

AXIS Camera Station Pro

Integrationsanleitung

AXIS Camera Station Pro

Informationen zur AXIS Camera Station Integrator Suite

Informationen zur AXIS Camera Station Integrator Suite

Die AXIS Camera Station Integrator Suite ist eine Toolbox, die die Bereitstellung des Überwachungssystems vereinfacht, Ihnen dabei hilft Fehler zu vermeiden und gleichzeitig Geld und Zeit in allen Phasen der Systemlebensdauer zu sparen. Die Toolbox besteht aus dem Folgenden:

- **AXIS Site Designer**

Ein browserbasiertes Tool, das Ihnen hilft, das Systemdesign und die Produktauswahl zu vereinfachen. Das Tool bietet Ihnen sofortigen Zugriff auf das gesamte Portfolio von Axis. Bandbreite und Speicher werden automatisch errechnet und geeignete Aufzeichnungslösungen werden Ihnen vorgeschlagen. Die Dokumentation über das Design des Systems werden automatisch erstellt und Sie können das Design einfach freigeben.
- **Automatische Konfiguration**

Um die Installationszeit zu verkürzen und Fehler während der Installation zu minimieren, können die Einstellungen aus AXIS Site Designer auf importiert werden.
- **AXIS Installation Verifier**

Eine integrierte Anwendung. Um sicherzustellen, dass alles funktioniert, wird eine Live-Systemüberprüfung durchgeführt. Dabei wird die Systemleistung überprüft und eine Dokumentation bereitgestellt, die dann bei der Erstinstallation und bei späteren Wartungsbesuchen an den Kunden weitergegeben werden kann.
- **AXIS System Health Monitoring**

Verwenden Sie AXIS System Health Monitoring, um den Status der Installation von zu überprüfen. Das Portal ermöglicht die Überwachung aller Installationen und benachrichtigt Sie bei Problemen mit verbundenen Geräten.

AXIS Camera Station Pro

Hilfreiche Links für Integratoren

Hilfreiche Links für Integratoren

Im Folgenden einige Links für den Einstieg. Viel Spaß beim Lesen!

- *Konzipieren Sie Ihr System auf Seite 5*
- *Was gibt's Neues in ?*
- *Benutzerhandbuch*
- *Installationsanleitung*

AXIS Camera Station Pro

Vorgehensweise

Vorgehensweise

Dies ist die Vorgehensweise, wenn Sie eine End-to-end-Lösung von Axis entwickeln möchten:

1. *Konzipieren Sie Ihr System auf Seite 5*
2. *Konfigurieren Sie Ihr System auf Seite 6*
3. *Testen Sie Ihr System auf Seite 12*

AXIS Camera Station Pro

Konzipieren Sie Ihr System

Konzipieren Sie Ihr System

Informationen über AXIS Site Designer

AXIS Site Designer ist ein browserbasiertes Tool, mit dem Sie das System designen und Produkte auswählen können. Das Tool beinhaltet sofortigen Zugriff auf das gesamte Portfolio von Axis. Bandbreite und Speicher werden automatisch errechnet und geeignete Aufzeichnungslösungen werden Ihnen vorgeschlagen. Die Dokumentation über das Design des Systems werden automatisch erstellt und Sie können das gesamte Design einfach freigeben.

Ein AXIS Site Designer-Projekt erstellen



Anhand dieses Beispiels erfahren sie, wie Sie im AXIS Site Designer eine Lösung erstellen und konfigurieren. Sie können diese Konfiguration nach importieren.

Hinweis

Voraussetzungen:

- Ein aktives MyAxis Konto

1. In AXIS Site Designer anmelden.
2. Ein Neues Projekt erstellen.
3. Fügen Sie Kameras zu Ihrem Projekt hinzu.

Verwenden Sie das 2D-Visualisierungs-Tool der Kamera und Filter, um eine geeignete Kamera zu finden. Dann klicken Sie auf **Add (Hinzufügen)**.

4. Die Kameras konfigurieren.

Sie können z. B. Zeitpläne für Ihre Aufzeichnungen erstellen: kontinuierliche Aufzeichnung während der Geschäftszeiten und bewegungsabhängige Aufzeichnung während der Schließzeiten. Sie können auch einstellen, für wie lange das System durchgehend aufzeichnen soll.

5. Fügen Sie Geräte zu Ihrem Projekt hinzu.

Sie können dem Projekt beispielsweise Lautsprechersysteme, Aufzeichnungslösungen, Zubehör und Netzwerk-Komponenten hinzufügen.

Nächster Schritt: *Ein AXIS Site Designer-Projekt importieren auf Seite 6*

AXIS Camera Station Pro

Konfigurieren Sie Ihr System

Konfigurieren Sie Ihr System

Ein AXIS Site Designer-Projekt importieren

Anhand dieses Beispiels erfahren Sie, wie Sie ein Projekt aus dem AXIS Site Designer importieren.

Hinweis

Voraussetzungen:

- Ein aktives MyAxis Konto
- Ein AXIS Site Designer-Projekt

1. In AXIS Site Designer anmelden.
2. Ihr Projekt öffnen.
3. Gehen Sie zu **Share with (Teilen mit)** und klicken Sie auf eine der folgenden Optionen:
 - **Generate access code (Zugangscodes generieren)** - Diese Option auswählen, wenn Ihr -Server Internetzugang hat.
 - **Download camera settings (Kameraeinstellungen herunterladen)** - Diese Option auswählen, wenn Ihr -Server keinen Internetzugang hat.
4. Rufen Sie in **Configuration > Devices > Add devices (Konfiguration > Geräte > Geräte hinzufügen)** auf.
5. Klicken Sie auf **Add (Hinzufügen)**, wählen Sie **Site Designer configuration (Site Designer-Konfiguration)** aus und klicken Sie auf **Next (Weiter)**.
6. Eine der folgenden Optionen auswählen und dann auf **Import (Importieren)** klicken:
 - Wenn Sie einen Zugangscodes generiert haben, wählen Sie **Access code (Zugangscodes)**.
 - Wenn Sie eine Datei heruntergeladen haben, wählen Sie **Choose file (Datei auswählen)**.
7. **Install (Installieren)** anklicken.

Der Import wird anhand der Konfiguration im AXIS Site Designer und den Modellen in die Konfiguration für ein spezifisches Modell anpassen. Wenn Sie mehrere Konfigurationen für ein Kameramodell haben, müssen Sie manuell die gewünschte Konfiguration auswählen.

Nächster Schritt: *Testen Sie Ihr System auf Seite 12*

Verbindung mit -Server herstellen

In diesem Bereich wird erklärt, wie auf einen Server der von einem Computer oder einer Mobil-App zugegriffen werden kann. Sie haben mehrere Möglichkeiten, um auf den Server zuzugreifen:

- Von einem lokalen Netzwerk auf den Server zugreifen
- Über das Internet auf den Server zugreifen:
 - über Axis Secure Remote Access
 - via Port-Mapping (nicht empfohlen)

Hinweis

Voraussetzungen:

- Ein aktives MyAxis Konto

AXIS Camera Station Pro

Konfigurieren Sie Ihr System

Das System vorbereiten

Vor dem Verbinden des Servers der von einem Clientgerät aus muss das System vorbereitet werden. Die folgenden Anweisungen helfen beim Verwalten der allgemeinen Einstellungen.

1. Windows® App installieren.
2. Zum Erstellen von Windows-Benutzern, siehe *Erstellen von Windows-Benutzern*.
3. Fügen Sie Windows-Benutzer zur Windows-App hinzu.
4. Die Firewall des Servers konfigurieren.
5. Installation der Mobile App.

Diese Schritte richten sich nach der Konfiguration des Systems, der Konfiguration des Clients und der Netzwerkinfrastruktur.

Informationen zu Benutzern und Benutzergruppen

Hinweis

Für fortgeschrittene Benutzer:

Um sicherzustellen, dass Benutzernamen und Kennwörter für Windows und vorliegen, Port xx und Port yy öffnen und die Mobil-App konfigurieren.

Um von einem Clientgerät aus eine Verbindung mit einem Server herzustellen, ist ein Windows-Benutzer mit der entsprechenden Berechtigung erforderlich. Dieser Benutzer kann entweder das Standardadministratorkonto des Windows-Gerät sein, auf dem der Server installiert ist, oder ein erstellter Benutzer.

ermöglicht sowohl lokale Windows-Benutzer und Benutzergruppen als auch Domain-Benutzer und Benutzergruppen. Domainbenutzer müssen dem Server der Domain beitreten. Dies muss eventuell von der IT-Abteilung durchgeführt werden.

Als aktueller Benutzer anmelden:

- Wenn der aktuelle Windows-Benutzer der Berechtigungsliste hinzugefügt wurde, **Current user (Aktueller Benutzer)** wählen und **Log on (Anmelden)** anklicken.

Sich als anderer Benutzer anmelden:

1. Wenn der aktuelle Windows-Benutzer nicht der Berechtigungsliste hinzugefügt wurde, **Current user (Aktueller Benutzer)** wählen und **Log on (Anmelden)** anklicken.
2. Auf der nächsten Seite **Other user (Anderer Benutzer)** auswählen.
3. Die Zugangsdaten eingeben und **Log on (Anmelden)** anklicken.

Benutzer oder Benutzergruppen können eine der folgenden Rollen einnehmen:

- **Administrator:**
 - Uneingeschränkter Zugriff auf die gesamte Funktionalität sowie alle Kameras und Geräte.
- **Bediener:**
 - Uneingeschränkter Zugriff auf alle Funktionen, außer auf die Optionen Configuration menu (Konfigurationsmenü), Configuration workspace (Konfigurationsbereich), Device management page (Seite Geräteverwaltung) und Audit log (Prüfprotokolle).
 - Uneingeschränkter Zugriff auf bestimmte Kameras und E/A-Ports.
 - Bestimmter Zugriff auf Wiedergabe und Aufzeichnungsexport.
- **Betrachter:**
 - Zugriff auf Live-Videos bestimmter Kameras.

AXIS Camera Station Pro

Konfigurieren Sie Ihr System

- Zugriff auf bestimmte E/A-Ports.

Hinweis

Um weitere Optionen zum Anpassen der Konten von Bedienern und Betrachtern anzuzeigen, unter der betreffenden Registerkarte die Option **Advanced (Erweitert)** anklicken.

Windows-App installieren (Client)

1. Die Windows-App von axis.com/products/axis-camera-station-pro herunterladen
2. Die Windows-App mit derselben Version wie der des Servers installieren.

Erstellen eines Windows-Benutzers

Um lokale Windows-Benutzer und Benutzergruppen zu verwenden, müssen diese dem Windows-Server hinzugefügt werden, auf dem installiert ist. Wir empfehlen, allen Benutzern ein eigenes Konto einzurichten.

1. **Computer Management (Computerverwaltung) > System tools (System-Tools) > Local Users and Groups (Lokale Benutzer und Gruppen) > Users (Benutzer)** aufrufen.
2. Den Ordner **Users (Benutzer)** anklicken und **New user (Neuer Benutzer)** wählen.
3. Die erforderlichen Informationen eingeben.
4. **User must change password at next logon (Benutzer muss Kennwort beim nächsten Anmelden ändern)** löschen.
5. Klicken Sie auf **Create (Erstellen)**.

Windows-Benutzer zu hinzufügen

Erstellte Windows-Benutzer müssen der hinzugefügt werden.

1. Den Client der öffnen und als aktueller Benutzer beim Server anmelden.
2. **Configuration > Server > User permissions (Konfiguration > Server > Benutzerrechte)** aufrufen.
3. **Add (Hinzufügen)** anklicken.
4. Den Umfang für das Konto auswählen.
 - **Server:** Ruft die lokalen Benutzer und Gruppen ab.
 - **Domain:** Ruft die Domain-Benutzer und Gruppen ab.
5. Den Benutzer auswählen und **Add (Hinzufügen)** anklicken.
6. Die Rolle und Berechtigungsstufe des Benutzers auswählen und **OK** anklicken.

Hinweis

Für lokale Konten empfehlen wir, sich als Test nach dem Hinzufügen als dieser Benutzer anzumelden.

Konfigurieren der Firewall auf dem Server

Während des Installierens konfiguriert automatisch die Ausnahmen für die Windows-Firewall für den eingehenden Datenverkehr. Wenn eine Firewall eines anderen Anbieters angezeigt wird, muss möglicherweise eine ähnliche Gruppe von Ausnahmen angefordert werden, die der Konfiguration hinzugefügt werden soll. In den meisten Fällen erfordert nur der **Eingangsportbereich** zwischen 55752 und 55757 eine Ausnahme.

Während des Installierens konfiguriert automatisch die Ausnahmen für die Windows-Firewall für den eingehenden Datenverkehr. Wenn eine Firewall eines anderen Anbieters angezeigt wird, muss möglicherweise eine ähnliche Gruppe von Ausnahmen angefordert werden, die der Konfiguration hinzugefügt werden soll. In den meisten Fällen erfordert nur der **Eingangsportbereich** zwischen 22900 und 29245 (eingeschlossen) eine Ausnahme.

Diese Tabelle fasst die Ports einer typischen zusammen:

AXIS Camera Station Pro

Konfigurieren Sie Ihr System

Portnummer	Protokoll	Eingehend/Ausgehend	Verwendet von	Anmerkung
80 und 443	HTTP und HTTPS	Ausgehend	Server und Client an Internet	Lizenz aktivieren, Firmware herunterladen, verbundene Dienste und mehr.
80	HTTP	Ausgehend	Server und Gerät	Videostream und Gerätedaten
5353	UDP	Multicast (Eingehend und ausgehend)	Server und Gerät	mDNS Discovery (Bonjour) Ermitteln von Kameras Multicast 224.0.0.251
1900	UDP	Multicast (Eingehend und ausgehend)	Server und Gerät	SSDP Discovery upnp Ermitteln von Geräten Multicast 239.255.255.250
3702	UDP	Multicast (Eingehend und ausgehend)	Server und Gerät	WS-Discovery Ermitteln von Webservices Onvif Multicast 239.255.255.250
29200	TCP	Eingehend	Server und Client	In der Standardeinstellung ausgeschaltet.
29202	TCP	Eingehend	Server und Client	Verschlüsselte Anwendungsdaten (Verschlüsselung TLS 1.2)
29204	TCP	Eingehend	Server und Mobil-App	Verschlüsselte Anwendungsdaten HTTPS Videostream MP4 über HTTPS
29205	TCP	Eingehend	Server und Mobil-App	Videostream RTSP über HTTP

Serverzugriff über Axis Secure Remote Access

Der sichere Fernzugriff ermöglicht es Clients oder Mobil-Apps, eine Verbindung zu einem Server ohne Portweiterleitung aufzubauen. Für gleichrangigen Verbindungen zwischen Clients oder Mobil-Apps und dem Server ist das Datenvolumen nicht begrenzt.

Wenn keine direkte Verbindung hergestellt werden kann, wird die Verbindung über Mediator-Server ermöglicht. Das Datenvolumen ist in diesem Fall auf 1 GB pro Monat und pro MyAxis Nutzer begrenzt.

Weitere Informationen zu Axis Secure Remote Access finden Sie unter axis.com/technologies/axis-secure-remote-access

Zum Verwalten von Axis Secure Remote Access sind erforderlich:

- Internetzugang (für Zugang über Proxyserver, siehe *Erweiterte Einstellungen auf Seite 11*)
- Ein MyAxis Konto

Den Server konfigurieren

1. Melden Sie sich beim Server mit einem Administratorbenutzer an. Beim Netzwerk des Servers anmelden.
2. **Configuration (Konfiguration) > Connected services (Verbundene Dienste) > Axis Secure Remote Access** aufrufen.
3. Melden Sie sich bei Ihrem MyAxis-Konto an.

AXIS Camera Station Pro

Konfigurieren Sie Ihr System

Herstellen einer Verbindung über die Windows-App (Client)

1. Öffnen Sie die App.
2. **AXIS Secure Remote Access** anklicken.
3. Die beim Konfigurieren des Servers verwendeten Zugangsdaten eingeben.
4. Wählen Sie **Remote Server** und einen Server aus der Liste.
Der Server wird als **ServerName (Secure Remote Access)** angezeigt.
5. Bitte **Anmelden** anklicken.

Eine Verbindung über die Mobil-App (Client) herstellen

1. Öffnen Sie die Mobil-App.
2. **Anmelden** anklicken.
3. Die Zugangsdaten für Ihr MyAxis Konto eingeben.
4. Eine Server auswählen.
5. Mit den konfigurierten Zugangsdaten des Windows-Kontos anmelden. Die Zugangsdaten müssen nur beim ersten Zugriff auf einen Server eingegeben werden. Die Mobil-App speichert die Zugangsdaten.

Hinweis

Je nach Systemkonfiguration muss möglicherweise das Format **Domain/Benutzer** oder **Server-Name/Benutzer** verwendet werden.

Den Server über Port-Mapping verbinden

⚠WARNUNG

Aus Gründen der Cybersicherheit wird nicht empfohlen, Port-Mapping zu verwenden. Axis Communications empfiehlt stattdessen, Axis Secure Remote Access zu verwenden. Weitere Informationen zur Cybersicherheit und Axis Secure Remote Access finden Sie auf axis.com.

Port-Mapping ermöglicht das Herstellen einer Verbindung mit dem Server von einem entfernten Standort auf dem Router. Je nach Infrastruktur des Netzwerks muss möglicherweise der Netzwerkadministrator zum Konfigurieren herangezogen werden.

Den Server konfigurieren

- Auf dem Router, über den der Server der -Server mit dem Internet verbunden ist, folgende Ports öffnen:
 - Um Windows-Clientverbindung zuzulassen: 29200 und 29202
 - Um Mobilverbindung zuzulassen: 29204 und 29205

Herstellen einer Verbindung über die Windows-App (Client)

1. Öffnen Sie die Windows-App.
2. **Remote-Server** wählen.
3. Die öffentliche IP-Adresse oder den vollständigen Namen des Netzwerks eingeben, in dem der Server der installiert ist.
4. Wenn der Port Regeln weiterleitet, nicht den Standardport verwenden. Um eine Verbindung mit Port 60009 herzustellen, 60009 in das Adressfeld eingeben.

Beispiel:

`myserver.axis.com:60009`

Eine Verbindung über die Mobil-App herstellen

AXIS Camera Station Pro

Konfigurieren Sie Ihr System

- Mobile App öffnen
- **Add System (System hinzufügen)** und die öffentliche IP-Adresse oder den vollständigen Namen eingeben.
- Wenn nicht die Standardwerte verwendet werden, die Portnummer entsprechend anpassen.
- Mit den konfigurierten Zugangsdaten des Windows-Kontos anmelden. Die Zugangsdaten müssen nur beim ersten Zugriff auf einen Server eingegeben werden. Die Mobil-App speichert die Zugangsdaten.

Erweiterte Einstellungen

Proxyeinstellungen des Servers

Wenn sich der Server in einem Netzwerk befindet, das Proxyeinstellungen für die Internetverbindung erfordert, müssen gegebenenfalls die Proxyinformationen zum Dienst hinzugefügt werden.

1. Dienststeuerung öffnen.
2. Im Server-Status **Stop** anklicken.
3. **Einstellungen ändern** wählen.
4. Die Proxyeinstellungen ändern.
5. Klicken Sie auf **Speichern**.
6. Den Dienst starten.

Proxyeinstellungen Client

Wenn eine eingesetzte Windows-App einen Server erfordert, der für den Zugriff auf bestimmte Websites einen Proxyserver benötigt, muss der Client der für den selben Proxyserver konfiguriert werden.

- Öffnen Sie die Windows-App.
- Klicken Sie auf **Proxyeinstellungen des Clients ändern**.
- Die Einstellungen nach Bedarf anpassen und **OK** anklicken.

Port-Mapping für mehr als einen Server.

Wenn mehrere Server im selben Netzwerk ausgeführt werden, die Port-Mapping erfordern, muss der Standardport der (29200) geändert werden. Jeder Server muss über einen eindeutigen Port verfügen.

Für jeden Server folgende Schritte durchführen:

1. Dienststeuerung öffnen.
2. Im Server-Status **Stop** anklicken.
3. **Einstellungen ändern** wählen.
4. Den HTTP-Port bearbeiten, alle anderen Ports werden auf die erwartete Nummer eingestellt.
5. Den Dienst speichern und neu starten.
6. Für die Portweiterleitung den neuen Portbereich nutzen.

AXIS Camera Station Pro

Testen Sie Ihr System

Testen Sie Ihr System

Informationen zum AXIS Installation Verifier

Axis Installation Verifier ist ein integriertes Tool. Es überprüft, dass Ihr System ordnungsgemäß funktioniert, indem eine Reihe von Tests durchgeführt wird, sobald die Systeminstallation- und Konfiguration abgeschlossen wurde.

Der AXIS Installation Verifier imitiert die Aufzeichnungsfunktion des -Servers. Das Tool führt die folgenden Tests durch: mit den aktuellen Einstellungen, mit simuliertem Schwachlicht und außerdem einen Belastungstest, um Systemprobleme herauszufinden.

AXIS Installation Verifier generiert einen Überprüfungsbericht im PDF-Format und dieser kann dann an den Kunden weitergegeben werden.

Den AXIS Installation Verifier ausführen

1. Schließen Sie die Installation und Konfiguration von ab.
2. Gehen Sie zum Hauptmenü im -Client und klicken Sie auf **Help > Installation Verifier (Hilfe > Installation Verifier)**. Dieser Test nimmt ca. 20 Minuten in Anspruch.

Während der Test durchgeführt wird, werden die Geräte in den Wartungsmodus versetzt und keinen Videostream für Live-Ansichten oder Aufzeichnungen anzeigen. Der Status der verschiedenen Tests kann folgendermaßen lauten:

- **Running (Wird ausgeführt):** Der Test wird gerade durchgeführt. Bitte warten.
 - **Bestanden:** Alle prüfbaren Geräte haben den Test bestanden. Einzelheiten finden Sie im Bericht.
 - **Nicht bestanden:** Nicht alle prüfbaren Geräte haben den Test bestanden. Einzelheiten finden Sie im Bericht.
 - **Fehlgeschlagen:** Der Test konnte nicht abgeschlossen werden und dadurch wurde kein Bericht erstellt. Es wird empfohlen, dass Sie einen Screenshot des Test-Fensters machen, einen -Systembericht generieren und den Axis Support kontaktieren.
3. Sobald alle Tests abgeschlossen sind, klicken Sie auf **View Report (Bericht ansehen)**, um den Bericht anzusehen oder klicken Sie auf **Save Report (Bericht speichern)**, um die Datei auf den PC herunterzuladen.

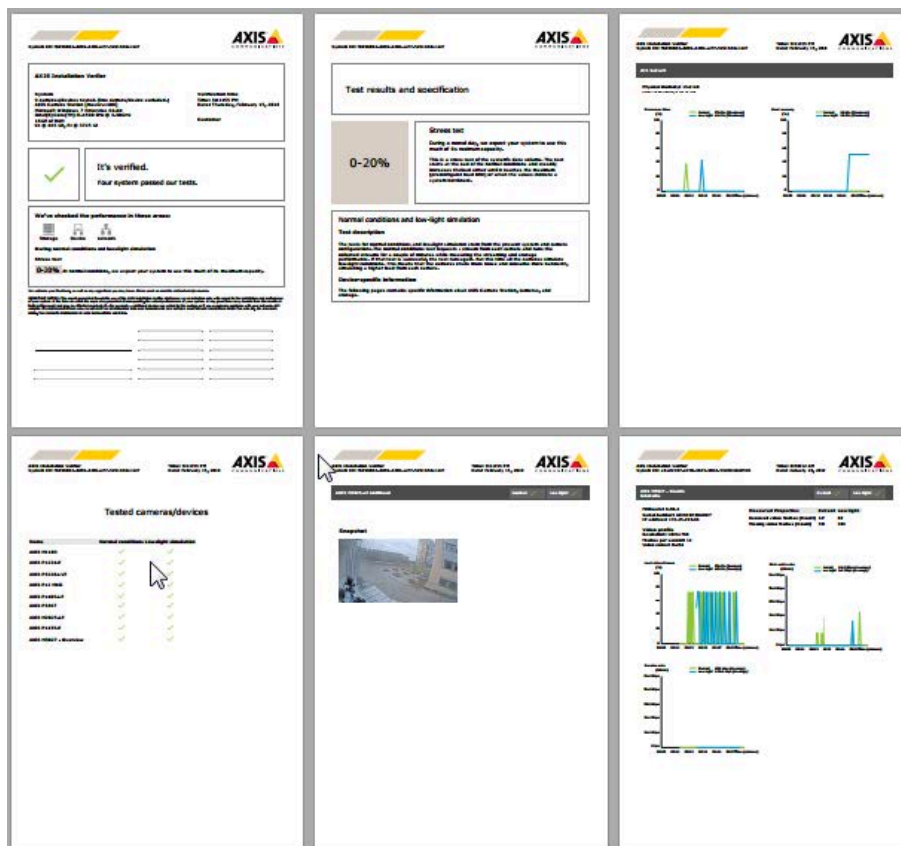
Den Bericht analysieren und verstehen

Ergebnisse der Prüfung: Allgemeine Informationen

Der Bericht wird als PDF-Datei generiert, die vom Systemintegrator zum Endkunden weitergeleitet werden kann, sobald die Installation abgeschlossen und das System validiert wurde.

AXIS Camera Station Pro

Testen Sie Ihr System



Der erste Bereich der ersten Seite enthält Systeminformationen, wie z. B. Hardware, Betriebssystem, Durchführungsdatum und -zeit des Tests. Es gibt außerdem einen Bereich, wo der Name des Kunden eingefügt werden kann.

AXIS Installation Verifier

<p>System 31 cameras/devices tested. (12 cameras/devices excluded.) AXIS Camera Station [master-1408] Microsoft Windows 7 Enterprise 64-bit Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz 16GB of RAM C: @ 465 GB, E: @ 3725 GB</p>	<p>Verification time Time: 8:16:51 AM Date: Friday, February 16, 2018</p> <p>Customer</p>
--	---


Der zweite Bereich zeigt die Ergebnisse des Tests. Jeder Test (normale Bedingungen, Schwachlicht und Belastungstest) dauert 5 Minuten. Speicher, Geräte und Netzwerk sind die drei Bereiche, die von dem Tool getestet werden. Es gibt zwei mögliche Ergebnisse der Überprüfung:

- Das System hat den Test bestanden und wurde verifiziert. Das System sollte mit der Auslastung und der aktuellen Konfiguration zurecht kommen. Sie können auch die zu erwartende Auslastung während der Schwachlichtsimulation sehen, welches normalerweise das ressourcenintensivste Szenario ist.

Im oben genannten Beispiel zeigt der Belastungstest die Grenzen des Systems auf und ist zu dem Ergebnis gekommen, das unter normalen und Schwachlichtbedingungen voraussichtlich 40-60% der Ressourcen verbraucht werden.

AXIS Camera Station Pro


Testen Sie Ihr System





It's verified.

Your system passed our tests.

We've checked the performance in these areas:


Storage


Device


Network

During normal conditions and low-light simulation

Stress test

40-60% At normal conditions, we expect your system to use this much of its maximum capacity.

Test results and specification

40-60%

Stress test

During a normal day, we expect your system to use this much of its maximum capacity.

This is a stress test of the system's data volume. The test starts at the load of the normal conditions and steadily increases the load either until it reaches the maximum (preconfigured load limit) or when the values indicate a system bottleneck.

Normal conditions and low-light simulation

Test description

The tests for normal conditions and low-light simulation stem from the present system and camera configurations. The normal conditions test requests a stream from each camera and runs the collected streams for a couple of minutes while measuring the streaming and storage performance. If that test is successful, the test runs again. But this time all the cameras simulate low-light conditions. This means that the cameras create more noise and consume more bandwidth, simulating a higher load from each camera.

Device-specific information

The following pages contains specific information about AXIS Camera Station, cameras, and storage.

- Es wurden Probleme gefunden und einige Dinge müssen geändert werden, um die Stabilität des Systems zu verbessern. Die Ergebnisse der einzelnen Tests und die gefundenen Probleme werden zusammen mit den Fehlermeldungen aufgelistet. Auf den nächsten Seiten des Berichts sind weitere Details zu finden.

In dem oben genannten Beispiel war eines der Geräte während der Überprüfung nicht verfügbar. Ein Netzwerk-Problem ist höchstwahrscheinlich der Grund dafür. Es kann aber auch sein, dass das Gerät überladen ist und deshalb nicht geantwortet hat.

AXIS Camera Station Pro

Testen Sie Ihr System

Issues found.

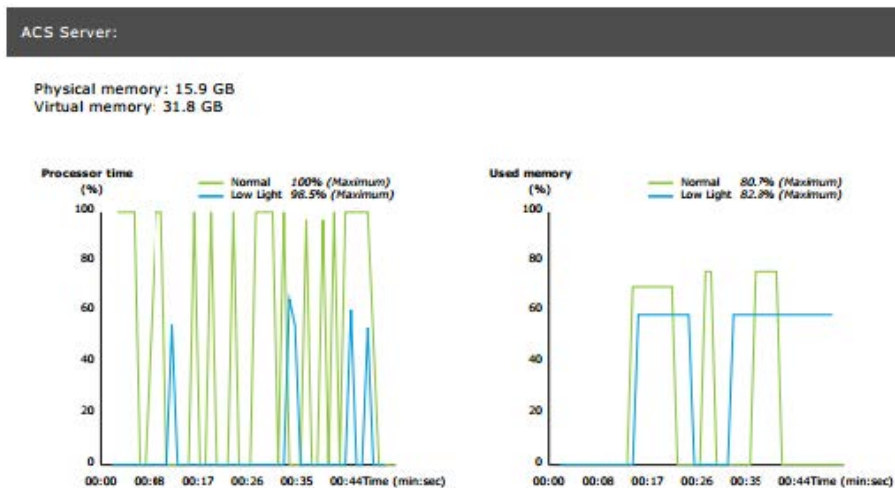
There's room for improvement.

This is what we found:

Test Results		Error Messages
Current Mode Test	NOT PASSED	[RecEng] Could not connect to device
Low Light Simulation Test	PASSED	[RecEng] Device omitted from test due to previous errors
Load Test	PASSED	

Am unteren Rand der ersten Seite gibt es einen Bereich, wo Sie Kundeninformationen, Kommentare zum Test oder andere wichtige Informationen eintragen können.

Ergebnisse der Prüfung: Server



Der physische und virtuelle Speicher wird oben auf der Seite aufgeführt.

- Random access memory (RAM) ist ein physischer Speicher, der Anwendungen, Dokumente und Vorgänge auf dem Server enthält.
- Virtueller Speicher ist ein Speicherplatz, der alle Dateien auf der Festplatte für den Wiederherstellungsvorgang bereithält, falls der Server keinen RAM mehr zur Verfügung hat. Der virtuelle Speicher ist wesentlich langsamer als der physische und sollte niemals verwendet werden.

Server wird gegen zwei Metriken geprüft:

- **Prozessorzeit:** Dies misst den prozentualen Anteil der Zeitspanne, die der Prozessor damit verbringt, einen non-idle-Thread auszuführen. Wenn der Prozentsatz über 85 liegt, ist der Prozessor überlastet und der Server braucht möglicherweise einen schnelleren Prozessor oder die Konfiguration muss angepasst werden.
- **Verwendeter Speicher:** Dies misst den Prozentsatz des verbrauchten physischen Speichers durch alle laufenden Prozesse. Wenn dieser Wert über 85 Prozent liegt, ist nicht genügend Speicherplatz vorhanden und die Aufrufaktivität kann

AXIS Camera Station Pro

Testen Sie Ihr System

sich erhöhen. Um das Problem zu beheben, müssen Sie dem Server mehr Speicherplatz hinzufügen oder die Anzahl der laufenden Anwendungen auf dem Server eingrenzen.

Ergebnisse der Prüfung: Geprüfte Geräte und Kameras

Tested cameras/devices

Name	Normal conditions	Low-light simulation
AXIS M1103	✓	✓
AXIS M2025-LE	✓	✓
AXIS P1435-E	✓	✓
AXIS M3027 - Overview	✓	✓
AXIS M3027 (2) - Quad View	✓	✓
AXIS P1425-E	✓	✓
AXIS P5515	✓	N/A
AXIS M3005 (12)	ⓘ	N/A

Die nächste Seite enthält eine Liste aller geprüften Kameras und Geräte. Ein Gerät kann mehrere Kameras beinhalten. Beispiel: Multi-Sensor-Geräte oder Mehrkanal-Encoder werden als ein Gerät gezählt aber 3,4, oder sogar 16 Kameras (eine Kamera pro Sensor/Kanal).

- Ein grüner Haken bedeutet, dass die Kamera alle zugehörigen Tests bestanden hat.
- **N/A (k. A.)** bedeutet, dass der Test nicht auf der Kamera durchgeführt wurde, wenn z. B. die Kamera den Belichtungswert für die Schwachlichtsimulation nicht unterstützt.
- Ein rotes Symbol wird angezeigt, wenn die Kamera den Test nicht bestanden hat. Auf den nächsten Seiten sind weitere Details in den kameraspezifischen Ergebnissen zu finden.

Ergebnisse der Prüfung: Hinweise und Kriterien

Kleinere Anpassungen, die die Installation verbessern können, aber die nicht durch den Test, der auf dieser Seite aufgelistet wird, durchfallen werden. Wenn beispielsweise der Standard-Router sich nicht im selben Subnetz wie das Gerät befindet oder der DNS oder NTP-Server fehlen.

Ergebnisse der Prüfung: ausgeschlossene Kameras und Geräte

Excluded cameras/devices

Name	Notes
AXIS 212 PTZ	Video codec not supported
AXIS T8508	Device has no enabled cameras
AXIS C8033	Device has no enabled cameras
AXIS A1001	Device has no enabled cameras
AXIS M1014	Device status is not OK
AXIS 216MFD	Video codec not supported
IPC-HD1200C	Device is not Vapix

Wenn ein Gerät einen der Tests nicht unterstützt, wird es nicht berücksichtigt. Die folgenden Geräte werden nicht mit getestet:

- **Device is not Vapix® (Gerät ist nicht Vapix®):** Geräte von Drittanbietern werden nicht getestet.
- **Device has no enabled cameras (Gerät hat keine aktivierten Kameras):** Geräte ohne Videosensor, wie z. B. Netzwerk-Schalter, Audiogeräte, Türsteuerungen und E/A-Audiomodule.
- **Video codec not supported (Videocodec wird nicht unterstützt):** Geräte ohne H.264-Unterstützung (normalerweise Firmware 4.x).

AXIS Camera Station Pro

Testen Sie Ihr System

- **Device status is not OK (Gerätstatus ist nicht OK):** Gerät befindet sich im Wartungsmodus, ist nicht erreichbar, falsche Anmeldedaten.

Ergebnisse der Prüfung: Kameraspezifische Ergebnisse:

Es werden alle Kamerainformationen, wie Firmware, Seriennummer, IP-Adresse und für Aufzeichnungen verwendete Videoprofile aufgelistet. Eine Zusammenfassung von empfangenen und fehlenden Videorahmen für jeden Test wird ebenfalls bereitgestellt.

Hinweis

- Wenn ein Gerät so konfiguriert ist, dass es mit zwei verschiedenen Videoprofilen aufzeichnet (z. B. Medium für Kontinuierlich und High für Bewegungserkennung), wird nur das oberste Profil getestet, unabhängig von den konfigurierten Zeitplänen.
- Wenn beide Aufzeichnungsarten deaktiviert sind, wird das Profil, das für die manuelle Aufzeichnung gewählt wurde, für den Test verwendet, auch wenn es momentan nicht aktiv ist.

Der Abschnitt "Gerätkonfiguration" führt die wichtigsten Informationen vom getesteten Gerät auf. Wenn einige Parameter falsch sind (nicht konfiguriert oder im anderen Subnetz), wird ein Ausrufezeichen vor dem Parameter angezeigt.

Device Configuration

Firmware: 8.40.1
Serial number: ACCC8E02A96D
IP address: 172.25.193.116
Is Using Dhcp: Yes
Subnet Mask: 255.255.255.0
Default Router: ⚠192.168.0.1
Primary DNS: ⚠0.0.0.0
NTP Server: 10.0.2.201

Der Grad stellt die 3 gemessenen Kriterien für normale und Schwachlichtbedingungen dar.

- **Lost video frames (Verlorene Videoframes):** Die Quote von fehlenden Videoframes pro eine Sekunde Intervall. Ein überdurchschnittlicher Wert weist auf einen Engpass im Netzwerk hin oder dass das Gerät überlastet ist. Der Durchschnitt von verlorenen Videoframes liegt meistens unter 1%.
- **Storage buffer (Speicherpuffer) :** Die Auslastung des Speicherpuffers pro eine Sekunde Intervall. Ein hoher Spitzenwert weist auf ein Problem mit dem Speicher hin. Der Speicherpuffer liegt normalerweise unter 20%.
- **Received rate (Empfangene Rate):** Die Datenrate (ohne Überhang), die von der Kamera gesendet und vom AXIS Camera Station-Server empfangen wurde.

Im unteren Graph wird eine hohe Quote von verlorenen Videoframes angezeigt.

AXIS Camera Station Pro

Testen Sie Ihr System



Dies kann folgende Gründe haben:

- Die Kamera ist überlastet, eventuell durch zu viele Ansichtsbereiche, die genutzt werden (360 Grad-Kameras z. B.) oder zu viele Streams werden gezogen.
- Engpass im Netzwerk, zwischen Kamera und Server.
- Fehlerhaftes oder qualitativ schlechtes Netzwerk-Kabel.
- Unzureichende oder unzuverlässige Stromquelle, einschließlich PoE.

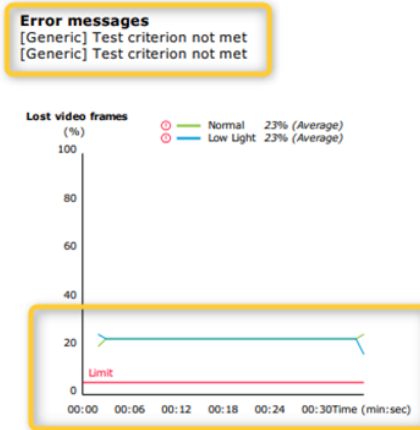
Ein zusätzliches Kriterium für den Verlust der Bildrate wird bei der Durchführung des Normal- und Schwachlichttests berücksichtigt:

- Für jedes Gerät, dass das Kriterium nicht erfüllt (mehr als 5 % Bildratenverlust), wird ein Aspekt hinzugefügt. Dies wird nicht durch den Test fallen.
- Wenn mehr als 5 % der Geräte, im Test das oben genannte Kriterium nicht erfüllen, ändert sich der Status auf "Nicht bestanden".

Nachfolgend ist ein Beispiel, in dem das Kriterium im Normal- und Schwachlichttest nicht erfüllt wurde:

AXIS Camera Station Pro

Testen Sie Ihr System



Der folgende Graph zeigt ein Beispiel, wo der Test nicht abgeschlossen werden konnte. Dies kann folgende Gründe haben:

- Die Kamera wurde getrennt oder die Netzwerk-Verbindung wurde während des Tests unterbrochen.
- Die Stromquelle konnte die Kamera während des Tests nicht versorgen.
- Die Kamera war überlastet und hat zu lange gebraucht, um auf die Anfrage des Servers reagieren.

AXIS M3005 (12) Normal Low light N/A

Firmware: 5.50.5.10
Serial number: 00408CF10BB8
IP address: 172.25.193.6

Measured Properties	Normal	Low light
Received video frames (Count)	0	N/A
Missing video frames (Count)	0	N/A

Video profile
Resolution: 1280x720
Frames per second: 15
Video codec: H.264

Error messages
[RecEng] Could not connect to device
[RecEng] Device omitted from test due to previous errors

Lost video frames

Condition	Normal	Low light
Normal	N/A	N/A
Low Light	N/A	N/A

No Data Available

Storage buffer

Condition	Normal	Low light
Normal	N/A	N/A
Low Light	N/A	N/A

No Data Available

Receives rate

Condition	Normal	Low light
Normal	0 bps (Average)	0 bps (Average)
Low Light	0 bps (Average)	0 bps (Average)

No Data Available

AXIS Camera Station Pro

Testen Sie Ihr System

Nachdem das Testergebnis der Kamera angezeigt wurde, wird ein Screenshot von der Kamera angezeigt:



Snapshot



Ergebnisse der Prüfung: Speichergeräte

Tested storage devices

Path	Normal conditions	Low-light simulation
E:\Recording	✓	✓
\\172.25.192.20\nas\Recording	✓	✓

Speichergeräte werden unter den gleichen Bedingungen getestet.

Das Tool testet lokale Festplatten anhand von zwei Metriken:

- **Disk write rate (Festplattenschreibrate):** Die gesamte Datenrate, die in diese Speichermaske pro Sekundenintervall geschrieben wird.
- **Used write buffers (count) (Verwendete Schreibpuffer (Anzahl)):** Die Auslastung des Speicherpuffers (300 Proben) pro eine Sekunde Intervall. Ein hoher Spitzenwert weist auf ein Problem mit dem Speicher hin. Allgemein sollte dieser Wert unter 1 oder 2 sein.

Hinweis

Derzeit wird das NAS (Network Attached Storage) nicht getestet.

Folgende Informationen über die Speichernutzung und -kapazität wird angezeigt:

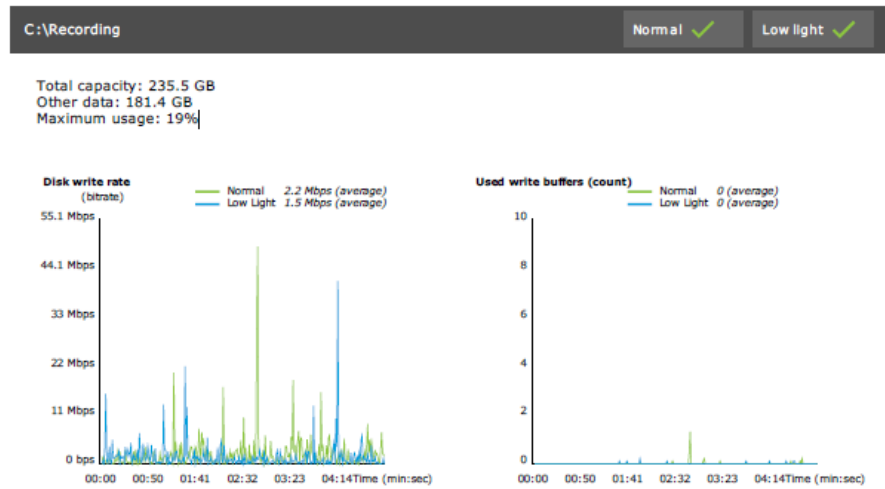
Gesamtkapazität: Die Gesamtgröße des Speichers.

Andere Daten: Daten, die nicht vom Server indiziert werden. Dabei kann es sich um externe Dateien, wie z. B. Dokumente, Betriebssystemdateien, Dateien im Papierkorb handeln.

Maximum usage (Maximale Nutzung): Aufzeichnungsbegrenzung von . ordnet den Aufzeichnungsdateien einen maximalen Prozentsatz des Speichers zu. Dieser Wert ist standardmäßig auf 99% für nicht-OS-Festplatten und auf eine *Gesamtgröße von 60 GB* für OS-Festplatten festgelegt.

AXIS Camera Station Pro

Testen Sie Ihr System



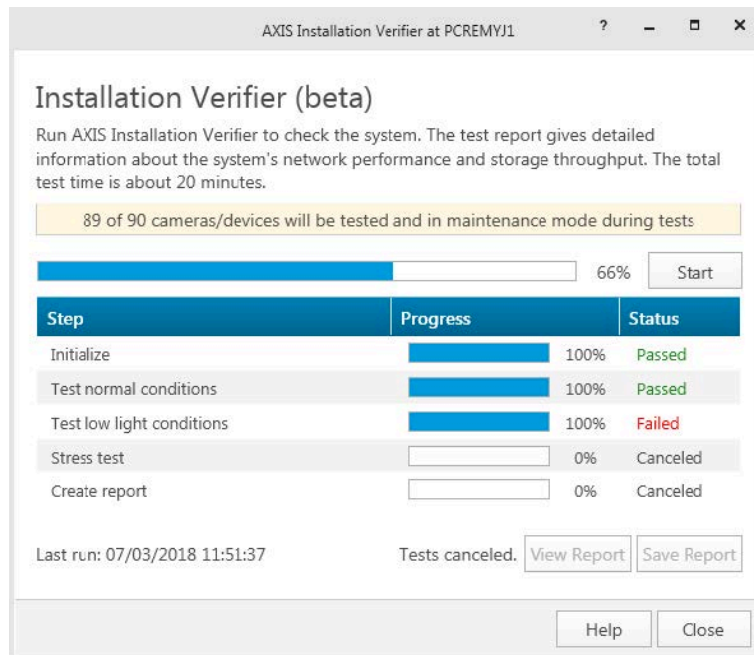
Fehlerbehebung

Wenn einer der Tests fehlschlägt (**Failed (Fehlgeschlagen)**) wird kein Bericht erstellt. Es wird empfohlen, dass Sie einen Screenshot des Test-Fensters machen, einen -Systembericht vom Hilfe-Menü erstellen und Axis Support über den online Helpdesk kontaktieren.

Hinweis

Es wird zwischen **Not passed (Nicht bestanden)** und **Failed (Fehlgeschlagen)**:

- **Not passed (Nicht bestanden)** zeigt an, dass der Server, einige Geräte oder der Speicher die Bedingungen nicht erfüllt haben, um den Test zu bestehen.
- **Failed (Fehlgeschlagen)** bedeutet, dass der Test nicht abgeschlossen wurde und kein Ergebnis in Bezug auf die Systemleistung verfügbar ist.



AXIS Camera Station Pro

Testen Sie Ihr System

Hinweise und Einschränkungen

- Nur H.264 wird unterstützt. Kameras ohne Unterstützung für H.264 werden ignoriert.
- Der Schwachlichttest wird nur an Kameras durchgeführt, die den Belichtungswertparameter unterstützen. Es wird "N/A" angezeigt, wenn Kameras den Belichtungswertparameter nicht unterstützen.
- Der Schwachlichttest kann die gleichen Ergebnisse haben wie der Test unter normalen Bedingungen bei Kameras mit WDR-Unterstützung.
- Kameras von Drittanbietern werden ignoriert.
- Das NAS (Network Attached Storage) wird nicht getestet, aber als validiert angezeigt.

AXIS Camera Station Pro

Überwachen Sie Ihr System

Überwachen Sie Ihr System

Information über AXIS Überwachung des Systemzustands ^{BETA}

Durch die Anmeldung bei AXIS System Health Monitoring wird der aktuelle Status der Installationen überprüft. AXIS System Health Monitoring ermöglicht die Überwachung aller Installationen und benachrichtigt Sie automatisch bei Problemen mit verbundenen Geräten.

Konfigurieren der AXIS Überwachung des Systemzustands ^{BETA}

Dieses Beispiel verdeutlicht die Konfiguration der AXIS Überwachung des Systemzustands.

1. Die neueste Version von *axis.com* herunterladen und installieren.
2. Konfigurieren Sie AXIS Überwachung des Systemzustands.
 - 2.1 Legen Sie unter **Configuration > System Health Monitoring > Settings (Konfiguration > Systemzustandsüberwachung > Einstellungen)** fest, ob eine Firewallregel eingerichtet werden muss, damit AXIS Überwachung des Systemzustands durch Windows Defender geleitet werden kann.
 - 2.2 Konfigurieren Sie unter **Configuration > System Health Monitoring > Notifications (Benachrichtigungen)** Ihren SMTP-Server, die E-Mail-Empfänger und die Benachrichtigungsregeln, für die eine E-Mail gesendet werden soll.
3. Konfigurieren Sie AXIS Überwachung des Systemzustands für das Multisystem-Setup.
 - 3.1 Gehen Sie zu **Konfiguration > Überwachung des Systemzustands > Multisystem**.
 - 3.2 Klicken Sie unter **Generate system configuration (Systemkonfiguration erstellen)** auf **Generate (Erstellen)**.
 - 3.3 Kopieren Sie die Konfiguration und übertragen Sie sie an das System, für das Sie die Daten erfassen möchten.
 - 3.4 Erweitern Sie die Option **Retrieve data from other systems (Daten von anderen Systemen abrufen)**, fügen Sie die zuvor kopierte Konfiguration ein und klicken Sie auf **Hinzufügen**. Wiederholen Sie die oben genannten Schritte für jedes System.

Funktionen

Funktion	Beschreibung
Inventar	Inventar mit Geräteübersicht.
Geräteinformationen	Typ, Modell, Firmwareversion, IP-Adresse, MAC-Adresse, API-Modus, Aufzeichnungstyp usw.
Informationen zum Video Management System (VMS)	Softwareversion, Betriebssystem, Hardware, CPU-/Speicher-/Netzwerk-Nutzung usw.
Systemberichte herunterladen	Auf der Systemseite kann ein -Systembericht oder AXIS Überwachung des Systemzustands-Bericht generiert werden.
Benachrichtigungsprotokoll	Zeigt einen Verlauf aller generierten Benachrichtigungsprotokolle an.
Speicherinformationen	Zeigt Speichernutzung und Vorhaltezeiten für die Kameraaufzeichnungen und andere aufzeichnungsbezogene Informationen an.

AXIS Camera Station Pro

Überwachen Sie Ihr System

Fehlerbehebung

Problemtyp	Fehlermeldung	Lösung
Betriebszeit	Das System wird bei der Multisystem-Einrichtung nicht angezeigt.	<p>AXIS Überwachung des Systemzustands hat keine Daten vom System erfasst. Warten Sie eine Minute, bis AXIS Überwachung des Systemzustands nach dem Hinzufügen eines neuen Systems Daten erfassen kann. Wenn auf der Seite „Manage servers (Server verwalten)“ ein Fehlersymbol angezeigt wird, überprüfen Sie Folgendes:</p> <ul style="list-style-type: none">• AXIS Überwachung des Systemzustands wird im System ausgeführt.• Das System wird im System angezeigt.• Die bereitgestellte Konfiguration (Host, Port, Token, Zertifikat) ist korrekt.• Der Server ist im Netzwerk erreichbar.• Ausnahme für die Firewall ist aktiviert. <p>Die QuickInfo des Fehlersymbols gibt möglicherweise auch einen Hinweis auf das Problem.</p>

Support-Protokolle

Die Debug-Protokolle für AXIS Überwachung des Systemzustands werden auf dem Server gespeichert unter: C:\ProgramData\Axis Communications\AXIS System Health Monitoring\logs.

FAQ

F: Wie oft wird das Gerät oder der VMS-Status aktualisiert?

A: Es kann bis zu 1 Minute dauern, bis der Status des Geräts oder VMS in der Schnittstelle für die AXIS Überwachung des Systemzustands aktualisiert wird.

Hinweise und Einschränkungen

- Speicher: Der verwendete Speicherplatz für die an AXIS S3008 angeschlossene Kameras wird nicht unterstützt.
- Nicht aktivierte Speichergeräte sind weiterhin sichtbar, und die erfassten Daten werden bis zu 2 Wochen lang aufbewahrt.
- Die Benachrichtigungseinstellungen wirken sich nur auf den lokalen AXIS Server zur Überwachung des Systemzustands aus.
- Für den Zugriff auf die AXIS Überwachung des Systemzustands sind Administratorrechte erforderlich.
- Warnungen zu Vorhaltezeiten unterstützen keine Aufzeichnungen der Bewegungserkennung.
- Aufzeichnungen, die mit anderen Methoden (manuell/ereignisbasiert usw.) außer „kontinuierlich“ oder „Bewegungserkennung“ erstellt wurden, werden als „Aufzeichnungstyp: Keine“ gekennzeichnet.

AXIS Camera Station Pro

Axis Produkte im System einrichten

Axis Produkte im System einrichten

Set up AXIS S3008 Recorder einrichten

Hinweis

- Erforderlich ist AXIS S3008 Recorder Firmware 10.4 oder höher oder die Firmware 5.50 oder höher des Axis Geräts.
- AXIS S3008 Recorder erfordert keine Lizenz.

Einschränkungen

Für die Verwendung von AXIS S3008 Recorder als Aufzeichnungsspeicher für Ihre Geräte in gibt es einige Einschränkungen:

- AXIS S3008 Recorder unterstützt keine Body-Worn-Kameraaufnahmen oder die vorab aufgezeichneten Videos, die in für Demozwecke verwendet werden.
- Aufzeichnungsstreams werden direkt von den Kameras in AXIS S3008 Recorder geschoben. Stellen Sie sicher, dass AXIS S3008 Recorder mit demselben Netzwerk wie die Kameras verbunden ist und dass alle Geräte miteinander kommunizieren können.
- Kameras von Drittanbietern werden nicht unterstützt.
- Geräte mit nicht numerischer Auflösung wie D1, CIF, 4CIF werden nicht unterstützt.
- Ausfallsichere Aufzeichnungen werden bei Kameras mit AXIS S3008 Recorder als Aufzeichnungsspeicher nicht unterstützt.
- Interne Ereignisse des AXIS S3008 Recorder werden derzeit nicht auf der Seite „Konfiguration der Geräteereignisauslöser“ aufgeführt.
- Das Sperren von Aufzeichnungen über Lesezeichen wird nicht unterstützt.
- Bei Verwendung von AXIS S3008 wird Audio von einem externen, an eine Kamera angeschlossenen Audiogerät nicht aufgezeichnet.
- Analysedaten werden nicht unterstützt.
 - Die automatische Videoaufbereitung wird nicht unterstützt.
 - Die intelligente Suche über Analysedaten wird nicht unterstützt.
- AXIS Installation Verifier wird für AXIS S3008 Recorder und die angeschlossenen Geräte nicht unterstützt.
- 2N IP-Gegensprechgeräte werden nicht unterstützt.
- Aufzeichnungen, die von AXIS Companion auf AXIS S3008 Recorder gemacht werden, können nicht in abgespielt werden.
- AXIS S3008 Recorder unterstützt bis zu 64 virtuelle Eingänge.
 - Eine Kamera, die auf AXIS S3008 Recorder aufzeichnet, verwendet drei virtuelle Eingänge. Eine für die Bewegungsaufzeichnung, eine für die dauerhafte und eine für die manuelle Aufzeichnung.

Wenn z. B. acht Kameras auf AXIS S3008 Recorder aufzeichnen, verwenden sie 24 virtuelle Eingänge (8 x 3) und es sind noch 40 virtuelle Eingänge (64 bis 24=40) für Aktionsregeln vorhanden.
 - Eine Netzwerk-Türanlage, die auf AXIS S3008 Recorder aufzeichnet, verwendet vier virtuelle Eingänge. Eine für Bewegungsaufzeichnung, eine für die dauerhafte Aufzeichnung, eine für die manuelle Aufzeichnung und eine für die standardmäßig erstellte Aktionsregel.

Wenn beispielsweise sieben Kameras und eine Türanlage auf AXIS S3008 Recorder aufzeichnen, verwenden sie 25 virtuelle Eingänge (7 x 3 und 1 x 4) und es sind noch 39 virtuelle Eingänge (64 bis 25 =39) für zusätzliche Aktionsregeln vorhanden.
 - Eine Aktionsregel, die die Aufzeichnung auf AXIS S3008 Recorder auslöst, verwendet einen virtuellen Eingang.

AXIS Camera Station Pro

Axis Produkte im System einrichten

- Für die Fallback-Aufzeichnung wird kein virtueller Eingang verwendet.

Vorgehensweise

1. *Rekorder hinzufügen auf Seite 26*
2. *Hinzufügen von Geräten und Auswahl des Rekorders als Aufzeichnungsspeicher auf Seite 26*
3. *Aufzeichnungen konfigurieren auf Seite 27*

Rekorder hinzufügen

Hinweis

entfernt Aufzeichnungen von allen vorherigen Systemen, wenn Sie den Rekorder zu einem neuen System hinzufügen.

1. Rufen Sie **Configuration > Devices > Add devices (Konfiguration > Geräte > Geräte hinzufügen)** auf.
2. Wählen Sie Ihren Rekorder aus der Liste aus und klicken Sie auf **Add (Hinzufügen)**. Ist Ihr Rekorder nicht aufgeführt, suchen Sie über die **Manuelle Suche** manuell danach.
3. Wählen Sie die Standardeinstellungen und klicken Sie auf **Weiter**.
4. Erstellen Sie ein neues Kennwort für die Speicherverschlüsselung oder verwenden Sie das aktuelle Kennwort. Weitere Informationen finden Sie unten. Klicken Sie auf **Next (Weiter)**.
5. Rufen Sie **Configuration > Devices > Other devices (Konfiguration > Geräte > Weitere Geräte)** auf und überprüfen Sie, ob der Rekorder hinzugefügt wurde.
6. Rufen Sie **Configuration > Storage > Management (Konfiguration > Speicher > Verwaltung)** auf und überprüfen Sie, ob der Rekorder zur Speicherliste hinzugefügt wurde.

Wichtig

Kennwort für die Speicherverschlüsselung ändern

- Das Kennwort für die Speicherverschlüsselung wird benötigt, um von außerhalb von auf den Rekorder zugreifen zu können oder wenn der Rekorder über die Weboberfläche des Geräts auf die Werkseinstellungen zurückgesetzt wird.
- Wenn das Gerät nicht formatiert ist, müssen Sie ein neues Kennwort für die Festplattenverschlüsselung verwenden. Hierdurch wird das Laufwerk formatiert und die vorherigen Aufzeichnungen wurden entfernt.
- Wenn das Gerät bereits formatiert wurde, können Sie wählen, ob Sie das aktuelle Kennwort verwenden oder ein neues erstellen möchten.
 - Mit Ihrem aktuellen Kennwort löscht das System alle Aufnahmen, formatiert das Gerät jedoch nicht. Diese Option kann Zeit sparen.
 - Wenn Sie ein neues Kennwort erstellen, wird das Gerät formatiert und alle Aufzeichnungen werden gelöscht.
- Wenn Sie mehrere Geräte gewählt haben und ein neues Kennwort erstellen möchten, werden alle Geräte formatiert und dem neuen Kennwort zugewiesen.
- Wenn Sie mehrere Geräte ausgewählt haben und Ihr aktuelles Kennwort verwenden möchten, werden nur die Geräte mit einem übereinstimmenden Kennwort hinzugefügt.

Hinzufügen von Geräten und Auswahl des Rekorders als Aufzeichnungsspeicher

1. Rufen Sie **Configuration > Devices > Add devices (Konfiguration > Geräte > Geräte hinzufügen)** auf.
2. Wählen Sie Ihre Geräte aus der Liste und klicken Sie auf **Hinzufügen**. Falls Ihre Geräte nicht aufgeführt sind, suchen Sie diese manuell mithilfe der **Manuellen Suche**.
3. Wählen Sie die Standardeinstellungen und klicken Sie auf **Weiter**.
4. Wählen Sie den Rekorder manuell aus der Auswahlliste **Recording storage (Aufzeichnungsspeicher)** aus und klicken Sie auf **Install (Installieren)**.

AXIS Camera Station Pro

Axis Produkte im System einrichten

Hinweis

Der Rekorder wird nicht automatisch als Aufzeichnungsspeicher ausgewählt, wenn Sie **Automatic (Automatisch)** wählen.

5. Gehen Sie zu **Konfiguration > Speicher > Auswahl**. Klicken Sie auf Ihre Geräte und überprüfen Sie, ob beim Aufzeichnungsspeicher der Rekorder angegeben ist.

Aufzeichnungen konfigurieren

1. Gehen Sie zu **Configuration > Storage > Selection (Konfiguration > Speicher > Auswahl)** und wählen Sie Ihr Gerät.
2. Konfigurieren Sie die **Retention time (Aufbewahrungszeit)**.
 - Wählen Sie **Unlimited (Unbeschränkte)** Aufbewahrungszeit, um die Aufzeichnungen zu speichern, bis der Speicher voll ist.
 - Wählen Sie **Limited (Begrenzte)** Aufbewahrungszeit und die Anzahl der Tage, für die die Aufzeichnung gespeichert werden soll.
3. Klicken Sie auf **Apply (Anwenden)**.

Hinweis

Fallback-Aufzeichnung ist als Standard aktiviert, um die Aufzeichnungen auf dem Rekorder zu speichern, wenn die Verbindung von zum Rekorder verloren geht. Siehe *Fallback recording (Fallback-Aufzeichnung)*.

Speicherort ändern

Sie können den Speicherort eines Geräts von einem Rekorder zum anderen ändern und alle Aufnahmen behalten.

1. Gehen Sie zu **Configuration > Storage > Selection (Konfiguration > Speicher > Auswahl)** und wählen Sie Ihr Gerät.
2. Wählen Sie den neuen Speicherort.
3. Klicken Sie auf **Apply (Anwenden)**.

Hinweis

Wenn der von Ihnen ausgewählte Rekorder bereits die maximale Anzahl an Aktionsregeln für Aufzeichnungsaktionen verwendet, führen Sie einen der folgenden Schritte aus:

- Entfernen Sie Aktionsregeln mit Aufzeichnungsaktionen von den vorhandenen Geräten, indem Sie den Rekorder als Speicher verwenden.
- Verschieben Sie Geräte mithilfe von Aktionsregeln mit Aufzeichnungsaktionen in einen anderen Speicher.

Einen Axis Netzwerk-Tür-Controller einrichten

In diesem Abschnitt wird erläutert, wie Sie einen Axis Netzwerk-Tür-Controller einrichten. Die Videos zur Vorgehensweise bei der Einrichtung finden Sie in *dieser Wiedergabeliste*.

Hinweis

- HTTPS ist erforderlich, um auf dem Controller aktiviert zu werden.
1. Fügen Sie den Axis Netzwerk-Tür-Controller zu hinzu. Siehe dazu *Geräte hinzufügen*.
 2. Aktualisieren Sie die Firmware des Netzwerk-Tür-Controllers. Siehe dazu *Firmware aktualisieren*.
 3. Aktivieren Sie die Zeitsynchronisierung, um den Server als NTP-Server zu verwenden. Siehe dazu *Server-Einstellungen*.
 4. Legen Sie Datum und Uhrzeit für den Controller fest. Siehe dazu *Datum und Uhrzeit festlegen*.
 5. Aktivieren Sie HTTPS auf dem Controller. Siehe dazu *Sicherheit*.

AXIS Camera Station Pro

Axis Produkte im System einrichten

6. Konfigurieren Sie die Zutrittskontrolle.
 - 6.1 Informationen zum Bearbeiten der vordefinierten Identifizierungsprofile oder zum Erstellen eines neuen Identifizierungsprofils finden Sie unter *Identifizierungsprofile*.
 - 6.2 Informationen zur Verwendung eines benutzerdefinierten Setups für Kartenformate und PIN-Längen finden Sie unter *Kartenformate und PIN*.
 - 6.3 Fügen Sie einen Zugang hinzu und wenden Sie ein Identifizierungsprofil auf den Zugang an. Siehe dazu *Zugang hinzufügen*.
 - 6.4 Konfigurieren Sie den Zugang.
 - *Zugangsmonteur hinzufügen*
 - *Notfall-Eingang hinzufügen*
 - *Leser hinzufügen*
 - *REX-Gerät hinzufügen*
 - 6.5 Fügen Sie eine Zone hinzu und fügen Sie der Zone Zugänge hinzu. Siehe dazu *Zone hinzufügen*.
7. Verwalten Sie die Zutrittskontrolle.
 - 7.1 Fügen Sie Zeitpläne hinzu. Siehe dazu *Zeitpläne*.
 - 7.2 Wählen Sie einen Workflow aus und fügen Sie Folgendes hinzu: Siehe dazu *Zugriffsverwaltung*.
 - *Karteneinhaber hinzufügen*
 - *Zugangsdaten hinzufügen*
 - *Gruppe hinzufügen*
 - *Zugangsregel hinzufügen*
 - 7.5 Wenden Sie Karteneinhaber, Gruppen, Zugänge und Zonen auf die Zugangsregeln an.
 - 7.6 Exportieren Sie Berichte. Siehe dazu *Berichte exportieren*.
8. Überwachen und verwalten Sie den Zugang manuell im Zugängedashboard. Siehe dazu *Zugängedashboard in der geteilten Ansicht*.
9. Suchen Sie nach Zutrittskontrolldaten.
 - 9.1 Verbinden Sie eine Ansicht mit einem Zugang. Siehe dazu *Externe Datenquellen*.
 - 9.2 Suchen Sie innerhalb eines Zeitraums oder mit bestimmten Schlüsselwörtern nach bestimmten Ereignisdaten. Siehe dazu *Datensuche*.

Hinweis

Wenn Sie einen Netzwerk-Tür-Controller entfernen, werden die Daten für den Netzwerk-Tür-Controller nicht entfernt. Um die Daten zu entfernen, führen Sie einen Reset auf die werksseitigen Standardeinstellung durch.

AXIS Camera Station Pro

Axis Produkte im System einrichten

Den 2N-Desktop-USB-Kartenleser einrichten



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

help.axis.com/?&tid=§ion=set-up-2n-desktop-usb-card-reader

1. Rufen Sie <https://www.elatec-rfid.com/int/> auf, laden Sie TWN4 DevPack herunter und extrahieren Sie diese in einen Ordner.
2. Öffnen Sie den extrahierten Ordner und führen Sie AppBlaster.exe aus.
 - 2.1 Wählen Sie die Firmware **Multi keyboard V4.80** für die Tastatur aus, um den Leser zu programmieren.
 - 2.2 Definieren Sie das Format für den Leser, indem Sie ein Projekt erstellen. Folgendes muss definiert werden:
 - Transpondertyp einschließlich Frequenz, Typ und Untertyp.
Beispiel: MIFARE Classic (UID, beliebige Länge)
 - Bitweise Verarbeitung für den Transpondertyp.
Beispiel: Byte-Reihenfolge umkehren
 - Ausgangsformat für den Transpondertyp.
Beispiel: Dezimal
 - Entfernen Sie das vordefinierte Suffix für die Ausgangsdaten.
 - 2.5 Laden Sie die Projektdatei in den Leser.
3. Wenn Sie Karten-Zugangsdaten in , legen Sie Ihre Zutrittskontrollkarte dem Leser vor, um die Kartendetails zu erhalten.

Ein Axis Body Worn-Systems einrichten




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

help.axis.com/?&tid=§ion=set-up-an-axis-body-worn-system

AXIS Camera Station Pro

Axis Produkte im System einrichten

Weitere Informationen zur Axis Body Worn-Lösung finden Sie im *Benutzerhandbuch zu Axis Body Worn*.

1. Erneuern Sie bei einer vorhandenen Installation von das für die Kommunikation mit dem Client verwendete Serverzertifikat.
 - 1.1 Gehen Sie in zu **Configuration > Security > Certificates > Certificate renewal (Konfiguration > Sicherheit > Zertifikate > Zertifikaterneuerung)**.
 - 1.2 Klicken Sie auf **Erneuern**.
 - 1.3 Dienst neu starten.
2. Erstellen Sie eine Verbindungsdatei.
 - 2.1 Gehen Sie in zu  > **Other > Connection file... (> Anderes > Verbindungsdatei...)**.
 - 2.2 Geben Sie einen neuen Namen ein, um den in Ihrem Body Worn-System angezeigten Standardnamen zu ändern.
 - 2.3 Klicken Sie auf **Exportieren**.
3. Richten Sie Ihr Body Worn-System ein. Siehe dazu *Erster Zugriff auf AXIS Body Worn Manager*. Wählen Sie die Verbindungsdatei aus, die Sie aus exportiert haben, wenn Sie zum Festlegen des Inhaltsziels aufgefordert werden.
4. Überprüfen Sie in , ob eine virtuelle Kamera mit dem Benutzernamen auf der Registerkarte „Aufzeichnungen“ hinzugefügt wurde.
5. Um die Aufbewahrungszeit zu ändern, gehen Sie zu **Konfiguration > Speicher > Auswahl**.
6. Machen Sie mit der körpernahen Kamera eine Aufzeichnung und setzen Sie die Kamera wieder in die Dockingstation ein. Die Aufzeichnungen werden automatisch hochgeladen in .
7. Sie können Aufzeichnungen von der Body Worn-Kamera in wiedergeben und exportieren.



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

help.axis.com/?tptald=&tsection=set-up-an-axis-body-worn-system

Wichtig

Verwenden Sie zum Entfernen von Benutzern stets den AXIS Body Worn Manager. Entfernen Sie niemals Body-Worn-Benutzer aus .

Eine Axis Netzwerk-Türstation einrichten

Dieses Beispiel erläutert wie:

- Eine Axis Netzwerk-Türstation zu hinzufügen
- Konfigurieren eines akustischen Alarms auf dem Client
- Annahme eines eingehenden Anrufs

AXIS Camera Station Pro

Axis Produkte im System einrichten

- Benachrichtigung über eingehende Anrufe von der Türanlage deaktivieren

Einschränkungen:

- Anrufe von der Türanlage zu können nicht gehalten werden.
- Die Bewegungserkennung kann für die Türanlage nicht aktiviert werden.
- Es können nur Aufzeichnungen vom Anrufer gemacht werden. Es kann kein Audio vom Bediener aufgezeichnet werden.

Eine Axis Netzwerk-Türstation zu hinzufügen

1. Rufen Sie in **Configuration > Devices > Add devices (Konfiguration > Geräte > Geräte hinzufügen)** auf.
2. Wählen Sie die Netzwerk-Türanlage und klicken Sie auf **Hinzufügen**.
3. Wählen Sie die Standardeinstellungen, klicken Sie auf **Weiter** und **Installieren**.
4. Gehen Sie zu **Konfiguration > Geräte > Kameras**, um zu überprüfen, ob die Türanlage hinzugefügt wurde.
5. Gehen Sie zu **Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln**, um zu überprüfen, ob folgende Aktionsregeln automatisch hinzugefügt wurden.
 - **Regel Tür öffnen:** Die Taste Tür öffnen wird hinzugefügt. Klicken Sie auf die Taste in der Live-Ansicht, um den E/A-Port der Türanlage standardmäßig für sieben Sekunden zu öffnen.
 - **Laufenden Anruf aufzeichnen:** Wenn ein Anruf läuft, beginnen Sie mit der Aufzeichnung an der Türanlage.

Konfigurieren eines eingehenden Anruftons

1. Rufen Sie in **Configuration > Client > Settings (Konfiguration > Client > Einstellungen)** auf.
2. Wählen Sie unter **Ton bei eingehendem Anruf** die Option **Sounddatei**.
3. Klicken Sie auf **Durchsuchen** und gehen Sie zur Sounddatei im .wav- oder .mp3-Format.
4. Klicken Sie auf **Wiedergabe**, um den Ton zu testen.

Annahme von eingehenden Anrufen

1. Sobald ein Anruf aktiviert wird, wird ein Benachrichtigungsfenster angezeigt.
2. Bewegen Sie die Maustaste auf die Miniaturansicht, um ein größeres Bild des Anrufers zu sehen.
3. Klicken Sie auf **Accept (Übernehmen)**, um auf den Anruf zu antworten. Es wird eine neue Registerkarte mit der Ansicht von der Türanlage angezeigt. Klicken Sie auf **Tür öffnen**, um den E/A-Port der Türanlage standardmäßig für sieben Sekunden zu öffnen.
4. Klicken Sie auf **Ignore (Ignorieren)**, um den Anruf auf diesem Client zu ignorieren. Der Anruf kann immer noch auf einem anderen Client beantwortet werden.
5. Klicken Sie zum Beenden des Anrufs auf **"1"**. Der Anruf wurde beendet und die Anrufbenachrichtigung wird auf allen Clients entfernt.

Hinweis

Wenn mehrere Anrufe eingehen, sollten Sie sie nacheinander entgegennehmen. Die anderen Anrufe werden so lange angezeigt, bis sie angenommen wurden oder unterbrochen werden.

Benachrichtigung von der Türanlage deaktivieren

1. Erstellen Sie einen separaten Benutzer für den Client.
 - 1.1 Gehen Sie zu **Konfiguration > Sicherheit > Benutzerrechte**.
 - 1.2 Klicken Sie auf **Add (Hinzufügen)**.

AXIS Camera Station Pro

Axis Produkte im System einrichten

- 1.3 Wählen Sie einen Benutzer oder eine Gruppe aus der Liste und klicken Sie auf **Hinzufügen**.
2. Konfigurieren Sie den Benutzer.
 - 2.1 Wählen Sie als **RolleBediener** aus.
 - 2.2 Wählen Sie **Zugriff** für die Türanlage aus, aber löschen Sie **Audio hören** und **Audio sprechen**.
 - 2.3 Klicken Sie auf **Speichern**.

Einrichten der Audioeinstellungen in

Dieses Beispiel erläutert wie:

- Installieren Sie ein Axis Netzwerk-Audiogerät in und verbinden Sie das Audiogerät mit einer Netzwerk-Kamera.
- Eine Schaltfläche in der Live-Ansicht der Kamera in erstellt wird, wodurch ein Audio-Clip auf dem Audio-Gerät abgespielt werden kann.


HINWEIS

Dieses System ist für nicht lebensbedrohliche Systeme wie zum Beispiel Einbruchmeldeanlagen oder Personal- und Kundenadressen geeignet. Es müssen für die Implementierung in kritischen Systeme, wie z.B. Brandevakuierung, spezifische Richtlinien und Standards (vor Ort) eingehalten werden.

Einschränkungen:

- Audio, das von an ein Netzwerkaudiogerät von Axis gesendet wird, kann nicht aufgezeichnet werden.
- Ein Audiogerät muss zuerst mit einer Kamera in verbunden werden.
- Sie können nur ein Audiogerät mit je einer Kamera verbinden.
- Für das Audiogerät in gibt es keine Lautstärkeregelung.

1. Netzwerkaudiogerät von Axis hinzufügen zu :

- 1.1 In  anklicken und **Configuration (Konfiguration)** wählen.
- 1.2 **Devices > Add devices (Geräte > Geräte hinzufügen)** aufrufen.
- 1.3 Wählen Sie das gewünschte Netzwerk-Audiogerät aus der Liste und klicken Sie auf **Hinzufügen**.
- 1.4 **Other devices (Andere Geräte)** aufrufen, um sicherzustellen, dass das Audiogerät der Liste hinzugefügt wurde.

2. Verbinden Sie das Audiogerät mit einer Kamera:

- 2.1 In **Devices > Streaming profiles (Geräte > Streaming-Profile)** aufrufen und die Kamera auswählen, die Sie mit dem Audiogerät verbinden möchten.
- 2.2 Im Streaming-Profil des Geräts wählen Sie das Audiogerät aus der **Lautsprecher**-Liste aus.
- 2.3 Klicken Sie auf **Übernehmen**.
- 2.4 Um die Verbindung zu testen, gehen Sie zur **Live view (Live-Ansicht)** der Kamera in und klicken Sie auf die Schaltfläche **Speak (Sprechen)**. Wenn Sie in das Mikrofon des Computers sprechen, spielt das Audiogerät das Audiomaterial ab.

3. Einen Link für den Audioclip vorbereiten:

- 3.1 **Audio > Audio clips (Audio-Clips)** aufrufen.
- 3.2 Linksymbol für einen Audioclip anklicken.

AXIS Camera Station Pro

Axis Produkte im System einrichten

- 3.3 Für den Clip die Lautstärke und die Anzahl der Wiederholungen einstellen.
- 3.4 Kopiersymbol anklicken, um den Link zu kopieren.
4. Eine Schaltfläche erstellen, die den Audioclip auslöst:
 - 4.1 Rufen Sie in **Configuration > Recording and events > Action rules (Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln)** und **New (Neu)** auf.
 - 4.2 Um einen Trigger hinzuzufügen, klicken Sie auf **Add (Hinzufügen)**.
 - 4.3 Wählen Sie der Liste der Auslöser **Action button (Aktionsschaltfläche)** aus und klicken Sie auf **OK**.
 - 4.4 Wenn eine Schaltfläche erstellt wurde, wählen Sie **Create new button (Neue Schaltfläche erstellen)** und klicken Sie auf **Next (Weiter)**.
 - 4.5 Wählen Sie **Command button (Befehlsschaltfläche)** aus und klicken Sie auf **Next (Weiter)**.
 - 4.6 Geben Sie Details zur Schaltfläche ein, z. B.:
 - Schaltflächenbeschriftung: Mitarbeiter zur Kasse
 - Tooltip: Mitarbeiter an die Kasse rufen
 - Zu Kamera hinzufügen: Kamera auswählen, die mit dem Audiogerät verbunden ist.
 - Zu Lageplan hinzufügen.
 - OK anklicken.

Hinweis

Eine Schaltfläche kann für mehrere Lagepläne oder Kameras verwendet werden.

- 4.6 Klicken Sie auf **Next (Weiter)**.
- 4.7 Um eine Aktion hinzuzufügen, klicken Sie auf **Add (Hinzufügen)**.
- 4.8 **Send HTTP Notification (HTTP-Benachrichtigung versenden)** in der Liste der Aktionen auswählen und **OK** anklicken.
- 4.9 Fügen Sie den konfigurierten Link vom Audiogerät in das **URL**-Feld ein.
- 4.10 **Authentication required (Authentifizierung erforderlich)** wählen und den **User name (Benutzernamen)** und **dasPassword (Passwort)** des Audiogeräts eingeben.
- 4.11 **OK** anklicken.
- 4.12 Klicken Sie zweimal auf **Weiter**.
- 4.13 Einen **Namen** für die Regel eingeben und **Abschließen** anklicken.

In der Live-Ansicht der Kamera in gibt es nun eine Schaltfläche namens **Staff to till (Mitarbeiter zur Kasse)**. Wenn Sie die Schaltfläche anklicken, spielt das Audiogerät den Audio-Clip ab.

AXIS Camera Station Pro

Axis Produkte im System einrichten

Axis Analytics einrichten



Erweitern Sie mit Analysefunktionen (AXIS Loitering Guard)

AXIS Barcode Reader einrichten

In diesem Abschnitt erfahren Sie, wie Sie den AXIS Barcode Reader auf Axis Gegensprechanlagen und Kameras einrichten und in AXIS Camera Station Secure Entry konfigurieren. Weitere Informationen zum AXIS Barcode Reader finden Sie im *Benutzerhandbuch*.

Hinweis

- Erfordert AXIS A1601 Network Door Controller mit Firmware 10.11.9 oder höher.
- Dazu ist eine Lizenz erforderlich.

Einschränkungen

Sie können den QR-Code® nur senden, nachdem Sie den Karteninhaber mit QR-Zugangsdaten abgespeichert haben.

Vorgehensweise

1. *AXIS Barcode Reader installieren auf Seite 34*
2. *AXIS Barcode Reader konfigurieren auf Seite 35*
3. *Eine Verbindung mit dem Zugangskontrollsystem erstellen auf Seite 35*
4. *QR-Zugangsdaten konfigurieren auf Seite 35*
5. *QR-Code® senden auf Seite 35*


AXIS Barcode Reader installieren

1. Laden Sie die Installationsdatei für die Anwendung von *axis.com* herunter
2. Gehen Sie zur Webseite zu Ihrer Axis Gegensprechanlage oder Kamera.
3. Installieren Sie die Anwendung.
4. Aktivieren Sie die Lizenz.
5. Starten Sie die Anwendung.
6. Wir empfehlen Ihnen, folgende Kameraeinstellung für eine höhere QR-Genauigkeit zu ändern.
 - 6.1 Gehen Sie zu Kameraeinstellungen.
 - 6.2 Bewegen Sie unter **Bild > Belichtungen** den Schieberegler **Kompromiss Rauschen** zu **Bewegungsunschärfe** in die Mitte.

AXIS Camera Station Pro

Axis Produkte im System einrichten



AXIS Barcode Reader konfigurieren

1. Um die QR-Zugangsdaten zu ändern, gehen Sie zu **Konfiguration > Zutrittskontrolle > Identifizierungsprofile** und klicken Sie auf . Siehe dazu *Identifizierungsprofile*.
2. Fügen Sie einen Zugang hinzu. Siehe dazu *Zugang hinzufügen*.
3. Wählen Sie **QR** als Identifizierungsprofil für diesen Zugang. Siehe dazu *Einstellungen des Zugangs*.
4. Fügen Sie einen Barcodeleser hinzu. Siehe dazu *Leser hinzufügen*.
 - 4.1 Klicken Sie für eine Seite des Zugangs auf **Leser hinzufügen**.
 - 4.2 Wählen Sie **AXIS Barcode Reader** in der Auswahlliste **Lesertyp**. Geben Sie einen Namen ein und klicken Sie auf **OK**.

Eine Verbindung mit dem Zugangscontroller erstellen

1. In :
 - 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 nicht konfiguriert ist, aktivieren Sie **Ignore server certificate validation (Validierung von Serverzertifikaten ignorieren)**. Weitere Informationen dazu finden Sie unter *Zertifikate*.
 - 2.3 Aktivieren Sie **AXIS Camera Station Secure Entry**.
 - 2.4 Klicken Sie auf **Add (Hinzufügen)**, geben Sie die IP-Adresse der Tür-Steuerung ein und fügen Sie den Authentifizierungsschlüssel ein.
 - 2.5 Wählen Sie im Drop-Down Menü für den Zugang den Leser zum Lesen der Barcodes aus.

QR-Zugangsdaten konfigurieren

1. *Karteneinhaber hinzufügen*.
2. *QR-Zugangsdaten hinzufügen*.
 - Klicken Sie unter **Zugangsdaten** auf  und .
 - Geben Sie einen Namen ein.
 - **Dynamic QR** ist standardmäßig aktiviert. Dynamic QR muss zusammen mit PIN-Zugangsdaten verwendet werden.
 - Legen Sie das Ablaufdatum fest und klicken Sie auf **Hinzufügen**.
3. *Fügen Sie eine Zutrittsregel für den Karteneinhaber dem Zugang hinzu, der mit dem AXIS Barcode Reader konfiguriert ist.*


QR-Code® senden

QR Code ist eine eingetragene Marke von Denso Wave Incorporated in Japan und anderen Ländern.

1. Stellen Sie sicher, dass der Karteneinhaber mit einer korrekten E-Mail-Adresse konfiguriert ist. Siehe dazu *Karteneinhaber hinzufügen*.

AXIS Camera Station Pro

Axis Produkte im System einrichten

2. Konfigurieren Sie zum Versenden von E-Mails zunächst einen SMTP-Server. Siehe dazu *Server-Einstellungen*.
3. Bearbeiten Sie die E-Mail-Vorlage, sofern gewünscht. Siehe dazu *Einstellungen der Zutrittsverwaltung*.
 - 3.1 Gehen Sie *Zutrittsverwaltung > Einstellungen*).
 - 3.2 Ändern Sie unter *E-Mail-Vorlage* den Betreff und den Textkörper.
 - 3.3 **Standardmäßig ist in der E-Mail die Besuchszeit enthalten.**
 - 3.4 Klicken Sie auf **Anwenden**.
4. Senden Sie den QR-Code. Siehe dazu *Karteneinhaber hinzufügen*.
 - 4.1 Rufen Sie **Access Management > Dashboard > Cardholders (Zugriffsverwaltung > Dashboard > Karteneinhaber)** auf.
 - 4.2 Wählen Sie einen Karteneinhaber, klicken Sie auf  und dann auf **QR-Code senden**.
 - 4.3 Klicken Sie auf **OK**.

Einrichten von AXIS Mobile Credential

Um den dynamischen QR-Code verwenden zu können, müssen Sie AXIS Mobile Credential einrichten.

Folgen Sie den Anweisungen in der E-Mail, die Sie erhalten haben:

1. Laden Sie die AXIS Mobile Credential App herunter.
2. Klicken Sie in der E-Mail auf den Aktivierungslink.
3. Öffnen Sie die Anwendung auf Ihrem Mobilgerät. Die Zugangsdaten werden unter **Meine Anmeldeinformationen** angezeigt.
4. Klicken Sie darauf und geben Sie die PIN ein, um den dynamischen QR-Code zu aktivieren.

AXIS Perimeter Defender PTZ Autotracking einrichten

Eine mit AXIS Perimeter Defender PTZ Autotracking konfigurierte Axis PTZ-Kamera kann in zur automatischen Erkennung und Verfolgung von sich im Sichtfeld bewegenden Objekten wie Personen oder Fahrzeuge verwendet werden. Es wurde für den Einsatz im Innen- oder Außenbereich in verkehrsarmen Bereichen wie Parkplätzen oder außerhalb der Öffnungszeiten in Schulen, Büros und Geschäften entwickelt.

Hinweis


Sie können jeweils nur einen Server bearbeiten.

Einschränkungen:

- In einer geteilten Ansicht werden die Triggerbereiche und Objektanzeigen möglicherweise nicht in der richtigen Position angezeigt.
 - Aktualisieren Sie die Konfigurationsseite der Kamera oder aktualisieren Sie die Seite mit den Anwendungseinstellungen:
 - Nachdem die Kamera in gewartet wird
 - Wenn die Kameraausrichtung gedreht wurde
 - Wenn die im Profil für automatische Nachverfolgung verwendete voreingestellte Position gelöscht wird, funktioniert der Auslöserbereich nicht und in diesem Bereich wird keine Warnung in ausgelöst.
1. Öffnen Sie die Konfigurationsseite der Kamera und richten Sie die Triggerbereiche ein.

AXIS Camera Station Pro

Axis Produkte im System einrichten

- 1.1 Wechseln Sie zu **Settings > Apps (Einstellungen > Apps)**.
 - 1.2 Klicken Sie auf **AXIS PTZ Autotracking** und starten Sie die Anwendung.
 - 1.3 Klicken Sie auf "Öffnen", um die Seite mit den Anwendungseinstellungen zu öffnen.
 - 1.4 Wechseln Sie zu **den > Profilen**.
 - 1.5 Klicken  Sie auf und erstellen Sie ein Profil.
 - 1.6 Verschieben Sie den Auslöserbereich und ändern Sie Größe und Form, indem Sie die Verankerungspunkte ziehen. Jeder Auslöserbereich kann bis zu zehn primäre Verankerungspunkte haben.
 - 1.7 Erstellen Sie nach Ihren Wünschen weitere Profile und Triggerbereiche. Sie können bis zu 10 PoE-Zeitplanprofile erstellen.
 - 1.8 Schließen Sie die Seite mit den Anwendungseinstellungen.
2. In :
- 2.1 Rufen Sie **Configuration > Devices > Add devices (Konfiguration > Geräte > Geräte hinzufügen)** auf.
 - 2.2 Wählen Sie die Kameras aus und klicken Sie auf **Hinzufügen**.
 - 2.3 Klicken Sie auf **Weiter und Installieren**.
3. Zur Live-Ansicht der Kamera wechseln. Sie sehen:
- Gelbe Bereiche: Die Auslöserbereiche, die Sie auf der Konfigurationsseite der Kamera konfiguriert haben. Jedes Objekt, das in einen gelben Auslöserbereich eindringt, wird automatisch verfolgt.
 - Grüne Bereiche: Die von der Kamera erkannten Objektanzeigen. Die Objektanzeigen sind nur verfügbar, wenn unter Streamingprofile **Show PTZ autotracking object indicators (Anzeigen von PTZ-Objekten mit automatischem Nachverfolgungsobjekt)** ausgewählt ist.
 - Klicken Sie auf einen grünen Bereich, um das erkannte Objekt zu verfolgen.
 - Klicken Sie auf das Objekt, um die Verfolgung zu beenden.
4. Erstellen Sie eine Aktionsregel, um beim Start der automatischen Nachverfolgung eine Aktion auszulösen.
- 4.1 Rufen Sie **Configuration > Recording and events > Action rules (Konfiguration > Aufzeichnung und Ereignisse > Aktionsregeln)** auf und klicken Sie auf **New (Neue)**.
 - 4.2 Den Autotracking-Ereignisauslöser hinzufügen.
 - 4.1 **Hinzufügen** anklicken und **Geräteereignis** wählen. Klicken Sie auf **OK**.
 - 4.2 Gehen Sie im Bereich **Configure device event trigger (Geräte-Ereignisauslöser konfigurieren)** folgendermaßen vor:
 - Wählen Sie in der Dropdown-Liste Ihre **Timezone (Zeitzone)** aus.
 - Wählen Sie in der **>-Dropdown-Liste** die Option **PtzAutotrackingaus**.
 - Legen Sie die **Auslöserzeit** und den **Status** auf **ja** fest.
 - 4.4 Klicken Sie auf **OK**.
 - 4.5 Klicken Sie auf **Next (Weiter)**.
 - 4.6 Fügen Sie eine Aufzeichnungsaktion hinzu.
 - 4.1 **Hinzufügen** anklicken und **Live-Ansicht** wählen. Klicken Sie auf **OK**.

AXIS Camera Station Pro

Axis Produkte im System einrichten


- 4.2 Wählen Sie in der Dropdown-Liste Ihre Timezone (Zeitzone) aus.
- 4.3 Videoeinstellungen konfigurieren:
- 4.4 Klicken Sie auf OK.
- 4.5 Einen Gateway-Knoten wählen und Weiter anklicken.
- 4.6 Finish (Fertigstellen) anklicken.

AXIS License Plate Verifier einrichten

Wenn ein Gerät mit einem Netzwerk AXIS License Plate Verifier konfiguriert wird, wird es in diesem Bereich als externe Datenquelle im Video Management System betrachtet. Sie können eine Ansicht mit der Datenquelle verbinden, nach vom Gerät erfassten Fahrzeugkennzeichen suchen und das entsprechende Bild anzeigen.

Hinweis

AXIS License Plate Verifier erfordert eine Lizenz.

1. Laden Sie die Anwendung und installieren Sie sie auf Ihrem Gerät.
2. Konfigurieren Sie die Anwendung. Siehe *AXIS License Plate Verifier Benutzerhandbuch*.
3. Bei einer vorhandenen Installation von AXIS Camera Station Pro erneuern Sie das für die Kommunikation mit dem Client verwendete Serverzertifikat. Siehe *Zertifikat erneuern*.
4. Aktivieren Sie die Zeitsynchronisierung, um den Server von AXIS Camera Station Pro als NTP-Server zu verwenden. Siehe dazu *Server-Einstellungen*.
5. Fügen Sie das Gerät zu AXIS Camera Station Pro hinzu. Siehe dazu *Geräte hinzufügen*.
6. Wenn das erste Ereignis empfangen wird, wird unter **Konfiguration > Geräte > externe Datenquelle** automatisch eine Datenquelle hinzugefügt.
7. Verbinden Sie die Datenquelle mit einer Ansicht. Siehe dazu *Externe Datenquellen*.
8. Suchen Sie nach Fahrzeugkennzeichen, die vom Gerät erfasst wurden. Siehe dazu *Datensuche*.
9. Klicken Sie auf , um die Suchergebnisse in eine txt-Datei zu exportieren.

Einrichten des AXIS Speed Monitors


Die AXIS Speed Monitor App kann auf einem mit einem Radar verbundenen Gerät oder direkt auf einem Radar installiert werden.

Wenn ein Gerät oder Radar mit einem AXIS Speed Monitor konfiguriert wird, wird es als externe Datenquelle betrachtet. Sie können eine Ansicht mit der Datenquelle verbinden, nach vom Gerät erfassten Objektgeschwindigkeiten suchen und das entsprechende Bild anzeigen.

1. Laden Sie die Anwendung und installieren Sie sie auf Ihrem Gerät.
2. Konfigurieren Sie die Anwendung und das Radar. Weitere Informationen finden Sie im *Benutzerhandbuch von AXIS Speed Monitor*.
3. Erneuern Sie bei einer vorhandenen Installation von das für die Kommunikation mit dem Client verwendete Serverzertifikat. Siehe *Zertifikat erneuern*.
4. Aktivieren Sie die Zeitsynchronisierung, um den Server als NTP-Server zu verwenden. Siehe dazu *Server-Einstellungen*.
5. Fügen Sie die zugehörigen Geräte zu hinzu. Siehe dazu *Geräte hinzufügen*.
 - Wenn die App auf einem mit dem Radar verbundenen Gerät installiert ist, das Gerät und den Radar hinzufügen.

AXIS Camera Station Pro

Axis Produkte im System einrichten

- Wenn die App auf einem Radar installiert ist, fügen Sie das Radar hinzu.
- 6. Wenn das erste Ereignis empfangen wird, wird unter **Konfiguration > Geräte > externe Datenquelle** automatisch eine Datenquelle hinzugefügt.
- 7. Verbinden Sie die Datenquelle mit einer Ansicht. Siehe dazu *Externe Datenquellen*.
- 8. Suchen Sie nach Objektgeschwindigkeiten, die vom Gerät erfasst wurden. Siehe dazu *Datensuche*.
- 9. Klicken Sie auf , um die Suchergebnisse in eine txt-Datei zu exportieren.

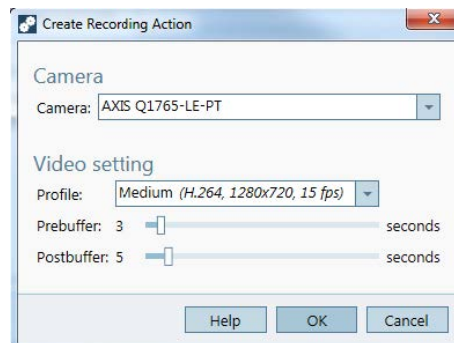
AXIS Perimeter Defender einrichten

In diesem Bereich wird erläutert, wie der AXIS Perimeter Defender mit dem Ereignissystem integriert wird. Es wird beschrieben, wie Sie:

- Eine Regel für die konfigurieren, um einen Alarm bei einem Einbruch auszulösen.
- Überprüfen, ob die Konfiguration korrekt durchgeführt wurde.
- 1. Den AXIS Perimeter Defender in der AXIS Perimeter Defender Setup-Software konfigurieren und kalibrieren. In dem AXIS Perimeter Defender Benutzerhandbuch oder unter *oder der Produktseite* erhalten Sie Hilfe bei der Installation und Kalibrierung des AXIS Perimeter Defender.
- 2. Um die Kamera zu hinzuzufügen, dem Assistenten für **Add Camera (Kamera hinzufügen)** folgen.
- 3. Einen Geräte-Ereignisauslöser konfigurieren:
 - 3.1 **Configuration (Konfiguration) > Recording & Events (Aufzeichnung und Ereignisse)** aufrufen und die Registerkarte **Advanced rules (Erweiterte Regeln)** aufrufen.
 - 3.2 Eine neue Regel erstellen und den Auslöser **Device Event (Geräte-Ereignis)** wählen.
 - 3.3 Wählen Sie die Kamera, auf der AXIS Perimeter Defender installiert ist.
 - 3.4 **AXIS Perimeter Defender** aus der Liste **Event (Ereignis)** aufrufen.
 - 3.5 In der Liste **Feature (Funktion)** den Namen der konfigurierten Einbruchsregel (in diesem Fall Einbruch-1) wählen. Wenn Sie diese Regel für alle konfigurierten Szenarios auslösen möchten, wählen Sie **ALL_SCENARIOS** aus.
 - 3.6 Wählen Sie **Yes (Ja)** aus, um die Aktionsregel auszulösen, wenn ein Einbruch stattfindet. Wenn ein Einbruch erkannt wird, zeigt das Aktivitätsfenster eine Statusänderung an, mit der bestätigt wird, dass das Setup korrekt ist.
 - 3.7 **OK** und **Next (Weiter)** anklicken, um die Aktionen zu konfigurieren.
 - 3.8 Im Dialogfenster **Add Action (Aktion hinzufügen)** können Sie eine oder mehrere Aktionen für die Regel hinzufügen.

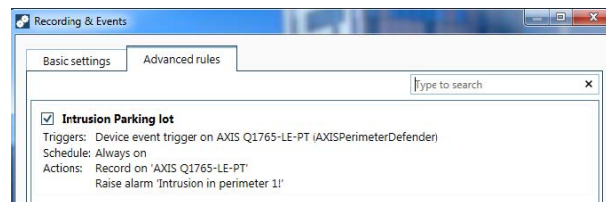
AXIS Camera Station Pro

Axis Produkte im System einrichten



In diesem Beispiel wird eine Aufnahmeaktion und eine Alarmaktion hinzugefügt.

3.9 Finish (Fertigstellen) anklicken.



Das Beispiel zeigt eine Regel, die zwei Aktionen auslöst, wenn ein Einbruch stattfindet.

4. Simulieren Sie einen Einbruch, z.°B. durch Betreten des überwachten Bereichs, um zu testen, ob die Konfiguration wie gewünscht funktioniert.

AXIS Camera Station Pro

Benötigen Sie weitere Hilfe?

Benötigen Sie weitere Hilfe?

Hilfreiche Links

- *Installationsparameter – Microsoft Installer*
- *Installationsschalter – ausführbar*
- *Benutzerhandbuch*
- *Lernvideos*

Support kontaktieren

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

