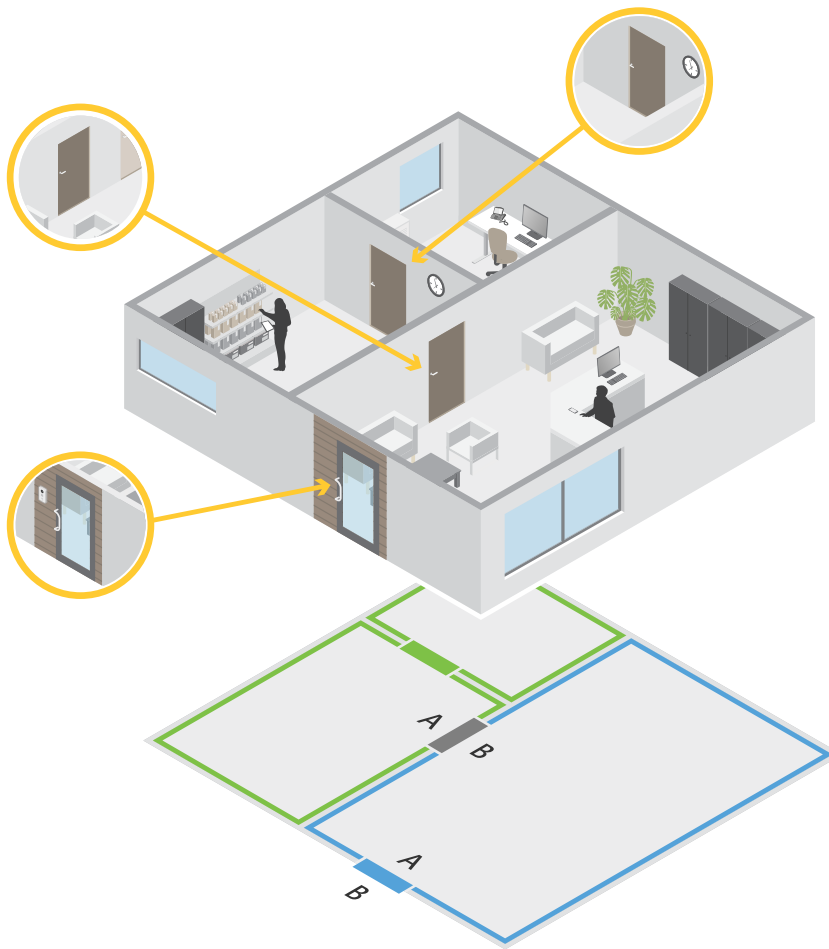
Rufen Sie **Configuration > Access control > Doors and zones** (**Konfiguration > Zutrittskontrolle > Zugänge und Zonen**) auf, um eine Übersicht zu erhalten und Zugänge und Zonen zu konfigurieren.

 Manuelle Aktionen	Legen Sie den Status eines Zugangs manuell fest. Wählen Sie eine der folgenden Optionen aus: Reset (Zurücksetzen) (gemäß den Systemregeln), Grant access (Zugriff gewähren) (Zugang für 7 Sekunden entriegeln), Unlock (Entriegeln) (Zugang entriegelt lassen), Lock (Verriegeln) (Zugang verriegelt lassen) oder Lockdown (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. Um die Pin Chart auszudrucken, 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.
Type (Typ):	Hierbei handelt es sich um die Art der Zugangsconfiguration.
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	Status des Zugangs. • Online: Der Zugang ist online und funktioniert einwandfrei. • Reader offline (Leser offline): Der in der Konfiguration des Zugangs angegebene Leser ist offline. • Reader error (Leserfehler): Der Leser unterstützt keinen sicheren Kanal oder dieser ist für den Leser deaktiviert. • Old firmware (Firmware veraltet): Das Gerät nutzt eine veraltete Firmware-Version. Aktualisieren Sie die Firmware, um die optimale Funktion und 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.

Fügen Sie einen Zugang hinzu

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.

Zum Hinzufügen einer Tür:

1. Rufen Sie **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen)** auf.
2. Klicken Sie auf **+ Add (Hinzufügen)** und wählen Sie einen Zugangstyp aus der Auswahlliste aus.

Türarten	
Tür	Eine herkömmliche Tür mit einem Zugangsmonitor, der Schlösser und Leser unterstützt. Erfordert eine Tür-Steuerung.
Etage	Ein Zugangstyp für die Aufzugssteuerung, der den Zugriff auf die Aufzugsetagen mithilfe von Kartenlesegeräten authentifiziert. Weitere Informationen finden Sie unter <i>Add a floor (Etage hinzufügen)</i> ^{BETA} , on page 162.
Überwachter Zugang	Ein Zugang, der melden kann, ob er geöffnet oder geschlossen ist. Weitere Informationen finden Sie unter <i>Überwachten Zugang hinzufügen</i> , on page 161.
Drahtloser Zugang	Ein Zugang, der sich mit Funkschlössern und Kommunikationshubs ASSA ABLOY Aperio® konfigurieren lässt. Weitere Informationen finden Sie unter <i>Drahtloses Schloss hinzufügen</i> , on page 159.
Vorgesehener Zugang	Ein Platzhalter für eine Tür, den Sie dem System hinzufügen können, ohne Hardware auszuwählen.

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. Die Steuerung wird ausgegraut, wenn kein weiterer Zutrittspunkt hinzugefügt werden kann, wenn die Steuerung offline ist oder wenn HTTPS deaktiviert 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 170.
8. Konfigurieren Sie den Zugang, indem Sie unter **Sensors (Sensoren)**, **Side A (Seite A)** und **Side B (Seite B)** Sensoren oder Leser hinzufügen.
9. Konfigurieren Sie die Einstellungen für den jeweiligen Zugang. Siehe *Einstellungen der Tür*, on page 156.
10. Konfigurieren Sie die Sicherheitsstufe. Siehe *Sicherheitsstufe der Tür*, on page 157.
11. Klicken Sie auf **Save (Speichern)**.

Konfiguration eines Zugangs kopieren:

1. Rufen Sie **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugang und Zonen)** auf.
2. Klicken Sie auf **+ Add (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. Klicken Sie auf **Save (Speichern)**.



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

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 unter **Door settings (Einstellungen des Zugangs)** die gewünschten Einstellungen und klicken Sie auf **Save (Speichern)**.

Zugangszeit (s)	Legen Sie die Dauer in Sekunden fest, für die der Zugang nach der Gewährung des Zutritts entriegelt bleibt. Der Zugang wird sofort nach dem Schließen wieder verriegelt, selbst wenn noch Zeit verbleibt.
Open-too-long time (sec) (Maximale Öffnungsdauer (s))	Diese Einstellung ist nur gültig, wenn ein Zugangsmonitor konfiguriert wurde. Legen Sie fest, wie lang der Zugang in Sekunden geöffnet bleiben darf. Wenn der Zugang bei Ablauf der Zeit weiterhin geöffnet ist, wird der Alarm „Door open too long“ (Tür zu lange geöffnet) ausgelöst. Konfigurieren Sie eine Aktionsregel, die die auszuführende Aktion bei Eintreten dieses Ereignisses festlegt.
Lange Zutrittszeiten (Sekunden)	Legen Sie mit dieser Einstellung die Dauer in Sekunden fest, für die ein Zutrittspunkt für Karteninhaber, bei denen diese Einstellung aktiviert ist, nach der Gewährung des Zutritts entriegelt bleibt. Diese Einstellung hat Vorrang vor der Standard-Zutrittszeit.
Long open-too-long time (sec) (Lange maximale Öffnungsdauer (s))	Diese Einstellung ist nur gültig, wenn ein Zugangsmonitor konfiguriert wurde. Legen Sie die Dauer in Sekunden fest, für die ein Zutrittspunkt für Karteninhaber geöffnet bleiben darf, wenn die Option Long access time (Lange Zutrittszeiten) aktiviert ist. Diese Einstellung hat Vorrang vor der Standardeinstellung für eine lange maximale Öffnungsdauer.
Verzögerungszeit bis zum Wiederverriegeln (ms)	Legen Sie die Dauer in Millisekunden fest, für die ein Zutrittspunkt nach dem Öffnen oder Schließen entriegelt bleibt.
Wieder verriegeln	• After opening (Nach dem Öffnen): Diese Einstellung ist nur gültig, wenn ein Zugangsmonitor hinzugefügt wurde.

	• After closing (Nach dem Schließen): Dieser Einstellung ist nur gültig, wenn ein Zugangsmonitor hinzugefügt wurde.
Zugang erzwungen	Wählen Sie, ob das System einen Systemalarm auslösen soll, wenn der Zugang erzwungen wird. 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.

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.

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 – Der Zugang bleibt entriegelt, bis Sie ihn zurücksetzen.

Verriegeln – 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.
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 Funktion wirkt sich nicht auf einen vorhandenen Zeitplan aus. Wenn z. B. 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 beim Hinzufügen eines neuen Zugangs konfigurieren oder sie auf einen vorhandenen Zugang anwenden.

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**.

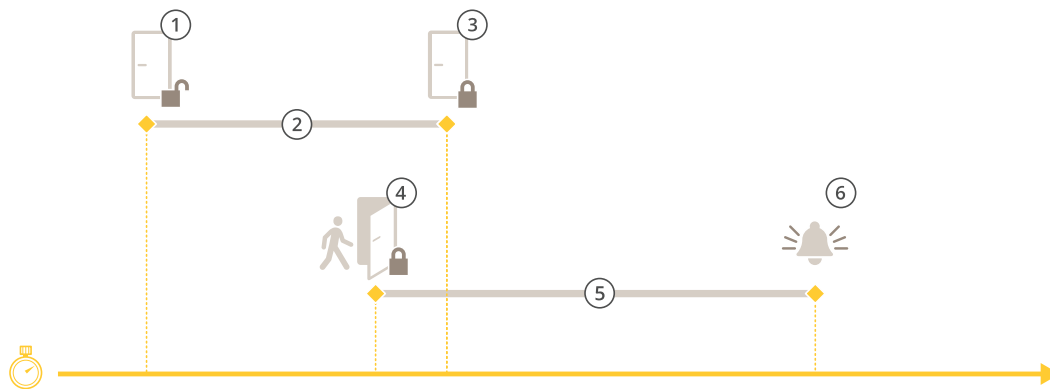
Zwei-Personen-Regel	
Side A (Seite A) und Side B (Seite B)	Wählen Sie aus, auf welchen Seiten der Tür die Regel verwendet werden soll.
Zeitschemata	Wählen Sie „While the rule is active“ (Während die Regel aktiv ist).
Zeitüberschreitung (Sekunden)	Diese Zeitüberschreitung gibt die maximal zulässige Zeit zwischen dem Durchziehen der Karte oder der Verwendung anderer gültiger Zugangsdaten vor.

So fügen Sie einem vorhandenen Zugang **Double Swipe** hinzu:

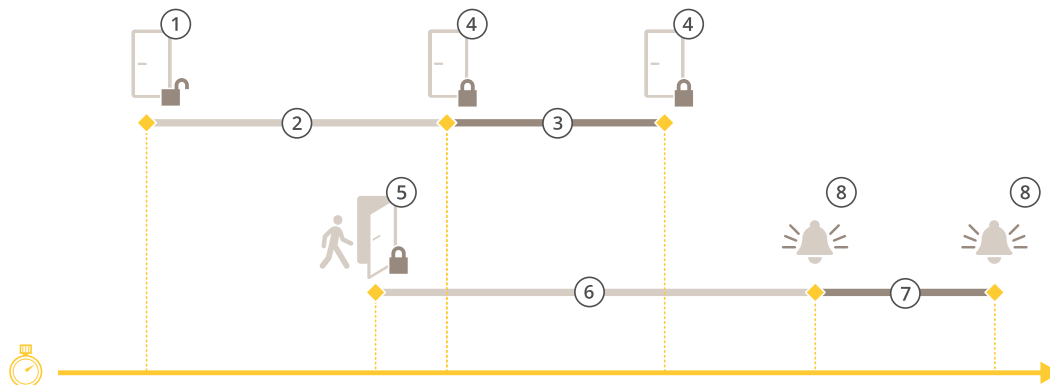
1. Rufen Sie **Configuration > Access control > Doors and zones** (Konfiguration > Zutrittskontrolle > Zugang und Zonen) auf.
2. Wählen Sie die Tür aus, für die Sie eine Sicherheitsstufe konfigurieren möchten.
3. Klicken Sie auf **Edit (Bearbeiten)**.
4. Klicken Sie auf **Security level (Sicherheitsstufe)**.
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)	Diese Zeitüberschreitung gibt die maximal zulässige Zeit zwischen dem Durchziehen der Karte oder der Verwendung anderer gültiger Zugangsdaten vor.

Zeitoptionen



- 1 Zugang gewährt – Schloss entriegelt
- 2 Zugangszeit
- 3 Keine Aktion ausgeführt – Schloss bleibt 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 bleibt 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 Kommunikations hubs 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.



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

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 der Axis Tür-Steuerung 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. Multidrop wird nicht unterstützt.
 - Die Funkschlösser folgen den 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 unter **Doors (Zugänge)** auf  **Add (Hinzufügen)**.
 - 4.3. Wählen Sie **Wireless door (Drahtloser Zugang)** als **Door type (Zugangstyp)** und die mit dem Aperio-Hub verbundene Tür-Steuerung aus.
 - 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 151*.

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

Nach der Verbindung des Funkschlusses 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	Akku austauschen. Das Schloss funktioniert nicht wie vorgesehen.

Sperrstatus	Aktion
Online	Keine
Verriegelungsstau	Mechanische Probleme mit dem Schloss beheben.

Türpositionssensor hinzufügen

Ein Türpositionssensor ist ein Schalter, der den physischen Zustand einer Tür erfasst. Sie können einen Türpositionssensor zu Ihrer Tür hinzufügen und die Verbindungsart konfigurieren.

1. Rufen Sie die Seite zur Zugangsconfiguration auf. Siehe *Fügen Sie einen Zugang hinzu*, on page 154.
2. Klicken Sie unter **Sensors (Sensoren)** auf **Add (Hinzufügen)**.
3. Wählen Sie **Door position sensor (Türpositionssensor)**.
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 der Tür-Steuerung und dem Zugangsmonitor abbricht, aktivieren Sie **Supervised input (Überwachter Eingang)**. Siehe *Überwachte Eingänge*, on page 169.

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 netzwerkbasierendes E/A-Relaismodul, das mit einer Tür-Steuerung verbunden ist. Sie können bis zu fünf Sensoren für die Türposition mit einem netzwerkbasierenden E/A-Relaismodul verbinden.

Hinweis

Für einen überwachten Zugang brauchen Sie das netzwerkbasierende 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 netzwerkbasierendes 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 (Türpositionssensor)** aus.
10. Wählen Sie den E/A, der mit dem Sensor für die Türposition verbunden ist.
11. Klicken Sie auf **Hinzufügen**.

Add a floor (Etage 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. Zum Hinzufügen Ihres Moduls zu einem Controller siehe .

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. Gehen Sie zu **Configuration (Konfiguration) > Access control (Zutrittskontrolle) > Doors and zones (Zugänge und Zonen)**.
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. Diese Option ist nur verfügbar, wenn Ihre Steuerung über Relais verfügt.
8. Klicken Sie auf **Save (Speichern)**, wenn Sie die Etage hinzugefügt haben. Die Etagen als „Aufzugsname – Etagenname“ angezeigt, zum 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.

Notfallsensor 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 Zugangsconfiguration auf. Siehe *Fügen Sie einen Zugang hinzu, on page 154*.
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.

IP-Leser hinzufügen

Sie können eine Axis Netzwerk-Türsprechanlage oder ein anderes IP-fähiges Gerät als Leser verwenden. Bevor Sie das Gerät einem Zugang zuweisen können, müssen Sie es in AXIS Camera Station Pro hinzufügen.

Hinweis

Stellen Sie sicher, dass der IP-Leser eingeschaltet und mit demselben Netzwerk wie AXIS Camera Station Pro verbunden ist, bevor Sie beginnen.

1. Gehen Sie zu **Configuration (Konfiguration) > Devices (Geräte) > Add devices (Geräte hinzufügen)**.
2. Wählen Sie Ihren IP-Leser aus der Liste der erkannten Geräte aus und klicken Sie auf **Add (hinzufügen)**.
3. Geben Sie die Zugangsdaten des Geräts ein, wenn Sie dazu aufgefordert werden.

Sobald das Gerät hinzugefügt wurde, können Sie es einem Zugang zuweisen. Siehe dazu *Leser hinzufügen, on page 164*.

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 eine benutzerdefinierte Konfiguration von Kartenformaten oder PIN-Längen auf einen Leser angewendet wird, erscheint dieses in **Card formats (Kartenformate)** unter **Configuration (Konfiguration) > Access control (Zutrittskontrolle) > Doors and zones (Zugänge und Zonen)**. Siehe *Türen und Bereiche, on page 151*.

Hinweis

- Sie können auch bis zu 16 Bluetooth-Leser zu einer Tür-Steuerung hinzufügen. Weitere Informationen finden Sie unter *Bluetooth-Leser hinzufügen, on page 165*.
 - Wenn Sie ein Axis IP-Türkontrollsystem als IP-Leser verwenden, nutzt das System die auf der Webseite des Geräts eingestellte PIN-Konfiguration.
1. Rufen Sie die Seite zur Zugangsconfiguration auf. Siehe *Fügen Sie einen Zugang hinzu, on page 154*.
 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. Zur Verwendung einer benutzerdefinierten 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, wiederholen Sie dieses Verfahren.

Informationen zur Installation eines AXIS Barcode Reader finden Sie unter *AXIS Barcode Reader installieren, on page 175*.

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. Sie können Netzwerk-Türkontrollsysteme von Axis als IP-Leser verwenden.

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 den Schaltkreiszustand, bei dem der Manipulationseingang des Lesers aktiviert wird. • Open circuit (Schaltkreis unterbrochen): Der Leser übermittelt dem Zutrittspunkt das Manipulationssignal, wenn der Schaltkreis unterbrochen ist. • Closed circuit (Schaltkreis geschlossen): 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 <i>Überwachte Eingänge</i> , on page 169.

Bluetooth-Leser hinzufügen

Mit dem AXIS A4612 Network Bluetooth Reader können Sie die Reichweite kabelgebundener Zutrittspunkte von Axis-Tür-Steuerungen erweitern. Jeder Tür-Steuerung können bis zu 16 dieser Leser zugewiesen werden. 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 166.
2. Rufen Sie die Seite zur Zugangsconfiguration auf. Siehe *Fügen Sie einen Zugang hinzu*, on page 154.
3. Klicken Sie unter einer Türseite 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-Leser zu einem Zutrittspunkt in AXIS Camera Station Pro 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 auf der Seite des Zugangs, auf der 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, siehe *Identifizierungsprofile, on page 170*.
6. Fügen Sie dem Karteninhaber die mobilen Zugangsdaten hinzu. Siehe *Zugangsdaten hinzufügen, on page 190*.
7. Koppeln Sie die mobilen Zugangsdaten mit dem gekoppelten Kartenleser:
 - 7.1. Halten Sie das Mobiltelefon des Karteninhabers an den kopplungsfähigen Bluetooth-Kartenleser.
 - 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 Zugangsconfiguration auf. Siehe *Fügen Sie einen Zugang hinzu, on page 154*.

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 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 der Netzwerk-Tür-Steuerung und dem REX-Gerät abbricht, aktivieren Sie **Supervised input (Überwachter Eingang)**. Siehe *Überwachte Eingänge*, on page 169.

Aktion	
Tür entriegeln	Wählen Sie diese Option aus, um die Tür zu entriegeln, wenn sie das REX-Signal empfängt.
Keine	Wählen Sie diese Option, um keine Aktion auslösen zu lassen, wenn der Zutrittspunkt das REX-Signal empfängt.

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 154.

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

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. Personen müssen den Bereich verlassen, bevor sie ihre Zugangsdaten erneut verwenden können.

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 beim Hinzufügen einer neuen Zone konfigurieren oder sie auf eine vorhandene Zone anwenden. 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. Aktivieren Sie die Sicherheitsfunktionen, die Sie der Zone hinzufügen möchten.
6. Klicken Sie auf **Anwenden**.

Anti-Passback	
Log violation only (Soft) (Nur Verstoß protokollieren (Soft))	Wählen Sie diese Option aus, um einer zweiten Person den Zugang mit denselben Zugangsdaten wie der ersten Person zu gestatten. Diese Option löst lediglich einen Systemalarm aus.

Deny access (Hard) (Zutritt verweigern (Hard))	Wählen Sie diese Option, um zu verhindern, dass eine zweite Person mit denselben Zugangsdaten wie die erste Person Zugang erhält. Diese Option löst ebenfalls einen Systemalarm aus.
Zeitüberschreitung (Sekunden)	Die Zeitspanne, bis das System einem Benutzer erneut den Zutritt gewährt. Geben Sie den Wert 0 für die Zeitüberschreitung ein, um die Anti-Passback-Funktion zu aktivieren, 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 zu einer Tür-Steuerung ein Ereignis auslösen.

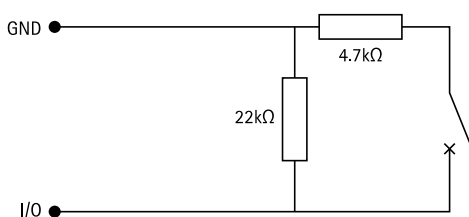
- Verbindung zwischen Tür-Controller und Türmonitor. Siehe *Türpositionssensor hinzufügen, on page 161*.
- Verbindung zwischen dem Tür-Controller und dem Leser, der Wiegand-Protokolle verwendet. Siehe *Leser hinzufügen, on page 164*.
- Verbindung zwischen Tür-Controller und REX-Gerät. Siehe *REX-Gerät hinzufügen, on page 166*.

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 K Ω parallel resistor and a 4.7 K Ω serial resistor (Parallelschaltung mit einem parallelen Widerstand (22 K Ω) und einem seriellen Widerstand (4,7 K Ω))**.
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.

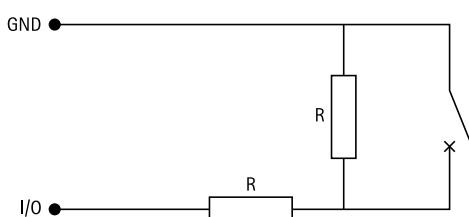
Paralleler Anschluss hat Vorrang

Die Widerstandswerte müssen 4,7 k Ω und 22 k Ω betragen.



Serielle erste Verbindung

Die Widerstandswerte müssen identisch sein und zwischen 1 und 10 k Ω 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) und wählen Sie eine Identifikationsart sowie 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) und wählen Sie eine Identifikationsart sowie 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**.

Zurücksetzen 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

Ein Kartenformat legt fest, wie ein Leser Daten von einer Karte interpretiert. Es sind vordefinierte Kartenformate zur Verwendung oder Bearbeitung verfügbar. Außerdem können Sie eigene Kartenformate 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.

Einrichtungscod – Eine Teilmenge der binären Zugangsdaten, die als Dezimal- oder Hexadezimalzahlen codiert ist. Verwenden Sie den Gebäude-Zugangscod, 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-Zugangscod)** 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).



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

Einrichten von Kartenformaten

Bearbeiten eines Kartenformats

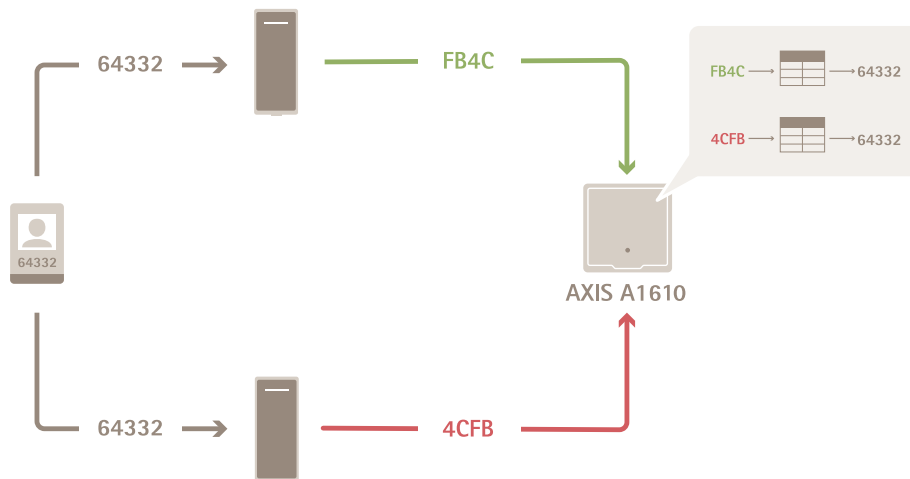
1. Rufen Sie **Configuration > Access Control > Card formats and PIN (Konfiguration > Zutrittskontrolle > Kartenformate und PIN)** auf.
2. Wählen Sie ein Kartenformat aus und klicken Sie auf .
3. Wenn Sie ein vordefiniertes Kartenformat bearbeiten, können Sie nur **Invert bit order (Bit-Reihenfolge invertieren)** 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 in 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.

64332 = 1111 1011 0100 1100 → 0011 0010 1101 1111 = 13023

→ Read from left Read from right ←

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.

64 332 = 1111 1011 0100 1100 → 0100 1100 1111 1011 = 19707

F B 4 C 4 C F B

26-Bit-Standard-Wiegand-Kartenformat



- 1 *Führende Parität*
- 2 *Einrichtungscode*
- 3 *Kartenummer*
- 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 ein 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*.

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. Einen vollständigen Arbeitsablauf zur Einrichtung von AXIS License Plate Verifier in AXIS Camera Station Pro finden Sie unter .

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. Die Anwendung starten.
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 > Belichtungen** 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 *Hinzufügen eines Zugangs*.
3. Wählen Sie **QR** als Identifizierungsprofil für diesen Zugang. Siehe *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. Informationen zur individuellen Konfiguration von Ports finden Sie unter *Allgemeine Servereinstellungen, on page 219*.
- 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 177*.
2. Konfigurieren Sie einen Server als Hauptserver und importieren Sie die Konfigurationsdatei der Subserver. Siehe *Importieren der Konfigurationsdatei auf den Hauptserver, on page 177*.
3. Konfigurieren Sie globale Karteninhaber und Karteninhabergruppen auf dem Hauptserver. Siehe *Karteninhaber hinzufügen, on page 188* und *Gruppe hinzufügen, on page 193*.
4. Auf dem Subserver können Sie die globalen Karteninhaber und Karteninhabergruppen anzeigen und überwachen. Siehe *Zugriffsverwaltung, on page 188*.

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 auf support.microsoft.com. Falls Sie ein Active Directory-Domainnetzwerk 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 178.

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 190.

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. Beide Server müssen 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 nutzen beide standardmäßig Port 443. Um Verbindungsprobleme zu vermeiden, konfigurieren Sie für einen Server einen anderen Port.

Sie können die Portkonfiguration in AXIS Camera Station Pro über *Allgemeine Servereinstellungen*, on page 219 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)**.

Wenn 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 210.

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

Mit „Intelligente Suche 2“ können Sie Filter festlegen, um in den Aufzeichnungen von Axis Kameras Personen und Fahrzeuge zu finden.



Informationen zu Anforderungen, Einschränkungen und Verwendung dieser Funktion finden Sie unter *Intelligente Suche 2*, on page 39.

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)** auf  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, sowie schaukelnde Objekte wie Laub ausschließen.
Die Suchfilter der intelligenten Suche verwenden alle vorhandenen Bewegungseinstellungsfiler 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 die Anzeige von Ergebnissen zu ermöglichen, für die keine Metadaten erfasst wurden.
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 als Auslöser in Aktionsregeln konfigurieren. 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 39*.
4. Klicken Sie auf **Next (Weiter)**.
5. Passen Sie unter **Confidence (Zuverlässigkeitsstufe)** die Vertrauenswürdigkeit der Erfassungen an. Bei einer höheren Zuverlässigkeitsstufe werden unsichere Klassifizierungen herausgefiltert und die Anzahl der Erfassungen sinkt.
6. Klicken Sie auf **Next (Weiter)**.
7. Geben Sie einen Namen für Ihren Auslöser ein und klicken Sie auf **Save (Speichern)**.

Hinweis

- „Intelligente Suche 2“ benötigt in der Regel einige Sekunden nach Verlassen des Kamerasichtfelds durch ein Objekt, um die Videodaten zu analysieren und die Erfassung gegenzuprüfen. Wenn Sie beispielsweise eine Aktionsregel erstellt haben, die bei Erfassung eines roten Fahrzeugs ausgelöst wird, erfolgt die Auslösung der Aktion erst einige Sekunden, nachdem das Objekt das Sichtfeld der Kamera verlassen 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 führen. Treten diese häufig auf, können Sie Ihren Auslöser so anpassen, dass er weniger Kameras einschließt, und Kamerafilter wie die Überquerung von Linien, Bereich, Größe und Dauer nutzen, um Verarbeitungsverzögerungen 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 105*.

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 die Zustandsdaten Ihres Systems von jedem Ort aus einsehen. Wenn Sie noch nicht verbunden sind, klicken Sie auf Manage (Verwalten) und befolgen Sie die Anweisungen auf dem Bildschirm.
Data retrieval frequency (Datenabruffrequenz)	Wählen Sie bei Warnungen bezüglich veralteter Daten oder allgemeiner Leistungsprobleme eine niedrigere Datenabruffrequenz. Bei einer Konfiguration mit mehreren Systemen empfiehlt es sich, für ein Untersystem dieselbe oder eine höhere Einstellung zu verwenden wie für das übergeordnete System. • Low (Niedrig) – Für Systeme mit über 100 Geräten. • Medium (Mittel) – Für Systeme mit 25–100 Geräten. • High (Hoch) – Für Systeme mit unter 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 129
2. Konfigurieren Sie die E-Mail-Adressen, um die Benachrichtigungen zu empfangen. Siehe *E-Mail-Empfänger konfigurieren*, on page 182.
3. Konfigurieren Sie die Benachrichtigungsregeln. Siehe *Benachrichtigungsregeln konfigurieren*, on page 182.

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 bestätigt, dass die Test-E-Mail gesendet wurde.

Benachrichtigungsregeln konfigurieren

Zwei Benachrichtigungsregeln sind standardmäßig aktiviert.

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. Sie können Benachrichtigungsregeln unter **Notification rules (Benachrichtigungsregeln)** aktivieren oder deaktivieren.
3. Unter **Applied rules (Angewandte Regeln)** wird eine Liste der Systeme und Geräte sowie der auf diese angewendeten Benachrichtigungsregeln 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 182.
2. Laden Sie im Hauptsystem die Systemkonfiguration hoch. Siehe *Daten von anderen Systemen abrufen*, on page 183.
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 200.

Systemkonfiguration erstellen

1. Rufen Sie **Konfiguration > Überwachung des Systemzustands > Multisystem** auf.

2. Klicken Sie auf **Erstellen**.
3. Klicken Sie auf **Copy (Kopieren)**, um die Datei zum Hochladen in das Hauptsystem zu kopieren.
4. Um die Details der Systemkonfiguration anzuzeigen, klicken Sie auf **Details anzeigen**.
5. Um die Systemkonfiguration neu zu erstellen, klicken Sie zunächst auf **Delete (Löschen)**, um die bestehende Konfiguration zu löschen.

Nach dem Hochladen der Systemkonfiguration in das Hauptsystem erscheinen die Hauptsysteminformationen unter **Systems with access (Systeme mit Zugriff)**.

Daten von anderen Systemen abrufen

Nachdem Sie die Systemkonfiguration eines sekundären Systems erstellt und kopiert haben, können Sie diese 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. Die folgenden Anwendungen und Szenarien werden unterstützt:
 - AXIS Object Analytics: Zählung von Linienüberquerungen und Belegung in einem Bereich
 - 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.
- Markieren Sie Szenarien mit einem Tag, um die Daten im Dashboard zu filtern und z. B. Kameras an einem 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

- Das AXIS Data Insights Dashboard erfordert TLS-Version 1.2 oder höher für verschlüsselte Verbindungen 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 Data Insights Dashboard zugeordnet.
- Die Kameras und der AXIS Camera Station Pro Server müssen sich im selben Netzwerk befinden.
- Für die optimale Funktion wird die Ausführung von AXIS Data Insights Dashboard in AXIS Camera Station Pro auf einem Server mit mindestens 16 GB RAM empfohlen.
- Es können maximal 100 MB Daten gespeichert werden, was zu einer begrenzten Speicherzeit führt. Zum Beispiel:
 - Die Belegungsschätzung für einen Parkplatz mit vier Kameras, die rund um die Uhr jeweils auf die Erkennung von fünf Fahrzeugunterklassen wie Autos und Fahrräder konfiguriert sind, ergibt eine Aufbewahrungszeit von 260 Tagen.
 - Die Personenzählung in einer Einzelhandelsumgebung mit acht Kameras und einem fortlaufenden Personenstrom über 12 Stunden ergibt eine Aufbewahrungszeit von etwa 1270 Tagen.
 - Für eine Kamera, die ein Szenario zur Zählung von Linienüberquerungen mit sechs Klassen und der fortlaufenden Zählung über 24 Stunden durchläuft, ergibt sich 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 21*.



Aktivieren von AXIS Data Insights Dashboard

Kennzeichenüberprüfung

Auf der Seite der Kennzeichenüberprüfung können Sie den Status von AXIS License Plate Verifier auf Ihren Kameras einsehen und Kameras zur leichten Verwaltung der Listen in Gruppen zusammenfassen.

Die Registerkarte **Cameras (Kameras)** enthält eine Liste aller angeschlossenen Geräte mit installiertem AXIS License Plate Verifier:

- **Camera (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.
- **Last event (Letztes Ereignis):** Der Zeitpunkt des letzten von der Kamera aufgezeichneten Ereignisses.
- **Allowed (Zugelassen):** Die Anzahl der Kennzeichen, die in der Zulassungsliste der Kamera enthalten sind.
- **Blocked (Nicht zugelassen):** Die Anzahl der Kennzeichen, die in der Sperrliste der Kamera enthalten sind.
- **Custom (Benutzerdefiniert):** Die Anzahl der Kennzeichen, die in der Liste „Benutzerdefiniert“ der Kamera enthalten sind.
- **(Group (Gruppe):** Die Gruppe, der die Kamera angehört.

Auf der Registerkarte **Groups (Gruppen)** werden alle Ihre Kameragruppen sowie die Kameras in den einzelnen Gruppen aufgelistet. 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 209*.

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:
 - **Connect directly (Direkt verbinden):** Geben Sie die IP-Adresse und die Zugangsdaten von Body Worn Manager ein.
 - **Generate connection file (Verbindungsdatei erstellen):** 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 145*.

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 dient zur Bezeichnung des Speicherorts für kopierte und übertragene Aufzeichnungen.
2. Wenn Sie alle bestehenden Verbindungen beenden möchten, wählen Sie **End existing connections (Bestehende Verbindungen beenden)**. Laden Sie die neue Verbindungsdatei auf jeden Controller des AXIS Body Worn-Systems hoch.
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)**. Laden Sie die neue Verbindungsdatei auf jeden Controller des AXIS Body Worn-Systems hoch.
 - 4.2. Klicken Sie auf **Export (Exportieren)** und speichern Sie die Verbindungsdatei.
 - 4.3. Laden Sie die Verbindungsdatei in Ihren Body Worn Manager hoch.



Ein Axis Body Worn-System 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 (Anrufrkategorie)**: 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 den standardmäßigen Speicherort für Aufzeichnungen von am Körper getragenen

Aufzeichnungsgeräten für neue Systembenutzer aus:

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 Auswahlménü **Disk (Datenträger)** einen Datenträger aus.
3. Klicken Sie auf **Save (Speichern)**.

Speicher abgelehnter Aufzeichnungen

Wählen Sie den Speicherort für Sie abgelehnte Inhalte aus dem Body Worn-System aus:

1. Wählen Sie unter **Rejected recordings storage (Speicher für abgelehnte Aufzeichnungen)** im Auswahlménü **Disk (Datenträger)** einen Datenträger aus und geben Sie einen Namen für Folder (Ordner) 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)**.

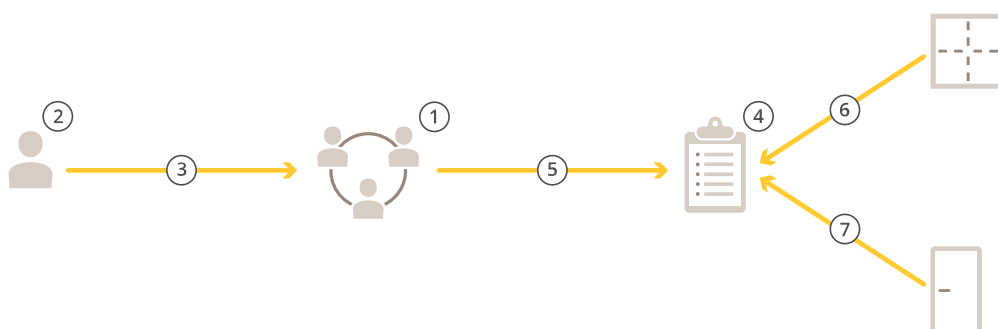
Zugriffsverwaltung

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, sodass Sie einen Arbeitsablauf entwickeln können, der den Anforderungen Ihrer jeweiligen Anwendung am besten gerecht wird. Beispielarbeitsablauf:



1. Gruppe hinzufügen, on page 193.
2. Karteninhaber hinzufügen, on page 188.
3. Fügen Sie Karteninhaber und Gruppen hinzu.
4. Fügen Sie eine Zugangsregel hinzu, on page 193.
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. Richten Sie einen Karteninhaber mit Zugangsdaten ein, die die Person identifizieren und festlegen, wann und wie die Person Zutritt an Zugängen erhält.

Sie können Benutzer auch über eine Active-Directory-Datenbank als Karteninhaber zuweisen. Siehe *Active-Directory-Einstellungen^{BETA}*, on page 178.

1. Öffnen Sie eine Registerkarte Access Management (Zugangsverwaltung).
2. Gehen Sie zu **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 190*.
7. Klicken Sie auf **Save (Speichern)**.
8. Um Ausweise auszudrucken, wählen Sie einen oder mehrere Karteninhaber aus und klicken Sie auf **Print badge (Ausweis drucken)** ^{BETA}. Weitere Informationen finden Sie unter *Print badge (Ausweis drucken)* ^{BETA}, on page 199.

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, um dem Karteninhaber eine lange Zutrittszeit und eine lange Dauer für einen zu lange geöffneten Zugang zu gewähren, 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. So kann der Karteninhaber zum Beispiel eine Tür außerhalb des regulären Zeitplans entriegeln.
Vom Lockdown ausgeschlossen	Wählen Sie diese Option aus, um dem Karteninhaber während eines Lockdowns Zutritt 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 <i>Multiserver</i> ^{BETA} , on page 176.



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

Zugangsdaten hinzufügen

Sie können einem Karteneinhaber die folgenden Arten von Zugangsdaten hinzufügen:

- *QR-Code als Zugangsdaten, on page 190*
- *PIN-Zugangsdaten, on page 191*
- *Smartphone-Zugangsdaten, on page 191*
- *Kartenzugangsdaten, on page 191*
- *Fahrzeugkennzeichen Zugangsdaten, on page 192*

Verfallsdatum	
Gültig ab	Legen Sie ein Datum und einen Zeitpunkt fest, damit die Zugangsdaten Gültigkeit erhalten.
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 müssen die Zeit auf dem Systemcontroller und die Zeit in der Kamera mit AXIS Barcode Reader synchronisiert werden. Es wird empfohlen, für beide Geräte dieselbe Zeitquelle zu verwenden, um eine langfristige Zeitsynchronisation zu gewährleisten.

So fügen Sie einem Karteneinhaber 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“ (Dynamischer QR-Code) ist standardmäßig aktiviert. Dieser ist mit PIN-Zugangsdaten zu verwenden.
4. Legen Sie das Start- und Enddatum für die Zugangsdaten fest.
5. Um nach dem Speichern des Karteneinhabers den QR-Code automatisch per E-Mail zu versenden, wählen Sie beim Speichern der Anmeldedaten **QR-Code an den Karteneinhaber 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**.

Ein Beispiel finden Sie unter *App AXIS Mobile Credential als Bluetooth-Zugangsdaten verwenden, on page 166*.

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. Geben Sie bei manueller Eingabe der Kartendaten einen Kartennamen, eine Kartennummer und eine Bitlänge an.

Hinweis

Die Bitlänge ist nur konfigurierbar, wenn Sie ein Kartenformat mit einer bestimmten Bitlänge erstellen, die im System noch nicht definiert wurde.

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 readers (Daten der zuletzt verwendeten Karte von Lesern des Zugangs abrufen)**.

Hinweis

Sie können einen 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 (Zugriffsverwaltung) > Settings (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 69*.
3. Fügen Sie einen neuen Zugang hinzu, die mit Ihrer Tür-Steuerung verbunden ist. Siehe *Fügen Sie einen Zugang hinzu, on page 154*.
 - 3.1. Fügen Sie auf **Seite A** einen Leser hinzu. Siehe *Leser hinzufügen, on page 164*.
 - 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. Klicken Sie auf **Ok**.
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. Überspringen Sie den Setup-Assistenten.
 - 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 **Authentication key (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 Zutritt gewähren möchten. Siehe *Karteninhaber hinzufügen, on page 188*.

8. Fügen Sie dem neuen Karteninhaber die Zugangsdaten zum Fahrzeugkennzeichen hinzu. Siehe *Zugangsdaten hinzufügen, on page 190*
9. Fügen Sie eine Zugangsregel hinzu. Siehe *Fügen Sie eine Zugangsregel hinzu, on page 193*.
 - 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

Mit Gruppen können Sie Karteninhaber und deren Zugangsregeln gemeinsam verwalten.

1. Öffnen Sie eine Registerkarte  Access Management (Zugangsverwaltung).
2. Gehen Sie zu **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, um die Karteninhaber auf den Subservern anzuzeigen und zu überwachen. Diese Option ist nur für auf dem Hauptserver erstellte Karteninhaber verfügbar. Siehe *Multiserver^{BETA}, on page 176*.
5. So fügen Sie der Gruppe Karteninhaber hinzu:
 - 5.1. Klicken Sie auf **+ Add (Hinzufügen)**.
 - 5.2. Wählen Sie die gewünschten Karteninhaber aus und klicken Sie auf **Add (Hinzufügen)**.
6. Klicken Sie auf **Save (Speichern)**.
7. Um Ausweise für alle Karteninhaber einer Gruppe auszudrucken, wählen Sie die Gruppe aus und klicken Sie auf **Print badge (Ausweis drucken)^{BETA}**. Weitere Informationen finden Sie unter *Print badge (Ausweis drucken)^{BETA}, on page 199*.

Fügen Sie eine Zugangsregel hinzu

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.

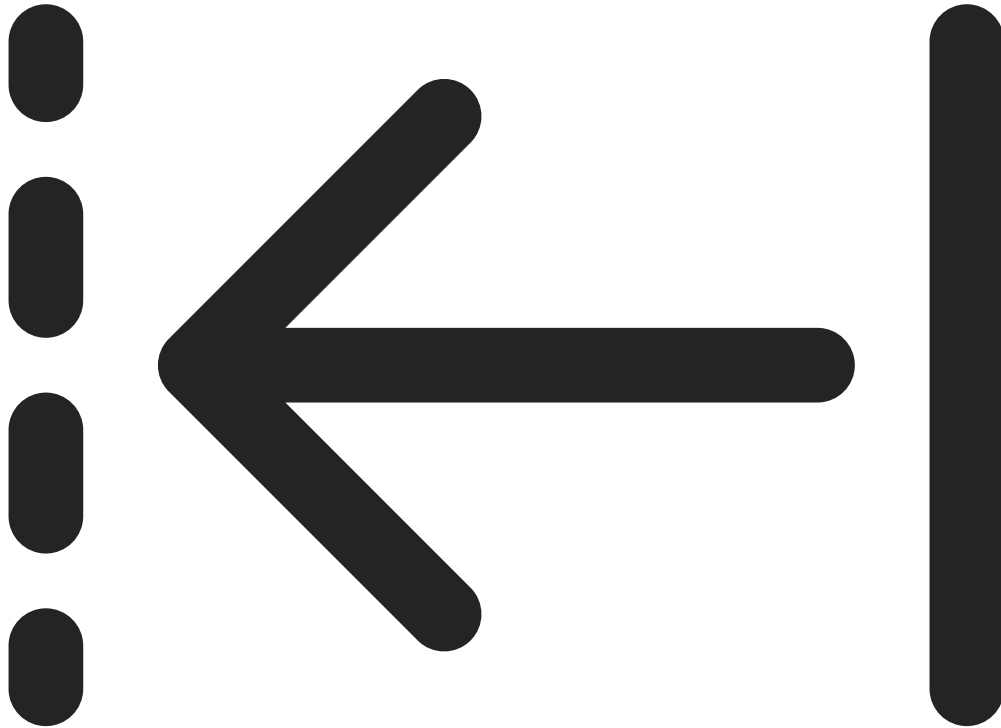
Türen und Bereiche – Geben an, wofür der Zugang gilt.

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 rules (Zugangsregeln)**



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

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 Arten von Systeminformationen enthalten. AXIS Camera Station Pro exportiert Berichte als Datei mit kommagetrennten Werten (CSV) und speichert sie 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. Es hilft Gebäudeverwaltern dabei, Mitarbeiter und Besucher nach einer Evakuierung ausfindig zu machen. Ein Sammelpunkt ist ein festgelegter Leser, an dem sich das Personal im Notfall einfinden muss. Das System erstellt einen Bericht darüber, welche Mitarbeiter anwesend sind und welche nicht. 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 **Roll call / Mustering (Appell / Musterung)** aus.
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 aus.
8. Wählen Sie einen Zeitrahmen für den Bericht aus.
9. Klicken Sie auf **Save (Speichern)**.
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 erstellt haben.
Nicht anwesend	Der Karteninhaber hat die angegebene Zone verlassen und sie nicht wieder betreten, bevor Sie den Bericht erstellt 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, Gruppen, Zugangsdaten und Bilder 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 Hardwareeinstellungen und löscht alle zuvor gespeicherten Konfigurationen.

Sie können Benutzer auch über eine Active-Directory-Datenbank als Karteninhaber zuweisen. Siehe *Active-Directory-Einstellungen^{BETA}*, on page 178.

Optionen importieren	
Neu	Vorhandene Karteninhaber werden entfernt und neue hinzugefügt.
Aktualisieren	Vorhandene Karteninhaber werden aktualisiert und neue hinzugefügt.
Hinzufügen	Vorhandene Karteninhaber werden beibehalten und neue hinzugefügt. 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 **New (Neu)**, **Update (Aktualisieren)** oder **Add (Hinzufügen)**.
4. Klicken Sie auf **Next (Weiter)**.
5. Klicken Sie auf **Choose a file (Datei wählen)**, suchen Sie die CSV-Datei und klicken Sie auf **Open (Öffnen)**.
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. Verwenden Sie diese Option, um den doppelten Import von Personaleinträgen zu verhindern.
Format der Kartennummer	In der Standardeinstellung ist Allow both hexadecimal and number (Hexadezimal und Zahl zulassen) aktiviert.

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. Mit der Option **Undo import (Import rückgängig machen)** werden die Daten des Karteninhabers und die Hardwarekonfiguration auf den Zustand vor dem letzten Import 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. Klicken Sie auf **+ Add (Hinzufügen)** und geben Sie einen Namen ein. Sie können bis zu 6 benutzerdefinierte Felder hinzufügen.
3. Klicken Sie auf **Hinzufügen**.

So aktivieren Sie die Verwendung eines Gebäude-Zugangscode, 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 170*.

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)**, um diese Vorlage als Standardvorlage festzulegen.
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 eine neue Vorlage zu erstellen.

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. Die Kartencodierung wird derzeit nicht unterstützt. 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 kompatibelem 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 diese auf das Minimum ein.

Wichtig

„Secure Entry“ unterstützt Drucker mit Windows-Treibern. Drucker der Serie HID Fargo werden nachweislich unterstützt. 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 Auswahlliste **Template (Vorlage)** die gewünschte Vorlage für den Ausweis aus.
5. Wenn der Karteninhaber über mehrere Kartenberechtigungen verfügt, wählen Sie eine aus dem Auswahlmenü **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}

Auf der Registerkarte „System Health Monitoring“ (Überwachung des Systemzustands) können Sie Zustandsdaten von einem oder mehreren AXIS Camera Station Pro-Systemen 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 <i>Lagerbestand</i> , on page 200.
	Zeigt eine Speicherübersicht und die Aufzeichnungsdetails der einzelnen Kameras der überwachten Systeme an. Siehe <i>Speicher</i> , on page 201.
	Zeigt die Protokolle der Überwachung des Systemzustands der überwachten Systeme an. Siehe <i>Benachrichtigungen</i> , on page 202.

Einschränkungen

- Bei den Recordern der Serien AXIS S30 und S40 lässt sich der Speicher für Aufzeichnungen nicht überwachen.
- Die Benachrichtigungseinstellungen wirken sich nur auf den lokalen Server zur Überwachung des Systemzustands aus.
- Das System kennzeichnet Aufzeichnungen, bei denen es sich um keine kontinuierlichen oder bewegungsgesteuerten Aufzeichnungen handelt, mit dem Aufzeichnungstyp **None (Kein)**.

Vorgehensweise

1. Konfigurieren Sie Überwachung des Systemzustands ^{BETA}, on page 181
 - 1.1. Benachrichtigungen einrichten. Siehe *Benachrichtigungen*, on page 181.
 - 1.2. Multisystem richten. Siehe *Multisystem*, on page 182.
2. Überwachen Sie den Systemzustand von AXIS Camera Station Pro Systemen.
 - 2.1. *Lagerbestand*, on page 200
 - 2.2. *Speicher*, on page 201
 - 2.3. *Benachrichtigungen*, on page 202

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**. Auf der rechten Seite werden System- und Serverdetails angezeigt.
3. Um eine Übersicht über ein Gerät anzuzeigen, klicken Sie auf das Gerät in der Liste. Auf der rechten Seite werden Geräte- und Speicherinformationen angezeigt, sofern 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 214.

5. So laden Sie einen Bericht zur Überwachung des Systemzustands herunter:
 - 5.1. Wählen Sie im Auswahlménü **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.

Speicher

Die Speicherseite zeigt die Speicherübersicht und die Aufzeichnungsdetails der einzelnen Kameras der überwachten Systeme an. Klicken Sie auf einen Spaltenkopf, um nach dieser 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 <i>Speicher konfigurieren, on page 76</i> .
Standort	Pfad und Name des Speichers.
Gesamt	Die Gesamtgröße des Speicherplatzes. Stimmt mit der in den Windows-Eigenschaften für den Speicherort angezeigten Gesamtgröße überein.
Zugewiesen:	Die maximale Menge an Speicherplatz, die für die Aufzeichnungen bereitgestellt wird.
Used (Verwendet)	Der derzeit von Aufzeichnungen belegte Speicherplatz.
Letzte Aktualisierung	Zeitpunkt, an dem die Information zuletzt aktualisiert wurde.

Kamera	
Status	(leer): Normaler Status. Warnung: Die Aufbewahrungszeit wird nicht eingehalten. Info-Symbol: Die Aufbewahrungszeit wird nicht eingehalten, da die Kamera-Aufzeichnungen zu kurz sind.
Bezeichnung	Der Kameraname.
Aufzeichnungstyp	Die für die Kamera verwendeten Aufzeichnungstypen.
Aufbewahrung einstellen	Die für die Kamera unter Configuration (Konfiguration) > Storage (Speicher) > Selection (Auswahl) eingestellte Aufbewahrungszeit.
Aktuelle Aufbewahrung	Die bisher verstrichene Speicherdauer der Aufzeichnungen in Tagen.
Älteste Aufzeichnung	Der Zeitpunkt der ältesten Aufzeichnung der Kamera im Speicher.
Neueste Aufnahme	Der Zeitpunkt der neusten Aufzeichnung der Kamera im Speicher.
Standort	Der von der Kamera verwendete Speicherort.
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 einen Spaltenkopf, um nach dieser 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 <code>device down</code> oder <code>system</code> ausgelöst wurden, für Benachrichtigungen, die durch <code>system down</code> ausgelöst wurden.
System	Der Name des Systems, in dem das Ereignis aufgetreten ist.
Regel	Die Regel, von der die Benachrichtigung ausgelöst wurde: <code>System down</code> oder <code>Device down</code>
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. Bewegen Sie den Mauszeiger auf das Warnsymbol, um den Konflikt anzuzeigen. 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 Tastatur-Wert einer Aktion leer ist, klicken Sie auf dieses Feld, um 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 zum Zuweisen die Taste am Joystick bzw. Jog Dial.
Hotkey bearbeiten	Klicken Sie auf den Tastatur-Wert einer Aktion, um diesen zu bearbeiten.
Hotkey entfernen	Klicken Sie auf den Tastatur-Wert einer Aktion, um diesen zu entfernen.
	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	⏭	-
Taste 12	Lesezeichen hinzufügen	📌	-

Hotkey- Zuord- nung – Joystick	Standardaktion	AXIS TU9002	AXIS T8311
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- Zuord- nung – 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	

Hotkey- Zuordnung – Jog	Standardaktion	AXIS T8313
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)** Live-Alarme, Ereignisse und Prüfprotokolle angezeigt. Sie können auch nach älteren Protokollen suchen. Konfigurieren Sie die Anzahl der Tage für die Speicherung von Protokollen unter **Configuration (Konfiguration) > Server > Settings (Einstellungen)**.

Time (Zeit)	Datum und Zeit der Aktion.
Type (Typ):	Typ der Aktion: Alarm, Ereignis oder Prüfung.
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	Diese Option ist nur bei Verbindung mit mehreren Servern verfügbar. Der Server auf dem die Aktion vorkommt.
Komponente	Protokollerzeugende Komponente.

Protokolle suchen

1. Klicken Sie auf der Registerkarte **Logs (Protokolle)** unter **Log search (Protokollsuche)** auf **Search (Suchen)**.
2. Geben Sie in das Filterfeld die Schlüsselwörter ein. AXIS Camera Station Pro durchsucht die Protokollliste mit Ausnahme von **Time (Zeit)** und zeigt die Suchergebnisse an, die alle Schlüsselwörter enthalten. Unterstützte Suchoperatoren finden Sie unter *Suche optimieren, on page 46*.
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 Protokoll **Alarms (Alarme)** 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 die Alarme quittiert wurden.
	Klicken Sie auf einen Alarm und  , um das Protokoll in eine Textdatei zu exportieren.

Ereignisprotokoll

Das Protokoll **Events (Ereignisse)** 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 Protokoll **Audit (Prüfung)** finden Sie alle Benutzeraktionen, wie beispielsweise manuelle Aufzeichnungen, gestartete oder gestoppte Videostreams und Aktionsregeln, die sowohl von Zutrittspunkten als auch von

Karteneinhabern erstellt wurden. Wählen Sie die Audits und klicken Sie auf  in der Werkzeugleiste, um diese zu exportieren und als Textdatei zu speichern.

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. Passen Sie die Liste an:
 - Um den Namen der Liste zu bearbeiten, klicken Sie auf **Edit list name (Listennamen bearbeiten)**.
 - Um ein neues Fahrzeugkennzeichen hinzuzufügen, geben Sie das Fahrzeugkennzeichen in die Spalte „License plate“ (Fahrzeugkennzeichen) und optional eine Beschreibung in die Spalte „Description“ (Beschreibung) ein. Klicken Sie auf **Hinzufügen**.
 - Um ein vorhandenes Fahrzeugkennzeichen zu bearbeiten oder zu entfernen, wählen Sie dieses aus und klicken Sie auf **Edit (Bearbeiten)** oder **Remove (Entfernen)**.
 - Um eine Liste mit Fahrzeugkennzeichen aus einer CSV-Datei zu importieren, klicken Sie auf **Import (Importieren)** und wählen Sie die Datei aus. Ihre aktuelle Liste wird überschrieben. Exportieren Sie sie also zuerst, wenn Sie eine Kopie behalten möchten.
 - Um eine Liste mit Fahrzeugkennzeichen in eine CSV-Datei zu exportieren, klicken Sie auf **Export (Exportieren)**.
4. Klicken Sie auf **Apply (Anwenden)**, um Ihre Änderungen zu speichern.

Hinweis

Sobald Sie die Änderungen angewendet haben, übernimmt AXIS Camera Station Pro die Verwaltung der Fahrzeugkennzeichenlisten für diese Gruppe bzw. diese Kamera. Die Kamera wird jede Nacht mit den in AXIS Camera Station Pro gespeicherten Listen aktualisiert, wodurch alle direkt auf der Kamera gespeicherten Fahrzeugkennzeichen überschrieben werden.

AXIS Audio Manager Pro

Auf der Registerkarte **AXIS Audio Manager Pro** können Sie direkt von AXIS Camera Station Pro auf die Serverschnittstelle von AXIS Audio Manager Pro zugreifen. Weitere Informationen zur Server-Schnittstelle finden Sie im *Benutzerhandbuch zu AXIS Audio Manager Pro*.

Die Registerkarte wird erst angezeigt, nachdem 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 178.

Wichtig

Es ist nicht möglich, per Secure Remote Access v2 auf die Schnittstelle eines AXIS Audio Manager Pro-Servers zuzugreifen.

Die Integration erlaubt Ihnen außerdem das Folgende:

- *Auslöser in AXIS Audio Manager erstellen*, on page 106.
- *Aktionen in AXIS Audio Manager erstellen*, on page 116.
- Hinzufügen von Audiobereichen zu Karten. Siehe dazu *Lageplan*, on page 23.
- *Verwendung von Durchsageschnittstellen in geteilten Ansichten*, on page 21.
- Festlegung von Benutzerrechten für AXIS Audio Manager Pro in AXIS Camera Station Pro. Siehe *Benutzer-/Gruppenberechtigungen*, on page 142.
- Auswahl von Audiogeräten über den AXIS Audio Manager Pro-Server als verknüpftes Audiogerät einer Kamera. Siehe *Videostreamprofile bearbeiten*, on page 56.

Alarmer

Die Registerkarte „Alarms“ (Alarmer) ist unten im AXIS Camera Station Pro-Client verfügbar und zeigt ausgelöste Ereignisse und Systemalarmer an. Informationen zum Erstellen eines Alarms finden Sie unter *Aktionsregeln*. Informationen zum Alarmtyp „Database maintenance is required (Wartung der Datenbank erforderlich)“ siehe *Datenbankwartung*, on page 232.

Time (Zeit)	Der Zeitpunkt des Alarms.
Kategorie	Die Kategorie des ausgelösten Alarms.
Beschreibung	Eine kurze Beschreibung des Alarms.
Server	Verfügbar bei einer Verbindung mit mehreren Servern. Der AXIS Camera Station Pro-Server, der den Alarm sendet.
Komponente	Alarmauslösende Komponente.
	Zeigt ein Alarmverfahren an. Nur verfügbar, wenn der Alarm mit einem Alarmverfahren verknüpft ist.
	Öffnet die Aufzeichnungen. Nur verfügbar, wenn der Alarm mit einer Aufzeichnung verknüpft ist.
	Ausgewählten Alarm bestätigen
	Entfernen Sie den Alarm. Der Alarm wird nur vorübergehend entfernt, wenn Sie ihn nicht zuvor quittieren.

Umgang mit einem spezifischen Alarm:

1. Klicken Sie auf  **Alarms and Tasks (Alarmer und Aufgaben)** am unteren Rand des AXIS Camera Station Pro-Clients und öffnen Sie die Registerkarte **Alarms (Alarmer)**.
2. Wählen Sie für Alarmer mit einer Aufzeichnung den Alarm aus und klicken Sie auf , um auf der Registerkarte **Recording alerts (Aufzeichnungsalarmer)** die Aufzeichnung aufzurufen.
3. Für Alarmer 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 (Aufzeichnungsalarmer)** anzuzeigen.
4. Für Alarmer 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 Alarmer quittiert wurden, wählen Sie die Alarmer aus und klicken Sie auf .
6. Um die Alarmer aus der Liste zu entfernen, wählen Sie die Alarmer 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 Benutzer angezeigt, der sie eingeleitet hat:

- Systembericht
- Vorfallbericht erstellen
- Aufzeichnungen exportieren

Administratoren können alle Aufgaben aller Benutzer, einschließlich benutzerspezifischer Aufgaben, aufrufen und ausführen.

Bediener und Betrachter können:

- Alle selbst eingeleiteten Aufgaben und die nicht-benutzerspezifischen Aufgaben anderer Benutzer aufrufen.
- Alle selbst eingeleiteten Aufgaben abbrechen oder wiederholen. 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.
Start (Starten)	Zeitpunkt, zu dem die Aufgabe gestartet wurde.
Nachricht	Zeigt den Status oder Informationen zur Aufgabe an. Mögliche Statusangaben sind: • Canceling (Wird abgebrochen): Bereinigung vor Abbruch der Aufgabe. • Canceled (Abgebrochen): Bereinigung ist abgeschlossen und die Aufgabe wurde abgebrochen. • Error (Fehler): Die Aufgabe schlug auf einem oder mehreren der gewählten Geräte fehl. • Finished (Abgeschlossen): Aufgabe wurde abgeschlossen. • Finished during lost connection (Beendet während Verbindungsabbruch): Die Aufgabe wurde abgeschlossen, während die Verbindung zum Server unterbrochen war. Der Aufgabenstatus konnte nicht ermittelt werden. • Lost connection (Verbindung unterbrochen): Die Verbindung zwischen Client und Server wurde während der Ausführung der Aufgabe unterbrochen. 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 abubrechen.
	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. Überprüfen und konfigurieren Sie alle fehlgeschlagenen Vorgänge manuell.

Für die meisten Aufgaben werden folgende Details aufgeführt. Doppelklicken Sie bei Aufgaben wie **Export recordings (Aufzeichnungen exportieren)** und **System report (Systembericht)** auf die Aufgabe, 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 über den Verlauf 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.

Zur Anzeige einer HTML-Übersicht über die Systemkonfiguration des Clients:

1. **Konfiguration > Server > Diagnose** aufrufen.
2. Klicken Sie auf **View client configuration sheet (Client-Konfigurationsdatei anzeigen)**.

Server-Konfigurationsdatei

Die Server-Konfigurationsdatei 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.

Zur Anzeige einer HTML-Übersicht über die Systemkonfiguration des Servers:

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. Gehen Sie zu  > **Help (Hilfe) > System report (Systembericht)**.
2. Bearbeiten Sie den Dateinamen, wenn Sie den automatisch generierten Namen ändern möchten.
3. Klicken Sie auf **Browse... (Durchsuchen...)**, um den Speicherort für den Systembericht auszuwählen.
4. Wählen Sie Ihre bevorzugten Einstellungen:
 - Mit der Option **Automatically open folder when report is ready (Ordner automatisch öffnen, wenn Bericht bereitsteht)** können Sie den Bericht sofort öffnen.
 - **Include all databases (Alle Datenbanken einbeziehen)**, um detaillierte Informationen über Aufzeichnungen und Systemdaten hinzuzufügen.
 - Aktivieren Sie die Option **Include screenshots of all monitors (Screenshots aller Monitore einbeziehen)**, um die Analyse des Systemberichts zu erleichtern.
5. Klicken Sie auf **OK**.



Einen Systembericht erstellen

Hinweis

- Falls der Server nicht gestartet wird, können Sie über die Registerkarte **Tools (Werkzeuge)** in der Dienststeuerung von AXIS Camera Station einen vereinfachten Systembericht erstellen.
- Falls sich der Client nicht bei einem Server anmelden kann, bittet der Axis Kundensupport möglicherweise stattdessen um die Client-Protokolle. Sie finden sie in einem speziellen Ordner für Ihre Client-Version: `C:\ProgramData\Axis Communications\AXIS Camera Station\Core\Client 6.xx`.
- Je nach Problem werden unter Umständen auch Windows-Ereignisprotokolle benötigt. Öffnen Sie dazu die Ereignisanzeige, gehen Sie zu **Windows Logs (Windows-Protokolle)**, klicken Sie mit der rechten Maustaste auf **Application (Anwendung)** und wählen Sie **Save all events as (Alle Ereignisse speichern als)** aus. Wiederholen Sie diesen Vorgang für **System**.

In diesen Fällen benötigt der Axis Kundensupport zur Untersuchung außerdem Ihre regulären Serverprotokolle.

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 der Datenübertragung und -speicherung mit den aktuellen Systemeinstellungen in AXIS Camera Station Pro. Als Ergebnis wird das Bestehen bzw. Nichtbestehen des Tests ausgegeben.
Schwaches Licht	Test der Datenübertragung und -speicherung mit den typischen Einstellungen für schwaches Licht. Als Ergebnis wird das Bestehen bzw. Nichtbestehen des Tests ausgegeben.
Stresstest	Tests, bei denen die Datenübertragungs- und Datenspeichermenge schrittweise erhöht wird, bis das System seine maximale Grenze erreicht. Als Ergebnis wird die maximale Systemleistung ausgegeben.

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. Klicken Sie nach Abschluss des Tests auf **View report (Bericht ansehen)**, um den Bericht zu öffnen, oder auf **Save report (Bericht speichern)**, um ihn 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 (Letzter 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)**.

Dienststeuerung von AXIS Camera Station Pro

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.

Klicken Sie mit der rechten Maustaste auf das Symbol und wählen Sie **Open AXIS Camera Station Service Control (Dienststeuerung von 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:

Öffnen Sie das Menü **Start (Startmenü)** und wählen Sie **All Programs (Alle Programme) > Tools (Werkzeuge) > Service Control (Dienststeuerung)** aus.

	Wird ausgeführt
	Wird gestartet
	Beendet

Modify Settings (Einstellungen ändern)	Wählen Sie diese Option, um die Servereinstellungen anzupassen.
Auf Werkseinstellungen zurücksetzen?	Klicken Sie darauf, um alle Einstellungen auf die ursprünglichen Standardeinstellungen zurückzusetzen.
Start (Starten)	Klicken Sie darauf, um den Serverstatus zu ändern.
Anhalten	
Neu starten	Klicken Sie darauf, um einen Neustart des Servers durchzuführen.

Allgemeine Servereinstellungen

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.

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. Die übrigen Ports werden automatisch geändert.
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. Die Portnummern werden auf der Grundlage des HTTP-Hauptports 29200 berechnet. In einigen Abschnitten werden sowohl erforderliche als auch optionale Ports aufgeführt. Damit AXIS Camera Station Pro funktioniert, müssen die erforderlichen Ports stets offen sein. Wenn die optionalen Ports nicht freigegeben sind, funktionieren die entsprechenden Funktionen nicht.

Server zu Geräten

Erforderlich				
Anschluss	Anzahl	Protokoll	Richtung	Beschreibung
HTTP- und HTTPS-Hauptport	443	HTTPS	Ausgehend	Wird zum Aktivieren von Lizenzen, Herunterladen von Firmware und für

				verbundene Dienste verwendet.
Optional				
Standardport für WS-Discovery	3702	UDP	Eingehend und ausgehend	WS-Discovery-Webdienste zur Erkennung von ONVIF-Geräten. Multicast 239.255.255.250.
Standardmäßiger Bonjour-Port	5353	UDP	Eingehend und ausgehend	Wird zur Geräteerkennung mit mDNS (Bonjour) verwendet. Multicast 224.0.0.251. Falls der Standard-Port nicht verfügbar ist, wird dieser möglicherweise von einer anderen Anwendung genutzt, die ihn nicht freigibt. In diesem Fall wird stattdessen ein anderer Port per Zufallsprinzip ausgewählt und verwendet. Beachten Sie, dass Geräte mit Adressen lokaler Links bei Verwendung eines zufällig ausgewählten Ports nicht über Bonjour erkannt werden können.

Client zu Server

Alle Ports erforderlich					
Anschluss	Anzahl	Protokoll	Richtung	Kommunikation zwischen	Beschreibung
HTTP-Port und HTTP-Hauptport für Streaming	29200	HTTP	Eingehend	ACS-Server und -Client	Wird für Video-, Audio- und Metadatenstream verwendet (AES-Verschlüsselung).
Haupt-TCP-Port	29202	TCP	Eingehend	ACS-Server und -Client	Wird seit Version 6.17

					ausschließlich für den Client-Wechsel verwendet. Wurde bisher als der TCP-Hauptport genutzt.
ACS-API-Webserverport	29204	HTTPS	Eingehend	ACS-Server und mobile App	Wird für Anwendungsdaten- und MP4-Videostreaming über HTTPS verwendet.
Lokaler HTTP-Port für Proxyserver	29206	TCP	Eingehend	Intern auf dem ACS-Server	Mobile Apps tätigen Anrufe zum SRA-Modul, das HTTPS empfängt, in HTTP konvertiert und an den HTTP-Port des lokalen Proxy weitersendet.
Port des Web-Proxy-Endpunkts	29207	TCP	Eingehend	ACS-Server und -Komponenten	Dient der sicheren Kommunikation zwischen Komponente und Geräten.

Domänen und Ports für sicheren Fernzugriff v2

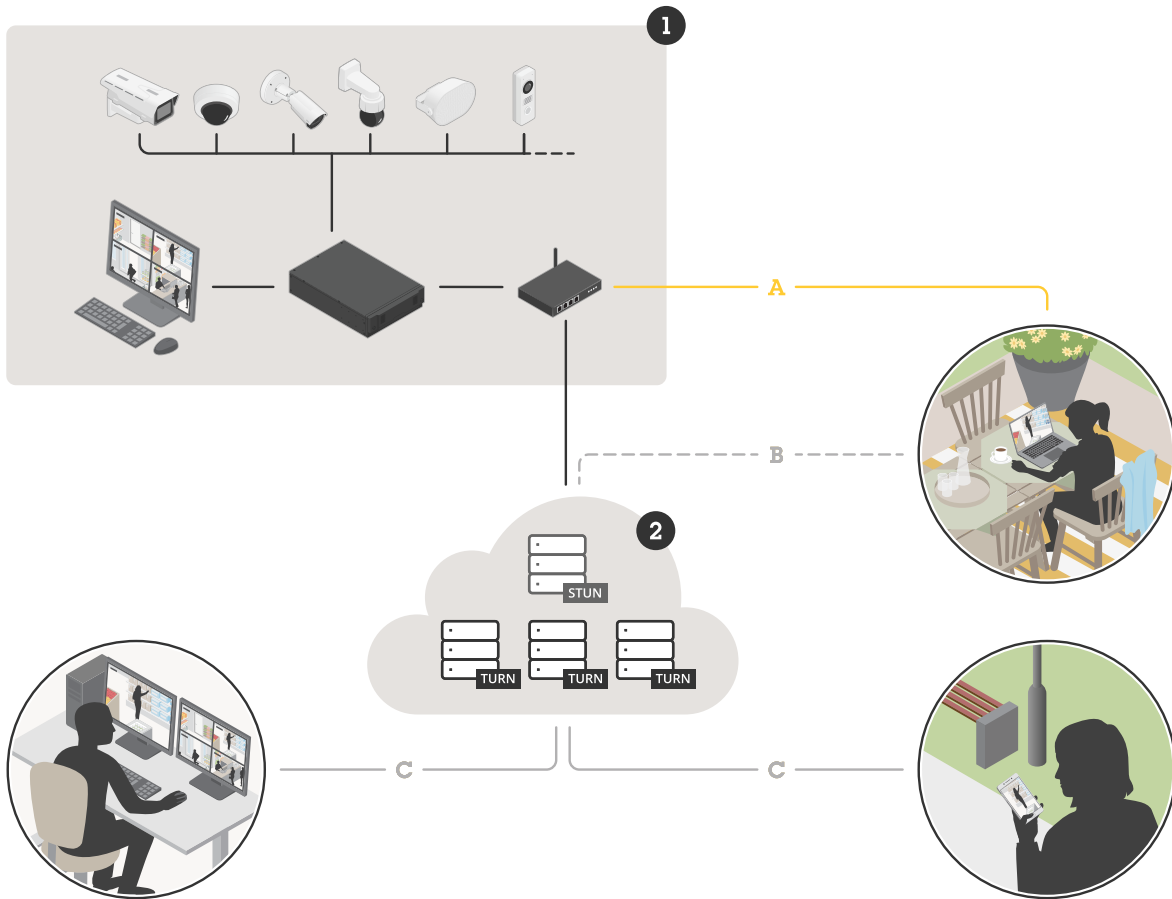


Abbildung: Lösungsübersicht zu Axis Secure Remote Access v2 in AXIS Camera Station Pro

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
SRA v2 – My Axis-Anmeldung	eu.login.connect.axis.com	443	TCP	Eingehend und ausgehend
Kommunikation mit Cloud-Dienst für SRA v2	eu.cs.connect.axis.com	443	TCP	Eingehend und ausgehend
Kommunikation mit Cloud-Dienst-API für SRA v2	api.vms.axis.cloud	443	TCP	Eingehend und ausgehend
Uplink-Komponente	acspro.mysystems.axis.com	443	-	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

Erforderlich						
Komponente	Abhören auf der Schnittstelle	Anzahl	Protokoll	Richtung	Kommunikation zwischen	Beschreibung
Lokaler WebRTC-Signalserver	localhost	29227	WSS	Eingehend	Embeddable Client, WebClient und WebRTC-Streamer zum Signalserver	Teil der WebRTC-Komponente vor Ort.
Lokale WebRTC-Konfiguration	localhost	29229	HTTPS	Eingehend	ACS-Client (Webseite)	Wird verwendet, um die Webseite und das Backend der WebRTC-Konfiguration zu hosten. Teil der WebRTC-Komponente vor Ort.
Lokaler TURN Server	Alle (0.0.0.0/INADDR_ANY)	29230	UDP	Eingehend und ausgehend	Embeddable Client/ WebClient zum TURN-Server	Wird für „Single-Port-WebRTC“ auf ACS vor Ort verwendet.
Local-IAM (IDP)	0.0.0.0	29232	HTTPS	Eingehend	Reverse-Proxy und Local-IAM, ACS-Windows-Client und Local-IAM	Öffentlicher IDP_OIDC-Port.

Local-IAM (IDP)	0.0.0.0	29233	HTTPS	Eingehend	Dienste anderer Anbieter	mTLS-Administrator-Port.
Local-IAM (IDP)	127.0.0.1	29234	HTTPS	Eingehend	Dienste anderer Anbieter	Tokenizer-Port.
WebRTC	localhost	29235	HTTPS	Eingehend	Cloud-Komponente	Wird zur Konfiguration der WebRTC-Cloud-Verbindung während Onboarding verwendet. Teil der WebRTC-Komponente.
Dienst-API	127.0.0.1	29244	NATS	Eingehend	Zwischen ACS und Komponenten sowie zwischen den Komponenten untereinander über NATS.	NATS Broker.

Optional

Sicherer Eingang (AC-MSM)	127.0.0.1	29214	HTTPS (WS)	Eingehend	ACS-Client (Webseite) und Komponente	Konfigurierbar über den ACS-Basis-Port. Ältere Installationen verwendeten Port 8081.
Sicherer Eingang (AC-MSM)	Alle (0.0.0.0/INADDR_ANY)	29215	HTTPS (WS)	Eingehend	Secure-Entry-Komponenten an verschiedenen Standorten	Konfigurierbar über den ACS-Basis-Port.
Überwachung des Systemzustands	Alle (0.0.0.0/INADDR_ANY)	29216	HTTPS	Eingehend	ACS (Webseite), SHM-Backend (Komponente)	Wird zum Hosten der Webseite von System Health Monitoring sowie zum Teilen von Daten in Konfigurationen mit mehreren

						Systemen verwendet.
Cloud-Dienst für System Health Monitoring/ Cloud-Dienst	localhost	29217	HTTPS	Eingehend	ACS (Webseite) und Cloud-Dienst-Backend (Komponente)	Wird für Cloud-Dienste verwendet.
Intelligente Suche 2	localhost	29218	HTTPS	Eingehend	ACS-Client (Registerkarte „Smart Search“ (Intelligente Suche) auf der Webseite) und Backend für intelligente Suche (Komponente)	Wird zum Hosten der API der intelligenten Suche und zum Bedienen der Clientwebseite verwendet.
VMS-API	127.0.0.1, ::1	29219	GraphQL	Eingehend	VMS API und GraphQL-Clients	Wird zum Ausweisen von ACS als GraphQL-API gegenüber einem Client verwendet.
Webclient	localhost	29223	HTTPS	Eingehend	WebClient in VMS-API/ Embeddable Client	Das Backend fungiert als Proxy vor der VMS-API.
Embeddable Client	localhost	29224	HTTPS	Eingehend	Embeddable Client zu VMS-API/ WebRTC-Streamer und Signalserver	Das Backend fungiert als Proxy vor der VMS-API.
Konfiguration des Webclients	localhost	29225	HTTPS	Eingehend	ACS-Client (Webseite)	Wird zum Hosten die Webseite und des Backend für die Konfiguration des Embeddable Client verwendet.
Konfiguration des Embeddable Client	localhost	29226	HTTPS	Eingehend	ACS-Client (Webseite)	Wird zum Hosten die Webseite und des Backend für die Konfiguration

						des Embeddable Client verwendet.
Opentelemetry	127.0.0.1	29236	gRPC	Eingehend	Dienste anderer Anbieter (ACS und andere Komponenten)	gRPC-Port.
Opentelemetry	127.0.0.1	29237	HTTPS	Eingehend	Dienste anderer Anbieter (ACS und andere Komponenten)	HTTP-Port.
Audio Manager		29238	HTTPS	Eingehend	Integrationsdienste und -komponenten anderer Anbieter	Webserverport.
Data Insights Dashboard	localhost	29241	HTTPS	Eingehend		Empfänger-Webserverport.
Data Insights Dashboard	0.0.0.0	29242	MQTT	Eingehend und ausgehend	Empfänger von Ereignismeldungen der Kamera	Makler.
Opentelemetry	127.0.0.1	29245	HTTP	Eingehend	Überwachung des Endpunkts zum Abruf von Metriken aus dem OpenTelemetry-Kollektor	HTTP-Port.
Intelligente Suche 2	localhost	29247	gRPC	Eingehend	VMS-API-Kern und Resolver für Intelligente Suche	Resolver für Intelligente Suche.
API-Gateway	0.0.0.0	29248	HTTPS	Eingehend	Edge-Host und API-Gateway	Vom Edge-Host verwendeter Fallback-Port für API-Gateway.
API-Gateway	0.0.0.0	29250	HTTPS	Eingehend	ACS-Clients und API-Gateway	Fallback-Port für HTTP- und HTTPS-

						Datenverkehr an Ports 80 und 443. Der Unterschied zu +48 besteht darin, dass bei +48 Komponentenzertifikate verwendet werden, während hier Serverzertifikate zum Einsatz kommen.
Überwachung des Systemzustands	127.0.0.1	29251	gRPC	Eingehend	ACS-Server und mögliche weitere Komponenten in Richtung des SHM-Kollektors	Wird von Herausgebern der Systemzustandsdaten zur Datenübertragung an den SHM-Kollektor verwendet.
Überwachung des Systemzustands	127.0.0.1	29252	HTTPS	Eingehend	ACS-Server und mögliche weitere Komponenten in Richtung des SHM-Kollektors	Wird von Herausgebern der Systemzustandsdaten zur Datenübertragung an SHM-Kollektor verwendet.
AXIS Body Worn Live-Empfänger	127.0.0.1	29254	TCP	Eingehend	Livestream-Server, der HTTPS-Anfragen vom ACS-Server entgegennimmt	Livestream-Server.

Weitere Ports

Erforderlich

Anschluss	Anzahl	Protokoll	Richtung	Kommunikation zwischen	Beschreibung
HTTP-Port	80	HTTP	Ausgehend	ACS-Server und -Geräte sowie ACS-Client und	Wird zum Aktivieren von Lizenzen, Herunterladen von

				ACS-Server mit dem Internet	Firmware und für verbundene Dienste verwendet.
HTTP-Port	80	HTTP	Eingehend	ACS-Client und ACS-Server	Wird für Videostreams und Gerätedaten verwendet.
HTTPS port (HTTPS-Port):	443	TCP	Eingehend	ACS-Clients und ACS-Server	Wird für Videostreams und Gerätedaten verwendet.
UDP-Port zum Aktualisieren des Status	15156	UDP	Eingehend und ausgehend	ACS-Server und ACS-Dienststeuerung	Die ACS-Dienststeuerung überwacht den Port, und der ACS-Server überträgt den Status einer laufenden Aktualisierung.
PostgreSQL	29210	TCP	Eingehend und ausgehend	PostgreSQL und alle Nutzer	Zu den derzeitigen Nutzern zählen das Data Insights Dashboard, die AXIS Audio Manager Pro-Komponente und die AXIS Body Worn-Komponente.

Optional

Dienste im Fahrzeug	29253	UDP	Eingehend	GNSS-Empfänger als Komponente für Dienste im Fahrzeug	
HTTP-Port	80	HTTP	Ausgehend	ACS-Server und -Geräte, ACS-Client und ACS-Server mit dem Internet	Zum Aktivieren von Lizenzen, Herunterladen von Firmware, für verbundene Dienste und weiteres verwendet.
HTTP-Port	80	HTTP	Eingehend	ACS-Client und ACS-Server	Wird für Videostreams und Gerätedaten verwendet.

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

Das System sichert die Datenbank jede Nacht und vor jeder Aktualisierung. Wählen Sie in AXIS Camera Station Pro **Modify settings (Einstellungen ändern)** aus und klicken Sie auf **Database (Datenbank)**, um die allgemeinen Backup Einstellungen 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. Sie können eine beliebige Zahl zwischen 1 und 30 wählen. 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

- Bei der Datenbanksicherung werden keine Aufzeichnungen gespeichert. Legen Sie unter **Configuration (Konfiguration) > Storage (Speicher)** einen Speicherort fest und 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 229*. Eine Systemsicherung umfasst sowohl die grundlegenden Datenbankdateien als auch die Datenbankdateien der Komponenten. Siehe *Datenbankdateien, on page 228*.

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 bei Verwendung von Komponenten wie AXIS Camera Station Secure Entry oder Intelligente Suche verfügbar. • webrtc: Dieser Ordner enthält WebRTC Konfigurationsdateien. • ACMSM: Dieser Ordner enthält die Datenbankdatei SecureEntry.db von AXIS Camera Station Secure Entry sowie Bilder von Karteninhabern. • smartsearch: Dieser Ordner enthält die Datenbankdatei smartSearch-backup-yyyyMMddHHmmssfff.sqlite3 für die Intelligente Suche.
backup_summary.json	Diese Datei enthält detailliertere Informationen zur Sicherung.
_cluster_YYYYMMddHHmmssfff.dbcbackup	Diese Datei enthält eine logische Sicherung des PostgreSQL-Datenbankclusters, einschließlich clusterweiter Daten wie Rollen und Tablespace.

Wartungssicherung

Geben Sie auf der Registerkarte **Database (Datenbank)** den Sicherungsordner für die Wartungssicherungen an. Siehe *Datenbankeinstellungen, on page 229*. 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 **Database maintainer (Datenbank-Instandhalter)** manuell über die Dienststeuerung von AXIS Camera Station Pro ausführen. Siehe *Datenbankwartung, on page 232*.
- Automatisch durch die im Aufgabenplaner von Windows konfigurierte geplante Datenbankwartung. Siehe *Werkzeuge, on page 234*.

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.

Es gibt zwei Optionen für die manuelle Sicherung:

- **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 `JJJJMMTThhmssfff` in dem Verzeichnis gespeichert, in dem Sie das Terminal geöffnet haben.
- **Option 2:** Erstellen Sie einen Systembericht und wählen Sie **Include all databases (Alle Datenbanken einbeziehen)**, um die Datenbank-Sicherungsdateien einzubeziehen. Siehe *Systembericht, on page 214*.

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 229*.

Hinweis

Bei der Datenbanksicherung werden keine Aufzeichnungen gespeichert. Legen Sie unter **Configuration (Konfiguration) > Storage (Speicher)** einen Speicherort fest und 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 229*.
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.dbcbakup 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 234.

Hinweis

AXIS Camera Station Secure Entry verwendet DB Janitor, um die Datenbankdateien zu überwachen und bei Bedarf zu verkleinern. Das Zutrittskontrollsystem ist vorübergehend nicht verfügbar, wenn eine erzwungene Verkleinerung stattfindet.

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 Virenskans aus, da bestimmte Antivirensoftwareprodukte diese beschädigen können. Bei Verwendung eines externen Sicherungssystems sichern Sie die 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 – Führen Sie regelmäßig die Windows-Speicherdiagnose aus, um den Arbeitsspeicher auf Fehler zu überprüfen.

Zertifikate

Auf der Registerkarte **Certificates (Zertifikate)** können Sie die Serverzertifikate für AXIS Camera Station Pro verwalten. 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. Die Dateiformate PEM und PFX/PKSC12 werden unterstützt. Nur RSA-Schlüssel mit einer Länge von mindestens 2048 Bits werden unterstützt.

Hinweis

Wenn Sie ein Zertifikat mit Zwischenzertifikaten im PEM-Format importieren, müssen sich alle Zwischenzertifikate in der .cer-Datei befinden. Wenn Sie Ihre eigenen Zertifikate erstellen, siehe *Zwischenzertifikate für den Import vorbereiten, on page 233*.

Aktuelles Zertifikat

Zeigt Informationen zum aktuellen Serverzertifikat an. Verwenden Sie diese Funktion, um manuell zu überprüfen, ob der Client eine Verbindung zum richtigen Server hergestellt hat.

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 und fügen Sie den Inhalt des einen Zertifikats in das andere ein 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

Wählen Sie in der Dienststeuerung von AXIS Camera Station Pro die Option **Modify settings (Einstellungen ändern)** aus und klicken Sie anschließend auf **Tools (Werkzeuge)**, um eine Datenbankwartung durchzuführen, einen Teilsystembericht zu erstellen, die Netzwerkprotokollierung zu aktivieren oder die Zertifizierungsstelle zurückzusetzen.

Datenbank-Instandhalter

Zum Ausführen des Datenbank-Instandhalters:

1. AXIS Camera Station Pro Dienststeuerung öffnen.
2. Klicken Sie auf **Tools**.
3. Klicken Sie unter **Database maintainer (Datenbank warten)** auf **Run (Ausführen)**.
4. 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.

Netzwerkprotokollierung

Zum Start der Netzwerkprotokollierung:

1. AXIS Camera Station Pro Dienststeuerung öffnen.
2. Klicken Sie auf **Tools**.
3. Klicken Sie auf den Link unter **Network logging (Netzwerkprotokollierung)**, um eine Anwendung zur Netzwerkprotokollanalyse herunterzuladen.
4. Klicken Sie nach der Installation auf **Start... (Starten...)**, um die Anwendung auszuführen.

Teilsystembericht

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.

Informationen zur Erstellung eines vollständigen Systemberichts finden Sie unter *Systembericht, on page 214*.

So erzeugen Sie einen Teilsystembericht:

1. Öffnen Sie die Dienststeuerung von AXIS Camera Station Pro.
2. Klicken Sie auf **Tools**.
3. Klicken Sie unter **Partial system report (Teilsystembericht)** auf **Run (Erzeugen)**.
4. Wählen Sie die angeforderten Informationen aus und geben Sie sie in das Dialogfeld ein.

5. Klicken Sie **Bericht erstellen**.

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. Die Probleme sind nach Themenbereichen geordnet, damit sie leichter zu finden sind. Mögliche Themen sind zum Beispiel Audio oder Live-Ansicht. Für jedes Problem ist ein Lösungsvorschlag enthalten.

Weitere Ressourcen, darunter Hardware-Anforderungen, Software-Aktualisierungen und Tutorials, finden Sie auf axis.com/support.

Bei allgemeinen Probleme starten Sie den Serverdienst von AXIS Camera Station Pro neu, bevor Sie weitere Maßnahmen zur Fehlerbehebung ergreifen:

1. **Konfiguration > Server > Diagnose** aufrufen.
2. Klicken Sie auf **Restart AXIS Camera Station server service...(AXIS Camera Station Serverdienst neu starten...)**.

Hinweis

Der Neustart des Serverdienstes kann eine Weile dauern und nicht abgebrochen werden. Während des Neustarts ist der Server nicht verfügbar und alle Geräteverbindungen werden getrennt.

Der AXIS Camera Station Pro Dienst

Der Dienst wird häufig neu gestartet

Der Server kann überlastet sein, was zu einer langen Aufgabenwarteschlange sowie Datenbankproblemen führen kann.

- Überprüfen Sie, ob AXIS Camera Station Pro oder eine andere Anwendung übermäßig viele Ressourcen beansprucht.
- Führen Sie den Datenbank-Instandhalter aus. Siehe *Datenbankwartung, on page 232*.

Falls alle diese Maßnahmen erfolglos bleiben, wenden Sie sich an den Axis Support. Wechseln Sie zu *Eskalationsverfahren, on page 252*.

Geräte im Video Management System

Übliche Probleme

Aufgeführte Kameras wurden nicht hinzugefügt, weil VMS keine Verbindung zu diesen herstellen kann	1. Stellen Sie sicher, dass die Kameras über eine Netzwerkverbindung verfügen, mit Strom versorgt werden und aktiv sind. 2. Gehen Sie zu Konfiguration > Geräte hinzufügen und versuchen Sie erneut, die Kamera hinzuzufügen.
Aufgeführte Kameras wurden nicht hinzugefügt, da Benutzer die Installation abgebrochen hat	Um die Kameras hinzuzufügen, Konfiguration > Geräte hinzufügen aufrufen.
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

Gerät wurde in anderem System verwendet, bevor es zu AXIS Camera Station Pro hinzugefügt wurde	• Setzen Sie das Gerät auf die Werkseinstellungen zurück. • Versuchen Sie, das Gerät zum AXIS Device Manager hinzuzufügen.
Anstelle des gewünschten Geräts wird ein anderes hinzugefügt	Hier kann ein Kompatibilitätsproblem vorliegen. Verwenden Sie immer die neueste Version von AXIS Camera Station Pro.
Kein anderes Gerätemodell kann hinzugefügt werden	Führen Sie auf axis.com/support/troubleshooting eine Fehlersuche an der Kamera aus.

Gerätefirmware kann nicht über AXIS Camera Station Pro aktualisiert werden.

Die Firmware der Kamera lässt sich nicht über deren Weboberfläche aktualisieren.	Führen Sie auf axis.com/support/troubleshooting eine Fehlersuche an der Kamera aus.
Firmware lässt sich nicht auf allen Geräten aktualisieren.	• Stellen Sie sicher, dass eine Netzwerkverbindung besteht. • Wenn es sich nicht um ein Netzwerkproblem handelt, wenden Sie sich an den Axis Support. Wechseln Sie zu <i>Eskalationsverfahren, on page 252</i>.
Die Firmware für bestimmte Modelle kann nicht aktualisiert werden.	Hier kann ein Kompatibilitätsproblem vorliegen. Wenden Sie sich an den Axis Support. Wechseln Sie zu <i>Eskalationsverfahren, on page 252</i> .

Keine Geräte ermittelt

Das Video Management System durchsucht das Netzwerk automatisch nach angeschlossenen Kameras und Video-Encodern, konnte jedoch keine finden.

- Stellen Sie sicher, dass die Kamera mit dem Netzwerk verbunden ist und mit Strom versorgt wird.
- Wenn sich Client, Server oder Kameras in verschiedenen Netzwerken befinden, konfigurieren Sie die Proxy- und Firewall-Einstellungen.
 - Wenn ein Proxyserver Client und Server voneinander trennt, müssen die Proxyeinstellungen des Clients angepasst werden.
 - Ändern Sie das NAT- oder Sicherheitssystem, wenn der Client und der Server durch ein NAT- oder Sicherheitssystem getrennt sind. Erteilen Sie für die in der Dienststeuerung von AXIS Camera Station angegebenen HTTP-, TCP- (Transmission Control Protocol) und Streaming-Ports eine Freigabe im Sicherheitssystem bzw. im NAT-System. Die vollständige Portliste finden Sie unter *Portliste für AXIS Camera Station Pro, on page 219*.
- Fügen Sie Kameras manuell hinzu. Gehen Sie zu *Geräte hinzufügen, on page 6*.

Wiederholte Meldung "Erneute Verbindung mit Kamera in 15 Sekunden"

Mögliche Probleme:

- Ein überlastetes Netzwerk.
- Kein Zugriff auf Kamera vorhanden. Überprüfen Sie, ob die Kamera über eine Netzwerkverbindung verfügt.
- 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. Wählen Sie diese Option in **Hardware decoding (Hardware-Decodierung)** unter **Graphics card (Grafikkarte)** aus. Diese Einstellung finden Sie unter **Configuration (Konfiguration) > Client > Streaming**.
- Passen Sie die Video- und Audioeinstellungen an. Optimieren Sie beispielsweise die Profileinstellungen so, dass Sie eine geringe Bandbreite erreichen.

Aufzeichnungen

Übliche Probleme

Kontinuierliche Aufzeichnung wird nicht 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	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 nicht möglich	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 nicht gestartet oder nach wenigen Sekunden abgebrochen werden, ist die Festplatte voll oder es liegen zu viele Stördaten vor.

- 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. Siehe *Speicher konfigurieren, on page 76*.

Aufzeichnungslücken bei kontinuierlicher Aufzeichnung

Lücken lösen automatische Benachrichtigungen mit dem Betreff **Recording errors (Aufzeichnungsfehler)** aus. Diese Lücken können verschiedene Ursachen haben wie zum Beispiel:

- Serverüberlastung
- Netzwerk-Problem
- Kameraüberlastung

- Laufwerksüberlastung

Prüfen Sie, ob die Aufzeichnungslücken bei allen Kameras auftreten. Wenn sie nicht bei allen Kameras auftreten, weist das auf eine mögliche Überlastung der Kamera hin. Ermitteln Sie die Ursache mithilfe der folgenden Fragen:

- Wie oft treten die Lücken auf? Stündlich 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 Server-Task-Manager, ob eine Hardware-Ressource stärker als üblich ausgelastet ist. Wenn das Laufwerk Anzeichen einer Überlastung aufweist, fügen Sie für mehrere Kameras zusätzliche Laufwerke hinzu.
- Reduzieren Sie die Datenmenge, die auf die Festplatte geschrieben wird (Videoeinstellungen, Zipstream, Bildrate, 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 240.

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 finden Sie unter *Aufzeichnungen mit AXIS File Player wiedergeben und überprüfen*, on page 7.

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 gespeichert. Um die Anzahl der Tage zu ändern, **Konfiguration > Speicher > Auswahl** aufrufen.

Wenn der Speicher voll ist, löscht das System möglicherweise Aufzeichnungen vor Ablauf der Aufbewahrungszeit. 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 für die Aufzeichnung das H.264-Videoformat. Das M-JPEG-Format benötigt mehr Speicherplatz.
 - Verwenden Sie Zipstream, um die Aufzeichnungsgröße weiter zu verringern.

Probleme mit der ausfallsicheren Aufzeichnung

Die Bandbreite für das Übertragen von Aufzeichnungen zwischen Kamera und Server reicht nicht aus	Erhöhen Sie die 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	- Richten Sie unbedingt NTP für zukünftige Aufzeichnungen ein. - Synchronisieren Sie die Kamerazeit mit der Server-Zeit oder verwenden Sie auf der Kamera denselben NTP-Server wie auf dem Server.

Hinweis

Die ausfallsichere Aufzeichnung funktioniert nicht bei kontrolliertem Herunterfahren des Servers oder Verbindungsunterbrechungen mit einer Dauer von weniger als 10 Sekunden.

Live-Ansicht

Live-Ansicht und Wiedergabeleistung

Dieser Abschnitt beschreibt mögliche Lösungen, wenn auf Ihrem AXIS Camera Station Pro Client Bilddatenverluste oder grafische Probleme auftreten.

Client-Hardware	
Stellen Sie sicher, dass der Treiber der Grafikkarte oder der des Netzwerks-Adapters aktuell ist.	- Öffnen Sie das DirectX Diagnostic Tool (auf dem Computer als Suchbegriff dxdiag eingeben). - Überprüfen Sie die Website des Herstellers auf aktuelle Treiber für das jeweilige Betriebssystem. - Überprüfen Sie, ob Client und Server auf demselben Computer ausgeführt werden. - Führen Sie nach Möglichkeit den Client auf einem eigens dafür eingerichteten Rechner aus.
Überprüfen Sie die Anzahl der Monitore.	Es wird empfohlen, nicht mehr als zwei Monitore pro Grafikkarte anzuschließen.
Hinweis Die Ausführung des Clients auf einer virtuellen Maschine wird nicht unterstützt.	
Grafikkarte unterstützt das unter Configuration (Konfiguration) > Devices (Geräte) > Stream Profiles (Videostreamprofile) konfigurierte Codierungsformat nicht.	- Stellen Sie sicher, dass die Grafikkarte das Codierungsformat Ihrer Streams unterstützt. - Versuchen Sie es mit anderen Codierungsformaten. - Sollte ein unterstütztes Codierungsformat auf mehreren Kameras nicht wie erwartet funktionieren, stellen Sie sicher, dass Ihre Grafikkartentreiber auf dem neuesten Stand sind.

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 <i>Anforderungen an den Server AXIS Camera Station Pro Installations- und Migrationsleitfaden</i> .
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)	Hierbei kann es sich um ein spezielles Problem einiger Kameras der M-Serie oder von Kameras mit mehreren Sensoren handeln. • Ändern Sie den Videostream auf dasselbe Streamingprofil oder auf eine niedrigere Auflösung. Siehe <i>Videostreamprofile, on page 56</i>.

Serverüberlastung

Ungewöhnlich hohe CPU- oder RAM-Auslastung zur Zeit des Problems	Stellen Sie sicher, dass keine anderen Anwendungen, die CPU-Leistung oder Arbeitsspeicher beanspruchen, gleichzeitig ausgeführt werden.
--	---

Netzwerk-Problem

Ungewöhnlich hoher Bandbreitenbedarf zur Zeit des Problems	Stellen Sie sicher, dass keine anderen Anwendungen, die viel Bandbreite beanspruchen, gleichzeitig ausgeführt werden.
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 Netzkabel).

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 auf **Auto** eingestellt. Siehe *Hardware-Dekodierung unter Streaming, on page 124*.
- Falls Sie eine Antivirensoftware installiert haben, kann diese unter Umständen Livestreams oder Ordner und Prozesse von AXIS Camera Station Pro sperren. Siehe *FAQ*.

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 Kameraserverbericht. Gehen Sie zu axis.com/support/troubleshooting.
- Stellen Sie sicher, dass die Firewall Verbindungen an bestimmten Ports nicht blockiert (siehe *Allgemeine Servereinstellungen, on page 219*).
- Stellen Sie sicher, dass für unterstützte Versionen des Betriebssystems Windows Server Desktop Experience installiert wurde. Siehe *Geplanter Export, on page 134*.
- Vergewissern Sie sich, dass der Stream mit der niedrigeren Auflösung einwandfrei funktioniert.

Falls alle diese Maßnahmen erfolglos bleiben, gehen Sie zu *Eskalationsverfahren, on page 252*.

Hardware-Decodierungsleistung optimieren

Diese Anleitung hilft Ihnen Probleme wie eine versetzte, ruckelnde oder abgehackte Videoübertragung, eine hohe CPU-Auslastung in der Live-Ansicht oder häufige Verbindungsausfälle der Kamera zu beheben.

1. Aktualisieren Sie die Treiber Ihrer Grafikkarte. Veraltete Treiber sind die häufigste Ursache für Probleme mit der Hardwarebeschleunigung. Besuchen Sie die Website des Herstellers (NVIDIA, AMD oder Intel) und laden Sie den neuesten Treiber für Ihren Grafikprozessor herunter.
2. Wählen Sie einen geeigneten Modus für die Hardware-Decodierung. Gehen Sie zu **Configuration (Konfiguration) > Client > Streaming**:
 - Wenn für den Modus **Automatic (Automatisch)** oder **On (Ein)** eingestellt ist und Probleme auftreten, setzen Sie ihn auf **Off (Aus)**. Sollte sich die Leistung verbessern, verfügt Ihr Grafikprozessor möglicherweise nicht über die erforderliche Kapazität für die aktuelle Streaming-Last. Fahren Sie mit Schritt 6 fort.
 - Wenn der Modus auf **Off (Aus)** gesetzt und die Auslastung des Hauptprozessors hoch ist, testen Sie die Einstellungen **Automatic (Automatisch)** oder **On (Ein)**, wobei die Voraussetzung hierfür ein entsprechend hohes Leistungsvermögen Ihres Grafikprozessors ist.
3. Beobachten Sie die Systemressourcen. Öffnen Sie den Windows-Task-Manager (Strg + Umschalt + Esc) und gehen Sie zur Registerkarte **Performance (Leistung)**:
 - Eine Auslastung des Hauptprozessors von durchgehend über ca. 80 % ohne Hardware-Decodierung deutet darauf hin, dass die Systemleistung für die Anzahl oder die Auflösung der Streams möglicherweise nicht ausreicht.
 - Wenn der für den Grafikprozessor reservierte Speicher bei aktivierter Hardware-Decodierung fast vollständig ausgelastet ist, weist das auf einen überlasteten Grafikprozessor hin.
4. Verringern Sie die Anzahl der gleichzeitig angezeigten Kamerabilder oder wechseln Sie zu Videostreamprofilen mit einer geringeren Auflösung, um die Systemlast zu verringern.
5. Achten Sie darauf, dass Ihre Kameras im H.264- oder AV1-Format streamen. Andere Codecs nutzen keine Hardware-Decodierung.
6. Überprüfen Sie die Fähigkeiten des Grafikprozessors. Selbst ein Grafikprozessor, der die Hardware-Decodierung unterstützt, kann eine eingeschränkte Auflösung oder Bildrate liefern. Bei Systemkonfigurationen mit vielen hochauflösenden Streams sollten Sie die *Systemanforderungen für den AXIS Camera Station Pro-Client* prüfen und die Aufrüstung auf einen Grafikprozessor mit einem größeren VRAM und einer höheren Decodierungsleistung erwägen.
7. Sollte keine der oben genannten Maßnahmen Abhilfe schaffen, wenden Sie sich bitte an den *Axis Support* und halten Sie folgende Informationen bereit:
 - Hardwarekomponenten des Systems (Hauptprozessor (CPU), Grafikprozessor (GPU), RAM).
 - Version des Betriebssystems.
 - Version des Grafiktreibers.
 - Version von AXIS Camera Station Pro.
 - Spezifische Symptome und Schritte zur Rekonstruktion des Problems.

Speicher

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 nicht möglich	Öffnen Sie zur manuellen Installation <i>Installation von Kamera-Anwendungen</i> , on page 70.
Aktuelle Bewegungserkennung kann nicht abgerufen werden	Setzen Sie die Kamera auf die Werkseinstellungen zurück: 1. Configuration > Devices > Management (Konfiguration > Geräte > Verwaltung) aufrufen. 2. Klicken Sie mit der rechten Maustaste auf die betroffene Kamera und klicken Sie auf Restore the camera to factory settings (Kamera auf Werkseinstellungen zurücksetzen). Während des Zurücksetzens ist die Kamera nicht verfügbar. Die IP- und HTTPS-Einstellungen werden nicht zurückgesetzt. Nach erfolgreichem Zurücksetzen wird in der Statusspalte Set password (Kennwort festlegen) angezeigt. Klicken Sie auf Set password (Kennwort festlegen), um die Kamera wieder mit dem Server zu verbinden.

Bewegungserkennung nicht konfiguriert	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 wird 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

Dieser Abschnitt bietet mögliche Lösungen, wenn Ihnen die bewegungsgesteuerte Aufzeichnung mehr oder weniger Erfassungen als erwartet liefert.

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 <i>Bearbeiten von AXIS Video Motion Detection 2 und 4, on page 89</i> .
Integrierte Bewegungserkennung	Sie können die Einschluss- und Ausschlussfenster konfigurieren. Siehe <i>Die integrierte Bewegungserkennung bearbeiten, on page 90</i> .

Anpassen der Triggerzeitspanne

Die Triggerzeitspanne/Auslösedauer ist der zeitliche Abstand zwischen zwei aufeinanderfolgenden Auslösern. Mit dieser Einstellung können Sie die Anzahl aufeinanderfolgender Aufzeichnungen reduzieren. Tritt innerhalb dieser Zeitspanne ein weiterer Auslöser ein, wird die Aufzeichnung fortgesetzt und die Triggerzeitspanne neu gestartet.

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 Auswahlménü **Microphone (Mikrofon)** ein Mikrofon aus.
5. Wählen Sie im Auswahlménü **Use microphone for (Mikrofon verwenden für)** aus, wann Audio verwendet werden soll.
6. Wählen Sie bei Bedarf im Auswahlménü **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, on page 56*.

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. Wenn Sie sich bei mehreren Servern anmelden, wird der Client gestartet und der Verbindungsstatus erscheint in der Statusleiste. Weitere Informationen zum Verbindungsstatus finden Sie unter *Verbindungsstatus, on page 136*.

Benutzername oder Kennwort sind nicht korrekt	• Überprüfen Sie die Schreibweise oder verwenden Sie ein anderes Konto. • Stellen Sie sicher, dass der Benutzer Zugriffsrechte für 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 ist, muss den Client als Administrator ausführen. • Weitere Informationen zu den Benutzerzugriffsrechten finden Sie unter <i>Benutzerberechtigungen, on page 140</i>.
Benutzer hat keine Berechtigung zur Anmeldung beim Server	Fügen Sie den Benutzer im Dialogfenster User permissions (Benutzerberechtigungen) hinzu.
Nachrichtensicherheit konnte nicht überprüft werden	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	• 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 ist. • Überprüfen Sie die Schreibweise der Server-Adresse.

	• Überprüfen Sie die Proxyeinstellungen des Clients.
Keine Antwort vom Server	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	Stellen Sie sicher, dass das Netzwerk richtig konfiguriert ist: • Überprüfen Sie, ob das Betriebssystem unterstützt wird. Eine vollständige Liste der unterstützten Betriebssysteme finden Sie in den <i>Versionshinweisen</i>. • Überprüfen Sie über die Dienststeuerung, ob der AXIS Camera Station Pro-Server ausgeführt wird, oder starten Sie ihn bei Bedarf. • Sicherstellen, dass Client und Server mit dem selben Netzwerk verbunden sind. Andernfalls den Client über die externe IP-Adresse des Servers verbinden. • Konfigurieren Sie auf dem Server-Computer in den Windows-Internetoptionen die Proxy-Einstellungen des Servers. • Konfigurieren Sie auf der Anmeldeseite die Proxy-Einstellung des Clients. Wählen Sie Change proxy settings (Proxy-Einstellungen des Servers ändern) aus. • Konfigurieren Sie auf dem Client-Computer in den Windows-Internetoptionen die Proxy-Einstellungen des Clients.
Verbindung zum Server kann nicht hergestellt werden	• Vergewissern Sie sich, dass die Adresse und der Port des AXIS Camera Station Pro-Servers korrekt sind. Überprüfen Sie die korrekte Einstellung des Portbereichs in der Dienststeuerung. • Stellen Sie sicher, dass die Server-Verbindung nicht durch NAT-, Firewall- oder Antivirensoftware blockiert wird. Weitere Informationen finden Sie unter <i>Domänen und Ports für sicheren Fernzugriff v2, on page 222</i>. • Verwenden Sie die AXIS Camera Station Pro Dienststeuerung, um sicherzustellen, dass der Server ausgeführt wird. – Öffnen Sie die AXIS Camera Station Pro Dienststeuerung (siehe <i>Dienststeuerung von AXIS Camera Station Pro, on page 217</i>). – 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	• Stellen Sie sicher, dass der Server-Computer eine Verbindung mit dem Netzwerk herstellen kann. • Vergewissern Sie sich, dass die Adresse und der Port des AXIS Camera Station Pro-Servers korrekt sind. • Stellen Sie sicher, dass die Server-Verbindung nicht durch NAT-, Firewall- oder Antivirensoftware blockiert wird. • Überprüfen Sie, ob die DNS-Einstellungen Ihres Clients korrekt sind. • Stellen Sie sicher, dass Ihr DNS-Server über einen Eintrag für den Host-Namen und die IP-Adresse des Servers verfügt.
Verbindung zum Server kann nicht hergestellt werden	Stellen Sie sicher, dass der Server-Computer und das Netzwerk nicht überlastet sind.

Server- und Clientversion sind unterschiedlich	Aktualisieren Sie den Server auf die gleiche Version, die auf dem Client ausgeführt wird.
Der lokale AXIS Camera Station Pro Server wird nicht ausgeführt.	Starten Sie AXIS Camera Station Pro über die Dienststeuerung oder wählen Sie einen Remote-Server für die Anmeldung.
AXIS Camera Station Pro Server ist nicht auf diesem Computer installiert	Installieren Sie AXIS Camera Station Pro Server oder wählen Sie einen anderen Server.
Ausgewählte Server-Liste ist 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.
- Gehen Sie zu **Configuration (Konfiguration)** und stellen Sie sicher, dass die Option **Automatic licensing (Automatische Lizenzierung)** aktiviert ist. Siehe *Lizenzen verwalten, on page 138*.
- Stellen Sie sicher, dass die Uhrzeit des Servers korrekt 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 Domainbenutzer fehlschlägt, ändern Sie das Anmeldekonto für den Dienst:

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	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	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 Weisen behoben werden:

- HTTPS auf einem Gerät aktivieren
- Ein vorhandene Zertifizierungsstelle importieren
- Neue Zertifizierungsstelle erstellen

HTTPS auf einem Gerät aktivieren:

1. **Configuration > Devices > Management** (Konfiguration > Geräte > Verwaltung) aufrufen.
2. Klicken Sie in der Liste mit der rechten Maustaste auf ein Gerät und wählen Sie **Security (Sicherheit) > HTTPS > Enable/Update (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. Gehen Sie zu **Configuration (Konfiguration) > Security (Sicherheit) > Certificates (Zertifikate) > Devices (Geräte)**.
2. Deaktivieren Sie unter HTTPS die Option **Validate device certificate (Gerätezertifikat prüfen)**.
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. **Configuration > Devices > Management** (Konfiguration > Geräte > Verwaltung) aufrufen.
7. Rechtsklicken Sie die Geräte und wählen Sie **Sicherheit > HTTPS > Aktivieren/Aktualisieren**.
8. Gehen Sie zu **Configuration (Konfiguration) > Security (Sicherheit) > Certificates (Zertifikate) > Devices (Geräte)** und aktivieren Sie **Validate device certificate** (Gerätezertifikat prüfen).

Hinweis

Die Geräteverbindung mit AXIS Camera Station Pro wird unterbrochen und einige Systemkomponenten werden neu gestartet.

So lassen Sie AXIS Camera Station Pro eine neue Zertifizierungsstelle generieren:

1. Gehen Sie zu **Configuration (Konfiguration) > Security (Sicherheit) > Certificates (Zertifikate) > Devices (Geräte)**.
2. Deaktivieren Sie unter HTTPS die Option **Validate device certificate** (Gerätezertifikat prüfen).
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. **Configuration > Devices > Management** (Konfiguration > Geräte > Verwaltung) aufrufen.
7. Rechtsklicken Sie die Geräte und wählen Sie **Sicherheit > HTTPS > Aktivieren/Aktualisieren**.
8. Gehen Sie zu **Configuration (Konfiguration) > Security (Sicherheit) > Certificates (Zertifikate) > Devices (Geräte)** und aktivieren Sie **Validate device certificate** (Gerätezertifikat prüfen).

Hinweis

Die Geräteverbindung mit AXIS Camera Station Pro wird unterbrochen und einige Systemkomponenten werden neu gestartet.

Zeitsynchronisierung

Windows Time-Dienst wird nicht ausgeführt

Der Windows Time-Dienst und der NTP-Server sind nicht synchron. Eine mögliche Ursache hierfür ist, 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 Firewall-Einstellungen 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 aufgenommen 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. Deaktivieren Sie die Option **Send alarm when the time difference between server and device is larger than 2 seconds** (Bei einer Zeitdifferenz zwischen Server und Gerät über 2 Sekunden Alarm senden, um die Alarmfunktion zu deaktivieren).

Wenden Sie sich an den AXIS Support.

Secure Remote Access v2

Keine Verbindung zu Cloud-Diensten lokal möglich

Lösung von Konnektivitätsproblemen mit Cloud-Diensten:

1. Öffnen Sie **AXIS Camera Station Pro** und gehen Sie zu **Configuration (Konfiguration) > Connected services (Verbundene Dienste) > Management (Verwaltung)**.
2. Stellen Sie sicher, dass **Status** grün ist. Ist dies nicht der Fall, überprüfen Sie Ihre Internetverbindung.
3. Wenn das Problem weiterhin besteht, wenden Sie sich an den Axis Support, um Hilfe zu erhalten.

Keine Verbindung zu Cloud-Diensten aus der Ferne möglich

In **AXIS Camera Station Pro**:

1. Rufen Sie **Menu (Menü) > Help (Hilfe)** auf und klicken Sie auf **Status of Axis services (Status der Axis Dienste)**. Dadurch wird die Statusseite von <https://status.axis.com> geöffnet, auf der Sie Wartungsbenachrichtigungen oder geplante Abschaltungen überprüfen können.
2. Erweitern Sie im Bereich **Axis Camera Station Pro** die Dropdown-Liste, um zu prüfen, ob auf Cloud-Dienste zugegriffen werden kann.
3. Vergewissern Sie sich, dass Ihr **My Axis** Konto bei der richtigen Organisation eingeladen ist.

In der **AXIS Camera Station Pro Mobile App**:

1. Rufen Sie **More (Mehr) > Help (Hilfe)** auf und klicken Sie auf **Status of Axis services (Status der Axis Dienste)**. Dadurch wird die Statusseite von <https://status.axis.com> geöffnet, auf der Sie Wartungsbenachrichtigungen oder geplante Abschaltungen überprüfen können.
2. Vergewissern Sie sich, dass Sie eine stabile Internetverbindung haben. Testen Sie mit einem anderen mobilen Gerät, um die Ursache des Problems zu ermitteln.
3. Vergewissern Sie sich, dass Ihr **My Axis** Konto bei der richtigen Organisation eingeladen ist.

Wenn das Problem weiterhin besteht, wenden Sie sich an den Axis Support, um Hilfe zu erhalten.

Allgemeine Probleme mit Paketverlust, Verzögerung und fehlerhafter Weiterleitung

1. Stellen Sie sicher, dass Sie Zugang zum Internet haben. Die wichtigsten verwendeten Ports sind 80 und 443, die auch für den Datenaustausch nach außen offen sein sollten.
2. Abhängig von Ihrem Router müssen Sie möglicherweise die folgenden zusätzlichen Domains mit Ports öffnen:
 - <https://eu.login.connect.axis.com> mit Port 433
 - <https://eu.cs.connect.axis.com> mit Port 433
 - <https://api.vms.axis.cloud> mit Port 433
 - <wss://signaling.prod.webrtc.connect.axis.com> mit Port 433
 - https://*.turn.prod.webrtc.connect.axis.com mit den Ports 443, 3478, 5349 und 49152-65535

Hinweis

Das Sternchen „*“ ist dynamisch und besteht aus einer Kombination von Region und einer nicht-statischen Server-ID).

Für weitere Unterstützung wenden Sie sich bitte 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.
- Der Zeitpunkt, zu dem das Problem aufgetreten ist, sowie gegebenenfalls der Name oder die IP-Adresse der betroffenen Kamera.
- 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. Sollte das Problem auf vorhersehbare Weise erneut auftreten, aktivieren Sie die Debug-Protokollierung auf dem Server und dem Client, um das Problem vollständiger zu erfassen. Denken Sie im Anschluss daran, die Debug-Protokollierung wieder zu deaktivieren.

Bei bestimmten Problemen kann das Support-Team weitere Informationen erbitten.

Hinweis

Übermitteln Sie Dateien ab einer Größe von 1 GB, z. B. Netzwerk-Trace- oder Datenbankdateien, über einen sicheren, vertrauenswürdigen File-Sharing-Dienst.

Weitere Informationen	
Debug-Protokolle	Die Debug-Protokolle sind standardmäßig deaktiviert, da die Größe von Protokolldateien begrenzt ist. Wenn Sie die Debug-Protokollierung aktivieren, denken Sie nach dem Erstellen des Systemberichts daran, diese wieder zu deaktivieren. Server: Configuration (Konfiguration) > Server > Settings (Einstellungen) > Enable debug logging (Debug-Protokollierung aktivieren) Client: Configuration (Konfiguration) > Client > Settings (Einstellungen) > Enable debug logging (Debug-Protokollierung aktivieren)
Live-Ansicht und Debug-Overlay bei der Wiedergabe	Bei einem Problem mit der Live-Ansicht oder der Wiedergabe kann eine Bildschirmaufzeichnung des Debug-Overlays hilfreich sein. Diese Aufzeichnung sollte den gesamten Bildschirm einschließlich der Systemzeit erfassen, damit sich das Problem in den Protokollen nachvollziehen lässt. • Drücken Sie einmal Strg + I, um sich Overlay-Informationen in der Live-Ansicht anzeigen zu lassen. • Drücken Sie zweimal Strg + I, um Debug-Informationen hinzuzufügen.

Weitere Informationen	
	• Drücken Sie dreimal Strg + I, um das Overlay auszublenden.
Datenbankdateien	Die folgende Anleitung gilt für Fälle, die 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. Das gilt für sämtliche Probleme beim Start des AXIS Camera Station-Dienstes.
Schnappschüsse	Wenn Sie Screenshots beifügen, nehmen Sie bitte den gesamten Bildschirm auf, damit der Kontext klarer ist. Wenn Sie der Meinung sind, dass ein Vollbild-Screenshot nicht eindeutig ist, markieren Sie den zu betrachtenden Bereich bitte mit Pfeilen.
Bildschirmaufzeichnungen	Nehmen Sie den Bildschirm auf, wenn sich das Problem nur schwer in Worten beschreiben lässt, zum Beispiel wenn die Reproduktion des Problems viele Interaktionen mit der Benutzeroberfläche erfordert.
Aufzeichnungsdateien	Der Support bittet Sie möglicherweise darum, Beispiele für die .acsm- und .acsi-Dateien vorzulegen, in denen AXIS Camera Station die Aufzeichnungen speichert. Das gilt für Probleme bei der Wiedergabe oder beim Export von Aufzeichnungen oder mit dem AXIS File Player. Sie finden diese Dateien an dem Speicherort, den Sie für die jeweilige Kamera ausgewählt haben.

T10196821_de

2026-07 (M33.8)

© 2023 – 2026 Axis Communications AB