AXIS Optimizer

AXIS Optimizer for XProtect®
AXIS Optimizer for Siemens Siveillance™

Benutzerhandbuch

Inhalt

AXIS Optimizer 7
Bestimmungsgemäßer Verwendungszweck des AXIS Optimizer 7
Systemanforderungen 7
Unterstützung für föderierte Systeme 7
Unterstützung für vernetzte Systeme 7
Versionshinweise 7
AXIS Optimizer installieren oder aktualisieren 8
AXIS Optimizer installieren 8
Welche Versionen sind in meinem System installiert? 8
Erweiterte Installationsmöglichkeiten 8
VMS-Migration 9
Integrität des Installationsprogramms prüfen 9
AXIS Optimizer aktualisieren 9
Manuelle Aktualisierung 10
Automatisches Aktualisieren des Systems 10
Automatische Aktualisierung aktivieren 11
Automatische Aktualisierung deaktivieren 11
Mehr erfahren 11
AXIS Optimizer deinstallieren 12
Werkseinstellung 12
Sichere Außerbetriebnahme 12
Benutzerrechte 12
Geräteeinstellungen aufrufen 14
Geräteassistent 14
Axis Gerät konfigurieren 14
Anwendungen auf einem Axis Gerät installieren 14
Anwendungen auf einem Axis Gerät konfigurieren 14
Anwendungen auf einem Axis Gerät aktualisieren 14
Axis Gerät neu starten 15
IP-Adresse eines Axis Geräts kopieren 15
Automatisierung durchführen 16
Aktionen für Axis Geräte erstellen 16
Plugin für Ereignisserver 16
Ereignis-Server-Plugin installieren 16
Mehrere Kameras mit einem Klick trocknen 16
Autofokus für mehrere Kameras mit einem Klick aktivieren 17
Auslösen mehrere Blitzsirenen mit einem Klick 18
Privatzonenmasken mehrerer Kameras automatisch deaktivieren 19
Aktivieren einer Blitzsirene bei Bewegungserkennung durch die Kamera 21
Audioclips bei Bewegungserkennung durch eine Kamera über einen Lautsprecher oder in einer Lautsprecherzone abspielen 23
Fehlerbehebung bei Regeln 25
Zentrale Verwaltung von Fahrzeugkennzeichenlisten 25
Eine Liste erstellen 25
Berechtigungen für die Liste konfigurieren 25
Eine Liste bearbeiten 26
Listen importieren 26
Eine Liste exportieren 27
Mehr erfahren über Listen 28
Auf Live-Ereignisse reagieren 29
Gerätesteuerelemente verwenden 29
Bedienelemente 29
Zugriff auf die Bedienelemente 29

Fokusbereich einer PTZ-Kamera speichern 29
Autofokus einer Kamera einstellen 30
Schnelltrocknen oder Wischer aktivieren 30
Punktgenaue Temperatur messen 31
Automatisches Heranzoomen und Verfolgen eines sich bewegenden Objekts 31
Benutzerdefinierte Bedienelemente erstellen 32
Zugriff auf Bedienelemente konfigurieren 32
Über Lautsprecher interagieren 33
Lautsprecherverwaltung 33
Modi 33
AXIS Audio Manager Pro-Modus 33
AXIS Audio Manager Edge-Modus 35
Legacy-Modus 36
Audio über Lautsprecher wiedergeben 37
Audiowiedergabe über Lautsprecher in der Kameraansicht 38
Bei Alarmen Audiowiedergabe über Lautsprecher 38
Darstellung für Interaktion mit Lautsprechern konfigurieren 38
Lesezeichen für Audioclips in der Kameraansicht oder in Alarmen 39
Besucher verwalten 39
IP-Türsprechanlage-Plugin 39
Eine IP-Türsprechanlage einrichten 39
Berechtigungen für IP-Türsprechanlage festlegen 40
Einen Testanruf durchführen 41
Echo bei Anrufen verhindern 41
IP-Türsprechanlage über die Live-Ansicht steuern 42
Anruf aus der Live-Ansicht annehmen 44
Mehrere Kameras im Anruffenster anzeigen 45
Aufruffensteraktionen 46
Seitenanzeige im Anruffenster 46
Nach Anrufweiterleitung filtern 47
Anrufverlauf anzeigen 48
Mikrofon deaktivieren, wenn kein aktiver Anruf vorliegt 48
Alarm empfangen, wenn eine Tür aufgebrochen wird 49
Alarm empfangen, wenn eine Tür zu lange geöffnet bleibt 49
Verhindern, dass ein Client Anrufe empfängt 49
Audio visualisieren 49
Mikrofonansicht 49
Konfigurieren von VMS für die Mikrofonansicht 50
Mikrofonansicht zum Smart Client hinzufügen 50
Mikrofonansicht verwenden 50
Mehrere Mikrofone gleichzeitig hören 51
Vorfälle mit Audio erfassen 51
Untersuchung von Vorfällen nach deren Eintreten 51
Forensische Suche 52
Forensische Suche 52
Vorbereitungen 52
Forensische Suche konfigurieren 52
Suche durchführen 53
Suche verfeinern 54
Einschränkungen 54
Fahrzeugsuche 55
Fahrzeugsuche konfigurieren 57
Fahrzeug suchen 57
Suche verfeinern 57
Suchgeschwindigkeit optimieren 58
Suche nach Geschwindigkeit im Bereich 58

Konfigurieren von Zone Speed Search 58
Suche nach geschwindigkeitsbezogene Ereignisse in einer Zone 59
Suche verfeinern 59
Containersuche 60
Containersuche konfigurieren 60
Container suchen 60
Suche verfeinern 61
PDF-Bericht in hoher Qualität erstellen 61
Axis Fahrzeugkennzeichen 62
Vorbereitungen 62
Axis Fahrzeugkennzeichen konfigurieren 62
Fahrzeugkennzeichen suchen 62
Live-Suche nach Fahrzeugkennzeichen 63
Suche verfeinern 63
Suchgeschwindigkeit optimieren 63
Fahrzeugkennzeichensuche als PDF-Bericht exportieren 63
Fahrzeugkennzeichensuche als CSV-Bericht exportieren 64
Axis Insights 64
Auf Axis Insights zugreifen 64
Neues Dashboard erstellen 65
Konfiguration der Dropdown-Liste im Dashboard 65
Einblicke für eine bestimmte Kameraansicht anzeigen 65
Axis Insights konfigurieren 65
Fehler in Axis Insights beheben 66
Video-Entzerrung 67
Eine Entzerrungsansicht erstellen 67
Erstellen einer Entzerrungsansicht für Panorama-Kameras mit mehreren Sensoren 68
Weitwinkelansicht 69
Home-Position festlegen 69
Bedienern erlauben, Entzerrungsansichten zu steuern und zu bearbeiten 70
Leistung und Fehlerbehebung 70
Body Worn Integration 72
Mehr erfahren 72
Zutrittskontrolle 73
Konfiguration der Zutrittskontrolle 73
Ihrem System einen Axis Netzwerk-Tür-Controller hinzufügen 73
Zugangslizenzen aktivieren 74
Konfigurieren Sie die Zutrittskontrolle 74
Integration der Zutrittskontrolle 75
Türen und Bereiche 75
Beispiel für Zugänge und Zonen 76
Fügen Sie einen Zugang hinzu 77
Einstellungen der Tür 78
Sicherheitsstufe der Tür 79
Zeitoptionen 80
Zugangsmonitor hinzufügen 81
Überwachten Zugang hinzufügen 81
Leser hinzufügen 82
REX-Gerät hinzufügen 83
Zone hinzufügen 84
Sicherheitsstufe der Zone 85
Überwachte Eingänge 86
Manuelle Aktionen 87
Kartenformate und PIN 87
Einstellungen für das Kartenformat 89
Identifizierungsprofile 90

Verschlüsselte Kommunikation 92
OSDP mit Secure Channel 92
Multiserver BETA 92
Vorgehensweise 92
Die Konfigurationsdatei vom Subserver erstellen 93
Importieren der Konfigurationsdatei auf den Hauptserver 93
Subserver sperren 93
Subserver entfernen 93
Zugriffsverwaltung 93
Vorgehensweise bei der Zugriffsverwaltung 94
Karteninhaber hinzufügen 94
Zugangsdaten hinzufügen 95
Gruppe hinzufügen 97
Fugen Sie eine Zugangsregel hinzu 98
Zugänge und Zonen manuell entriegeln 98
Berichte zur Systemkonfiguration exportieren 98
Berichte über Karteninhaberaktivitäten erstellen 99
Zugriffsverwaltungseinstellungen 100
Import und Export 100
Sichern und Wiederherstellen 102
Zutrittsverwaltung in Smart Client 102
Einstellungen für die Rolle „AXIS Secure Entry" 102
Systemverwaltung und Sicherheitskontrollen 104
Anpassen des Funktionszugriffs für Bediener 104
Rolleneinstellungen 104
Rolleneinstellungen konfigurieren 104
Geräteverwaltung 105
AXIS Device Manager Extend 105
Edge-Host installieren 105
Den Edge-Host beanspruchen und Geräte synchronisieren 106
Konfiguration von Geräten mithilfe von AXIS Device Manager Extend 107
Fehlerbehebung beim Hinzufügen von Geräten zum Edge-Host 107
AXIS Site Designer Import 107
Designprojekt importieren 107
Importierte Einstellungen 108
Einschränkungen 108
Kontenverwaltung 109
Herstellung einer Verbindung zu Geräten mit dem XProtect-Dienstkonto 109
Axis Ereignisse 109
Ein Ereignis für mehrere Geräte einrichten 110
Informationen zu Ereignissen 110
Metadaten und Suche 110
Einstellungen für die Metadaten konfigurieren 110
Axis Suchkategorien konfigurieren 111
Cybersicherheit 112
Schwachstellen-Management 112
Sicherheitsbenachrichtigungen 112
Sicherer Produktlebenszyklus 112
Hardening Guide 112
Benötigen Sie Hilfe? 113
FAQ 113
Fehlerbehebung 113
Support 113
Tipps und Tricks 114
Webseite in eine Ansicht des Smart Client hinzufügen 114
Videoexport mit eingebetteten Suchfunktionen 114

Videos im XProtect-Format exportieren 114
Exportsperrung auf empfangenden Computern aufheben 114
Exportierte AXIS Dewarp-Ansicht wiedergeben 114

AXIS Optimizer

Mit dem AXIS Optimizer werden Axis Funktionen direkt in XProtect oder Siemens Siveillance Video freigeschaltet. Die Anwendung optimiert die Leistung von Axis Geräten in diesen Videoverwaltungssystemen, wodurch Sie beim Konfigurieren eines Systems oder beim täglichen Betrieb Zeit und Aufwand sparen können. Die Anwendung ist kostenlos.

Bestimmungsgemäßer Verwendungszweck des AXIS Optimizer

Dieses Produkt ist für den Einsatz durch Fachleute bestimmt, die über umfassende Kenntnisse im Betrieb eines Video Management Systems (VMS) verfügen.

Systemanforderungen

AXIS Optimizer wird auf folgenden Plattformen unterstützt:

- XProtect Essential+
- XProtect Express+
- XProtect Professional+
- XProtect Expert
- XProtect Corporate
- Siemens Siveillance Video Pro
- Siemens Siveillance Video Advanced
- Siemens Siveillance Video Core Plus
- Siemens Siveillance Video Core

Es wird empfohlen, die neuesten Versionen des Verwaltungsclients und des Smart Client zu verwenden. Die neueste Version von AXIS Optimizer ist immer mit der neuesten Version des VMS getestet und kompatibel. Mehr lesen Sie hierzu in *Versionshinweise, on page 7*.

Hinweis

Mindestens unterstützte Plattform

- VMS-Version 2019 R3.

Wenn wir in der Hilfe den Smart Client erwähnen, meinen wir sowohl den Milestone XProtect Smart Client als auch den Video Client eines Siemens-Systems.

Unterstützung für föderierte Systeme

AXIS Optimizer wird in föderierten Systemen voll unterstützt.

Unterstützung für vernetzte Systeme

AXIS Optimizer bietet volle Unterstützung für vernetzte Systeme.

Hinweis

Anforderungen

- VMS-Version 2022 R3 oder höher.

Versionshinweise

Die aktuellen Versionshinweise finden Sie auf *axis.com/ftp/pub_soft/cam_srv/optimizer_milestone/latest/relnote.txt*.

AXIS Optimizer installieren oder aktualisieren

AXIS Optimizer installieren



Hinweis

Um den AXIS Optimizer zu aktualisieren, müssen Sie über Administratorrechte verfügen.

1. Stellen Sie sicher, dass die richtige Clientversion vom VMS haben.
2. Melden Sie sich bei Ihrem MyAxis-Konto an.
3. Laden Sie den AXIS Optimizer von *axis.com/products/axis-optimizer-for-milestone-xprotect* auf jedes Gerät herunter, auf dem der Management Client oder der Smart Client ausgeführt wird.
4. Führen Sie die heruntergeladene Datei aus und befolgen Sie die Schritt-für-Schritt-Anleitung.

Welche Versionen sind in meinem System installiert?

In der **Systemübersicht** finden Sie, welche Versionen von AXIS Optimizer und AXIS Optimizer Body Worn Extension auf verschiedenen Servern und Clients in Ihrem System installiert sind.

Hinweis

Um die Clients oder Server Ihres Systems in der **Systemübersicht** zu sehen, muss darauf AXIS Optimizer Version 3.7.17.0, AXIS Optimizer Body Worn Extension version 1.1.11.0 oder neuere Versionen ausgeführt werden.

Aktive Server und Clients anzeigen:

1. Gehen Sie im Management Client zu **Site Navigation > AXIS Optimizer > System overview (Standortnavigation > AXIS Optimizer > Systemübersicht)**.

So aktualisieren Sie einen bestimmten Server oder Client:

1. Wechseln Sie zu diesem Server oder Client und aktualisieren Sie diesen lokal.

Erweiterte Installationsmöglichkeiten

AXIS Optimizer gleichzeitig auf mehreren Geräten ohne Benutzerinteraktion installieren:

1. Klicken Sie mit der rechten Maustaste auf das **Start menu (Startmenü)**.
2. Klicken Sie auf **Ausführen**.
3. Suchen Sie die heruntergeladene Installationsdatei und klicken Sie auf **Open (Öffnen)**.
4. Fügen Sie am Pfadende einen oder mehrere Parameter hinzu.

Parameter	Beschreibung
`/SILENT`	Bei einer automatischen Installation werden weder die Schritt-für-Schritt-Anleitung noch das Hintergrundfenster angezeigt. Das Fenster Installationsfortschritt wird jedoch angezeigt.
`/VERYSILENT`	Bei einer vollautomatischen Installation werden weder die Schritt-für-Schritt-Anleitung und das

	Hintergrundfenster noch das Statusfenster zur Anzeige des Installationsfortschritts angezeigt.
/FULL	Installieren Sie alle Komponenten, beispielsweise das optionale Ereignisserver-Plugin und das Secure-Entry-Plugin. Dies ist sinnvoll bei einer vollautomatischen Installation mit /VERYSILENT.
/SUPPRESSMSGBOXES	Alle Meldungsfelder unterdrücken. Wird üblicherweise bei einer vollautomatischen Installation mit /VERYSILENT verwendet.
/log=<filename>	Erstellung einer Protokolldatei.
/NORESTART	Verhindert einen Neustart des Rechners während des Installationsvorgangs.
/EVENTSERVERPLUGIN	Installieren Sie das Ereignisserver-Plugin, wenn der Zielcomputer der Ereignisserver ist.
/SECUREENTRY	Installieren Sie den Secure Entry-Zutrittskontrolldienst, wenn der Zielcomputer der Ereignisserver ist.

5. Drücken Sie **Enter (Eingabe)**.

Beispiel:
Vollautomatische Installation, Protokollierung in output.txt, ohne Neustart des Rechners

```
.\AxisOptimizerXProtectSetup.exe /VERYSILENT /log=output.txt /NORESTART
```

VMS-Migration

AXIS Optimizer speichert die meisten Daten in der VMS-Datenbank, weshalb die Informationen bei einer Migration des VMS auf einen anderen Server erhalten bleiben.

Informationen zur Migration Ihres VMS auf einen anderen Server finden Sie unter *How to move an XProtect VMS installation/version from old servers to new servers* (Migration einer XProtect VMS-Installation/Version von alten zu neuen Servern).

Integrität des Installationsprogramms prüfen

So überprüfen Sie die Integrität des AXIS Optimizer-Installationsprogramms:

1. Klicken Sie mit der rechten Maustaste auf die Installationsdatei und wählen Sie **Properties (Eigenschaften)**.
2. Rufen Sie **Digital Signatures (Digitale Signaturen)** auf und klicken Sie auf **Details**.
3. Überprüfen Sie Folgendes:
   - Unter **Digital Signature Information (Informationen zur digitalen Signatur)** wird This digital signature is OK (Diese digitale Signatur ist in Ordnung) angezeigt.
   - Unter **Signer information (Ausstelleinformationen)** > **Name** wird Axis Communications AB angezeigt.

AXIS Optimizer aktualisieren

Für AXIS Optimizer stehen regelmäßig neue Funktionen, Optimierungen und Sicherheitsverbesserungen zur Verfügung. AXIS Optimizer bietet nur einen einzigen Versionstrack (neueste und größte Version) und nur diese neueste Version steht auf axis.com zum Download bereit. Es wird empfohlen, stets die aktuelle Version von AXIS Optimizer zu nutzen.

AXIS Optimizer verfügt zusätzlich über eine Funktion, mit der Sie alle Clients in Ihrem VMS aktualisieren können. Weitere Informationen finden Sie unter *Automatisches Aktualisieren des Systems*.

Hinweis

Um den AXIS Optimizer zu aktualisieren, müssen Sie über Administratorrechte verfügen.

Benachrichtigungen über Aktualisierungen

AXIS Optimizer sucht regelmäßig nach neuen Versionen und benachrichtigt Sie, wenn neue Updates verfügbar sind. Wenn Sie über eine Netzwerk-Verbindung verfügen, erhalten Sie im Smart Client Benachrichtigungen zu Aktualisierungen.

Zur Änderung des Typs empfangener Benachrichtigungen:

1. Gehen Sie im Smart Client zu **Settings (Einstellungen)** > **Axis General Options (Allgemeine Axis Optionen)** > **Notification preference (Benachrichtigungseinstellung)**.
2. Wählen Sie **All (Alle)**, **Major (Wichtige)** oder **None (Keine)**.

Zur Einrichtung dieser Benachrichtigungen für alle Clients in Ihrem VMS:

1. Gehen Sie zu **Management Client** > **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **System overview (Systemübersicht)**.
2. Klicken Sie auf **System upgrade settings (Einstellungen für die Systemaktualisierung)**.
3. Aktivieren oder deaktivieren Sie **Auf allen Clients Aktualisierungsbenachrichtigungen anzeigen**.

Manuelle Aktualisierung

Sie können AXIS Optimizer sowohl über den Management Client als auch über den Smart Client manuell aktualisieren.

Hinweis

Um den AXIS Optimizer zu aktualisieren, müssen Sie über Administratorrechte verfügen.

In Management Client

1. Gehen Sie auf **Site Navigation > Basics > AXIS Optimizer (Standortnavigation > Grundlegendes > AXIS Optimizer)**.
2. Klicken Sie auf **Aktualisieren.**

In Smart Client

1. Wechseln Sie zu **Settings > Axis general options (Allgemeine Axis Optionen)**.
2. Klicken Sie auf **Aktualisieren.**

Automatisches Aktualisieren des Systems

Über den VMS-Verwaltungs-Server können Sie eine lokale Version von AXIS Optimizer in Ihrem System veröffentlichen. Wenn Sie das tun, wird AXIS Optimizer automatisch für alle Client-Geräte aktualisiert. Die automatische Aktualisierung unterbricht niemals die Arbeit des Bedieners. Stille Installationen werden während des Neustarts der Geräte oder des VMS-Clients durchgeführt. Die automatische Aktualisierung wird auch unterstützt, wenn der Client nicht mit dem Internet verbunden ist.

Hinweis

Die automatische Aktualisierung wird für Clients unterstützt, die AXIS Optimizer 4.4 oder höher ausführen.

Automatische Aktualisierung aktivieren



Hinweis

Anforderungen

- Ein System, in dem der Management Client auf demselben Computer wie der VMS-Management-Server ausgeführt wird.
- PC-Administratorrechte auf dem VMS Verwaltungs-Server.

Um ein automatisches Update abzuschalten, müssen Sie eine bestimmte Version von AXIS Optimizer Version in Ihrem System veröffentlichen:

1. Installieren Sie auf dem VMS-Verwaltungs-Server die Version von AXIS Optimizer, die im gesamten System veröffentlicht werden soll.
2. Öffnen Sie den Management Client auf dem Computer mit dem VMS-Verwaltungs-Server.
3. Gehen Sie zu **Standortnavigation > AXIS Optimizer > Systemübersicht**.
4. Klicken Sie auf **System upgrade settings (Einstellungen für die Systemaktualisierung)**.
5. Stellen Sie sicher, dass die **Local Version (Lokale Version)** korrekt ist und klicken Sie auf **Publish (Veröffentlichen)**.
   Wenn bereits eine veröffentlichte AXIS Optimizer-Version existiert, wird sie durch die neue Version ersetzt.

Hinweis

Clientgeräte mit einer früheren Version von AXIS Optimizer als 4.4 müssen manuell aktualisiert werden.

Automatische Aktualisierung deaktivieren

Um die automatische Aktualisierung zu deaktivieren, müssen Sie die veröffentlichte Version zurücksetzen:

1. Öffnen Sie den Management Client auf dem Computer mit dem VMS-Verwaltungs-Server.
2. Gehen Sie zu **Standortnavigation > AXIS Optimizer > Systemübersicht**.
3. Klicken **Sie auf die Systemaktualisierungseinstellungen > Veröffentlichte Version zurücksetzen** .

Mehr erfahren

- Smart Clients ohne AXIS Optimizer können über die Webseite des Verwaltungs-Servers (*http://[serveradress]/installation/*) auf die veröffentlichte Installationsdatei zugreifen, auch wenn sie nicht mit dem Internet verbunden sind.
- Das Installationspaket für AXIS Optimizer ist im VMS Download Manager verfügbar und konfigurierbar.
- Bei Verbund- oder vernetzten Systemen müssen Sie AXIS Optimizer auf jedem Verwaltungs-Server veröffentlichen.
- Nachdem Sie eine neue Version von AXIS Optimizer veröffentlicht haben, können Sie nachverfolgen, welche Clients auf die veröffentlichte Version aktualisiert wurden. Geräte, auf denen die veröffentlichte Version läuft, werden auf der Seite **Systemübersicht** mit einem grünen Häkchen dargestellt.
- Die automatische Aktualisierung ist bei Computern mit einem VMS Management-Server ausgeschaltet.

AXIS Optimizer deinstallieren

Werkseinstellung

Um AXIS Optimizer auf die werkseitige Standardeinstellung zurückzusetzen, deinstallieren Sie das Programm im VMS und installieren Sie anschließend erneut.

Sichere Außerbetriebnahme

Um AXIS Optimizer und die gespeicherten Daten vollständig aus dem VMS zu entfernen, müssen Sie bei Bedarf zunächst die folgenden Schritte ausführen, bevor Sie das Programm auf Ihrem lokalen Computer deinstallieren.

1. Zum Entfernen der Fahrzeugkennzeichenlisten:
   - Öffnen Sie den Management Client und gehen Sie zu**AXIS Optimizer** > **License plate lists (Fahrzeugkennzeichenlisten)**.
   - Entfernen Sie alle Standorte aus der Liste.
2. Zur Trennung des AXIS Audio Manager Pro-Servers:
   - Öffnen Sie den Management Client und gehen Sie zu**AXIS Optimizer** > **Lautsprecherverwaltung (Speaker Manager)**.
   - Klicken Sie auf **Trennen**.

Zum Entfernen von AXIS Optimizer und lokal gespeicherten Daten vom lokalen Computer:

1. Öffnen Sie das **Startmenü** und gehen Sie zu **Settings (Einstellungen)** > **Apps** > **Installed Apps (Installierte Apps)**.
2. Wählen Sie **AXIS Optimizer** aus.
3. Klicken Sie auf p,255mm,sfx)=″graphics:graphic33F82CE7811D4EA41E6D94479F2055A5″ und wählen Sie **Uninstall (Deinstallieren)** aus.

Hinweis

Nach der Deinstallation von AXIS Optimizer müssen unter Umständen einige VMS-Dienste neu gestartet werden.

Benutzerrechte

AXIS Optimizer beinhaltet eine bestimmte Benutzerrolle für Axis Optimizer . Dies soll es Ihnen einfacher machen, den Benutzern die erforderlichen Smart-Client-Rechte zu geben, damit sie die Funktionen und Möglichkeiten von AXIS Optimizer nutzen können.

Wenn Sie XProtect 2018 R3 oder ältere Versionen ausführen, ist diese Rolle nur in XProtect Corporate verfügbar.

Wenn Sie XProtect 2019 R1 oder höher ausführen, ist diese Rolle für die folgenden XProtect-Versionen verfügbar:

- Corporate
- Expert
- Professional+
- Essential+
- Express+

Wenn Sie die Zugriffsrechte lieber manuell konfigurieren möchten, verwenden Sie diese Konfiguration, damit ein Smart-Client-Bediener alle in AXIS Optimizer enthaltenen Funktionen nutzen kann:

- Hardware: Treiberbefehle
- Kameras: AUX-Befehle

Hinweis

Weitere Informationen zur Handhabung von Benutzerrollen finden Sie unter *Anpassen des Funktionszugriffs für Bediener, on page 104*.

Geräteeinstellungen aufrufen

Geräteassistent

Mit dem Geräteassistenten können Sie direkt im VMS Management-Client auf alle Geräteeinstellungen von Axis zugreifen. Um verschiedene Geräteeinstellungen zu ändern, können Sie im VMS die Webseite Ihres Axis Geräts leicht finden und erreichen. Sie können auch Anwendungen konfigurieren, die auf Ihren Geräten installiert sind.

Wichtig

- Um den Geräte-Assistenten verwenden zu können, muss das Axis Gerät mit demselben Netzwerk wie der Management Client verbunden sein.
- Der Geräteassistent wird in IPv6-Netzwerken nicht unterstützt.

Axis Gerät konfigurieren

1. Im Management Client gehen Sie zu **Site Navigation > AXIS Optimizer > Device assistant (Standortnavigation > AXIS Optimizer > Geräteassistent)**.
2. Wählen Sie ein Gerät und gehen Sie zu **Device settings (Geräteeinstellungen)**. Die Webseite des Geräts öffnet sich.
3. Konfigurieren Sie die gewünschten Einstellungen.

Anwendungen auf einem Axis Gerät installieren

1. Im Management Client gehen Sie zu **Site Navigation > AXIS Optimizer > Device assistant (Standortnavigation > AXIS Optimizer > Geräteassistent)**.
2. Wählen Sie ein Gerät und gehen Sie zu **Device settings (Geräteeinstellungen)**. Die Webseite des Geräts öffnet sich.
3. Wechseln Sie zu **Apps**. Wo Sie die Funktionen der **Apps** finden, hängt von der Softwareversion des Geräts ab. Weitere Informationen finden Sie in der Hilfe Ihres Geräts.
4. Installieren Sie die gewünschten Anwendungen.

Anwendungen auf einem Axis Gerät konfigurieren

1. Im Management Client gehen Sie zu **Site Navigation > AXIS Optimizer > Device assistant (Standortnavigation > AXIS Optimizer > Geräteassistent)**.
2. Wählen Sie ein Gerät und gehen Sie zu **Applications (Anwendungen)**. Wenn Anwendungen auf dem Gerät installiert sind, werden sie hier angezeigt.
3. Rufen Sie die entsprechende Anwendung auf, z. B. AXIS Object Analytics.
4. Konfigurieren Sie die Anwendung nach Ihren Anforderungen.

Anwendungen auf einem Axis Gerät aktualisieren

1. Im Management Client gehen Sie zu **Site Navigation > AXIS Optimizer > Device assistant (Standortnavigation > AXIS Optimizer > Geräteassistent)**.
2. Klicken Sie mit der rechten Maustaste auf ein Gerät und wählen Sie **Show updates (Aktualisierungen anzeigen)**. Wenn Anwendungen aktualisiert werden können, wird eine Liste verfügbarer Aktualisierungen angezeigt.
3. Laden Sie die Aktualisierungsdatei herunter.
4. Klicken Sie auf **How to update (So funktioniert die Aktualisierung)** und befolgen Sie die Anweisungen.

Axis Gerät neu starten

1. Im Management Client gehen Sie zu **Site Navigation > AXIS Optimizer > Device assistant (Standortnavigation > AXIS Optimizer > Geräteassistent)**.
2. Klicken Sie mit der rechten Maustaste auf ein Geräte und wählen Sie **Restart device (Gerät neu starten)**.

IP-Adresse eines Axis Geräts kopieren

1. Im Management Client gehen Sie zu **Site Navigation > AXIS Optimizer > Device assistant (Standortnavigation > AXIS Optimizer > Geräteassistent)**.
2. Klicken Sie mit der rechten Maustaste auf ein Gerät und wählen Sie **Copy device address (Geräteadresse kopieren)**.

Automatisierung durchführen

Aktionen für Axis Geräte erstellen

Plugin für Ereignisserver

Mit dem Ereignis-Server-Plugin von AXIS Optimizer können Sie benutzerdefinierte Aktionen für Axis Geräte erstellen. Wenn Sie die XProtect Rule Engine und das Ereignis-Server-Plugin verwenden, können Sie zum Beispiel:

- Benutzerdefinierte Aktionen durch Anklicken einer Schaltfläche im Smart Client ausführen. Ein Setup-Beispiel finden Sie unter *Mehrere Kameras mit einem Klick trocknen, on page 16*.
- Aktionen ohne menschliche Interaktion ausführen (Automation). Ein Setup-Beispiel finden Sie unter *Privatzonenmasken mehrerer Kameras automatisch deaktivieren, on page 19*.

Das Ereignis-Server-Plugin besteht aus zwei Teilen:

- Einem separaten Plugin, das auf dem Ereignis-Server ausgeführt wird. Dies füllt die Rule Engine mit neuen Aktionen.
- Einer Seite mit dem Namen **Axis action (Axis Aktionen)** auf dem Verwaltungs-Server, wo Sie neue Aktionsvoreinstellungen erstellen können.

Die benutzerdefinierten Aktionen für Axis Geräte lauten: Bedienersteuerung ausführen, Radar ein- und ausschalten, Anruf von IP-Türsprechanlage starten und Kamera trocknen (SpeedDry/Wischer).

Das Ereignisserver-Plugin ist in AXIS Optimizer enthalten. Auf einem Multi-PC-System muss AXIS Optimizer sowohl auf dem Computer des Verwaltungsclients als auch auf dem Ereignis-Server-Computer installiert werden.

Ereignis-Server-Plugin installieren

Das Ereignis-Server-Plugin ist eine optionale Komponente, die im AXIS Optimizer enthalten ist. Sie können sie nur auf einem VMS-Ereignis-Server (Video Management System) installieren. Wenn die Anforderungen erfüllt sind, werden Sie bei der Ausführung des Installationsprogramms von AXIS Optimizer aufgefordert, das Ereignis-Server-Plugin zu installieren.

Hinweis

Der VMS-Ereignis-Server erfordert während der Installation und gelegentlich auch während der Aktualisierung von AXIS Optimizer einen kurzen Neustart. Sie werden in diesem Fall benachrichtigt.

Mehrere Kameras mit einem Klick trocknen

Mit dem Ereignis-Server-Plugin können Sie benutzerdefinierte Regeln einrichten, um die Bediener zu entlasten. Dieses Beispiel zeigt Ihnen, wie Sie alle Kameras in einem bestimmten Bereich durch Anklicken einer Overlay-Schaltfläche trocknen.



Hinweis

Anforderungen

- AXIS Optimizer Version 4.0 oder höher auf Ereignis-Server und Management Client
- Eine oder mehrere Kameras, die SpeedDry oder Wiper unterstützen, z. B. der Serie AXIS Q86, Q87 oder Q61

1. Benutzerdefinierte Ereignisse hinzufügen:
   1.1. Rufen Sie **Site Navigation > Rules and Events (Standortnavigation > Regeln und Ereignisse)** auf, und klicken Sie mit der rechten Maustaste auf **User-defined Event (Benutzerdefiniertes Ereignis)**.
   1.2. Wählen Sie **Add User-defined Event (Benutzerdefiniertes Ereignis hinzufügen)** und geben Sie einen Namen ein, in diesem Beispiel „Alle Kameras trocknen".
2. Eine neue Regel erstellen:
   2.1. Wechseln Sie zu **Site Navigation > Rules and Events (Standortnavigation > Regeln und Ereignisse)** und klicken Sie mit der rechten Maustaste auf **Rules (Regeln)**.
   2.2. Wählen Sie **Add Rule (Regel hinzufügen)** und geben Sie einen Namen ein, in diesem Beispiel „Alle Kameras trocknen".
   2.3. Wählen Sie **Perform an action on <event> (Aktion ausführen bei <Ereignis>)**.
   2.4. Klicken Sie im Feld **Edit the rule description (Regelbeschreibung bearbeiten)** auf **event (Ereignis)**.
   2.5. Wechseln Sie zu **Events > External Events > User-defined Events (Ereignisse > Externe Ereignisse > Benutzerdefinierte Ereignisse)** und wählen Sie **Dry all cameras (Alle Kameras trocknen)**.
   2.6. Klicken Sie auf **Next (Weiter)**, bis Sie zu **Step 3: Actions (Schritt 3: Aktionen)** gelangen.
   2.7. Wählen Sie die Aktion: **Axis: Dry <camera> (Axis: Trocknen <Kamera>)**.
   2.8. Klicken Sie im Feld **Edit the rule description (Regelbeschreibung bearbeiten)** auf **Axis: Dry camera (Kamera trocknen)**.
   2.9. Wählen Sie im Fenster **Select Triggering Devices (Auslösende Geräte auswählen)** die Option **Select devices (Geräte auswählen)** und klicken Sie auf **OK**.
   2.10. Wählen Sie die Geräte aus, die die Aktion auslösen sollen, und klicken Sie auf **OK** und anschließen auf **Finish (Fertigstellen)**.
3. Fügen Sie im Smart Client das benutzerdefinierte Ereignis als Overlay-Schaltfläche in eine Karten- oder Videoansicht ein.
4. Klicken Sie auf die Overlay-Schaltfläche und vergewissern Sie sich, dass die Regel wie von Ihnen wünschen funktioniert.

Autofokus für mehrere Kameras mit einem Klick aktivieren

Mit dem Ereignis-Server-Plugin können Sie benutzerdefinierte Regeln einrichten, um die Bediener zu entlasten. Dieses Beispiel zeigt Ihnen, wie Sie mit nur einem Klick den Autofokus für alle Kameras aktivieren.

Hinweis

Anforderungen

- AXIS Optimizer Version 4.1 oder höher auf dem Ereignis-Server sowie Management Client
- Eine oder mehrere Kameras mit Autofokus-Unterstützung

1. Benutzerdefinierte Ereignisse hinzufügen:
   1.1. Rufen Sie **Site Navigation > Rules and Events (Standortnavigation > Regeln und Ereignisse)** auf, und klicken Sie mit der rechten Maustaste auf **User-defined Event (Benutzerdefiniertes Ereignis)**.
   1.2. Wählen Sie **Add User-defined Event (Benutzerdefiniertes Ereignis hinzufügen"** und geben Sie einen Namen ein, in diesem Beispiel „Autofokus".
2. Eine neue Regel erstellen:
   2.1. Wechseln Sie zu **Site Navigation > Rules and Events (Standortnavigation > Regeln und Ereignisse)** und klicken Sie mit der rechten Maustaste auf **Rules (Regeln)**.
   2.2. Wählen Sie **Add Rule (Regel hinzufügen)** und geben Sie einen Namen ein, in diesem Beispiel „Autofokus ausführen".

2.3. Wählen Sie **Perform an action on <event> (Aktion ausführen bei <Ereignis>)**.

2.4. Klicken Sie im Feld **Edit the rule description (Regelbeschreibung bearbeiten)** auf **event (Ereignis)**.

2.5. Wechseln Sie zu **Events > External Events > User-defined Events (Ereignisse > Externe Ereignisse > Benutzerdefinierte Ereignisse)** und wählen Sie **Autofocus (Autofokus)**. Klicken Sie auf **OK**.

2.6. Klicken Sie auf **Next (Weiter)**, bis Sie zu **Step 3: Actions (Schritt 3: Aktionen)** gelangen.

2.7. Wählen Sie die Aktion **Axis: Run autofocus on <camera> (Axis: Autofokus ausführen auf Kamera)**.

2.8. Klicken Sie im Feld **Edit the rule description (Regelbeschreibung bearbeiten)** auf **Axis: Run autofocus on camera (Axis: Autofokus ausführen auf Kamera)**.

2.9. Wählen Sie im Fenster **Select Triggering Devices (Auslösende Geräte auswählen)** die Option **Select devices (Geräte auswählen)** und klicken Sie auf **OK**.

2.10. Wählen Sie die Geräte aus, auf denen die Aktion auslöst werden soll, und klicken Sie auf **OK** und anschließend auf **Finish (Fertigstellen)**.

3. Fügen Sie im Smart Client das benutzerdefinierte Ereignis „Autofokus" als Overlay-Schaltfläche in eine Karten- oder Videoansicht ein.
4. Klicken Sie auf die Overlay-Schaltfläche und vergewissern Sie sich, dass die Regel wie von Ihnen wünschen funktioniert.

Auslösen mehrere Blitzsirenen mit einem Klick

Mit dem Ereignis-Server-Plugin können Sie benutzerdefinierte Regeln einrichten, um die Bediener zu entlasten. Dieses Beispiel zeigt Ihnen, wie Sie mehrere Blitzsirenen mit einem Klick im Smart Client aktivieren können.

Hinweis

Anforderungen

- AXIS Optimizer Version 4.4 oder höher auf Ereignis-Server und Management Client
- Eine oder mehrere Axis Blitzsirenen
- Ausgang 1 der Blitzlichtsirene von Axis aktiviert und zu den Geräten im Management Client hinzugefügt

1. Erstellen Sie ein benutzerdefiniertes Ereignis:
   1.1. Rufen Sie **Site Navigation > Rules and Events (Standortnavigation > Regeln und Ereignisse)** auf, und klicken Sie mit der rechten Maustaste auf **User-defined Event (Benutzerdefiniertes Ereignis)**.
   1.2. Wählen Sie **Add User-defined Event (Benutzerdefiniertes Ereignis hinzufügen)** aus und geben Sie einen Namen ein, z. B. „Trigger all strobe sirens (Alle Blitzsirenen auslösen)".
2. Blitzsirenen-Profile im Geräteassistenten erstellen:
   2.1. Rufen Sie **Site Navigation > AXIS Optimizer > Device Assistant (Standortnavigation > AXIS Optimizer > Geräteassistent)** auf.
   2.2. Wählen Sie eine Blitzsirene aus. Die Webseite der Blitzsirene wird geöffnet.
   2.3. Wechseln Sie zu **Profiles (Profile)**, und klicken Sie auf **Add profile (Profil hinzufügen)**.
   2.4. Konfigurieren Sie, was sich die Sirene verhalten soll, wenn der Bediener die Blitzsirenen im Smart Client auslöst.
   2.5. Erstellen Sie für die anderen Blitzsirenen dieselben Profile. Sie müssen auf allen Geräten denselben Profilnamen verwenden.
3. In den Axis Aktionen eine Aktionsvoreinstellung erstellen:
   3.1. Rufen Sie **Site Navigation > Rules and Events > Axis actions (Standortnavigation > Regeln und Ereignisse > Axis Aktionen)** auf.
   3.2. Klicken Sie auf **Add new preset (Neue Voreinstellung hinzufügen)**.

3.3. Wechseln Sie zu **Select strobe siren (Blitzsirene auswählen)**, und klicken Sie auf **Strobe siren (Blitzsirene)**.

3.4. Wählen Sie die Blitzsirenen aus, die Sie verwenden möchten, und klicken Sie auf **OK**.
Es wird eine Liste mit Profilen der Stroboskop-Sirenen angezeigt

3.5. Wählen Sie das im vorherigen Schritt erstellte Blitzsirenenprofil aus. Die Aktionsvoreinstellung wird automatisch gespeichert

3.6. Drücken Sie auf F5, um die Serverkonfiguration zu aktualisieren. Jetzt können Sie die von Ihnen erstellte neue Aktionsvoreinstellung verwenden.

4. Eine Regel erstellen:
   4.1. Wechseln Sie zu **Site Navigation > Rules and Events (Standortnavigation > Regeln und Ereignisse)** und klicken Sie mit der rechten Maustaste auf **Rules (Regeln)**.
   4.2. Wählen Sie **Add Rule (Regel hinzufügen)** aus und geben Sie einen Namen ein, z. B. „Trigger all strobe sirens rule (Regel zum Auslösen aller Blitzsirenen)".
   4.3. Wählen Sie **Perform an action on <event> (Aktion ausführen bei <Ereignis>)**.
   4.4. Klicken Sie im Feld **Edit the rule description (Regelbeschreibung bearbeiten)** auf **event (Ereignis)**.
   4.5. Wechseln Sie zu **Events > External Events > User-defined Events (Ereignisse > Externe Ereignisse > Benutzerdefinierte Ereignisse)** und wählen Sie **Trigger all strobe sirens (Alle Blitzsirenen auslösen)**.
   4.6. Klicken Sie auf **Next (Weiter)**, bis Sie zu **Step 3: Actions (Schritt 3: Aktionen)** gelangen.
   4.7. Wählen Sie die Aktion **Axis: Run a profile on a strobe siren: <preset> (Axis: Ausführen eines Profils für eine Blitzlichtsirene: <Voreinstellung>)** aus.
   4.8. Klicken Sie im Feld **Edit the rule description (Regelbeschreibung bearbeiten)** auf **preset (Voreinstellung)**.
   4.9. Wählen Sie die zu verwendende Voreinstellung aus.
   4.10. Klicken Sie auf **Weiter** und dann auf **Finish (Fertig stellen)**.
5. Fügen Sie im Smart Client das benutzerdefinierte Ereignis als Overlay-Schaltfläche in eine Karten- oder Videoansicht ein.
6. Klicken Sie auf die Overlay-Schaltfläche und vergewissern Sie sich, dass die Regel wie von Ihnen wünschen funktioniert.

Privatzonenmasken mehrerer Kameras automatisch deaktivieren

Mit dem Ereignis-Server-Plugin lassen sich bestimmte Aktionen automatisieren. In diesem Beispiel wird gezeigt, wie Privatzonenmasken auf mehreren Kameras automatisch deaktiviert werden, wenn ein Analyseereignis auftritt. Das Ereignis in diesem Beispiel besteht darin, dass Personen oder Fahrzeuge einen Bereich betreten, in dem sie sich normalerweise nicht aufhalten sollten. Daher sollen die Privatzonenmasken automatisch deaktiviert werden, um einen besseren Überblick über das Geschehen zu ermöglichen.



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

Der Ablauf sieht folgendermaßen aus:

1. *Analyseszenario konfigurieren, on page 20* in AXIS Object Analytics (oder anderen Analyse-Anwendungen Ihrer Wahl)

2. *Bedienelemente zu relevanten Kameras hinzufügen, on page 20*
3. *Aktionsvoreinstellungen erstellen, on page 20*
4. *Regel erstellen, um Datenschutzmasken zu deaktivieren, wenn das Analyseereignis eintritt, on page 20*
5. *Regel erstellen, um die Privatzonenmasken erneut zu aktivieren, on page 21*
6. *Regel testen, on page 21* und sicherstellen, dass alles wie gewünscht funktioniert.

Hinweis

Anforderungen

- AXIS Optimizer Version 4.0 oder höher auf Ereignis-Server und Management Client
- Kameras mit AXIS OS 7.40 oder höher
- Kameras, die Ereignisse generieren können, in diesem Beispiel eine Kamera mit AXIS Object Analytics

Analyseszenario konfigurieren

1. Gehen Sie auf **Sie Navigation > AXIS Optimizer > Device Assistant (Standortnavigation > AXIS Optimizer > Geräteassistent)** und suchen Sie das Gerät mit den Analysefunktionen, die Sie verwenden möchten.
2. Klicken Sie auf **Applications (Anwendungen)** und erstellen Sie ein Analyseszenario, das die Aktion auslöst.
3. Wechseln Sie zu **Devices > Cameras (Geräte > Kameras)** und suchen Sie die Kamera, auf der Sie das Analyseszenario erstellt haben.
4. Klicken Sie im Fenster **Properties (Eigenschaften)** auf **Events > Add (Ereignisse > Hinzufügen)**.
5. Wählen Sie ein Treiberereignis aus, in diesem Beispiel „Objektanalyse: Ereignistest steigend“ und klicken Sie auf **OK**.
6. Klicken Sie auf **Add (Hinzufügen)** und wählen Sie das Treiberereignis „Object Analytics (Objektanalyse): Event test Failing (Objektanalyse: Ereignistest fallend). Klicken Sie anschließend auf **OK**.
7. Klicken Sie auf **Save (Speichern)**.

Bedienelemente zu relevanten Kameras hinzufügen

1. Gehen Sie auf **AXIS Optimizer > Operator controls (AXIS Optimizer > Bedienelemente)** öffnen Sie die Steuerungs-Bibliothek.
2. Wählen Sie im Fenster **Configuration (Konfiguration)** den entsprechenden Ordner aus und aktivieren sie **Turn off privacy mask (Privatzonenmaske deaktivieren)** sowie **Turn on privacy mask (Privatzonenmaske aktivieren)**.

Aktionsvoreinstellungen erstellen

1. Gehen Sie auf **Rules and Events > Axis actions (Regeln und Ereignisse > Axis Aktionen)** und klicken Sie auf **Add new preset (Neue Voreinstellung hinzufügen)**.
2. Klicken Sie auf **Cameras (Kameras)** und wählen Sie die entsprechenden Kameras aus. In diesem Beispiel: AXIS P1375 und AXIS Q6075-E. Wählen Sie dann das Bedienelement **Turn off privacy mask (Privatzonenmaske ausschalten)**.
3. Klicken Sie auf **Add new preset > Cameras (Neue Voreinstellung hinzufügen > Kameras)** wählen Sie die entsprechenden Kameras aus. In diesem Beispiel: AXIS P1375 und AXIS Q6075-E. Wählen Sie dann das Bedienelement **Turn off privacy mask (Privatzonenmaske ausschalten)**.

Regel erstellen, um Datenschutzmasken zu deaktivieren, wenn das Analyseereignis eintritt

1. Wechseln Sie zu **Site Navigation > Rules and Events (Standortnavigation > Regeln und Ereignisse)** und klicken Sie mit der rechten Maustaste auf **Rules (Regeln)**.
2. Wählen Sie **Add Rule (Regel hinzufügen)** und geben Sie einen Namen ein, in diesem Beispiel „Privatzonenmaske bei Analyse deaktivieren“.

3. Wählen Sie **Perform an action on <event> (Aktion ausführen bei <Ereignis>)**.
4. Klicken Sie im Feld **Edit the rule description (Regelbeschreibung bearbeiten)** auf **event (Ereignis)**. Rufen Sie **Devices > Configurable Events (Geräte > Konfigurierbare Ereignisse)** auf und wählen Sie Object Analytics: **Event test Rising (Objektanalyse: Ereignistest steigend)**.
5. Wählen Sie im Feld **Edit the rule description (Regelbeschreibung bearbeiten)** ein Gerät aus, in diesem Beispiel AXIS P1375.
6. Klicken Sie auf **Next (Weiter)**, bis Sie zu **Step 3: Actions (Schritt 3: Aktionen)** gelangen.
7. Wählen Sie die Aktion **Axis: Run operator control: <preset> (Axis: Bedienelement ausführen: <Voreinstellung>)**.
8. Klicken Sie im Feld **Edit the rule description (Regelbeschreibung bearbeiten)** auf **preset (Voreinstellung)**. Fügen Sie dann das Ziel **Turn on privacy mask on 2 cameras (Privatzonenmaske auf 2 Kameras aktivieren)** ein und klicken Sie auf **OK**.
9. Klicken Sie auf **Finish** (Fertig).

Regel erstellen, um die Privatzonenmasken erneut zu aktivieren

1. Wählen Sie **Add Rule (Regel hinzufügen)** und geben Sie einen Namen ein, in diesem Beispiel „Privatzonenmaske bei Analyse-Stopp aktivieren".
2. Wählen Sie **Perform an action on <event> (Aktion ausführen bei <Ereignis>)**.
3. Klicken Sie im Bereich **Edit the rule description (Regelbeschreibung bearbeiten)** auf **event (Ereignis)**. Rufen Sie **Devices (Geräte) > Configurable Events (Konfigurierbare Ereignisse)** und wählen Sie **Object Analytics: Event test Failing (Objektanalyse: Ereignistest fehlgeschlagen)**.
4. Wählen Sie im Bereich **Edit the rule description (Regelbeschreibung bearbeiten)** ein Gerät aus, in diesem Beispiel AXIS P1375.
5. Klicken Sie auf **Next (Weiter)**, bis Sie zu **Step 3: Actions (Schritt 3: Aktionen)** gelangen.
6. Wählen Sie die Aktion **Axis: Run operator control: <preset> (Axis: Bedienelement ausführen: <Voreinstellung>)**.
7. Klicken Sie im Bereich **Edit the rule description (Regelbeschreibung bearbeiten)** auf **preset (Voreinstellung)**. Fügen Sie dann das Ziel **Turn on privacy mask on 2 cameras (Privatzonenmaske auf 2 Kameras aktivieren)** hinzu und klicken Sie auf **OK**.
8. Klicken Sie auf **Finish** (Fertig).

Regel testen

1. Gehen Sie Sie zu **AXIS Optimizer > Device Assistant (AXIS Optimizer > Geräteassistent)** und suchen Sie das Gerät mit den Analysefunktionen, mit der Sie die Automation erstellt haben. In diesem Beispiel AXIS P1375.
2. Öffnen Sie das entsprechende Szenario und klicken Sie auf **Test alarm (Testalarm)**.

Aktivieren einer Blitzsirene bei Bewegungserkennung durch die Kamera

Mit dem Ereignisserver-Plugin können Sie benutzerdefinierte Regeln zur Automatisierung von Aktionen einrichten. Dieses Beispiel zeigt Ihnen, wie Sie bei einer Bewegungserkennung durch eine Kamera automatisch eine oder mehrere Blitzsirenen aktivieren.

Hinweis

Anforderungen

- AXIS Optimizer Version 4.4 oder höher auf Ereignis-Server und Management Client
- Eine oder mehrere Axis Blitzsirenen
- Ausgang 1 der Blitzlichtsirene von Axis aktiviert und zu den Geräten im Management Client hinzugefügt.
- Bei älteren Versionen vor VMS-Version 2022 R2 können Axis Aktionen nicht als Stoppaktionen ausgeführt werden. Bei älteren Versionen müssen zwei separate Regeln zum Ein- und Abschalten der Sirene erstellt werden.

1. Blitzsirenenprofile erstellen:
   1.1. Rufen Sie **Site Navigation > AXIS Optimizer > Device Assistant (Standortnavigation > AXIS Optimizer > Geräteassistent)** auf.
   1.2. Wechseln Sie zu **Axis output devices (Axis Ausgabegeräte)**, und wählen Sie eine Blitzsirene aus. Die Webseite der Blitzsirene wird geöffnet.
   1.3. Wechseln Sie zu **Profiles (Profile)**, und klicken Sie auf **Add profile (Profil hinzufügen)**.
   1.4. Stellen Sie sicher, dass für alle Sirenen derselbe Profilname verwendet wird.
   1.5. Konfigurieren Sie, wie sich die Blitzsirene bei Bewegungserkennung verhalten soll.
2. Start- und Stoppvorgaben für Aktionen erstellen:
   2.1. Rufen Sie **Site Navigation > Rules and Events > Axis actions (Standortnavigation > Regeln und Ereignisse > Axis Aktionen)** auf.
   2.2. Wechseln Sie zur Erstellung einer Startvorgabe zu **Strobe siren (Blitzsirene)**, und klicken Sie auf **Add new preset (Neue Voreinstellung hinzufügen)**.
   2.3. Wechseln Sie zu **Select strobe siren (Blitzsirene auswählen)**, und klicken Sie auf **Strobe siren (Blitzsirene)**.
   2.4. Wählen Sie eine oder mehrere Blitzsirenen aus der Liste aus.
   2.5. Wählen Sie das zuvor erstellte Sirenenprofil aus der Liste aus. Die Aktionsvoreinstellung wird automatisch gespeichert
   2.6. Klicken Sie zur Erstellung einer Stoppvorgabe auf **Add new preset (Neue Voreinstellung hinzufügen)**.
   2.7. Wechseln Sie zu **Select strobe siren (Blitzsirene auswählen)**, und klicken Sie auf **Strobe siren (Blitzsirene)**.
   2.8. Wählen Sie die gleichen Blitzsirenen wie bei der Voreinstellung der Startvorgabe aus der Liste aus.
   2.9. Wechseln Sie zu **Select action (Aktion auswählen)**, und wählen Sie **Stop (Stoppen)**.
   2.10. Wählen Sie dasselbe Sirenenprofil wie für die erstellte Startaktion aus. Die Aktionsvoreinstellung wird automatisch gespeichert
   2.11. Klicken Sie auf **Click to refresh (Zum Aktualisieren klicken)** oder drücken Sie auf F5, um die Serverkonfiguration zu aktualisieren.
3. Eine Regel erstellen:
   3.1. Rufen Sie **Site Navigation > Rules and Events > Axis actions (Seitennavigation > Regeln und Ereignisse > Regeln)** auf.
   3.2. Klicken Sie mit der rechten Maustaste auf **Rules (Regeln)**, wählen Sie **Add Rule (Regel hinzufügen)** und geben Sie einen Namen ein.
   3.3. Klicken Sie unter **Edit the rule description (Regelbeschreibung bearbeiten)** auf **event (Ereignis)**.
   3.4. Rufen Sie **Devices > Predefined Events (Geräte > Vordefinierte Ereignisse)** auf und wählen Sie **Motion Started (Bewegung gestartet)** aus.
   3.5. Klicken Sie unter **Edit the rule description (Regelbeschreibung bearbeiten)** auf **devices/recording_server/management_server (Geräte/Aufnahmeserver/Managementserver)**.
   3.6. Wählen Sie die Kamera aus, die die Blitzsirenen auslösen soll.

3.7. Klicken Sie auf **Next (Weiter)**, bis Sie zu **Step 3: Actions (Schritt 3: Aktionen)** gelangen.

3.8. Wählen Sie die Aktion **Axis: Start or stop a profile on a strobe siren: <preset> (Axis: Starten oder Stoppen eines Profils für eine Blitzlichtsirene: <Voreinstellung>)** aus.

3.9. Klicken Sie unter **Edit the rule description (Regelbeschreibung bearbeiten)** auf **preset (Voreinstellung)**.

3.10. Wählen Sie die zuvor voreingestellte Startvorgabe aus.

3.11. Klicken Sie auf **Next (Weiter)** und wählen Sie **Perform stop action on <event>(Stoppaktion für <Ereignis> ausführen)**.

3.12. Klicken Sie auf **Next (Weiter)** und wählen Sie **Axis: Start or stop a profile on strobe siren: <event> (Starten oder Stoppen eines Profils für eine Blitzlichtsirene: <Ereignis>)** aus.

3.13. Klicken Sie unter **Edit the rule description (Regelbeschreibung bearbeiten)** auf **preset (Voreinstellung)**.

3.14. Wählen Sie die zuvor voreingestellte Stoppvorgabe aus.

3.15. Wählen Sie **Finish (Fertigstellen)**.

4. Überprüfen Sie, ob die Blitzsirenen bei einer Bewegungserkennung durch die Kamera ordnungsgemäß funktionieren.

Audioclips bei Bewegungserkennung durch eine Kamera über einen Lautsprecher oder in einer Lautsprecherzone abspielen



Mit dem Ereignis-Server-Plugin können Sie benutzerdefinierte Regeln zur Automatisierung von Aktionen, d. h. sogenannte Aktionsvorgaben, erstellen. In diesem Beispiel zeigen wir Ihnen, wie Sie bei Bewegungserkennung durch eine Kamera einen automatischen Audioclip über einen Lautsprecher oder in einer Lautsprecherzone abspielen.

Hinweis

Anforderungen

- AXIS Optimizer Version 4.6 oder höher auf Ereignis-Server und Management Client.
- Ein oder mehrere dedizierte Axis Lautsprecher oder Axis Geräte mit integrierten Lautsprechern.
- Die Wiedergabe eines Audioclips in einer Lautsprecherzone erfordert ein korrekt konfiguriertes AXIS Audio Manager Edge- oder AXIS Audio Manager Pro-System. Weitere Informationen zur Konfiguration dieser Systeme finden Sie unter *Konfigurationsmodus, on page 33*.

1. Audioclip hochladen:

1.1. Legen Sie bei Verwendung des AXIS Audio Manager Edge- oder Legacy-Modus den Audioclip, den Sie in den Lautsprecher hochladen möchten, im Standardordner **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect – Audio Clips** ab.
Bei Nutzung des AXIS Audio Manager Pro-Modus laden Sie Audioclips über die Weboberfläche von AXIS Audio Manager Pro hoch.

1.2. Gehen Sie im Management Client zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Speaker manager (Lautsprecherverwaltung)** und wählen Sie einen Lautsprecher, eine Gerätegruppe oder eine Lautsprecherzone aus der Liste aus.

Hinweis

Weitere Informationen zur Auswahl eines Modus in der Lautsprecherverwaltung finden Sie unter *Konfigurationsmodus, on page 33*.

1.3. Rufen Sie **Audio clips (Audioclips)** auf und klicken Sie auf das **+**-Symbol vor dem Clip, den Sie in den Lautsprecher hochladen möchten.

1.4. Im Legacy-Modus wiederholen Sie die Schritte 1.2 bis 1.3 für jeden Lautsprecher, über den Sie den Audioclip wiedergeben möchten. Stellen Sie sicher, dass Sie in jeden Lautsprecher die gleiche Audiodatei hochladen.

2. Aktionsvorgaben für das Abspielen von Audioclips über einen Lautsprecher oder in einer Lautsprecherzone erstellen:

2.1. Gehen Sie zu **Site Navigation (Seitennavigation)** > **Rules and Events (Regeln und Ereignisse)** > **Axis actions (Axis Aktionen)**.

2.2. Rufen Sie zur Erstellung einer Voreinstellung **Audio clips (Audioclips)** auf und klicken Sie auf **Add new preset (Neue Voreinstellung hinzufügen)**.

2.3. Gehen Sie im AXIS Audio Manager Edge- oder AXIS Audio Manager Pro-Modus zu **Select playback destination (Wiedergabeziel auswählen)**.
Gehen Sie im Legacy-Modus zu **Select speaker (Lautsprecher auswählen)**.

2.4. Wählen Sie einen Lautsprecher oder eine Lautsprecherzone aus.

2.5. Wählen Sie aus der Liste den Audioclip aus, den Sie in Schritt 1 hochgeladen haben. Die Aktionsvoreinstellung wird automatisch gespeichert

2.6. Gehen Sie im AXIS Audio Manager Pro-Modus zu **Select visual profile (Visuelles Profil auswählen)** und konfigurieren Sie das gewünschte visuelle Profil und den Text.

Hinweis

Wählen Sie in der Liste der visuellen Profile die Option **Default (Standard)** aus, um beim Auslösen der Audioclip-Aktion das visuelle Standardprofil auf dem AXIS Audio Manager Pro-Server zu verwenden.

2.7. Klicken Sie auf **Refresh (Aktualisieren)** oder drücken Sie F5, um die Serverkonfiguration zu aktualisieren.

3. Regeln erstellen:

3.1. Gehen Sie zu **Site Navigation (Seitennavigation)** > **Rules and Events (Regeln und Ereignisse)** > **Rules (Regeln)**.

3.2. Klicken Sie mit der rechten Maustaste auf **Rules (Regeln)**, wählen Sie **Add Rule (Regel hinzufügen)** und geben Sie einen Namen ein.

3.3. Klicken Sie unter **Edit the rule description (Regelbeschreibung bearbeiten)** auf **event (Ereignis)**.

3.4. Gehen Sie zu **Devices (Geräte)** > **Predefined Events (Vordefinierte Ereignisse)** und wählen Sie **Motion Started (Bewegung gestartet)** aus.

3.5. Klicken Sie unter **Edit the rule description (Regelbeschreibung bearbeiten)** auf **devices/recording_server/management_server (Geräte/Aufnahmeserver/Managementserver)**.

3.6. Wählen Sie die Kamera aus, die die Aktionsvorgabe oder den Audioclip auslösen soll.

3.7. Klicken Sie auf **Next (Weiter)**, bis Sie zu **Step 3: Actions (Schritt 3: Aktionen)** gelangen.

3.8. Wählen Sie die Aktion **Axis: Play audio clip: <preset> (Axis: Audioclip abspielen: Voreinstellung)**.

3.9. Klicken Sie unter **Edit the rule description (Regelbeschreibung bearbeiten)** auf **preset (Voreinstellung)**.

3.10. Wählen Sie die im vorherigen Schritt erstellte Voreinstellung aus.

3.11. Wählen Sie **Finish (Fertigstellen)**.

4. Testen Sie, ob der Audioclip bei Bewegungserkennung durch die Kamera richtig abgespielt wird.

Fehlerbehebung bei Regeln

Wenn eine Regel nicht funktioniert, überprüfen Sie zunächst die Meldungen des Ereignis-Servers, um sicherzustellen, dass der Ereignisdienst ausgeführt wird.

Sie können auch die AXIS Optimizer-Protokolle auf dem Ereignis-Server überprüfen. Wenn Sie über einen Management Client oder Smart Client verfügen, verwenden Sie diese, um die entsprechenden Protokolle zu aktivieren und zu speichern.

Zentrale Verwaltung von Fahrzeugkennzeichenlisten

Mit dem AXIS Optimizer List Manager können Sie die Fahrzeugkennzeichenlisten für alle Kameras gleichzeitig zentral verwalten. Sie können Freigabe-, Sperr- und benutzerdefinierte Listen direkt aus dem VMS erstellen und verwalten. Das System unterstützt die Kombination von Listen. Dies bedeutet, dass Sie eine globale Liste erstellen können, die für alle Kameras im System gilt, sowie lokale Listen, die nur für bestimmte Kameras gelten.

Eine zentrale Listenverwaltung ist zum Beispiel dann sinnvoll, wenn Sie die Ein- und Ausfahrt von Parkplätzen automatisieren wollen oder einen Alarm erhalten möchten, wenn das System ein bestimmtes Kennzeichen registriert.

Sie müssen Administrator sein, um Listen zu erstellen und zu bearbeiten. Sie können Lese- und Bearbeitungsrechte anderen Rollen zuweisen (siehe Abschnitt *Berechtigungen für die Liste konfigurieren, on page 25*).

Eine Liste erstellen

Hinweis

Anforderungen

- AXIS License Plate Verifier 1.8 oder höher wird auf den Kameras ausgeführt.
- Um benutzerdefinierte Listen zu erstellen, benötigen Sie AXIS License Plate Verifier 2.0 oder höher

1. Rufen Sie im Management Client **Site Navigation > AXIS Optimizer > License plates (Standortnavigation > AXIS Optimizer > Fahrzeugkennzeichen)** auf.
2. Wählen Sie die Kameras aus, an die Sie die Freigabe-, Sperr- und benutzerdefinierte Liste übertragen möchten.
3. (Optional) Fügen Sie Benutzerrollen hinzu, die die Freigabe- und die Sperrliste einsehen und bearbeiten dürfen
4. Fügen Sie der Freigabe-, Sperr- und benutzerdefinierten Liste die entsprechenden Fahrzeugkennzeichen hinzu.
   Sie können auch bestehende Fahrzeugkennzeichenlisten importieren.
   Sobald die Liste den Status **Synchronized (Synchronisiert)**erhält, wurde sie an die ausgewählten Kameras übergeben.

Berechtigungen für die Liste konfigurieren

Sie können konfigurieren, welche Benutzerrollen die Freigabe- und Sperrliste bearbeiten dürfen. Dies ist z. B. nützlich, wenn Sie nach Einrichtung der Listen durch den Administrator die Möglichkeit haben wollen, je nach Bedarf Tagesbesucher hinzufügen zu können.

In Management Client

Alle Berechtigungen zum Anzeigen und Bearbeiten von Listen können für jede Liste einzeln ausgewählt werden.

1. Gehen Sie zu **Security > Roles (Sicherheit > Rollen)** und wählen Sie eine Rolle aus.
2. Rufen Sie die Registerkarte **AXIS Optimizer** auf.
3. Rufen Sie **Role settings (Rolleneinstellungen)** > **AXIS Optimizer** > **License plate lists (Fahrzeugkennzeichenlisten)** auf.
4. Wählen Sie **Read (Lesen)** im Feld **License plate lists (node) (Kennzeichenlisten (Knoten))**.

5. Wählen Sie eine Liste unter **License plate lists (Kennzeichenlisten)** und wählen Sie **Edit license plates (Kennzeichen bearbeiten)**.
   - Bei älteren Versionen als XProtect 2023 R2 rufen Sie **MIP > AXIS Optimizer > AXIS Optimizer Security > License plate lists (MIP > AXIS Optimizer > AXIS Optimizer Security > Fahrzeugkennzeichenlisten)** auf und wählen Sie **Edit license plate lists (Fahrzeugkennzeichenlisten bearbeiten)** aus.

Eine Liste bearbeiten

In Management Client

1. Rufen Sie **Site Navigation > AXIS Optimizer > License plates (Standortnavigation > AXIS Optimizer > Fahrzeugkennzeichen)** auf.
2. Wählen Sie den Standort aus, den Sie bearbeiten möchten.
3. Aktualisieren Sie je nach Bedarf die Einstellungen **Cameras (Kameras)** oder **License plates (Fahrzeugkennzeichen)**.
   Sobald die Liste den Status **Synchronized (Synchronisiert)** erhält, wurden Ihre Änderungen an die ausgewählten Kameras weitergegeben.

In Smart Client

1. Rufen Sie *Axis Fahrzeugkennzeichen, on page 62* auf und klicken Sie auf **License plate lists (Fahrzeugkennzeichenlisten)**.
   Falls die Registerkarte nicht angezeigt wird, gehen Sie zu **Settings > Axis search options (Einstellungen > Axis Suchoptionen)** und wählen die Registerkarte **Show license plate tab (Fahrzeugkennzeichen anzeigen)**.
2. Wählen Sie den Standort aus, den Sie bearbeiten möchten.
3. Fügen Sie der Freigabe-, Sperr- und benutzerdefinierten Liste die entsprechenden Fahrzeugkennzeichen hinzu.
   Sie können auch vorhandene Fahrzeugkennzeichenlisten importieren.
   Sobald die Liste den Status **Synchronized (Synchronisiert)**erhält, wurde sie an die ausgewählten Kameras übergeben.

Listen importieren

Sie können Listen in verschiedenen Text- oder CSV-Formaten importieren.

- Zulässiges Textformat: ein Fahrzeugkennzeichen pro Zeile
- Zulässige CSV-Formate:
  - ein Fahrzeugkennzeichen pro Zeile
  - Zwei Felder: Fahrzeugkennzeichen und Datum
  - Drei Felder: Fahrzeugkennzeichen, Fahrzeughalter und Kommentar
  - Vier Felder: Fahrzeugkennzeichen, Fahrzeughalter, Kommentar und die Zeichenfolge „Aktiv" oder „Inaktiv". (Gleiches Format wie beim Exportieren einer Liste.)

In Management Client

1. Rufen Sie **Site Navigation > AXIS Optimizer > License plates (Standortnavigation > AXIS Optimizer > Fahrzeugkennzeichen)** auf.
2. Wählen Sie den Standort aus, den Sie bearbeiten möchten.
3. Wechseln Sie zu **Allowed (Freigegeben)**, **Blocked (Gesperrt)** oder **Custom (Benutzerdefiniert)**.
4. Klicken Sie auf ⋮ und wählen Sie anschließend **Import to allow list (In Freigabeliste importieren)**, **Import to block list (In Sperrliste importieren)** oder **Import to custom list (In benutzerdefinierte Liste importieren)**.
5. Im Dialogfeld **Reset list (Liste zurücksetzen)**:

- Klicken Sie auf **Yes (Ja)**, um alle vorhandenen Fahrzeugkennzeichen zu entfernen und nur die neu importierten Fahrzeugkennzeichen zur Liste hinzuzufügen.
- Klicken Sie auf **No (Nein)**, um die neu importierten Fahrzeugkennzeichen mit den bereits vorhandenen Fahrzeugkennzeichen in der Liste zusammenzuführen.

In Smart Client

1. Rufen Sie *Axis Fahrzeugkennzeichen, on page 62* auf und klicken Sie auf **License plate lists (Fahrzeugkennzeichenlisten)**.
   Falls die Registerkarte nicht angezeigt wird, gehen Sie zu **Settings > Axis search options (Einstellungen > Axis Suchoptionen)** und wählen die Registerkarte **Show license plate tab (Fahrzeugkennzeichen anzeigen)**.
2. Wählen Sie den Standort aus, den Sie bearbeiten möchten.
3. Wechseln Sie zu **Allowed (Freigegeben)**, **Blocked (Gesperrt)** oder **Custom (Benutzerdefiniert)**.
4. Klicken Sie auf ⋮ und wählen Sie anschließend **Import to allow list (In Freigabeliste importieren)**, **Import to block list (In Sperrliste importieren)** oder **Import to custom list (In benutzerdefinierte Liste importieren)**.
5. Im Dialogfeld **Reset list (Liste zurücksetzen)**:
   - Klicken Sie auf **Yes (Ja)**, um alle vorhandenen Fahrzeugkennzeichen zu entfernen und nur die neu importierten Fahrzeugkennzeichen zur Liste hinzuzufügen.
   - Klicken Sie auf **No (Nein)**, um die neu importierten Fahrzeugkennzeichen mit den bereits vorhandenen Fahrzeugkennzeichen in der Liste zusammenzuführen.

Eine Liste exportieren

Hinweis

Um Fahrzeugkennzeichenlisten zu exportieren, müssen Sie über Administratorrechte verfügen.

In Management Client

1. Rufen Sie **Site Navigation > AXIS Optimizer > License plates (Standortnavigation > AXIS Optimizer > Fahrzeugkennzeichen)** auf.
2. Wählen Sie den Standort aus, den Sie bearbeiten möchten.
3. Wechseln Sie zu **Allowed (Freigegeben)**, **Blocked (Gesperrt)** oder **Custom (Benutzerdefiniert)**.
4. Klicken Sie auf ⋮ und wählen Sie anschließend **Export to allow list (In Freigabeliste exportieren)**, **Export to block list (In Sperrliste exportieren)** oder **Export to custom list (In benutzerdefinierte Liste exportieren)**.
   Die Liste wird mit vier Feldern im CSV-Format exportiert: Fahrzeugkennzeichen, Fahrzeughalter, Kommentar oder Status „Aktiv“ bzw. „Inaktiv“.

In Smart Client

1. Rufen Sie *Axis Fahrzeugkennzeichen, on page 62* auf und klicken Sie auf **License plate lists (Fahrzeugkennzeichenlisten)**.
   Falls die Registerkarte nicht angezeigt wird, gehen Sie zu **Settings > Axis search options (Einstellungen > Axis Suchoptionen)** und wählen die Registerkarte **Show license plate tab (Fahrzeugkennzeichen anzeigen)**.
2. Wählen Sie den Standort aus, den Sie bearbeiten möchten.
3. Wechseln Sie zu **Allowed (Freigegeben)**, **Blocked (Gesperrt)** oder **Custom (Benutzerdefiniert)**.
4. Klicken Sie auf ⋮ und wählen Sie anschließend **Export to allow list (In Freigabeliste exportieren)**, **Export to block list (In Sperrliste exportieren)** oder **Export to custom list (In benutzerdefinierte Liste exportieren)**.

Die Liste wird mit vier Feldern im CSV-Format exportiert: Fahrzeugkennzeichen, Fahrzeughalter, Kommentar oder Status „Aktiv“ bzw. „Inaktiv“.

Mehr erfahren über Listen

- Sie können mehrere Standorte erstellen.
- Jeder Standort ist mit einer oder mehreren Kameras verknüpft, auf denen AXIS License Plate Verifier installiert ist.
- Jeder Standort ist mit einer oder mehreren VMS-Benutzerrollen verknüpft. Die Benutzerrolle definiert, wer zum Lesen und Bearbeiten der Fahrzeugkennzeichenlisten berechtigt ist.
- Alle Listen werden in der VMS-Datenbank gespeichert.
- Wenn Sie die Kamera zu einem Standort hinzufügen, werden bereits vorhandene Fahrzeugkennzeichen in der Kamera überschrieben.
- Ist dieselbe Kamera für mehrere Standorte aufgeführt, erhält die Kamera die Summe aller Listen.
- Wenn dasselbe Nummernschild auf mehreren Listen aufgeführt ist, hat "Block" die höchste Priorität, "erlaubt" hat mittlere und "Benutzerdefiniert" die niedrigste Priorität.
- Für jedes Fahrzeugkennzeichen können Sie Informationen zum Fahrzeughalter hinzufügen. Diese Informationen werden jedoch nicht mit den Kameras synchronisiert.

Auf Live-Ereignisse reagieren

Gerätesteuerelemente verwenden

Bedienelemente

Über die Bedienelemente können Sie direkt vom Smart Client aus auf die spezifischen Funktionen einer Axis Kamera zugreifen. Welche Funktionen Sie nutzen können, hängt von den in Ihrem System installierten Kameras und deren Funktionen ab. Neben den vorinstallierten Bedienelementen können auch benutzerdefinierte Bedienelemente erstellt werden. Sie können auch konfigurieren, auf welche Steuerelemente ein Bediener Zugriff hat.

Einige Beispiele für Bedienelemente:

- Wischer ein- oder ausschalten
- Heizung ein- oder ausschalten
- Infrarot ein- oder ausschalten
- Fokusabruf
- WDR ein- oder ausschalten
- Elektronische Bildstabilisierung (Electronic Image Stabilization, kurz EIS) ein- oder ausschalten
- Privatzonenmasken ein- oder ausschalten

Informationen über die spezifischen Bedienelemente Ihrer Kamera finden Sie im Datenblatt.

Zugriff auf die Bedienelemente

Hinweis

Anforderungen

- Axis Geräte mit AXIS OS 7.10, 7.40 oder höher. (Die Versionen 7.20 und 7.30 unterstützen keine Bedienelemente.)

1. Klicken Sie im Smart Client auf **Live**, und wechseln Sie zur gewünschten Axis Kamera.
2. Klicken Sie auf und wählen Sie die zu verwendende Funktion aus.

Fokusbereich einer PTZ-Kamera speichern

Mit der Funktion Fokusabruf können Sie Fokusbereiche speichern, in die die PTZ-Kamera automatisch zurückkehrt, wenn sie sich in diesen Bereich der Szene bewegt. Dies ist vor allem bei schlechten Lichtverhältnissen nützlich, wo die Kamera sonst Schwierigkeiten bei der Scharfstellung hätte.



1. Bewegen Sie die Kamera im Smart Client in den Bereich, den Sie fokussieren möchten.

Hinweis

Beim Festlegen des Fokusbereichs müssen die Lichtbedingungen gut sein.

2. Fokussieren Sie die Kamera.
3. Wählen Sie **Add Focus Recall Zone (Fokusabrufzone hinzufügen)**.

Wenn Sie die Kamera später schwenken oder neigen und die Ansicht in einen Bereich bewegen, ruft die Kamera automatisch den für diese Ansicht voreingestellten Fokus ab. Selbst beim Heran- oder Herauszoomen bleibt die Fokusposition der Kamera erhalten.

Wenn die Zone nicht richtig konfiguriert ist, wählen Sie **Remove Focus Recall Zone (Fokusabrufzone entfernen)**.

Autofokus einer Kamera einstellen



Kameras mit Autofokus können das Objektiv mechanisch und automatisch so einstellen, dass das Bild auf den ausgewählten Bereich fokussiert bleibt, wenn sich der Blickwinkel ändert.

Autofokus einer PTZ-Kamera einstellen

1. Wählen Sie im Smart Client eine Kameraansicht aus.
2. Klicken Sie auf und rufen Sie **Set Focus > AF (Fokus einstellen > AF)** auf.
   Mit der **Focus Control (Scharfeinstellung)** kann der Fokuspunkt näher oder weiter entfernt liegen:
   - Klicken Sie für einen großen Schritt auf den großen Balken.
   - Klicken Sie für eine kurze Schrittweite auf den kleinen Balken.

Autofokus bei unbeweglichen Kameras und Fixed-Dome-Kameras

1. Wählen Sie im Smart Client eine Kameraansicht aus.
2. Klicken Sie auf und rufen Sie **Autofocus (Autofokus)** auf.

Schnelltrocknen oder Wischer aktivieren



Mit der Schnelltrocknungs-Funktion kann sich die Kuppel selbst abschütteln, wenn sie nass wird. Wenn die Kuppel mit hoher Geschwindigkeit vibriert, bricht die Oberflächenspannung des Wassers und entfernt die Tropfen. So kann die Kamera auch bei Regen scharfe Bilder erzeugen.

Schnelltrocknungsfunktion aktivieren

1. Wählen Sie im Smart Client eine Kameraansicht aus.
2. Klicken Sie auf und rufen Sie **PTZ > Speed Dry (PTZ > Schnelltrocknung)** auf.

Wichtig

Die Schnelltrocknungs-Funktion ist nur bei Kameras der Serie AXIS Q61 erhältlich.

So aktivieren Sie die Wischfunktion

Der Wischer befreit das Objektiv der Axis Positionierungskameras von überschüssigem Kondens- und Regenwasser.

1. Wählen Sie im Smart Client eine Kameraansicht aus.
2. anklicken.

Wichtig

Die Wischfunktion ist nur bei Kameras der Serie AXIS Q86 verfügbar.

Punktgenaue Temperatur messen



Wenn Sie in Ihrem System eine Kamera mit Spot-Temperaturmessung einsetzen, können Sie die diese direkt in der Kameraansicht messen. AXIS Kameras mit Spot-Temperaturmessung sind die AXIS Q1961-TE, AXIS Q2101-E und AXIS Q2901-E.

1. Öffnen Sie im Smart Client die Kameraansicht einer Kamera mit integrierter Spot-Temperaturmessung.
2. Zur Spot-Temperaturmessung klicken und wählen Sie auf und wählen Sie:
   - **Measure spot temperature(Spot-Temperatur messen)** für die AXIS Q2901-E.
   - **Enable temperature spot meter (Temperatur-Spotmeter aktivieren)** für AXIS Q1961-TE und AXIS Q2101-E.
3. Klicken Sie auf einen beliebigen Bereich in der Ansicht, um die aktuelle Spot-Temperatur anzuzeigen. Klicken Sie für Q1961-TE und AXIS Q2101-E auf **Done (Erledigt)**.
4. Bei der AXIS Q1961-TE und AXIS Q2101-E verbleibt die Spot-Temperaturanzeige bis zur erneuten Deaktivierung im Bild.
   - Wählen Sie hierzu > **Disable temperature spot meter (Spot-Temperaturmessung deaktivieren)**.

Hinweis

Wenn der digitale Zoom verwendet wird, können Temperaturmessungen zu falschen Ergebnis führen.

Automatisches Heranzoomen und Verfolgen eines sich bewegenden Objekts

Automatische Nachführung

Bei der automatischen Verfolgung zoomt die Kamera automatisch auf bewegte Objekte und verfolgt diese, wie z. B. ein Fahrzeug oder eine Person. Sie können ein Objekt manuell auswählen, um es zu verfolgen, oder Auslöserbereiche einrichten und die Kamera sich bewegende Objekte erkennen lassen. Wenn die Kamera kein Objekt verfolgt, kehrt sie nach 5 Sekunden in die Home-Position zurück.

- Konfigurieren Sie Auslöserzonen in der Weboberfläche der PTZ-Kamera.
- Im Smart Client sehen Sie folgende Markierungen:
  - Rotes Quadrat: verfolgtes Objekt.
  - Blaue Zonen: Objekte, die nicht verfolgt werden, aber verfolgt werden können, wenn sie eine Auslöserzone betreten oder wenn sie mit der rechten Maustaste angeklickt werden.

Objektverfolgung konfigurieren

Hinweis

Anforderungen

- AXIS OS 12.0
- Eine oder mehrere Axis Kameras, die Autotracking 2 unterstützen, z. B. AXIS Q6075 PTZ Dome Network Camera

1. Stellen Sie sicher, dass die Kamera und die entsprechenden Metadatengeräte aktiviert sind.
2. Wählen Sie „Metadata 1" (Metadaten 1) für Ihre Kamera aus, und klicken Sie auf **Settings (Einstellungen)**.
3. Rufen Sie **Metadata Stream > Event data (Metadatenstream > Ereignisdaten)** auf, und wählen Sie **Yes (Ja)**.
4. Klicken Sie auf **Save (Speichern)**.
5. Konfigurieren Sie Auto-Tracking in der Weboberfläche der PTZ-Kamera.

Objektverfolgung ein- oder ausschalten

1. Klicken Sie im Smart Client auf .
2. Wählen Sie **Turn on autotracking (Objektverfolgung aktivieren)** oder **Turn off autotracking (Objektverfolgung deaktivieren)**.

Hinweis

Wenn es mehrere Optionen zum Ein- und Ausschalten von Auto-Tracking gibt, verwenden Sie die letzte Option in der Liste.

Auto-Tracking manuell starten

Wenn Sie die Maus über einem Objekt bewegen, wird das Overlay gefüllt. Wenn Sie mit der rechten Maustaste auf ein Objekt klicken, wird dieses Objekt als Ziel festgelegt und die Kamera beginnt dann mit der Verfolgung des Zielobjekts. Die Kamera wird nach 5 s zurückgesetzt, wenn das Objekt nicht mehr verfolgt werden kann.

Ein Rechtsklick außerhalb der blauen Felder beendet Auto-Tracking.

Benutzerdefinierte Bedienelemente erstellen

1. Rufen Sie im Management Client **Site Navigation > AXIS Optimizer > Operator controls (Standortnavigation > AXIS Optimizer > Bedienelemente)** auf.
2. Ein Gerät oder eine Gruppe von Geräten wählen.
3. Klicken Sie auf **Add new control (Neues Bedienelement hinzufügen)**.
4. Geben Sie **Name** und **Beschreibung** ein.
5. Wählen Sie **Administrator**, wenn die Bedienersteuerung nur Benutzern mit Administratorrechten zur Verfügung stehen soll.
6. Fügen Sie die VAPIX-URL für ein bestimmte Steuerelement hinzu.
   Beispiel: Um das Bedienelement Entnebeln hinzuzufügen, geben Sie diese URL ein: `/axis-cgi/param.cgi?action=update&imageSource.IO.Sensor.Defog=on`.
   Weitere Informationen zu APIs für Axis Netzwerkgeräte finden Sie in der .
7. Wechseln Sie zum Smart Client, und überprüfen Sie, ob das Bedienelement ordnungsgemäß funktioniert.

Zugriff auf Bedienelemente konfigurieren

Sie können konfigurieren, auf welche Bedienelemente ein Bediener im Smart Client Zugriff hat.

1. Rufen Sie im Management Client **Site Navigation > AXIS Optimizer > Operator controls (Standortnavigation > AXIS Optimizer > Bedienelemente)** auf.
2. Ein Gerät oder eine Gruppe von Geräten wählen.
3. Wählen Sie aus, auf welche Bedienelemente im Smart Client Bediener zugreifen dürfen.

Über Lautsprecher interagieren

Lautsprecherverwaltung

Der Lautsprecher-Manager integriert Axis Audioprodukte in das VMS, damit Sie den vollen Funktionsumfang Ihrer Axis Geräte nutzen können.

- Greifen Sie auf Lautsprecher zu, die mit Ihrer Kamera verbunden sind
  Verbinden Sie Kameras mit einem Lautsprecher oder Lautsprechergruppen, und greifen Sie aus der Live-Ansicht auf die entsprechenden Lautsprecher zu. Sie müssen Ihre Lautsprecher nicht mehr manuell finden.
- Audio an eine Lautsprechergruppe senden
  Übertragen Sie den Ton mit nur einem Klick an viele Lautsprecher.
- Audioclips verwalten
  Sie können Ihre Audioclips ganz einfach verwalten.
- Sofort über Lautsprecher reagieren
  Reagieren Sie schnell auf einen Alarm, ohne den Alarm Manager zu verlassen.
- Audio zwischen Lautsprechern synchronisieren
  Wenn Sie Ihr Audiosystem für Hintergrundmusik verwenden möchten, können Sie mit dem Lautsprecher-Manager Zonen zur Audiosynchronisierung zwischen Ihren Lautsprechern einrichten (nur in den Modi „AXIS Audio Manager Pro“ und „Edge“).

Modi

Die Lautsprecherverwaltung unterstützt drei verschiedene Modi für unterschiedliche Lautsprecherkonfigurationen.

- **Pro** für AXIS Audio Manager Pro-Systeme
  Eine umfassende Software-Lösung für groß angelegte oder hochentwickelte Beschallungsanlagen. Sie unterstützt mehr als 5.000 Lautsprecher und mehr als 500 Zonen und bietet flexible Optionen für Lizenz und Installation. Sie wird für größere Systeme oder für Benutzer mit komplexeren Zeitplänen empfohlen.
- **Edge** für AXIS Audio Manager Edge-Systeme
  Eine optimierte Software-Lösung für die Verwaltung von bis zu 200 Lautsprechern in 20 Zonen. Die Funktion ist direkt in die Netzwerklautsprecher von Axis integriert und erfordert weder Server noch zusätzliche Lizenzen. Sie wird für kleinere Systeme ohne komplexe Zeitpläne empfohlen.
- **Aus dem Bestand**
  Der Legacy-Modus nutzt die Integration von Lautsprechern für die Audioübertragung an eine Lautsprechergruppe oder zum Auslösen von Audioclips. Sie unterstützt keine synchronisierte Übertragung. Sie wird für Systeme mit einzelnen Lautsprechern empfohlen, bei denen keine synchronisierte Übertragung erforderlich ist.

Konfigurationsmodus

Wenn Sie diese Seite zum ersten Mal öffnen, werden Sie aufgefordert, einen Modus auszuwählen, Sie können den Modus jedoch jederzeit ändern. Die Konfiguration, die Sie in den einzelnen Modi vornehmen, sind voneinander unabhängig, bleiben aber beim Wechsel zwischen den Modi erhalten.

1. Rufen Sie **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Speaker manager (Lautsprecherverwaltung)** auf.
2. Klicken Sie unter **Mode (Modus)** auf den Modus, in dem Sie sich gerade befinden, und wählen Sie im Popup-Fenster den gewünschten Modus aus.
3. Klicken Sie auf **Switch mode (Modus wechseln)**.

AXIS Audio Manager Pro-Modus

So verwenden Sie diesen Modus:

- Installieren Sie die Software „AXIS Audio Manager Pro“ auf einem Server, beispielsweise einem Server für Aufzeichnungen.
- Lizenzieren und konfigurieren Sie AXIS Audio Manager Pro mit API-Zugriff.
- Optional: Richten Sie ein Serverzertifikat für die Weboberfläche ein (siehe *Zertifikate*).
- Ändern Sie den Port des AXIS Audio Manager Pro-Servers von 443, falls dieser auf einem VMS-Server installiert ist.

In diesem Modus müssen im VMS keine Lautsprecher hinzugefügt oder lizenziert werden, es wird jedoch automatisch eine Hardware für die Verbindung zum AXIS Audio Manager Pro-Server erstellt (es ist eine VMS-Gerätelizenz erforderlich). Weitere Informationen zu AXIS Audio Manager Pro finden Sie im *Benutzerhandbuch zu AXIS Audio Manager Pro*.

Hinweis

Der AXIS Audio Manager Pro-Modus ist auf die Unterstützung eines einzelnen lokalen Standorts beschränkt. Architekturen mit mehreren Standorten, Verbundarchitekturen und miteinander vernetzte Standorte fallen nicht in den Anwendungsbereich dieser Integration.

Verbindung zu einem AXIS Audio Manager Pro-Server im Pro-Modus herstellen

1. Im Management Client gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Speaker manager (Lautsprecherverwaltung)**.
2. **Connect (Verbinden)** anklicken.
3. Im Dialogfeld:
   - Wählen Sie einen Aufzeichnungsserver aus, zu dem die Hardware des AXIS Audio Manager Pro-Servers hinzugefügt werden soll.
   - Geben Sie die Adresse und den HTTPS-Port des AXIS Audio Manager Pro-Servers ein.
   - Geben Sie den API-Benutzernamen und das API-Kennwort ein (der API-Zugriff muss auf dem AXIS Audio Manager Pro-Server aktiviert sein).
   - **Connect (Verbinden)** anklicken.

Auf der linken Seite sehen Sie alle in AXIS Audio Manager Pro verfügbaren Ziele und Zonen. Wenn Sie **AXIS Audio Manager Pro-Server** anklicken, wird auf der rechten Seite die Weboberfläche von AXIS Audio Manager Pro angezeigt.

Hinweis

Um auf die Weboberfläche zugreifen zu können, benötigen Sie eine direkte Verbindung zwischen dem Management-Client-Rechner und dem AXIS Audio Manager Pro-Server.

Bei Änderungen an Zonen, Zielen, Audioclips oder visuellen Profilen in der Weboberfläche von AXIS Audio Manager Pro:

- Rufen Sie **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Speaker manager (Lautsprecherverwaltung)** auf.
- Klicken Sie auf **Aktualisieren**

Kamera mit einem Ziel oder einer Zone verbinden

Sie können eine Kamera einem bestimmten Ziel oder einer bestimmten Zone zuordnen und diese direkt in der Kameraansicht des Smart Client nutzen.

1. Gehen Sie im Management Client zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Speaker manager (Lautsprecherverwaltung)** und wählen Sie ein Ziel oder eine Zone.
2. Klicken Sie unter **Associated camera(s) (Zugeordnete Kamera(s))** auf **Add cameras... (Kameras hinzufügen...)** und wählen Sie die Kameras aus, die Sie mit dem Ziel oder der Zone verknüpfen möchten.

Wenn eine Kamera mit einem Ziel oder einer Zone verknüpft ist, erscheint in der Symbolleiste in der Kameraansicht des Smart Client die Anzeige .

Visuelle Profile erstellen

- Gehen Sie im Management Client zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Speaker manager (Lautsprecherverwaltung)**.
- Klicken Sie auf**Audio Manager Pro server (Audio Manager Pro-Server)**, um die Weboberfläche anzuzeigen.
- Klicken Sie auf **Visual profiles (Visuelle Profile)**, um visuelle Profile zu erstellen oder zu bearbeiten.

Weitere Informationen zu visuellen Profilen finden Sie im*Benutzerhandbuch zu AXIS Audio Manager Pro*.

AXIS Audio Manager Edge-Modus

Der AXIS Audio Manager Edge ist auf den meisten Axis Lautsprechern vorinstalliert und wird automatisch detektiert, wenn Sie diesen Modus auswählen. Die Hauptgeräte des Standorts, Zwischengeräte für Durchsagenquellen und eigenständige Lautsprecher müssen im VMS hinzugefügt werden, damit der Modus AXIS Audio Manager Edge ordnungsgemäß funktioniert.

Hinweis

Im AXIS Audio Manager Edge-Modus können keine integrierten Kamera-Audioausgänge und andere inkompatible Audiogeräte verwendet werden.

Weitere Informationen zu AXIS Audio Manager Edge finden Sie im *Benutzerhandbuch zu AXIS Audio Manager Edge*.

Konfiguration von Lautsprechern und Zonen im Modus AXIS Audio Manager Edge

Für die Wiedergabe von Audioclips und Liveansagen müssen Sie zunächst die Durchsagensprache für Ihre Zonen aktivieren.

1. Rufen Sie im Management Client **Site Navigation (Standortnavigation)** > **Devices (Geräte)** > **Speakers (Lautsprecher)** auf und fügen Sie die gewünschten Gerätegruppen hinzu, oder fügen Sie den einzelnen Gerätegruppen Lautsprecher hinzu oder entfernen Sie diese.
2. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Speaker manager (Lautsprecherverwaltung)** und stellen Sie sicher, dass der **Edge**-Modus ausgewählt ist.
   Der Lautsprechermanager durchsucht das VMS-System anschließend nach allen Lautsprechern und zeigt alle Standorte und Zonen in AXIS Audio Manager Edge an, die in Smart Client verwendet werden können.
3. Wählen Sie in der Standortliste eine Zone mit ausgeschalteten Durchsagen.
4. Wählen Sie **Durchsagen für die Zone aktivieren**.

Wenn Sie Zonen oder Durchsagequellen ändern:

5. Rufen Sie **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Speaker manager (Lautsprecherverwaltung)** auf.
6. Klicken Sie auf **Aktualisieren**

Hinweis

Wenn die Einrichtung fehlschlägt, überprüfen Sie Konfiguration von AXIS Audio Manager Edge und versuchen Sie es erneut.



Kamera mit einem Lautsprecher oder einer Zone verbinden

Um einen bestimmten Lautsprecher oder eine Zone direkt in der Kameraansicht des Smart Client zu verwenden, können Sie diese mit einer Kamera verknüpfen.

1. Gehen Sie im Management Client zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Speaker manager (Lautsprecherverwaltung)** und wählen Sie einen Lautsprecher oder eine Zone.
2. Klicken Sie im Fenster **Associated cameras) (Verknüpfte Kameras)** auf **Add cameras (Kameras hinzufügen)**, und wählen Sie die Kameras aus, die Sie mit dem Lautsprecher oder der Zone verknüpfen möchten.

Wenn eine Kamera mit einem Lautsprecher, einer Gerätegruppe oder einer Zone verknüpft ist, erscheint in der Symbolleiste in der Kameraansicht des Smart Client die Anzeige .

Audioclips in einen Lautsprecher hochladen

Um Audioclips vom Smart Client aus auf einem Lautsprecher oder in einer bestimmten Zone abspielen zu können, müssen Sie die diese zunächst im Management Client in die Lautsprecher hochladen.

1. Legen Sie die Audioclips, die Sie in den Lautsprecher hochladen möchten, im Standardordner **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect – Audio Clips** ab.
2. Gehen Sie im Management Client zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Speaker manager (Lautsprecherverwaltung)** und wählen Sie einen Lautsprecher oder eine Zone.
3. Wechseln Sie zu **Audio clips (Audioclips)**, und klicken Sie vor den Clips, die Sie in den Lautsprecher hochladen möchten, auf das **+**-Symbol.

Legacy-Modus

Der Legacy-Modus erweitert die nativen Funktionen Ihrer Axis Lautsprecher und anderer audiofähiger Axis Geräte, die dem VMS hinzugefügt wurden. Im Gegensatz zu den anderen Modi unterstützt der Legacy-Modus keine synchronisierte Übertragung über mehrere Lautsprecher.

Lautsprecher im Legacy-Modus konfigurieren

1. Rufen Sie im Management Client **Site Navigation (Standortnavigation)** > **Devices (Geräte)** > **Speakers (Lautsprecher)** auf und fügen Sie die gewünschten Gerätegruppen hinzu, oder fügen Sie den einzelnen Gerätegruppen Lautsprecher hinzu oder entfernen Sie diese.
2. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Speaker manager (Lautsprecherverwaltung)** und stellen Sie sicher, dass der Legacy-Modus ausgewählt ist.
3. anklicken 
   3.1. Wählen Sie im Fenster **Manage Side Panel (Seitenwand verwalten)** die Lautsprecher aus, die im Smart Client angezeigt werden sollen.
   3.2. Klicken Sie auf **Add (Hinzufügen)** und anschließend auf **OK**.
   Die Lautsprecher im Bereich **Visible (Sichtbar)** werden jetzt im Smart Client für alle Benutzer angezeigt, die Zugriff auf den Lautsprecher haben.
4. Lautsprecher entfernen:
   4.1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Speaker manager (Lautsprecherverwaltung)** und klicken Sie auf .
   4.2. Wählen Sie im Fenster **Manage Side Panel (Seitenwand verwalten)** die Lautsprecher aus, die Sie entfernen möchten.
   4.3. Klicken Sie auf **Remove (Entfernen)** und anschließend auf **OK**.

Kamera mit einem Lautsprecher oder einer Lautsprechergruppe verbinden

Sie können eine Kamera einem bestimmten Ziel oder einer bestimmten Zone zuordnen und diese direkt in der Kameraansicht des Smart Client nutzen.

1. Gehen Sie im Management Client zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** >**Speaker manager (Lautsprecherverwaltung)** und wählen Sie einen Lautsprecher oder eine Lautsprechergruppe.
2. Klicken Sie unter **Associated camera(s) (Zugeordnete Kamera(s))** auf **Add cameras... (Kameras hinzufügen...)** und wählen Sie die Kameras aus, die Sie mit dem Lautsprecher oder der Lautsprechergruppe verknüpfen möchten.

Wenn eine Kamera mit einem Lautsprecher, einer Lautsprechergruppe verknüpft ist, erscheint in der Symbolleiste in der Kameraansicht des Smart Client die Anzeige .

Audioclips in einen Lautsprecher hochladen

Um Audioclips vom Smart Client aus auf einem Lautsprecher oder in einer bestimmten Zone abspielen zu können, müssen Sie die diese zunächst im Management Client in die Lautsprecher hochladen.

1. Legen Sie die Audioclips, die Sie in den Lautsprecher hochladen möchten, im Standardordner **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect - Audio Clips** ab.
2. Gehen Sie im Management Client zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** >**Speaker manager (Lautsprecherverwaltung)** und wählen Sie einen Lautsprecher oder eine Lautsprechergruppe.
3. Wechseln Sie zu **Audio clips (Audioclips)**, und klicken Sie vor den Clips, die Sie in den Lautsprecher hochladen möchten, auf das **+**-Symbol.

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

Lautstärke ändern

So ändern Sie die Lautstärke Ihrer Lautsprecher:

1. Gehen Sie im Management Client zu **Site Navigation (Standortnavigation) > Speaker manager (Lautsprecherverwaltung)** und wählen Sie einen Lautsprecher oder eine Lautsprechergruppe.
2. Wechseln Sie zu **Volume (Lautstärke)**, und stellen Sie die gewünschte Lautstärke ein.

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

Audio über Lautsprecher wiedergeben

1. Rufen Sie im Smart Client **Live** > **MIP plug-ins (MIP Plugins)** > **Axis speaker control (Axis Lautsprechersteuerung)** auf, und wählen Sie in der Dropdown-Liste einen Lautsprecher oder eine Zone aus.
2. Übertragen Sie das Audiosignal über Ihr Mikrofon an den Lautsprecher:

2.1. Halten Sie die Taste gedrückt, während Sie sprechen.
Stellen Sie sicher, dass die Pegelanzeige des Mikrofons die Sprachaktivität signalisiert.

3. Wiedergabe eines Audioclips über den Lautsprecher:
   3.1. Wechseln Sie zu **Media clip (Medien-Clip)**, und wählen Sie in der Dropdown-Liste einen Audioclip aus.
   3.2. Klicken Sie auf Wiedergabe, um die Wiedergabe des Audioclips über den ausgewählten Lautsprecher zu starten.

Audiowiedergabe über Lautsprecher in der Kameraansicht

1. Wechseln Sie im Smart Client zu einer Kameraansicht.
2. Falls eine Verknüpfung mit einem Lautsprecher, einer Gerätegruppe oder einer Zone besteht, erscheint in der Symbolleiste .
3. Klicken Sie auf , um das Fenster **Axis speaker control (Axis Lautsprechersteuerung)** aufzurufen.
4. Übertragen Sie das Audiosignal über Ihr Mikrofon an den Lautsprecher:
   4.1. Halten Sie die Taste gedrückt, während Sie sprechen.
   Stellen Sie sicher, dass die Pegelanzeige des Mikrofons die Sprachaktivität signalisiert.
5. Wiedergabe eines Audioclips über den Lautsprecher:
   5.1. Wechseln Sie zu **Media clip (Medien-Clip)**, und wählen Sie in der Dropdown-Liste einen Audioclip aus.
   5.2. Klicken Sie auf Wiedergabe, um die Wiedergabe des Audioclips über den ausgewählten Lautsprecher zu starten.

Bei Alarmen Audiowiedergabe über Lautsprecher

1. Wechseln Sie im Smart Client zu **Alarms (Alarme)**.
2. Wählen Sie einen Alarm aus, dessen Quelle eine Kamera ist.
   Wenn eine Zuordnung zu einem Lautsprecher oder einer Zone besteht, werden die Lautsprechersteuerelemente angezeigt.
3. Übertragen Sie das Audiosignal über Ihr Mikrofon an den Lautsprecher:
   – Halten Sie die Taste gedrückt, während Sie sprechen.
   Stellen Sie sicher, dass die Pegelanzeige des Mikrofons die Sprachaktivität signalisiert.
4. Wiedergabe eines Audioclips über den Lautsprecher:
   – Wechseln Sie zu **Media clip (Medien-Clip)**, und wählen Sie in der Dropdown-Liste einen Audioclip aus.
   – Klicken Sie auf Wiedergabe, um die Wiedergabe des Audioclips über den ausgewählten Lautsprecher zu starten.

Darstellung für Interaktion mit Lautsprechern konfigurieren

In Smart Client können Sie die Darstellung Ihres Geräts in der Axis Lautsprechersteuerung, direkt in der Kameraansicht oder in der Alarmverwaltung konfigurieren.

Hinweis

Visuelle Profile werden nur im AXIS Audio Manager Pro-Modus unterstützt.

- Im Seitenbereich **Axis speaker control (Axis Lautsprechersteuerung)**:
  – Klicken Sie auf .
  – Wählen Sie ein visuelles Profil aus der Auswahlliste aus.

  - Geben Sie im Textfeld einen Text ein, wenn Sie die aktuellen Texte des ausgewählten visuellen Profils überschreiben möchten.
- In der Kameraansicht:
  - Öffnen Sie eine bestimmte Kameraansicht.
  - Falls eine Verknüpfung mit einem Lautsprecher, einer Gerätegruppe oder einer Zone besteht, erscheint in der Symbolleiste .
  - Klicken Sie auf , um das Fenster **Axis speaker control (Axis Lautsprechersteuerung)** aufzurufen.
  - Klicken Sie auf .
- In **Alarm Manager (Alarmverwaltung)**:
  - Wählen Sie ein Ereignis aus, wechseln Sie zur Kameraansicht und klicken Sie auf .

Lesezeichen für Audioclips in der Kameraansicht oder in Alarmen

Wenn Sie einen Audioclip über die Lautsprechersteuerelemente in einer Kameraansicht oder unter Alarme abspielen, wird ein Lesezeichen mit Informationen darüber erstellt, wer und von welchem Gerät der Audioclip abgespielt wurde.

So suchen Sie nach Audio-Clip-Lesezeichen:

1. Wechseln Sie im Smart Client zu **Search (Suche)**.
2. Wählen Sie ein Zeitintervall sowie eine oder mehrere Kameras aus.
3. Klicken Sie auf **Search for (Suche nach)** > **Bookmarks (Lesezeichen)** > **New search (Neue Suche)**.

Besucher verwalten

IP-Türsprechanlage-Plugin

Die Netzwerk basierten IP-Türsprechanlagen von Axis vereinen Kommunikation, Videoüberwachung und ferngesteuerte Zugangskontrolle in einem Gerät. AXIS Optimizer ermöglicht eine einfache Konfiguration und Verwendung von Axis IP-Türsprechanlagen mit dem VMS. Sie können z. B. Anrufe empfangen und Türen öffnen.

Eine IP-Türsprechanlage einrichten



Das Türschloss sollte normalerweise an das erste Relais der IP-Türsprechanlage angeschlossen werden. AXIS Optimizer legt anhand der Informationen zur **Usage (Nutzung)** fest, welcher Ausgangsanschluss verwendet werden soll. Es wird der erste Port mit **Usage = Door (Nutzung = Tür)** (RELAY1 in der Standardeinstellung) verwendet.

Hinweis

Anforderungen

- Axis IP-Türsprechanlage
- Ein Mikrofon auf dem rufannehmenden PC installiertes Mikrofon.
- Laufender Smart Client

Hinweis

Ab Version 5.0.X.X konfiguriert AXIS Optimizer IP-Türsprechanlagen im VMS mit einer anderen Konfigurationsmethode als in früheren Versionen. Das Metadaten-Gerät kann anstelle von Eingang 1 zur Anruferkennung verwendet werden. Die alte Konfigurationsmethode wird zwar weiterhin unterstützt, für Neuinstallationen wird jedoch die neue Methode empfohlen.

1. Installieren Sie die neueste Version von AXIS Optimizer auf jedem Client, von dem aus Sie Anrufe empfangen und die Tür steuern möchten.
2. Melden Sie sich im Management Client an.
3. Fügen Sie dem Aufzeichnungsserver Ihre Axis IP-Türsprechanlage hinzu.
4. Aktivieren Sie im Management Client alle benötigten Geräte. Für den Empfang von Anrufen im Smart Client benötigen Sie:
   - Kamera 1
   - Mikrofon
   - Lautsprecher
   - Metadaten
   - Eingang 2 (optional, wenn an Port 2 der IP-Türsprechanlage ein Sicherheitsrelais angeschlossen ist)
   - An die Tür angeschlossener Ausgang Wenn Sie wissen, welcher Ausgang an die Tür angeschlossen ist, wählen Sie diesen aus. Wenn nicht, wählen Sie alle Ausgänge aus.
5. Gehen Sie zu **Standortnavigation > Geräte > Metadaten** und wählen Sie das Metadatengerät für die IP-Türsprechanlage, die Sie neu installieren.
6. Klicken Sie auf **Einstellungen**.
7. Setzen Sie die **Ereignisdaten** auf **Ja**.
8. Klicken Sie auf **Save (Speichern)**.
9. Wenn Sie Eingang 2 aktiviert haben, müssen Sie diesen auch einrichten.
   9.1. Gehen Sie zu **Standortnavigation > Geräte > Eingang** und wählen Sie Eingang 2 aus.
   9.2. Klicken Sie auf **Ereignisse** und dann auf **... hinzufügen**.
   9.3. Wählen Sie **Input Falling event (Fallendes Eingangsereignis)**, und fügen Sie dies den aktivierten Eingängen hinzu. Wiederholen Sie dies bei **Input Rising event (Steigendes Eingangsereignis)**.
   9.4. Klicken Sie auf **Save (Speichern)**.
10. Informationen zum Einrichten von Berechtigungen für bestimmte Rollen finden Sie unter *Berechtigungen für IP-Türsprechanlage festlegen, on page 40*.
11. *Einen Testanruf durchführen, on page 41*.

Berechtigungen für IP-Türsprechanlage festlegen

Für die richtige Abwicklung von Anrufen müssen Sie zunächst die erforderlichen Berechtigungen aktivieren.

1. Wechseln Sie zu **Site Navigation > Security > Roles (Standortnavigation > Sicherheit > Rollen)**.
2. Wählen Sie eine Rolle aus.
3. Wechseln Sie zu **Overall Security (Gesamtsicherheit)**.
4. Stellen Sie sicher, dass für jede Sicherheitsgruppe die erforderlichen Berechtigungen festgelegt sind. Wechseln Sie zu **Hardware**, und wählen Sie **Driver commands (Treiberbefehle)**.
5. Wechseln Sie zur Festlegung von Berechtigungen auf Systemebene zu **Overall Security (Gesamtsicherheit)**.
   Wechseln Sie zur Festlegung von Berechtigungen auf Geräteebene zu **Device (Gerät)**.
6. Legen Sie die erforderlichen Berechtigungen für die einzelnen Sicherheitsgruppen fest:
   6.1. Wechseln Sie zu **Cameras (Kameras)**. wählen Sie die Option **Lesen** und dann **Live ansehen**.

6.2. Gehen Sie zu **Mikrofone**. Wählen Sie die Option **Lesen** und dann **Mithören**.

6.3. Gehen Sie unter **Gesamtsicherheit** zu **Lautsprecher**. Wählen Sie die Option **Lesen** und dann **Sprechen**.
Gehen Sie unter **Gerät** zu **Lautsprecher** und wählen Sie **Lesen**. Gehen Sie dann auf der Registerkarte **Rede** und wählen Sie **Sprechen**.

6.4. Gehen Sie zu **Metadata (Metadaten)**. Wählen Sie die Option **Lesen** und dann **Live**.

6.5. Gehen Sie zu **Eingang**. Wählen Sie die Option **Read (Lesen)** aus.

6.6. Gehen Sie zu **Ausgang**. Wählen Sie die Option **Lesen** und dann **Aktivieren**.

Um zu steuern, welche Bediener Anrufe von einer bestimmten IP-Türsprechanlage bearbeiten dürfen, weisen Sie diesen wie folgt entsprechende Berechtigungen zu:

1. Wählen Sie für das Metadatengerät 1 der jeweiligen IP-Türsprechanlage die Berechtigungsart **Lesen**.
2. Löschen Sie diese Berechtigung für alle anderen Rollen. Benutzer ohne Berechtigung können keine Anrufe entgegennehmen.

Zur Anzeige der Anrufliste sind zusätzliche Berechtigungen erforderlich.

1. Wechseln Sie zur Festlegung von Berechtigungen auf Systemebene zu **Overall Security (Gesamtsicherheit)**.
Wechseln Sie zur Festlegung von Berechtigungen auf Geräteebene zu **Device (Gerät)**.
2. Wählen Sie die Berechtigungen für die einzelnen Sicherheitsgruppen wie folgt aus:
   2.1. Wechseln Sie zu **Cameras (Kameras)**. Wählen Sie die Option **Wiedergabe** und dann **Sequenzen lesen**.
   2.2. Gehen Sie zu **Mikrofone**. Wählen Sie die Option **Wiedergabe** und dann **Sequenzen lesen**.
   2.3. Gehen Sie zu **Lautsprecher**. Wählen Sie **Mithören**, **Wiedergabe** und **Sequenzen lesen**.

Einen Testanruf durchführen

1. Gehen Sie im Smart Client zu **Settings > Axis intercom options (Einstellungen > Optionen Axis IP-Türsprechanlage)**.
2. Klicken Sie auf **Test call (Testanruf)**.
3. Wählen Sie eine IP-Türsprechanlage und klicken Sie auf **Anrufen**.

Echo bei Anrufen verhindern

Mit Push-to-Talk senden Sie Audio über die IP-Türsprechanlage immer nur in eine Richtung. Sie können Push-to-Talk einschalten, wenn bei einem Anruf ein Echo zu hören ist.

So schalten Sie **Push-to-talk (Push-to-Talk)** ein:

- Gehen Sie in Smart Client zu **Settings (Einstellungen)** > **Axis intercom options (Optionen Axis IP-Türsprechanlage)**.
- Rufen Sie **Call (Anruf)** auf und wählen Sie **Push-to-talk (Push-to-Talk)** aus.

IP-Türsprechanlage über die Live-Ansicht steuern

Klicken Sie für jede IP-Türsprechanlage auf



, um das Gerät schnell zu steuern.

Wie funktioniert das?	Anweisungen	Kommentar
Schloss öffnen	Klicken Sie auf  > **Access (Zugang)** oder **Extended access (Erweiterter Zugang)**.	Wenn das Schloss entriegelt ist, können Sie nicht auf **Access (Zugriff)** oder **Extended Access (Erweiterter Zugriff)** klicken.
Wissen, ob eine Tür verriegelt oder entriegelt ist	Klicken Sie auf  und lesen Sie den Status unten im Menü.	-

Wie funktioniert das?	Anweisungen	Kommentar
Mit einer Person vor der IP-Türsprechanlage sprechen	Klicken Sie auf  > **Start call (Anruf starten)**.	Das Anruffenster wird geöffnet und startet die 2-Wege-Kommunikation mit der IP-Türsprechanlage.
Finden Sie heraus, wer gestern angerufen hat	Klicken Sie auf  > **Call history (Anrufverlauf)**.	Es wird eine Liste mit Anrufen angezeigt, die mit der aktuellen IP-Türsprechanlage getätigt wurden.

Anruf aus der Live-Ansicht annehmen

Wenn ein Besucher die Anruftaste an der IP-Türsprechanlage drückt, wird auf jedem ausgeführten Smart Client ein Anruffenster angezeigt. Das Anruffenster wählt automatisch die passende Kameraansicht, wenn Sie die Größe des Fensters ändern, z. B. Korridor- oder Landschaftsansicht.

Wie funktioniert das?	Anweisungen	Kommentar
Anruf annehmen	Klicken Sie auf **Accept (Akzeptieren)**	Ein Zwei-Wege-Audiokanal zwischen dem Bediener und der Person an der IP-Türsprechanlage wird geöffnet.
Anruf an einen anderen Bediener weiterleiten, weil ich ausgelastet bin	Schließen Sie das Fenster, indem Sie auf **X** klicken.	Wenn Sie einen Anruf ablehnen, kann ein anderer Bediener den Anruf auf einem anderen Client annehmen. Die IP-Türsprechanlage klingelt und blinkt weiter, bis der Anruf angenommen wird. Wenn niemand antwortet, erhält der Anruf den Status missed (verpasst) im Anrufverlauf.
Anruf ablehnen, da ich die Tür bereits anhand der visuellen Bestätigung geöffnet habe und	Klicken Sie auf **Decline (Ablehnen)**	Wenn Sie einem Anruf ablehnen, schließen die Anruffenster auf anderen Clients automatisch. Kein

Wie funktioniert das?	Anweisungen	Kommentar
nicht mit der Person sprechen muss Anruf ablehnen, da ich nicht mit einem ungewollten Besucher sprechen möchte		anderer Bediener kann den Anruf annehmen. Wenn die IP-Türsprechanlage nicht mehr klingelt und blinkt, schließt sich das Anruffenster. Der Anruf erhält den Status answered (beantwortet) im Anrufverlauf.
Tür öffnen	Klicken Sie auf **Access (Zugang)**.	Das Türschloss der IP-Türsprechanlage wird 7 s lang entriegelt. Um die Türöffnungszeit zu konfigurieren, gehen Sie wie folgendermaßen vor: 1. Gehen Sie im Smart Client zu **Einstellungen > Optionen Axis IP-Türsprechanlage > Zutritt**. 2. Ändern Sie die **Access time (Zutrittszeit)**.
Vorübergehende Unterbrechung der Tonübertragung zwischen dem Bediener und der IP-Türsprechanlage.	Klicken Sie auf **Mute (Stummschalten)**	-
Sprechen Sie mit dem Besucher, wenn Push-to-Talk aktiviert ist.	Klicken Sie auf **Talk (Sprechen)**.	Lassen Sie die Sprachtaste los, um den Besucher sprechen zu hören.
Anruf beenden	Klicken Sie auf **Hang up (Aufhängen)**	Bei der Standardeinstellung „automatisch Schließen" wird das Anruffenster geschlossen, wenn Sie einen Anruf ablehnen oder auflegen. Um das Standardverhalten des Anruffensters zu ändern, gehen Sie folgendermaßen vor: 1. Gehen Sie im Smart Client zu **Einstellungen > Optionen Axis IP-Türsprechanlage > Anruf)**. 2. Löschen Sie **Auto-close window (Fenster automatisch schließen)**.

Mehrere Kameras im Anruffenster anzeigen

Im Anruffenster können bis zu drei Kameras gleichzeitig angezeigt werden. Dies bedeutet, dass die Videostreams der IP-Türsprechanlage sowie die Videostreams von zwei anderen Kameras im selben Anruffenster angezeigt werden. Dies ist z.B. nützlich, wenn Sie z. B. gleichzeitig den Paketzusteller und den Bereich um die Anlieferungstür beobachten möchten.

Mehrere Kameras im Anruffenster konfigurieren:

1. Gehen Sie im Smart Client zu **Settings > Axis intercom options (Einstellungen > Optionen Axis IP-Türsprechanlage)**. Gehen Sie zu **Call > Intercom settings (Anruf > Einstellungen IP-Türsprechanlage)**.
2. Gehen Sie zu **Selected device (Ausgewähltes Gerät)** und wählen Sie aus, welches Gerät Sie konfigurieren möchten.
3. Gehen Sie zu **Multiple cameras (Mehrere Kameras)**. Wählen Sie aus, welche IP-Türsprechanlage Sie als **camera 1 (Kamera 1)** im Anruffenster sehen möchten.
4. Wählen Sie aus, welche zugeordneten Kameras im Anruffenster als **Kamera 2** und **Kamera 3** angezeigt werden sollen, wenn die IP-Türsprechanlage anruft.
5. Schließen Sie das Fenster **Intercom settings (Einstellungen für die IP-Türsprechanlage)**.

Aufruffensteraktionen

Mit Aufruffensteraktionen können Sie benutzerdefinierte Ereignisse einrichten, die an Regeln in der XProtect-Regel-Engine gebunden sind. Welche Ereignisse Sie einrichten und verwenden können, hängt von Ihrer Rolle ab.

So richten Sie Aufruffensteraktionen ein:

1. Gehen Sie im Smart Client zu **Settings > Axis intercom options (Einstellungen > Optionen Axis IP-Türsprechanlage)**.
2. Gehen Sie zu **Call > Intercom settings (Anruf > Einstellungen IP-Türsprechanlage)**.
3. Gehen Sie zu **Selected device (Ausgewähltes Gerät)** und wählen Sie aus, welches Gerät Sie konfigurieren möchten.
4. Gehen Sie zu **Call window actions (Aufruffensteraktionen)**, um die Aufruffensteraktionen auszuwählen, die Sie verwenden möchten.

Es gibt zwei Arten von Anruffensteraktionen:

- **Access button action (Zugriffsschaltflächenaktion)**: Wenn Sie eine Zugriffsschaltflächenaktion einrichten, überschreiben Sie die Standardaktion der Taste **Access (Zugriff)**. Sie können beispielsweise das Öffnen einer Reihe von Türen mit der Taste **Access (Zugriff)** festlegen.
- **Custom action (Benutzerdefinierte Aktion)**: Wenn Sie eine benutzerdefinierte Aktion einrichten, wird im Anruffenster eine Schaltfläche angezeigt. Sie können die benutzerdefinierte Aktion auslösen, indem Sie auf diese Schaltfläche klicken. Eine benutzerdefinierte Aktion ist eine Aktion, die nicht unbedingt mit dem Türzugang in Zusammenhang steht, beispielsweise das Versenden von E-Mails, das Auslösen von Alarmen oder das Starten kontinuierlicher Aufzeichnungen.

Seitenanzeige im Anruffenster

Bei Verwendung von AXIS I8307-VE Network Intercom können Sie Seiten im Anruffenster anzeigen. Das erlaubt die Anzeige nützlicher Informationen für Personen, die vor der IP-Türsprechanlage stehen, wie zum Beispiel Lagepläne oder Öffnungszeiten.

Dazu konfigurieren Sie zunächst die Seiten in der Weboberfläche Ihrer IP-Türsprechanlage (siehe *AXIS I8307-VE Network Intercom*).

Bei Eingang eines Anrufs über die IP-Türsprechanlage:

1. Klicken Sie auf **Show page (Seite anzeigen)**, um ein Dialogfeld mit allen konfigurierten Seiten auf Ihrem Gerät zu öffnen.
2. Klicken Sie auf **Load previews (Vorschau laden)**, um eine Vorschau aller Seiten anzuzeigen.
   Die Vorschau einer konfigurierten Seite können Sie anzeigen, indem Sie den Mauszeiger über die Seite bewegen und auf das Bildsymbol klicken.
3. Klicken Sie auf eine konfigurierte Seite, um sie in der IP-Türsprechanlage anzuzeigen.

Sie können das Anruffenster so konfigurieren, dass sowohl das Kamerabild der IP-Türsprechanlage als auch die angezeigte Seite über verschiedene verknüpfte Kameras angezeigt werden, d. h. Kamera 1 für das Kamerabild und Kamera 2 für die Seitenanzeige (siehe *Mehrere Kameras im Anruffenster anzeigen, on page 45*).

Hinweis: Die Seite wird bei Beenden des Anrufs geschlossen. Wiederholen Sie die Schritte oben, um eine Seite für einen neuen Anruf anzuzeigen.

Nach Anrufweiterleitung filtern

Standardmäßig empfangen alle an eine IP-Türsprechanlage angeschlossenen PCs die Anrufe. Durch das Hinzufügen von Anrufweiterleitungen und Filtern im VMS können Sie die IP-Türsprechanlage so konfigurieren, dass Anrufe an bestimmte Smart Clients in Ihrem VMS-System weitergeleitet werden. Sie können Zeitpläne für die Weiterleitung von Anrufen einrichten und Ausweichkontakten hinzufügen. Sie können Anrufe auch an SIP-basierte Kontakte senden und diese als Ausweichkontakten hinzufügen.

Auf der Weboberfläche der IP-Türsprechanlage

1. Gehen Sie zu **Communication (Kommunikation)** > **SIP**.
2. **Enable SIP (SIP aktivieren)** wählen.
3. Klicken Sie auf **Save (Speichern)**.
4. Gehen Sie zu **Communication (Kommunikation)** > **VMS Calls (VMS-Anrufe)**.
5. Stellen Sie sicher, dass **Allow calls in the video management system (VMS) (Anrufe im Video Management System (VMS) zulassen)** aktiviert ist.
6. Rufen Sie **Communication (Kommunikation)** > **Contact list (Kontaktliste)** auf.
7. Klicken Sie unter **Recipients (Empfänger)** auf +, um einen neuen Kontakt hinzuzufügen. Geben Sie die Informationen für den neuen Kontakt ein und klicken Sie auf **Speichern**. Sie können mehrere Kontakte hinzufügen.
   - Geben Sie unter **SIP address (SIP-Adresse)** `VMS_CALL:<extension>` ein. Ersetzen Sie `<extension>` durch den Namen der Anrufweiterleitung für Ihren Kontakt, z. B. `ReceptionA`.
   - Wenn Sie einen Zeitplan für den Kontakt einrichten möchten, wählen Sie die **Verfügbarkeit** des Kontakts.
   - Sie können einen Ausweichkontakt hinzufügen, der den Anruf erhält, wenn keiner der ursprünglichen Kontakte antwortet, z. B. `ReceptionB`.
8. Gehen Sie zu **Communication (Kommunikation)** > **Calls (Anrufe)**.
9. Bei Geräten mit AXIS OS vor Version 11.6 deaktivieren Sie **Make calls in the video management system (VMS) (Anrufe im Video Management System (VMS))**.
10. Entfernen Sie unter **Recipients (Empfänger)** den Kontakt **VMS** und fügen Sie den neuen Kontakt hinzu, den Sie erstellt haben.

In Management Client

Die IP-Türsprechanlage im VMS sollte so konfiguriert werden, dass ein Metadatengerät für die Anruferkennung verwendet werden kann. Siehe *Eine IP-Türsprechanlage einrichten, on page 39*.

In Smart Client

Richten Sie für jeden Benutzer, der die Anrufe empfangen soll, eine Anrufweiterleitung ein. Die Einstellung wird auf Benutzerebene gespeichert. Dies bedeutet, dass der Benutzer Anrufe unabhängig vom genutzten PC erhält.

1. Melden Sie sich beim Smart Client als der Benutzer an, der die Anrufe empfangen soll.
2. Gehen Sie zu **Einstellungen > Optionen Axis IP-Türsprechanlage**.
3. Geben Sie unter **Anrufe > Anrufweiterleitung** den Namen für die Anrufweiterleitung an den Kontakt ein, z. B. `ReceptionA`. Der Benutzer erhält nun nur Anrufe, wenn die Anrufweiterleitung mit dem Filterwert übereinstimmt.
   Wenn Sie mehrere Namen für Anrufweiterleitungen hinzufügen möchten, trennen Sie diese durch Semikolon, z. B. `ReceptionA;ReceptionC`

Anrufverlauf anzeigen

Im Anrufverlauf können Sie beantwortete und verpasste Anrufe einsehen und kontrollieren, ob dabei die Tür entriegelt wurde. Sie können einzelne Anrufe aus der Verlaufsliste auswählen und das entsprechende Wiedergabevideo ansehen, sofern verfügbar.

1. Gehen Sie im Smart Client zur Ansicht der IP-Türsprechanlage.
2. Klicken Sie auf 
   > **Call history (Anrufverlauf)**.

Hinweis

Der Anrufverlauf ist auf 39 Anrufe und 1000 Zugangsprotokolleinträge begrenzt. Die zulässige Anzahl von Anrufen kann geringer sein, wenn Sie diese häufig stummschalten.

Um zu registrieren, wann eine Tür entriegelt wurde, müssen Sie die Vorhaltezeit (Tage) für die Axis IP-Türsprechanlage festlegen:

1. Rufen Sie **Tools > Options > Alarm and Events > Event retention (Tools > Optionen > Alarm und Ereignisse > Ereignisaufbewahrung)** auf.
2. Legen Sie die Zeit für **Output Activated (Ausgang aktiviert)** und **Output Deactivated (Ausgang deaktiviert)** fest.

Mikrofon deaktivieren, wenn kein aktiver Anruf vorliegt

Es ist möglich, das Mikrofon auszuschalten, wenn keine Anrufe an der Axis IP-Türsprechanlage eingehen. Das Mikrofon wird bei aktivem Anruf eingeschaltet.

Hinweis

- Sie benötigen Administratorrechte, um das Mikrofon zu deaktivieren.
- Dies wird in einer Verbundarchitektur oder bei der Verwendung von Ersatzkontakten nicht unterstützt.

1. Gehen Sie in Smart Client zu **Settings (Einstellungen)** > **Axis intercom options (Optionen Axis IP-Türsprechanlage)**.
2. Wählen Sie **Mikrofon der IP-Türsprechanlage deaktivieren, wenn kein aktiver Anruf vorliegt**.

Alarm empfangen, wenn eine Tür aufgebrochen wird

Wenn eine Tür über ein Sicherheitsrelais (Eingang 2) verfügt, wird das Tür-Overlay im Anruffenster des Smart Client angezeigt, wenn die Tür geöffnet oder geschlossen ist. Dies bedeutet, dass ein Alarm angezeigt wird, wenn die Tür bei verriegelten Türen mit Gewalt geöffnet wird.

Hinweis

Um einen Alarm zu erhalten, muss mindestens ein Smart Client ausgeführt werden.

So konfigurieren Sie den Alarm:

1. Gehen Sie im Smart Client zu **Settings (Einstellungen) > Axis intercom options (Optionen Axis IP-Türsprechanlagen) > Administrator options (Administratoroptionen)**.
2. Wählen Sie **Trigger an alarm when a door has been forced open (Alarm auslösen, wenn eine Tür aufgebrochen wurde)**.

Alarm empfangen, wenn eine Tür zu lange geöffnet bleibt

Wenn eine Tür über ein Sicherheitsrelais (Eingang 2) verfügt, wird das Tür-Overlay im Anruffenster des Smart Client angezeigt, wenn die Tür geöffnet oder geschlossen ist. Das heißt, wenn die Tür geöffnet wird und zu lange geöffnet bleibt, kann ein Alarm ausgelöst werden.

Hinweis

Um einen Alarm zu erhalten, muss mindestens ein Smart Client ausgeführt werden.

So konfigurieren Sie den Alarm:

1. Gehen Sie im Smart Client zu **Settings (Einstellungen) > Axis intercom options (Optionen Axis IP-Türsprechanlagen) > Administrator options (Administratoroptionen)**.
2. Wählen Sie **Trigger an alarm when a door has been open longer than (s) (Alarm auslösen, wenn eine Tür länger geöffnet ist als (s))**.
3. Geben Sie ein, wie lange die Tür geöffnet bleiben kann, bevor der Alarm ausgelöst wird.

Verhindern, dass ein Client Anrufe empfängt

Sie können einen Client so konfigurieren, dass keine Anrufe empfangen werden. Das heißt, wenn jemand einen Anruf tätigt, öffnet sich auf dem jeweiligen Client kein Anruffenster.

1. Gehen Sie im Smart Client zu **Einstellungen > Optionen Axis IP-Türsprechanlage > Anruf)**.
2. Löschen Sie **Receive calls on this client (Anrufe auf diesem Client empfangen)**.

Audio visualisieren

Mikrofonansicht

Sie können Audiosignale in Ihrem System visualisieren, indem Sie dem Smart Client eine oder mehrere Mikrofonansichten hinzufügen. Damit können Sie Audiosignale sowohl in der Live-Ansicht als auch bei der Wiedergabe überwachen. Mit der integrierten Audioerfassung Ihres Axis Geräts sehen Sie sofort, wann der Audiopegel einen bestimmten Wert übersteigt. Typische Anwendungsfälle sind:

- *Mehrere Mikrofone gleichzeitig hören, on page 51*

- *Vorfälle mit Audio erfassen, on page 51*
- *Untersuchung von Vorfällen nach deren Eintreten, on page 51*

Hinweis

Anforderungen

- VMS Smart Client 2020 R2 oder höher.

Konfigurieren von VMS für die Mikrofonansicht

1. Erfassungsstufen festlegen:
   1.1. Im Management Client gehen Sie zu **Site Navigation > AXIS Optimizer > Device assistant (Standortnavigation > AXIS Optimizer > Geräteassistent)** und wählen Sie Ihr Gerät aus.
   1.2. Öffnen Sie die Einstellungen für **Detectors (Melder)**. Wie Sie diese Einstellungen öffnen, hängt von der Softwareversion Ihres Geräts ab.
   1.3. Gehen Sie auf **Audioerfassung** und ändern Sie **Eingang 1 Schallpegel** entsprechend Ihren Bedürfnissen.
2. Erhalten Sie Ereignisse von der Kamera im VMS:
   2.1. Gehen Sie im Management Client zu **Site Navigation > Devices > Microphones (Standortnavigation > Geräte > Mikrofone)**.
   2.2. Klicken Sie auf Ihr Mikrofon und dann auf **Ereignisse**.
   2.3. Ereignisse **Audio wird leiser** und **Audio wird lauter** hinzufügen.
3. Konfigurieren, wie lange das System Metadaten zu erfasstem Audio speichert:
   3.1. Gehen Sie auf **Tools > Options > Alarm and Events > Device events (Tools > Optionen > Alarm und Ereignisse > Geräteereignisse)**.
   3.2. Finden Sie **Audio wird leiser** und stellen Sie die Aufbewahrungszeit ein.
   3.3. Finden Sie **Audio wird lauter** und stellen Sie die Aufbewahrungszeit ein.
4. Stellen Sie sicher, dass Sie die Audioaufzeichnung eingerichtet haben. Sie können beispielsweise kontinuierlich Audio aufnehmen oder eine Aufzeichnungsregel, die auf der Veränderung der Audio-Lautstärke beruht, erstellen.
5. Wiederholen Sie die oben genannten Schritte für jedes Mikrofon, das Sie mit der Mikrofonansicht nutzen möchten.
6. Gehen Sie im Smart Client zu **Settings > Timeline > Additional data (Einstellungen > Zeitachse > Zusätzliche Daten)** und wählen Sie **Show (Anzeigen)**.

Mikrofonansicht zum Smart Client hinzufügen

1. Öffnen Sie den Smart Client, und klicken Sie auf **Setup (Einrichten)**.
2. Rufen Sie **Views (Ansichten)** auf.
3. Klicken Sie auf **Create new view (Neue Ansicht erstellen)**, und wählen Sie ein Format aus.
4. Gehen Sie zu **Systemübersicht > AXIS Optimizer**.
5. Klicken Sie auf **Microphone view (Mikrofonansicht)** und ziehen Sie sie in die Ansicht.
6. Ein Mikrofon wählen.
7. Klicken Sie auf **Setup**.

Mikrofonansicht verwenden

- Live-Ansicht
  - Lautstärken werden als Balkendiagramm dargestellt, mit dem augenblicklichen Wert auf der rechten Seite und bis zu 60 s Audioverlauf, der zur linken Seite wandert.
  - Klicken Sie in die Ansicht, um Audio vom Mikrofon anzuhören.

  - Bei jeder Mikrofonansicht gibt es ein Kopfhörersymbol. Klicken Sie auf das Symbol, um das Audio von jeder Ansicht ein- oder auszuschalten, ohne dass Sie die Ansicht selbst auswählen müssen. Dadurch können Sie mehrere Mikrofone gleichzeitig abhören.

- Wiedergabe
  - Wenn für das Mikrofon erkannte Audiosignale verfügbar sind, wird ein Symbol angezeigt.
  - Gelbe Balken zeigen an, dass Audio entsprechend der am Gerät eingestellten Erkennungsstufen erkannt wurde.
  - Klicken Sie in die Ansicht, um Audio vom Mikrofon anzuhören.
  - Bei jeder Mikrofonansicht gibt es ein Kopfhörersymbol. Klicken Sie auf das Symbol, um das Audio von jeder Ansicht ein- oder auszuschalten, ohne dass Sie die Ansicht selbst auswählen müssen. Dadurch können Sie mehrere Mikrofone gleichzeitig abhören.

Mehrere Mikrofone gleichzeitig hören

In der Mikrofonansicht können Sie mehrere Mikrofone gleichzeitig abhören, sowohl in der Live-Ansicht als auch bei der Wiedergabe.

1. *Konfigurieren von VMS für die Mikrofonansicht, on page 50*.
2. Öffnen Sie den Smart Client, und klicken Sie auf **Setup (Einrichten)**.
3. Rufen Sie **Views (Ansichten)** auf.
4. Klicken Sie auf **Create new view (Neue Ansicht erstellen)**, und wählen Sie eine geteilte Ansicht aus.
5. Gehen Sie zu **Systemübersicht > AXIS Optimizer**.
6. Für jedes Mikrofon, auf das Sie hören möchten:
   6.1. Klicken Sie auf **Microphone view (Mikrofonansicht)** und ziehen Sie sie in die Ansicht.
   6.2. Ein Mikrofon wählen.
7. Klicken Sie auf **Setup**.
8. Entscheiden Sie für jedes Mikrofon, ob Sie es stummschalten oder die Stummschaltung aufheben möchten, indem Sie auf das Kopfhörersymbol in jeder Mikrofonansicht klicken. Jetzt können Sie alle nicht stummgeschalteten Mikrofone gleichzeitig abhören.

Vorfälle mit Audio erfassen

Vielleicht möchten Sie die Geschehnisse in Bereichen, in denen Sie keine Kameras installieren dürfen, wie beispielsweise in Toiletten, überwachen. In der Mikrofonansicht können Sie schnell erkennen, wenn ein Ereignis stattfindet, d. h. wenn die Lautstärke die Erfassungswerte überschreitet.

1. *Konfigurieren von VMS für die Mikrofonansicht, on page 50*. Denken Sie daran, relevante Erfassungswerte für das Gerät und den zu überwachenden Bereich einzugeben.
2. Fügen Sie eine Mikrofonansicht dem Gerät hinzu, um eine Live-Ansicht in Smart Client zu erhalten (siehe *Mikrofonansicht zum Smart Client hinzufügen, on page 50*).

Untersuchung von Vorfällen nach deren Eintreten

Nachdem ein Vorfall aufgetreten ist, können Sie schnell die Zeiträume in der Wiedergabezeitachse identifizieren, in denen Audio von Ihren Mikrofonen erkannt wurde.

1. *Konfigurieren von VMS für die Mikrofonansicht, on page 50*.
2. Fügen Sie eine oder mehrere Mikrofonansichten mit relevanten Geräten zur Wiedergabe im Smart Client hinzu (siehe *Mikrofonansicht zum Smart Client hinzufügen, on page 50*).

Forensische Suche

AXIS Optimizer bietet in der zentralisierten Suche vier Suchkategorien für Axis Geräte an:

- *Forensische Suche, on page 52* (Objektsuche)
- *Fahrzeugsuche, on page 55*
- *Suche nach Geschwindigkeit im Bereich, on page 58*
- *Containersuche, on page 60*

Sie können dem Smart Client auch eine separate Registerkarte für die Nummernschildsuche hinzufügen (siehe *Axis Fahrzeugkennzeichen, on page 62*).

Sie können diese Suchkategorien in einem zentralen Bereich konfigurieren. Weitere Informationen dazu finden Sie unter *Axis Suchkategorien konfigurieren, on page 111*.

Forensische Suche

Axis Kameras mit AXIS OS 9.50 oder höher generieren Metadaten, die alle derzeit sich bewegenden Objekte im Sichtfeld einer Kamera beschreiben. Das VMS kann diese Daten zusammen mit den entsprechenden Video- und Audiodaten aufzeichnen. Mit der Forensischen Suche in AXIS Optimizer können Sie diese Daten analysieren und durchsuchen. Nutzen Sie die Forensischen Suche, um einen Überblick über alle Aktivitäten in der Szene zu erhalten oder schnell ein bestimmtes Objekt oder Ereignis von Interesse zu finden.

Vorbereitungen

1. Stellen Sie sicher, dass die aktuelle AXIS OS Version auf der Kamera installiert ist.
2. Stellen Sie sicher, dass Ihr VMS die richtige Version hat:
   - Corporate 2019 R3 oder höher bzw. Expert 2019 R3 oder höher
   - Professional+ 2022 R3 oder höher bzw. Express+ 2022 R3 oder höher
3. Die Uhrzeit der Kamera muss über NTP synchronisiert werden.
4. Objekttypen nach **Personen**, **Fahrzeugen**, **Fahrrädern**, **Bussen**, **Pkw** oder **Lkw** filtern:
   4.1. Verwenden Sie ein Axis Gerät, das AXIS Object Analytics unterstützt. Siehe Analysefilter im *Produktauswahl-Tool*.
   4.2. Wechseln Sie zu **System > Analytics metadata (System > Analytische Metadaten)**, und aktivieren Sie auf der Webseite der Kamera die Option **Analytics Scene Description (Analytische Szenenbeschreibung)**.
5. So filtern Sie nach **Fahrzeugfarbe**, **Farbe der Oberkörperbekleidung** oder **Farbe der Unterkörperbekleidung**:
   5.1. Verwenden Sie ein Axis Gerät, das AXIS Object Analytics unterstützt. Siehe Analysefilter im *Produktauswahl-Tool*.
   5.2. Verwenden Sie ein Axis Gerät mit ARTPEC-8 oder CV25. Siehe System-on-Chip-Filter im *Produktauswahl-Tool*.

Forensische Suche konfigurieren



1. Stellen Sie sicher, dass im Management Client das Metadatengerät für die Kameras aktiviert ist.

2. Vergewissern Sie sich, dass das Gerät für die Metadaten mit der Kamera verbunden ist:
   - Wechseln Sie zu **Devices (Geräte)** > **Camera (Kamera)** und wählen Sie Ihr Gerät aus.
   - Gehen Sie auf die Registerkarte **Client** und vergewissern Sie sich, dass das Gerät mit den Metadaten der Kamera unter **Related metadata (Verwandte Metadaten)** ausgewählt ist.
3. Rufen Sie **Site Navigation > Devices > Metadata (Standortnavigation > Geräte > Metadaten)** auf.
4. Wählen Sie Ihr Gerät aus, und klicken Sie auf **Record (Aufzeichnen)**. Stellen Sie sicher, dass **Recording (Aufzeichnung)** aktiviert ist.
   Metadaten werden standardmäßig nur aufgezeichnet, wenn das VMS Bewegungen in einer Szene erkennt. Daher sollte die Bewegungsschwelle so an die Umgebung angepasst werden, dass keine Objektbewegungen übersehen werden.
5. Klicken Sie auf **Settings (Einstellungen)** und stellen Sie sicher, dass **Analytics data (Analysedaten)** aktiviert ist.
6. Öffnen Sie die Live-Ansicht des Smart Client, und stellen Sie sicher, dass Sie Umgrenzungsfelder über Objekten sehen und diese richtig angezeigt werden.
   Es kann eine Weile dauern, bis sich die Uhr an die NTP-Zeit angepasst hat.
7. Warten Sie mindestens 15 Minuten, bis das System Videodateien und Metadaten aufzeichnen kann. Anschließend können Sie die Suche starten (siehe *Suche durchführen, on page 53*).
8. Schalten Sie **Consolidated metadata (Konsolidierte Metadaten)** ein, um die Suchgeschwindigkeit auf Geräten mit AXIS OS 11.10 oder höher zu verbessern. Siehe *Metadaten und Suche, on page 110*.

Suche durchführen



Hinweis

Vor Verwendung dieser Suchfunktion müssen Sie diese im Management Client konfigurieren. Weitere Informationen hierzu finden Sie unter *Forensische Suche konfigurieren, on page 52*.

1. Wechseln Sie im Smart Client zu **Search (Suche)**.
2. Wählen Sie ein Zeitintervall sowie eine oder mehrere Kameras aus.
3. Klicken Sie auf **Search for > Vehicle search > New search (Suche > Fahrzeugsuche > Neue Suche)**. Bei jedem Suchergebnis werden das Objekt und der Objektpfad in der Miniaturansicht angezeigt.
   - In der Miniaturansicht wird das Videobild angezeigt, als das Objekt am sichtbarsten war.
   - Der grüne Punkt markiert die Stelle, an der die Kamera das Objekt zuerst erkannt hat.
   - Der rote Punkt markiert die Stelle, an der die Kamera das Objekt zuletzt erkannt hat.
   - Um die vollständige Videosequenz für ein Suchergebnis anzuzeigen, wählen Sie diese aus und klicken Sie im Vorschaubereich auf **Play forward (Wiedergabe vorwärts)**.
   - Um die grafischen Overlays auszublenden, gehen Sie zu **Bounding boxes (Umgrenzungsfelder)** und wählen **Hide (Ausblenden)**.

   Hinweis

   Analyseanwendungen, die auf der Kamera ausgeführt werden, z. B. AXIS Object Analytics und AXIS Loitering Guard, können auch unwiderruflich in Overlays im Video integriert werden. Um diese Overlays zu entfernen, öffnen Sie die Webkonfigurationsseite der Anwendung.
4. Wählen Sie die Suchfilter aus, um die Anzahl der Suchergebnisse einzugrenzen.

Weitere Informationen zur Verwendung der verschiedenen Filter finden Sie unter *Suche verfeinern, on page 54*.

5. Wählen Sie die Suchergebnisse aus, die Sie näher prüfen möchten. Sie können diese zu den Lesezeichen hinzufügen oder *PDF-Bericht in hoher Qualität erstellen, on page 61*.

Suche verfeinern

Sie können einen oder mehrere Suchfilter verwenden, um die Suchergebnisse einzugrenzen.

- **Region of interest (Interessensbereich)**
  Zur Erfassung von Objekten, die sich in einem bestimmten Bereich bewegt haben.
- **Objektrichtung**
  Zur Erfassung von Objekten, die sich in einer Szene entlang einer bestimmten Strecke bewegt haben: Nach links, rechts, unten oder oben.
- **Objekttyp**
  Objekte eines bestimmten Typs erfassen: Personen, Fahrzeuge, Fahrräder, Busse, Pkw oder Lkw.

Hinweis

- Geschwindigkeit (km/h) und Fahrzeugkennzeichen werden nur für die AXIS Q1686-DLE Radar-Video Fusion Camera unterstützt.
- Sie müssen die Geschwindigkeit (km/h) und das Fahrzeugkennzeichen einschalten, damit Sie diese verwenden können. Weitere Informationen hierzu finden Sie unter *Axis Suchkategorien konfigurieren, on page 111*.
- **Geschwindigkeit (km/h)**
  Zur Erfassung von Fahrzeugen, die in einem bestimmten Geschwindigkeitsbereich fahren.
- **Nummernschild**
  Zur Erfassung von Fahrzeugen mit einem bestimmten Fahrzeugkennzeichen. Sie können damit auch nach Fahrzeugkennzeichen suchen, die bestimmte Namen oder Zahlen enthalten.
- **Fahrzeugfarbe**
  Zur Erfassung von Fahrzeugen in einer bestimmten Farbe.
- **Farbe der Oberkörperbekleidung**
  Zur Erfassung der Oberkörperkleidung in einer bestimmten Farbe.
- **Farbe der Unterkörperbekleidung**
  Zur Erfassung der Unterkörperkleidung in einer bestimmten Farbe.
- **Time-of-day (Tageszeit)**
  Zur Erfassung von Objekten, die zu einer bestimmten Tageszeit erfasst wurden. Dieser Filter ist nützlich, wenn Sie über mehrere Tage hinweg suchen, aber nur an Objekten zu einer bestimmten Tageszeit interessiert sind, zum Beispiel am Nachmittag.
- **Mindestzeit in Szene (Sekunde)**
  Zur Erfassung von Objekten, die für eine Mindestanzahl von Sekunden erfasst und verfolgt wurden. Dieser Filter filtert uninteressant Objekte heraus, z. B weit entfernte und falsche Objekte (Lichteffekte). Der Standardwert ist 1 s, d. h. ohne Filtereinstellung werden alle Objekte ausgeschlossen, die weniger als 1 s lang im Bild sind.
- **Schwankende Objekte (% des Bildes)**
  Schließen Sie Objekte aus, die sich nur in einem begrenzten Bereich bewegen, z. B. eine Fahne oder ein Baum, der sich im Wind bewegt. Der Standardwert beträgt 5–100 %. Wenn der Filter also nicht eingestellt ist, werden Objekte ausgeschlossen, die sich in weniger als 5 % des Bildbereichs bewegt haben.

Einschränkungen

- Um die richtige Videodatei für die Suchergebnisse zu erhalten, ist die korrekte Uhrensynchronisierung unerlässlich.

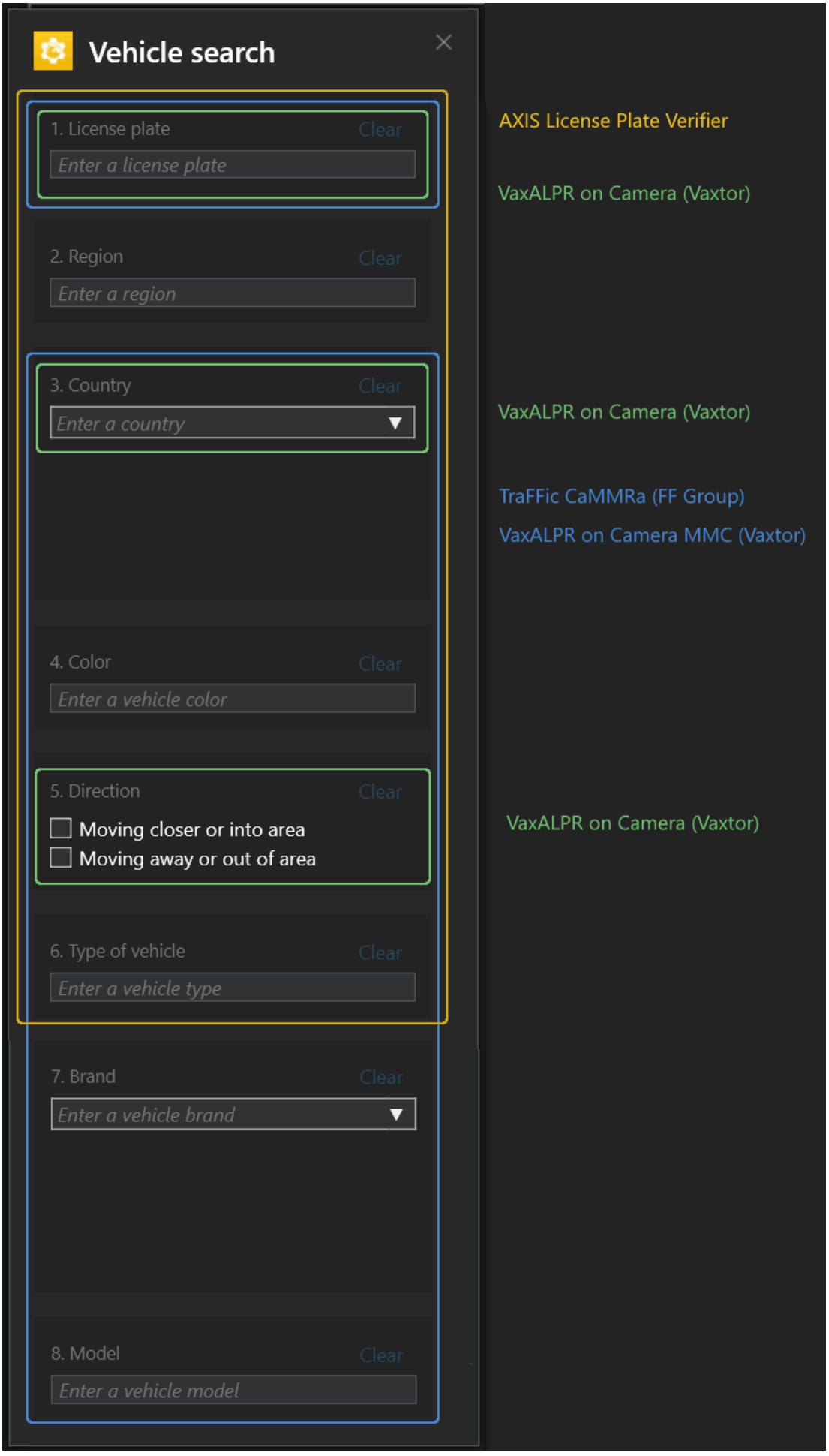
- Die in der forensischen Suche analysierten Daten berücksichtigen nicht die Perspektive der Szene. Dies bedeutet, dass die Größe und Geschwindigkeit eines Objekts je nach dessen Nähe zur Kamera unterschiedlich sein können.
- Bestimmte Witterungsbedingungen wie starker Regen oder Schneefall können die Erfassungsgenauigkeit beeinträchtigen.
- Wenn bei schwachen Lichtverhältnissen ein guter Kontrast des Objekts besteht, wird die Analyse genauer.
- Ein einzelnes Objekt kann unter bestimmten Bedingungen mehrere Ergebnisse generieren. Beispielsweise kann die Verfolgung unterbrochen werden, wenn ein Objekt vorübergehend durch ein anderes Objekt verdeckt wird.
- Overlays können sich je nach XProtect-Version unterscheiden. Zum Beispiel: Für Overlays in der Videovorschau ist XProtect 2020 R3, für Overlay-Farben XProtect 2020 R2 erforderlich.
- Damit die forensische Suche in um 180 Grad gedrehten Videostreams funktioniert, sind folgende Voraussetzungen erforderlich:
  - Kameras mit AXIS OS 10.6 oder höher bzw.
  - Device Pack 11.0 oder höher auf dem Aufzeichnungsserver
- Für eine zuverlässige Farberkennung sollte der Weißabgleich in der Kamera genau eingestellt werden

Fahrzeugsuche

Wenn Sie AXIS Optimizer zusammen mit bestimmten, auf der Kamera installierten Anwendungen verwenden, können Sie Videobeweise zu Fahrzeugen durchsuchen, identifizieren und teilen. Die Fahrzeugsuche unterstützt Fahrzeugkennzeichendaten aus folgenden Anwendungen:

- *AXIS License Plate Verifier* von Axis Communications
- *CAMMRA AI* von FF Group (Version 1.3 oder höher erforderlich)
- *VaxALPR On Camera* von Vaxtor Recognition Technologies
- *VaxALPR On Camera MMC* von Vaxtor Recognition Technologies

Welche Suchfilter Sie verwenden können, hängt von der Anwendung ab, die Sie auf den Kameras installiert haben (siehe *Suche verfeinern, on page 57*).


Vehicle search
1. License plate
Clear
Enter a license plate
2. Region
Clear
Enter a region
3. Country
Clear
Enter a country
4. Color
Clear
Enter a vehicle color
5. Direction
Clear
Moving closer or into area
Moving away or out of area
6. Type of vehicle
Clear
Enter a vehicle type
7. Brand
Clear
Enter a vehicle brand
8. Model
Clear
Enter a vehicle model
AXIS License Plate Verifier
VaxALPR on Camera (Vaxtor)
VaxALPR on Camera (Vaxtor)
TraFFic CaMMRa (FF Group)
VaxALPR on Camera MMC (Vaxtor)
VaxALPR on Camera (Vaxtor)

Fahrzeugsuche konfigurieren

Hinweis

Anforderungen

- VMS-System:
  - Corporate oder Expert 2019 R3 oder höher
  - Professional+ oder Express+ 2022 R3 oder höher
- Über NTP synchronisierte Kamera-Uhrzeit
- Eine der in aufgeführten Anwendungen

1. Fügen Sie im Management Client die Kamera hinzu, auf der die ausgewählte Anwendung läuft.
2. Aktivieren Sie alle benötigten Geräte. Um den AXIS License Plate Verifier verwenden zu können, sind Kamera 1 und Metadaten 1 erforderlich.
3. Vergewissern Sie sich, dass das Gerät für die Metadaten mit der Kamera verbunden ist:
   - Wechseln Sie zu **Devices (Geräte)** > **Camera (Kamera)** und wählen Sie Ihr Gerät aus.
   - Gehen Sie auf die Registerkarte **Client** und vergewissern Sie sich, dass das Gerät mit den Metadaten der Kamera unter **Related metadata (Verwandte Metadaten)** ausgewählt ist.
4. Metadaten konfigurieren:
   4.1. Gehen Sie auf **Site Navigation > Recording Server (Standortnavigation > Aufzeichnungs-Server)** und suchen Sie das Gerät.
   4.2. Wählen Sie Metadaten 1 aus und klicken Sie auf **Settings (Einstellungen)**.
   4.3. Rufen Sie **Metadata Stream > Event data (Metadatenstream > Ereignisdaten)** auf, und wählen Sie **Yes (Ja)**.
5. Wechseln Sie zur Registerkarte **Record settings (Aufzeichnungseinstellungen)**, und prüfen Sie, ob die Metadatenaufzeichnung aktiviert ist.
6. Klicken Sie auf **Save (Speichern)**.
7. Konfigurieren Sie die Anwendung so, dass sie von einem Standardbenutzer bedient werden kann:
   7.1. Fügen Sie Lese- und Wiedergaberechte für eine bestimmte Kamera und einen bestimmten Benutzer hinzu.
   7.2. Fügen Sie Lese- und Wiedergaberechte für Metadaten für die bestimmte Kamera und den jeweiligen Benutzer hinzu.

Fahrzeug suchen

1. Wechseln Sie im Smart Client zu **Search (Suche)**.
2. Wählen Sie ein Zeitintervall sowie eine oder mehrere Kameras aus.
3. Klicken Sie auf **Search for > Vehicle search > New search (Suche > Fahrzeugsuche und > Neue Suche)**.
4. Wählen Sie die Suchfilter aus, um die Anzahl der Suchergebnisse einzugrenzen.
   Weitere Informationen zu den verschiedenen Filtern finden Sie unter *Suche verfeinern, on page 57*.
5. Wählen Sie die Suchergebnisse aus, die Sie näher prüfen möchten. Sie können diese zu den Lesezeichen hinzufügen oder *PDF-Bericht in hoher Qualität erstellen, on page 61*.

Suche verfeinern

Sie können einen oder mehrere Suchfilter verwenden, um die Suchergebnisse einzugrenzen. Für verschiedene Anwendungen stehen verschiedene Filteroptionen zur Verfügung.

- **Nummernschild**
  Bestimmtes Fahrzeugkennzeichen finden
  Anwendung: Axis License Plate Verifier, VaxALPR On Camera, CAMMRA AI oder VaxALPR On Camera MMC.

- **Region**
  Fahrzeuge aus einer bestimmten Region finden
  Anwendung: AXIS License Plate Verifier 2.9.19.

Hinweis

Standort der Kamera in den Einstellungen des AXIS License Plate Verifier für eine optimale Erkennung in einer bestimmten Region festlegen

- **Land**
  Fahrzeuge aus einem bestimmten Land finden
  Anwendung: Axis License Plate Verifier 2.9.19, VaxALPR On Camera, CAMMRA AI oder VaxALPR On Camera MMC.
- **Farbe**
  Fahrzeuge einer bestimmten Farbe finden
  Anwendung: Axis License Plate Verifier 2.9.19, CAMMRA AI oder VaxALPR On Camera MMC.
- **Richtung**
  Fahrzeuge finden, die sich in eine bestimmte Richtung bewegen.
  Anwendung: Axis License Plate Verifier 2.9.19, VaxALPR On Camera, CAMMRA AI oder VaxALPR On Camera MMC.
- **Fahrzeugtyp**
  Bestimmten Fahrzeugtyp finden.
  Anwendung: Axis License Plate Verifier 2.9.19, CAMMRA AI oder VaxALPR On Camera MMC.
- **Die Marke Axis**
  Bestimmten Fahrzeugtyp finden.
  Anwendung: CAMMRA AI oder VaxALPR On Camera MMC.
- **Modell**
  Bestimmten Fahrzeugtyp finden.
  Anwendung: CAMMRA AI oder VaxALPR On Camera MMC.

Suchgeschwindigkeit optimieren

Sie können die Suchgeschwindigkeit verbessern, indem Sie die Daten steuern, die Ihr System auf dem Gerät für Metadaten des VMS speichert.

- Deaktivieren Sie die Analysedaten, wenn Sie diese nicht benötigen.
  - Wechseln Sie zu **Devices (Geräte)** > **Metadata (Metadaten)** und wählen Sie Ihr Gerät aus.
  - Klicken Sie auf **Settings (Einstellungen)** und deaktivieren Sie **Analytics data (Analysedaten)**.
- Wenn Sie Analysedaten benötigen, können Sie stattdessen konsolidierte Metadaten verwenden, sofern diese verfügbar sind. Siehe *Metadaten und Suche, on page 110*.
- Deaktivieren Sie nicht benötigte Ereignisse in AXIS License Plate Verifier. Damit der AXIS Optimizer funktioniert, benötigen Sie lediglich das Ereignis **Lost (Verloren)**. Siehe *AXIS License Plate Verifier*.
- Stellen Sie sicher, dass Sie AXIS OS 12.8 oder eine neuere Version verwenden.

Suche nach Geschwindigkeit im Bereich

Mit AXIS Optimizer können Sie mit Zone Speed Search nach schnell fahrenden Fahrzeugen suchen, die beim Eintritt in eine vordefinierten Zone in der Ansicht einer Kamera erkannt wurden. Zusammen mit der Anwendung *AXIS Speed Monitor* visualisiert Zone Speed Search von Fahrzeugen in einer Radarerkennungszone in der Live-Ansicht der Kamera. Mit der Schnellsuche in Zonen von Axis können Sie spezifische Filter einrichten, um die Suche einzugrenzen und Videobeweise für Ermittlungsarbeiten zu exportieren und zu teilen.

Konfigurieren von Zone Speed Search

Hinweis

Anforderungen

- VMS-System:

  - Corporate oder Expert 2019 R3 oder höher
  - Professional+ oder Express+ 2022 R3 oder höher
- Über NTP synchronisierte Kamera-Uhrzeit

1. Fügen Sie im Management Client die Kamera hinzu, auf der die ausgewählte Anwendung läuft.
2. Aktivieren Sie alle benötigten Geräte. Um AXIS Zone Speed Search verwenden zu können, sind Kamera 1 und Metadaten 1 erforderlich.
3. Vergewissern Sie sich, dass das Gerät für die Metadaten mit der Kamera verbunden ist:
   - Wechseln Sie zu **Devices (Geräte)** > **Camera (Kamera)** und wählen Sie Ihr Gerät aus.
   - Gehen Sie auf die Registerkarte **Client** und vergewissern Sie sich, dass das Gerät mit den Metadaten der Kamera unter **Related metadata (Verwandte Metadaten)** ausgewählt ist.
4. Metadaten konfigurieren:
   4.1. Gehen Sie auf **Site Navigation > Recording Server (Standortnavigation > Aufzeichnungs-Server)** und suchen Sie das Gerät.
   4.2. Wählen Sie Metadaten 1 aus und klicken Sie auf **Settings (Einstellungen)**.
   4.3. Rufen Sie **Metadata Stream > Event data (Metadatenstream > Ereignisdaten)** auf, und wählen Sie **Yes (Ja)**.
5. Wechseln Sie zur Registerkarte **Record settings (Aufzeichnungseinstellungen)**, und prüfen Sie, ob die Metadatenaufzeichnung aktiviert ist.
6. Klicken Sie auf **Save (Speichern)**.
7. Anwendung für einen einfachen Standardbenutzer konfigurieren:
   7.1. Fügen Sie Lese- und Wiedergaberechte für eine bestimmte Kamera und einen bestimmten Benutzer hinzu.
   7.2. Fügen Sie Lese- und Wiedergaberechte für Metadaten für die bestimmte Kamera und den jeweiligen Benutzer hinzu.

Suche nach geschwindigkeitsbezogene Ereignisse in einer Zone



1. Wechseln Sie im Smart Client zu **Search (Suche)**.
2. Wählen Sie ein Zeitintervall sowie eine oder mehrere Kameras aus.
3. Klicken Sie auf **Suche > Zone Speed Search > Neue Suche**.
4. Wählen Sie die Suchfilter aus, um die Anzahl der Suchergebnisse einzugrenzen.
   Weitere Informationen zu den verschiedenen Filtern finden Sie unter *Suche verfeinern, on page 59*.
5. Wählen Sie die Suchergebnisse aus, die Sie näher prüfen möchten. Sie können diese zu den Lesezeichen hinzufügen oder *PDF-Bericht in hoher Qualität erstellen, on page 61*.

Suche verfeinern

Sie können einen oder mehrere Suchfilter verwenden, um die Suchergebnisse für geschwindigkeitsbezogene Ereignisse einzugrenzen.

- **Max. Geschwindigkeit**

Filtern Sie nach der maximalen Geschwindigkeit von Objekten in der Zone während der Ereignisdauer. Sie können sowohl einen unteren als auch einen oberen Grenzwert für die maximale Geschwindigkeit festlegen.

- **Objekttyp**
  Wenn **Fahrzeug** ausgewählt ist, werden bei der Suche nur geschwindigkeitsbezogene Ereignisse angezeigt, bei denen das schnellste Objekt in der Zone als Fahrzeug klassifiziert wurde.
- **Zonenname**
  Suchen und filtern Sie Zonen nach Namen.

Containersuche

Wenn Sie AXIS Optimizer zusammen mit bestimmten Anwendungen verwenden, können Sie Videobeweise zu Containern suchen, identifizieren und weitergeben. Die Containersuche unterstützt Daten dieser Anwendung:

- *VaxOCR Containers* by Vaxtor Recognition Technologies

Containersuche konfigurieren

Hinweis

Anforderungen

- VMS-System:
  - Corporate oder Expert 2019 R3 oder höher
  - Professional+ oder Express+ 2022 R3 oder höher
- Über NTP synchronisierte Kamera-Uhrzeit
- Die in aufgeführte Anwendung

1. Fügen Sie im Management Client die Kamera hinzu, auf der die ausgewählte Anwendung läuft.
2. Aktivieren Sie alle benötigten Geräte.
3. Vergewissern Sie sich, dass das Gerät für die Metadaten mit der Kamera verbunden ist:
   - Wechseln Sie zu **Devices (Geräte)** > **Camera (Kamera)** und wählen Sie Ihr Gerät aus.
   - Gehen Sie auf die Registerkarte **Client** und vergewissern Sie sich, dass das Gerät mit den Metadaten der Kamera unter **Related metadata (Verwandte Metadaten)** ausgewählt ist.
4. Metadaten konfigurieren:
   4.1. Gehen Sie auf **Site Navigation > Recording Server (Standortnavigation > Aufzeichnungs-Server)** und suchen Sie das Gerät.
   4.2. Wählen Sie Metadaten 1 aus und klicken Sie auf **Settings (Einstellungen)**.
   4.3. Rufen Sie **Metadata Stream > Event data (Metadatenstream > Ereignisdaten)** auf, und wählen Sie **Yes (Ja)**.
5. Wechseln Sie zur Registerkarte **Record settings (Aufzeichnungseinstellungen)**, und prüfen Sie, ob die Metadatenaufzeichnung aktiviert ist.
6. Klicken Sie auf **Save (Speichern)**.
7. Konfigurieren Sie die Anwendung so, dass sie von einem Standardbenutzer bedient werden kann:
   7.1. Fügen Sie Lese- und Wiedergaberechte für eine bestimmte Kamera und einen bestimmten Benutzer hinzu.
   7.2. Fügen Sie Lese- und Wiedergaberechte für Metadaten für die bestimmte Kamera und den jeweiligen Benutzer hinzu.

Container suchen

1. Wechseln Sie im Smart Client zu **Search (Suche)**.
2. Wählen Sie ein Zeitintervall sowie eine oder mehrere Kameras aus.

3. Klicken Sie auf **Search for > Container search > New search (Suche > Containersuche > Neue Suche)**.
4. Wählen Sie die Suchfilter aus, um die Anzahl der Suchergebnisse einzugrenzen.
   Weitere Informationen zu den verschiedenen Filtern finden Sie unter *Suche verfeinern, on page 61*.
5. Wählen Sie die Suchergebnisse aus, die Sie näher prüfen möchten. Sie können diese zu den Lesezeichen hinzufügen oder *PDF-Bericht in hoher Qualität erstellen, on page 61*.

Suche verfeinern

Sie können einen oder mehrere Suchfilter verwenden, um die Suchergebnisse einzugrenzen. Alle Filteroptionen kommen von der Anwendung VaxOCR Containers.

- **Containercode**
  Bestimmten Containercode finden
- **Besitzer**
  Container eines bestimmten Eigentümers finden
- **Eigentümercode**
  Container eines bestimmten Eigentümers finden
- **Größe**
  Container einer bestimmten Größe und eines bestimmten Typs finden
- **Größencode**
  Container einer bestimmten Größe und eines bestimmten Typs finden
- **City or country (Stadt oder Land)**
  Suchen Sie nach Container aus einer bestimmten Stadt oder einem bestimmten Land.
- **Überprüfung**
  Suchen Sie nach Containern, die anhand des Eigentümercodes oder der Steuerziffer bereits überprüft wurden.

PDF-Bericht in hoher Qualität erstellen



Erstellen Sie anhand Ihrer Suchergebnisse einen Bericht. Verwenden Sie diese Funktion, um Bilder in hoher Auflösung in das Ergebnis einzubinden.

1. Führen Sie im Smart Client eine Suche durch.
2. Wählen Sie die Suchergebnisse aus, die im Bericht enthalten sein sollen.
3. Klicken Sie auf $\mathrm{p,255mm,sfx)=\text{″}graphics:graphic33F82CE7811D4EA41E6D94479F2055A5\text{″}}$ > **Create high quality PDF report (Hochwertigen PDF-Bericht erstellen)**.
4. (Optional) Geben Sie den **Report name (Namen des Berichts)**, das **Report destination (Ziel des Berichts)** und **Notes (Hinweise)** ein.
5. Wählen Sie für jedes Suchergebnis aus, welches Bild Sie in den Bericht aufnehmen möchten. Doppelklicken Sie auf ein Bild, um es zu vergrößern.
6. Klicken Sie auf **Create (Erstellen)**. Wenn der Bericht fertig ist, erhalten Sie eine Benachrichtigung.

Axis Fahrzeugkennzeichen

Sie können im Smart Client eine separate Registerkarte für Fahrzeugkennzeichensuche und -management hinzufügen. Auf dieser Registerkarte werden basierend auf den Informationen Ihrer LPR-fähigen Axis Kameras alle Bedieneraufgaben im Zusammenhang mit der Verwaltung, Suche und dem Export von Fahrzeugkennzeichen zentralisiert.



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

Vorbereitungen

- Stellen Sie sicher, dass die VMS-Version 2018 R3 oder höher ist
- Stellen Sie sicher, dass Sie das VMS Device Pack 10.1 oder höher installiert haben.
- Die Uhrzeit der Kamera muss über NTP synchronisiert werden.
- Verwenden Sie eine der unter aufgelisteten Anwendungen.

Axis Fahrzeugkennzeichen konfigurieren

1. Fügen Sie im Management Client die Kamera hinzu, auf der die ausgewählte Anwendung läuft.
2. Aktivieren Sie alle benötigten Geräte. Um den AXIS License Plate Verifier verwenden zu können, sind Kamera 1 und Metadaten 1 erforderlich.
3. Vergewissern Sie sich, dass das Gerät für die Metadaten mit der Kamera verbunden ist:
   - Wechseln Sie zu **Devices (Geräte)** > **Camera (Kamera)** und wählen Sie Ihr Gerät aus.
   - Gehen Sie auf die Registerkarte **Client** und vergewissern Sie sich, dass das Gerät mit den Metadaten der Kamera unter **Related metadata (Verwandte Metadaten)** ausgewählt ist.
4. Metadaten konfigurieren:
   4.1. Gehen Sie auf **Site Navigation > Recording Server (Standortnavigation > Aufzeichnungs-Server)** und suchen Sie das Gerät.
   4.2. Wählen Sie Metadaten 1 aus und klicken Sie auf **Settings (Einstellungen)**.
   4.3. Rufen Sie **Metadata Stream > Event data (Metadatenstream > Ereignisdaten)** auf, und wählen Sie **Yes (Ja)**.
5. Wechseln Sie zur Registerkarte **Record settings (Aufzeichnungseinstellungen)**, und prüfen Sie, ob die Metadatenaufzeichnung aktiviert ist.
6. Klicken Sie auf **Save (Speichern)**.

Fahrzeugkennzeichen suchen

1. Wechseln Sie im Smart Client zu **Axis license plates (Axis Fahrzeugkennzeichen)**.
   Falls die Registerkarte nicht angezeigt wird, gehen Sie zu **Settings > Axis search options (Einstellungen > Axis Suchoptionen)** und wählen die Registerkarte **Show license plate tab (Fahrzeugkennzeichen anzeigen)**.
2. Klicken Sie auf **Kamera ... hinzufügen** und wählen Sie die entsprechenden Kameras aus. > Klicken Sie auf **Schließen**.
   Sie müssen Administrator sein, um dem System Kameras hinzufügen zu können. Wenn Fahrzeugkennzeichen von der Kamera detektiert werden, erscheinen sie live in der Liste, einschließlich ausgeschnittener Bilder der von der Kamera aufgenommenen Nummernschilder. Die Suchergebnisanzeige ist auf maximal 5000 Treffer beschränkt.

3. Geben Sie ein Fahrzeugkennzeichen und unter **Time interval (Zeitintervall)** ein Zeitintervall ein, um das Suchergebnis zu filtern.
   – Geben Sie unter **Time interval (Zeitintervall)** das gewünschte Zeitintervall zwischen einem gewählten Start- und Enddatum ein, um das Suchergebnis zu filtern.

Live-Suche nach Fahrzeugkennzeichen

1. Wechseln Sie im Smart Client zu **Axis license plates (Axis Fahrzeugkennzeichen)**.
   Falls die Registerkarte nicht angezeigt wird, gehen Sie zu **Settings > Axis search options (Einstellungen > Axis Suchoptionen)** und wählen die Registerkarte **Show license plate tab (Fahrzeugkennzeichen anzeigen)**.
2. Klicken Sie auf **Kamera ... hinzufügen** und wählen Sie die entsprechenden Kameras aus. > Klicken Sie auf **Schließen**.
   Sie müssen Administrator sein, um dem System Kameras hinzufügen zu können. Wenn Fahrzeugkennzeichen von der Kamera detektiert werden, erscheinen sie live in der Liste, einschließlich ausgeschnittener Bilder der von der Kamera aufgenommenen Nummernschilder. Die Suchergebnisanzeige ist auf maximal 5000 Treffer beschränkt.
3. Geben Sie ein Fahrzeugkennzeichen ein und wählen Sie **Zeitintervall** > **Live**, um das Suchergebnis zu filtern.

Suche verfeinern

Sie können einen oder mehrere Suchfilter verwenden, um die Suchergebnisse einzugrenzen.

- **Zeitintervall**
  Nach Suchergebnissen innerhalb eines Zeitraums filtern.
- **Nummernschild**
  Nach teilweisem oder vollständigem Text auf dem Fahrzeugkennzeichen filtern.
- **Kameras**
  Nach Suchergebnissen filtern, die von bestimmten Kameras erkannt werden.
- **Richtung**
  Nach Fahrzeugen filtern, die sich in eine bestimmte Richtung bewegen.
- **Listen**
  Nach Suchergebnisses an bestimmten Standorten filtern und nach Suchergebnissen in Freigabe-, Sperr- und benutzerdefinierte Listen filtern. Weitere Informationen zum Einrichten von Listen finden Sie unter *Zentrale Verwaltung von Fahrzeugkennzeichenlisten, on page 25*.

Suchgeschwindigkeit optimieren

Sie können die Suchgeschwindigkeit verbessern, indem Sie die Daten steuern, die Ihr System auf dem Gerät für Metadaten des VMS speichert.

- Deaktivieren Sie die Analysedaten, wenn Sie diese nicht benötigen.
  – Wechseln Sie zu **Devices (Geräte)** > **Metadata (Metadaten)** und wählen Sie Ihr Gerät aus.
  – Klicken Sie auf **Settings (Einstellungen)** und deaktivieren Sie **Analytics data (Analysedaten)**.
- Wenn Sie Analysedaten benötigen, können Sie stattdessen konsolidierte Metadaten verwenden, sofern diese verfügbar sind. Siehe *Metadaten und Suche, on page 110*.
- Deaktivieren Sie nicht benötigte Ereignisse in AXIS License Plate Verifier. Damit der AXIS Optimizer funktioniert, benötigen Sie lediglich das Ereignis **Lost (Verloren)**. Siehe *AXIS License Plate Verifier*.
- Stellen Sie sicher, dass Sie AXIS OS 12.8 oder eine neuere Version verwenden.

Fahrzeugkennzeichensuche als PDF-Bericht exportieren

Verwenden Sie diese Funktion, um aus den Suchergebnissen, die Sie interessieren, einen PDF-Bericht mit qualitativ hochwertigen Bildern zu erstellen.

1. Klicken Sie auf **Export... (Exportieren...)**.
2. Wählen Sie **PDF...**.
3. (Optional) Geben Sie unter **Report name (Berichtname)**, unter **Report destination (Berichtziel)** das Ziel des Berichts und unter **Notes (Hinweise)** etwaige Anmerkungen ein.
4. Wählen Sie für jedes Suchergebnis aus, welches Bild Sie in den Bericht aufnehmen möchten. Um ein Bild zu vergrößern, doppelklicken Sie auf das Bild.
5. Klicken Sie auf **Create (Erstellen)**. Wenn der Bericht fertig ist, erhalten Sie eine Benachrichtigung.

Fahrzeugkennzeichensuche als CSV-Bericht exportieren

Verwenden Sie diese Funktion, um umfangreiche Suchergebnisse als CSV-Bericht auszugeben.

1. Klicken Sie auf **Export... (Exportieren...)**.
2. Wählen Sie **CSV...**.
3. Wählen Sie ein Ziel für die zu exportierende Datei aus.

Axis Insights

Über Diagramme und Dashboards erhalten Sie in Axis Insights einen Überblick über die Daten Ihrer Geräte. Sie können Metadaten für all Ihre Geräte anzeigen. Sie können Daten über erfasste Objekte, identifizierte Fahrzeuge und Alarme anzeigen. Sie können auch neue Dashboards erstellen und diese mit anderen Benutzern teilen.

Axis Insights ist in den Standardadministrator- und Bedieneransichten verfügbar. Die standardmäßige Administratoransicht in Axis Insights ist nur für Benutzer mit Administratorrechten verfügbar, während die standardmäßige Bedieneransicht für alle Bediener mit entsprechenden Rechten verfügbar ist. Vgl. *Rolleneinstellungen konfigurieren, on page 104*. Die Bedieneransicht liefert spezifische Daten von ausgewählten, von Ihnen eingestellten Kameraansichten, während die Administratoransicht einen Überblick über das gesamte System bietet.

Auf Axis Insights zugreifen

- Gehen Sie zu **Smart Client** und klicken Sie auf **Axis Insights**.
- **Dashboard**: Wählen Sie ein Dashboard aus der Dropdown-Liste aus.
- **Camera view (Kameraansicht)**: Wählen Sie eine bestimmte Kameraansicht für die Datenübersicht aus.
- **Time range (Zeitspanne):**: Wählen Sie eine bestimmte Zeitspanne aus.
- **Auto update (Automatisch aktualisieren)**: Aktivieren Sie diese Option, um die Daten automatisch zu aktualisieren.

••• Das Kontextmenü enthält:

- **Edit dashboard (Dashboard bearbeiten)**: Das Dashboard bearbeiten, teilen oder entfernen.
- **Add chart (Diagramm hinzufügen)**: Klicken Sie hier, um ein neues Diagramm in einem Dashboard zu erstellen.
- **About Axis insights (Über Axis Insights)**: Unter diesem Menüpunkt erhalten Sie Informationen über Axis Insights.

••• Das Kontextmenü in jeder Karte enthält:

- **Maximize chart (Karte maximieren)**: Klicken Sie hier, um das Diagramm zu vergrößern.
- **Copy as image (Als Bild kopieren)**: Klicken Sie hier, um das Diagramm in die Zwischenablage zu kopieren.
- **Exportieren**: Klicken, um die Karte als PNG oder CSV zu exportieren.
- **Edit chart (Diagramm bearbeiten)**: Klicken Sie hier, um das Diagramm zu bearbeiten.

- **Remove chart (Diagramm entfernen)**: Klicken Sie hier, um das Diagramm zu entfernen.

Hinweis

- In einigen Karten können Sie auf die Abbildung klicken, um zusätzliche Informationen zu erhalten.
- : Hierüber werden die jeweils für ein Diagramm in Ihrem Dashboard ausgewählten Optionen angezeigt.

Neues Dashboard erstellen

1. **Dashboard**: Wählen Sie **Add dashboard (Dashboard hinzufügen)** in der Dropdown-Liste aus.
2. Klicken Sie auf **Empty (Leer)**, um ein neues Dashboard zu erstellen, oder klicken Sie auf **From existing dashboard (Aus vorhandenem Dashboard)**, um ein Dashboard zu erstellen, das einem im System vorhandenen ähnelt.
3. **Name**: Geben Sie einen Namen für das Dashboard ein.
4. **Anderen Benutzern die Anzeige dieses Dashboards erlauben**: Klicken Sie hier, um Ihr Dashboard für andere Benutzer im schreibgeschützten Modus freizugeben.
5. Klicken Sie auf **Anwenden**.
6. **Add chart (Diagramm hinzufügen)**: Klicken Sie hier, um ein neues Diagramm hinzuzufügen.
   - **Select chart type (Diagrammtyp wählen)**: Wählen Sie den gewünschten Diagrammtyp aus und klicken Sie auf **Next (Weiter)**. Mit Tags oder Diagrammtiteln wie Videoanalyse, Fahrzeuge, Liniendiagramme usw. können Sie einen Diagrammtyp suchen.
   - **Modify data selections (Ausgewählte Optionen anpassen)**: Wählen Sie in jeder Kategorie anwendbare Filter aus.
   - **Adjust appearance (Darstellung anpassen)**: Mit dieser Option können Sie Texte bearbeiten und die Diagrammgröße auswählen.

Konfiguration der Dropdown-Liste im Dashboard

Hinweis

- Standardmäßig können Sie nur die von Ihnen erstellten Dashboards sehen.

So zeigen Sie Dashboards an, die von anderen Benutzern in der Dropdown-Liste **Dashboard** freigegeben wurden:

1. Wechseln Sie zu **Shared dashboards (Gemeinsam genutzte Dashboards)**.
2. Schalten Sie den Schalter für jedes freigegebene Dashboard ein, das Sie der Dropdown-Liste hinzufügen möchten.

Einblicke für eine bestimmte Kameraansicht anzeigen

Wenn Sie Live- und Aufzeichnungsvideos in einer Kameraansicht anzeigen, können Sie Axis Insights so öffnen, dass die aktive Kameraansicht bereits vorausgewählt ist.

So öffnen Sie Axis Insights für eine bestimmte Kameraansicht:

1. Rufen Sie **Smart Client** auf und öffnen Sie eine Ansicht.
2. Klicken Sie auf **Show insights (Insights anzeigen)**.

Axis Insights konfigurieren

1. Überprüfen Sie, ob die Kamera Axis Object Analytics unterstützt. Informationen zu Analysefunktionen finden Sie unter *Axis Product Selector*.
2. Überprüfen Sie, ob Datum und Uhrzeit der Kamera korrekt eingestellt sind.
3. Stellen Sie sicher, dass im Management Client das Metadatengerät für die Kameras aktiviert ist.
4. Vergewissern Sie sich, dass das Gerät für die Metadaten mit der Kamera verbunden ist:

- Wechseln Sie zu **Devices (Geräte)** > **Camera (Kamera)** und wählen Sie Ihr Gerät aus.
- Gehen Sie auf die Registerkarte **Client** und vergewissern Sie sich, dass das Gerät mit den Metadaten der Kamera unter **Related metadata (Verwandte Metadaten)** ausgewählt ist.

5. Um alle in Axis Insights verfügbaren Daten anzuzeigen, aktivieren Sie die Szenenanalyse an Ihrer Kamera unter *AXIS Scene Metadata*:
   5.1. Wechseln Sie zu **Devices (Geräte)** > **Metadata (Metadaten)** und wählen Sie Ihr Gerät aus.
   - Klicken Sie auf **Record (Aufzeichnen)** und vergewissern Sie sich, dass **Recording (Aufzeichnung)** aktiviert ist.
   - Klicken Sie auf **Settings (Einstellungen)** und stellen Sie sicher, dass **Analytics data (Analysedaten)** aktiviert ist.

   5.1. Aktivieren Sie **Consolidated metadata (Zusammengeführte Metadaten)**, um die Ladezeit zu verkürzen (falls verfügbar). Siehe *Metadaten und Suche, on page 110*.
6. So aktivieren Sie Daten für Diagrammtypen mit *AXIS Object Analytics*, *AXIS Image Health Analytics* oder *Umweltsensoren*:
   - Wechseln Sie zu **Devices (Geräte)** > **Metadata (Metadaten)** und wählen Sie Ihr Gerät aus.
   - Klicken Sie auf **Record (Aufzeichnen)** und vergewissern Sie sich, dass **Recording (Aufzeichnung)** aktiviert ist.
   - Klicken Sie auf **Settings (Einstellungen)**, und stellen Sie sicher, dass **Event data (Ereignisdaten)** aktiviert ist.
   - Wir empfehlen Ihnen, im VMS eine Regel zu erstellen, um stets Metadaten von diesem Gerät aufzunehmen.
7. Legen Sie die erforderlichen Berechtigungen für die einzelnen Sicherheitsgruppen fest:
   7.1. Navigieren Sie zu **Site Navigation (Standortnavigation)** > **Security (Sicherheit)** > **Roles (Rollen)**.
   7.2. Wählen Sie eine Rolle aus.
   7.3. Wechseln Sie zu **Cameras (Kameras)**. Wählen Sie die Option **Read (Lesen)** aus.
   7.4. Gehen Sie zu **Metadata (Metadaten)**. Wählen Sie **Read (Lesen)**, **Live** und **Playback (Wiedergabe)** aus.
8. Informationen zum Hinzufügen von Fahrzeugkennzeichen-Metadaten zu Axis Insights finden Sie unter *Axis Fahrzeugkennzeichen konfigurieren, on page 62*.

Fehler in Axis Insights beheben

Problem	Lösung
In den Diagrammen wird „no data" (keine Daten) angezeigt.	Sie müssen Axis Insights konfigurieren. Siehe *Axis Insights konfigurieren, on page 65*.
Das Laden der Bedieneransicht dauert sehr lange.	• Verringern Sie den Zeitraum. • Erstellen und verwenden Sie eine Kameraansicht mit weniger Kameras zur Szenenanalyse. • Aktivieren Sie zusammengeführte Metadaten, siehe *Metadaten und Suche, on page 110*.

Video-Entzerrung

Die Bildentzerrung (Dewarping) bewirkt eine Glättung und Korrektur der perspektivischen Bildverzerrung geometrischer Bilder bei Aufnahmen mittels Weitwinkel- oder Fischaugenobjektiv. Das Axis Dewarping im VMS kann mit jeder Axis 360°-Panoramakamera verwendet werden. Die Bildentzerrung erfolgt entweder direkt in der Kamera oder im Smart Client.

Weitere Informationen zur Bildentzerrung:

- Bei Verwendung einer client-seitigen Bildentzerrung werden sowohl Live-Videos als auch Aufnahmen gleichmäßig entzerrt.
- Wenn Sie zurück zu einer Ansicht gehen, wechseln Sie automatisch zum aktuellen Dewarping-Standort.
- Der Export von Videos beinhaltet Dewarping.
- Sie können eine Home-Position speichern (siehe *Home-Position festlegen, on page 69*).
- Sie können konfigurieren, ob Bediener Dewarping-Ansichten steuern und bearbeiten dürfen (siehe *Bedienern erlauben, Entzerrungsansichten zu steuern und zu bearbeiten, on page 70*).

Eine Entzerrungsansicht erstellen

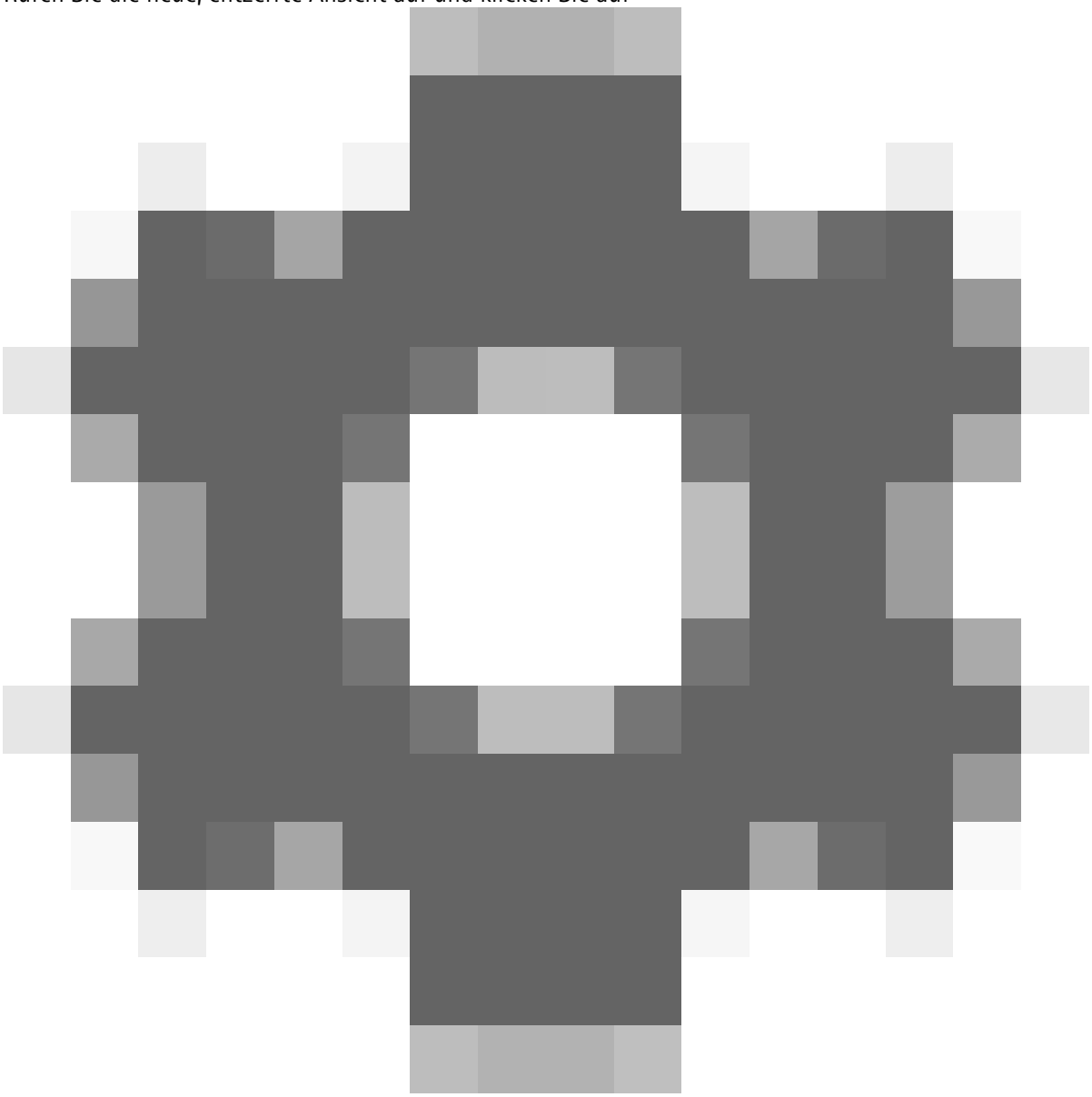


Hinweis

Um den Videostream für die Entzerrung zu optimieren, wählen Sie im Management Client für **Video stream 1 (Videostream 1)** der **Camera 1 (Kamera 1)** die maximale verfügbare Auflösung. Weitere Informationen finden Sie unter *Leistung und Fehlerbehebung, on page 70*.

1. Öffnen Sie den Smart Client, und klicken Sie auf **Setup (Einrichten)**.
2. Rufen Sie **Views (Ansichten)** auf.
3. Klicken Sie auf **Create new view (Neue Ansicht erstellen)**, und wählen Sie ein Format aus.
4. Gehen Sie zu **Systemübersicht > AXIS Optimizer**.
5. Klicken Sie auf **Dewarping view (Entzerrungsansicht)** und ziehen Sie sie in die Ansicht.
6. Wählen Sie eine Kamera und die aktuelle Montageposition der Kamera aus.
7. Klicken Sie auf **Setup**.

8. Rufen Sie die neue, entzerrte Ansicht auf und klicken Sie auf



.

9. Klicken Sie auf **Set view type (Ansichtstyp festlegen)** und wählen Sie eine Option. Je nach Montage der Kamera können Sie **Quad**, **Normal**, **Normal with overview (Normal mit Übersicht)** oder **Panorama** wählen.

Hinweis

Wir empfehlen die Verwendung von 100 % DPI. Wenn die Auflösung nicht 100 % beträgt, ist die Axis Entzerrung auf der zweiten Anzeige möglicherweise nicht vollständig sichtbar.

Bei Verwendung anderer DPI-Einstellungen sind die entzerrten Fenster möglicherweise nur teilweise sichtbar. Befolgen Sie die Anweisungen in diesen externen Artikel, um dieses Problem zu lösen:

- *Probleme mit XProtect bei hochauflösenden Anzeigen (4K und höher)*
- *Skalierung der Client GUI bei hochauflösenden Anzeigen*

Erstellen einer Entzerrungsansicht für Panorama-Kameras mit mehreren Sensoren

Sie können Dewarping-Ansichten für Multisensor-Panorama-Kameras wie AXIS P3807-PVE Network Camera und AXIS Q3819-PVE Panoramic Camera verwenden.

- Zusammenfügen durch Client Wenn die Kamera auf den Aufnahmemodus Entzerren durch Client eingestellt ist, fügt AXIS Optimizer die vier Bilder zu einem nahtlosen Panorama zusammen (nur AXIS P3807-PVE).
- Anpassung des Horizonts Der Panorama-Horizont kann angepasst werden. Dies könnte erwünscht sein, wenn die Kamera zum Boden geneigt und der Welthorizont gekrümmt ist. Dadurch wird auch die virtuelle PTZ-Steuerung intuitiver.
- PTZ-Steuerung Ermöglicht das Heranzoomen und Bewegen im Bild wie bei einer PTZ-Kamera.



Hinweis

Anforderungen

- Benutzer mit einem der folgenden Benutzerrechte:
  - Optimierer
  - Hardware > Treiberbefehle = Zulassen
- Eine Axis Multisensor-Panorama-Kamera

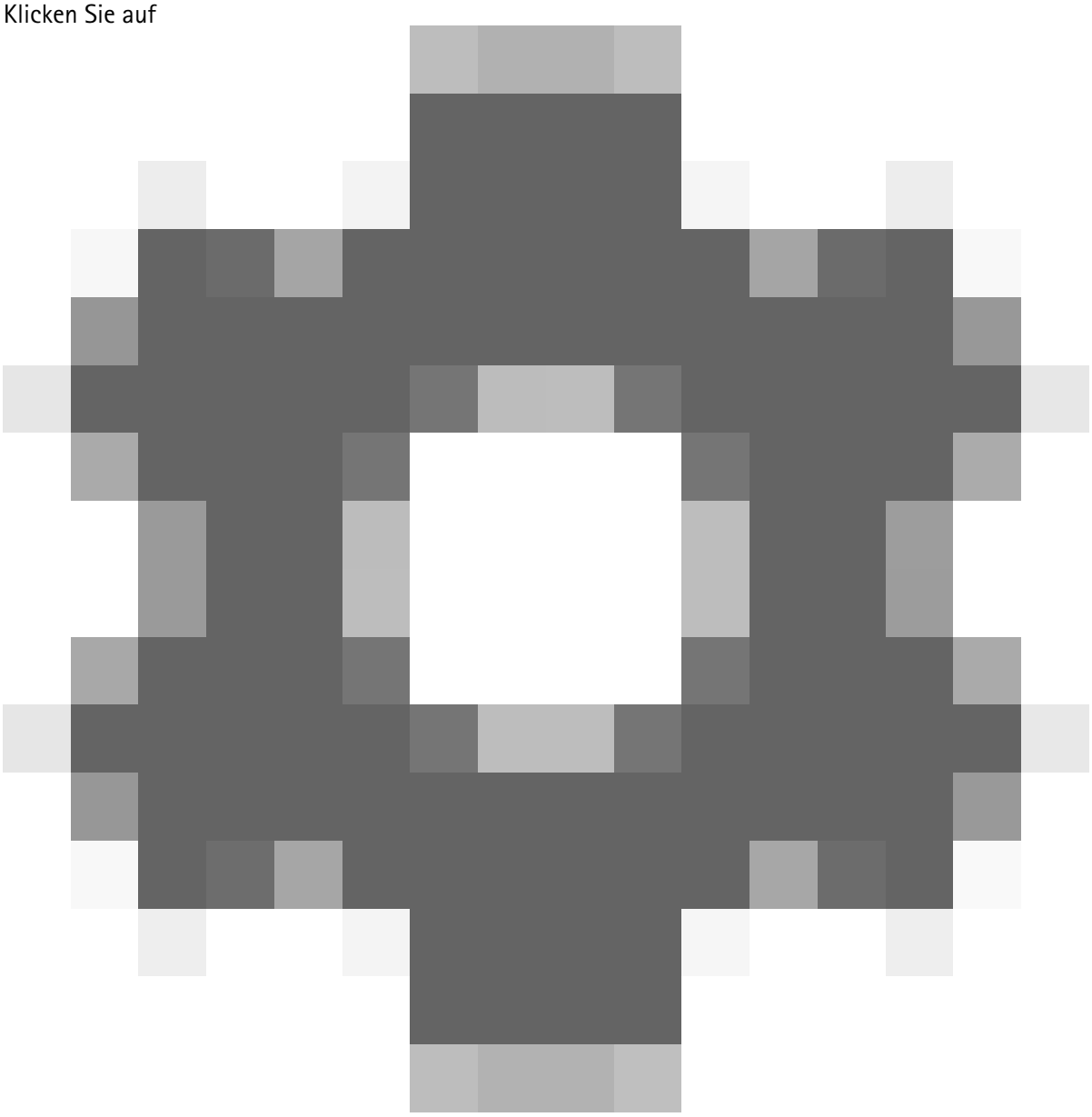
1. Stellen Sie den Aufnahmemodus während der ersten Gerätekonfiguration ggf. auf **Client Dewarp (Entzerren durch Client)** ein.
2. Öffnen Sie den Smart Client, und klicken Sie auf **Setup (Einrichten)**.
3. Rufen Sie **Views (Ansichten)** auf.
4. Klicken Sie auf **Create new view (Neue Ansicht erstellen)**, und wählen Sie ein Format aus.
5. Gehen Sie zu **Systemübersicht > AXIS Optimizer**.
6. Klicken Sie auf **Dewarping view (Entzerrungsansicht)** und ziehen Sie sie in die Ansicht.
7. Wählen Sie eine Multisensor-Panorama-Kamera aus.
   Beim ersten Hinzufügen der Multisensor-Panorama-Kamera zu einer Dewarping-Ansicht wird oberhalb der Ansicht ein Kalibrierungsfenster für den Horizont angezeigt.
8. Klicken Sie auf die Pfeile, damit sich die rote Linie am Welthorizont auszurichtet.
9. Klicken Sie auf **Done (Fertig)**, um Ihre Einstellungen zu speichern und den Kalibrierungsmodus zu beenden.

Weitwinkelansicht

Weitwinkelansicht ist ein Ansichtstyp für Mehrfachsensor-Panoramakameras. Schalten Sie **wide view (Weitwinkel)** ein, wenn das normale Sichtfeld von 120° nicht ausreicht. Bei Weitwinkelansicht wird das Bild immer entzerrt. Schalten Sie **wide view (Weitwinkel)** aus, um bei vollständiger Verkleinerung einen Übergang zur Normalansicht zu erhalten.

Home-Position festlegen

1. Öffnen Sie im Smart Client eine Entzerrungsansicht.
2. Wechseln Sie zu der Position, die Sie als Home-Position speichern möchten.

3. Klicken Sie auf 

und anschließend auf **Set home position (Home-Position festlegen)**.

Bedienern erlauben, Entzerrungsansichten zu steuern und zu bearbeiten

Sie können konfigurieren, ob Bediener Dewarping-Ansichten steuern und bearbeiten dürfen, (siehe *Anpassen des Funktionszugriffs für Bediener, on page 104*).

Leistung und Fehlerbehebung

Leistungsaspekte

- Das Axis Video-Dewarping wird nach Möglichkeit in der GPU durchgeführt, allerdings wird durch das Video-Dewarping auch die CPU belastet.
- Um zu verhindern, dass die Bildrate bei einer großen Ansicht mit vielen Dewarping-Ansichten sinkt, sollten Sie Folgendes beachten:
  - Kameraauflösung Eine hohe Kameraauflösung (zum Beispiel 2880 x 2880) erfordert viel Computerleitung im Vergleich zu beispielsweise 1920 x 1920.
  - Kamerabildrate. Wenn Sie keine hohe Bildrate benötigen, kann durch die Änderung zu einer niedrigeren Bildrate verhindert werden, dass die Dewarping-Ansicht und andere Ansichten ruckeln.

– Monitorauflösung. Hochauflösende Monitore, zum Beispiel 4K, benötigen viele Ressourcen für die Wiedergabe des Videos. Wenn die höhere Auflösung nicht benötigt wird, können durch eine niedrigere Auflösung des Monitors auch entzerrte Ansichten ohne Ruckeln ausgeführt werden.

Dynamische Auflösung

- Der Videostream wird nach Möglichkeit automatisch herunterskaliert, ohne die Videoqualität zu verringern. Dadurch kann die Leistung der Dewarping-Ansichten verbessert werden.
- Wenn Sie beim Zoomen aus der Übersicht heraus ein Bildflimmern feststellen, kann es helfen, die dynamische Auflösung zu deaktivieren.
- So aktivieren oder deaktivieren Sie die dynamische Auflösung: Gehen Sie in Smart Client zu **Settings (Einstellungen) > Axis dewarping options (Axis Entzerrungsoptionen) > Rendering options (Rendering-Optionen)** und wählen oder löschen Sie **Dynamic resolution (Dynamische Auflösung)**.
- **Dynamic resolution (Dynamische Auflösung)** ist in der Standardeinstellung aktiviert.

Kompatibilitätsrendering

- Wenn das Dewarping-Bild visuelle Fehler aufweist, z. B. ein schwarzes Bild, oder die Leistung schlechter als erwartet ist, aktivieren Sie das Kompatibilitätsrendering. Ein negativer Effekt des Kompatibilitätsrenderings ist, dass Übergänge zwischen Ansichten und Scrubbing bei der Wiedergabe flimmern können.
- So aktivieren oder deaktivieren Sie das Kompatibilitätsrendering: Öffnen Sie Smart Client, gehen Sie zu **Settings (Einstellungen) > Axis dewarping options (Axis Entzerrungsoptionen) > Rendering options (Rendering-Optionen)** und wählen oder löschen Sie **Use compatibility rendering (Kompatibilitäts-Rendering verwenden)**.
- **Use compatibility rendering (Kompatibilitäts-Rendering verwenden)** ist in der Standardeinstellung deaktiviert.

Was zu erwarten ist

In einem Referenzsystem mit Intel i7 8700 NVIDIA Gefore 1050 GTX und drei 1920 x 1080 Monitoren ist zu erwarten:

- 7 Dewarping-Ansichten mit einer Auflösung von 1920 x 1920 und 25 BpS können ohne Bildausfälle ausgeführt werden
- 4 Dewarping-Ansichten mit einer Auflösung von 2880 x 2880 und 25 BpS

Wenn eines der drei Displays mit einer Auflösung von 4K statt 1920 x 1080 ausgeführt wird, ist Folgendes zu erwarten:

- 5 Dewarping-Ansichten mit einer Auflösung von 1920 x 1920 und 25 BpS können ohne Bildausfälle ausgeführt werden
- 3 Dewarping-Ansichten mit einer Auflösung von 2880 x 2880 und 25 BpS Eine Dewarping-Ansicht auf jedem Monitor

Bildrate und Auflösungsskalen sind linear. Ein Computer, der 5 Dewarping-Ansichten mit 30 BpS ausführen kann, kann 10 Ansichten ausführen, wenn die Bildrate auf 15 Bps reduziert wird.

Body Worn Integration

Mit AXIS Optimizer Body Worn Extension können die Benutzer der Kameras vor Ort Videos aufzeichnen, kennzeichnen und mit den Ermittlern im Büro teilen, die mit VMS nach Videobeweisen suchen und diese verwalten können. Der Service ermöglicht eine sichere Verbindung und Übertragung zwischen dem Axis Body Wear System und dem VMS. AXIS Body Worn Extension ist ein kostenloser, eigenständiger Dienst, den Sie auf dem Aufzeichnungs-Server installieren müssen.

Hinweis

Unterstützte Versionen:

- VMS-Version 2020 R1 Corporate oder neuere Versionen
- VMS-Version 2020 R1 Professional+ oder neuere Versionen
- VMS-Version 2020 R1 Expert oder neuere Versionen

Verwenden Sie stets die aktuellen VMS-Hotfixes und kumulativen Patch-Installationsprogramme.

Mehr erfahren

- Um den Dienst selbst herunterzuladen oder den Integrationsleitfaden und die Anmerkung zur Lösung zu lesen, gehen Sie auf *axis.com*.
- Um das Benutzerhandbuch zu lesen, gehen Sie auf *axis.help.com*.

Zutrittskontrolle

Die Zutrittskontrolle ist eine Lösung, die physische Zutrittskontrolle mit Videosicherheit kombiniert. Mit dieser Integration können Sie ein Axis Zutrittssystem direkt über den Management Client konfigurieren. Das System lässt sich nahtlos in XProtect integrieren, sodass Bediener den Zugang überwachen und Zutrittskontrolle-Aktion im Smart Client durchführen können.

Hinweis

Anforderungen

- VMS-Version 2024 R1 oder höher.
- XProtect Zugriff-Lizenzen, siehe *Zugriff-Lizenzen*.
- Installieren Sie AXIS Optimizer auf dem Ereignis-Server und dem Management Client.

Die Ports 53459 und 53461 werden für eingehenden Datenaustausch (TCP) geöffnet, wenn Sie AXIS Optimizer über AXIS Secure Entry installieren.

Um Zugänge in AXIS Secure Entry nutzen zu können, benötigen Sie eine Lizenz pro Zugang; siehe *Zugangslizenzen aktivieren, on page 74*.

Konfiguration der Zutrittskontrolle

Hinweis

Stellen Sie vor dem Start Folgendes sicher:

- Aktualisieren Sie die Software des Netzwerk-Tür-Controllers. Die Mindest- und empfohlene AXIS OS-Version für Ihre VMS-Version finden Sie in der folgenden Tabelle.
- Stellen Sie sicher, dass Datum und Uhrzeit korrekt sind.

AXIS Optimizer Version	AXIS OS Mindestversion	Empfohlene AXIS OS Version
6.0	12.6.94.1	12.10.73.4
5.8	12.6.94.1	12.8.55.1
5.6	12.6.94.1	12.6.94.1

Ihrem System einen Axis Netzwerk-Tür-Controller hinzufügen

1. Rufen Sie **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** auf.
2. Wählen Sie unter **Configuration (Konfiguration)** die Option **Devices (Geräte)**.
3. Wählen Sie **Discovered devices (Erfasste Geräte)**, um die Liste der Geräte anzuzeigen, die Sie dem System hinzufügen können.
4. Wählen Sie die hinzuzufügenden Geräte aus.
5. Klicken Sie im Popup-Fenster auf **+ Add (+ Hinzufügen)** und geben Sie die Anmeldedaten für den Controller ein.

Hinweis

- Die hinzugefügten Controller sollten auf der Registerkarte **Management (Verwaltung)** zu sehen sein.
- Um einen Controller manuell zum System hinzuzufügen, klicken Sie auf **+ Add (+ Hinzufügen)** auf der Registerkarte **Management (Verwaltung)**.
- Um Ihre Aktualisierung in das VMS zu integrieren, wenn Sie einen Tür-Controller-Name hinzufügen, entfernen oder bearbeiten:
  - Gehen Sie zu **Site Navigation (Standortnavigation)** > **Access control (Zutrittskontrolle)** und klicken Sie auf die Integration der Zutrittskontrolle.
  - Klicken Sie auf **Refresh Configuration (Konfiguration aktualisieren)** auf der Registerkarte **General settings (Allgemeine Einstellungen)**.

Zugangslizenzen aktivieren

Bevor Sie Zugänge hinzufügen können, müssen Sie die in Ihrem System vorhandenen Lizenzen aktivieren.

1. Rufen Sie in **Site Navigation (Standortnavigation)** die Option **License Information (Lizenzinformationen)** auf.
2. Klicken Sie auf **Activate License Manually (Lizenz manuell aktivieren)** und wählen Sie entweder **Online** oder **Offline**.
3. So aktivieren Sie Zugangslizenzen online:
   – Den Benutzernamen und das Kennwort eingeben.
4. Informationen zum Offline-Aktivieren von Zugangslizenzen finden Sie unter *Lizenzen offline aktivieren*.

Falls Sie die Anzahl der zu aktivierenden Zugangslizenzen anpassen müssen:

1. Rufen Sie **AXIS Optimizer** > **Access control (Zutrittskontrolle)** auf.
2. Wählen Sie unter **Configuration (Konfiguration)** die Option **Devices (Geräte)**.
3. Rufen Sie **Allocated door licenses (Zugewiesene Zugangslizenzen)** > **Custom license allocation (Benutzerdefinierte Lizenzzuweisung)** auf und geben Sie die Anzahl der Zugangslizenzen ein, die Sie verwenden möchten.
4. Klicken Sie auf **Anwenden**.
5. Rufen Sie **License Information (Lizenzinformationen)** auf und reaktivieren Sie Ihre Lizenzen.

Konfigurieren Sie die Zutrittskontrolle

1. Rufen Sie **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** auf.
2. Informationen zum Bearbeiten der vordefinierten Identifizierungsprofile oder zum Erstellen eines neuen Identifizierungsprofils finden Sie unter *Identifizierungsprofile, on page 90*.
3. Informationen zur Verwendung eines benutzerdefinierten Setups für Kartenformate und die PIN-Länge finden Sie unter *Kartenformate und PIN, on page 87*.
4. Fügen Sie einen Zugang hinzu und wenden Sie ein Identifizierungsprofil auf den Zugang an. Siehe *Fügen Sie einen Zugang hinzu, on page 77*.
5. Fügen Sie eine Zone hinzu und fügen Sie der Zone Zugänge hinzu. Siehe *Zone hinzufügen, on page 84*.

Kompatibilität der Gerätesoftware für Tür-Steuerungen

Wichtig

Beachten Sie bei der Aktualisierung des AXIS OS auf Ihrer Tür-Steuerung die folgenden Punkte:

- **Unterstützte Versionen von AXIS OS:** Die unten aufgeführten unterstützten Versionen von AXIS OS gelten nur bei einer Aktualisierung von der empfohlenen VMS-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 VMS-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 Optimizer Version 6.0 und aktualisieren alle Geräte auf die empfohlene AXIS OS-Version 12.10.73.4. Dann ist AXIS OS-Version 12.6.94.1 als die unterstützte Mindestversion Ihres Systems.
- **Aktualisierung auf eine neuere als die empfohlene AXIS OS-Version:** Angenommen, Sie aktualisieren AXIS OS auf eine höhere Version als die für eine bestimmte VMS-Version empfohlene Version. Dann können Sie jederzeit problemlos auf die von empfohlene AXIS OS Version zurückstufen, solange diese innerhalb der Unterstützungsgrenzen für die VMS-Version liegt.
- **Zukünftige empfohlene AXIS OS-Versionen:** Verwenden Sie immer die empfohlene AXIS OS-Version für die jeweilige VMS-Version, um die Systemstabilität und vollständige Kompatibilität zu gewährleisten.

Integration der Zutrittskontrolle

Um die Zutrittskontrolle in das VMS zu integrieren:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **Access Control (Zutrittskontrolle)**.
2. Klicken Sie mit der rechten Maustaste auf **Access Control (Zutrittskontrolle)** und klicken Sie auf **Create new... (Neu erstellen...)**.
3. Im Dialogfeld **Create Access Control System Integration (Systemintegration von Zutrittskontrolle erstellen)**:
   - Geben Sie einen Namen für die Integration ein.
   - Wählen Sie **AXIS Secure Entry** aus dem Drop-Down-Menü unter **Integration plug-in (Integrations-Plug-in)**.
   - Klicken Sie auf **Next (Weiter)**, bis Sie das Dialogfeld **Associate cameras (Kameras zuordnen)** sehen.
     So ordnen Sie Kameras Türzugriffspunkten zu:
     - Klicken Sie unter **Cameras (Kameras)** auf Ihr Gerät, um die Liste der im XProtect-System konfigurierten Kameras anzuzeigen.
     - Wählen Sie eine Kamera aus und ziehen Sie sie auf den Zugriffspunkt, mit dem Sie sie verbinden möchten.
     - Klicken Sie auf **Schließen**, um das Dialogfeld zu schließen.

Hinweis

- Weitere Informationen zur Integration der Zutrittskontrolle in XProtect finden Sie unter *Verwendung der Zutrittskontrolle in XProtect Smart Client*.
- Weitere Informationen zu den Eigenschaften der Zutrittskontrolle, wie allgemeine Einstellungen, Zugänge und zugehörige Kameras, Ereignisse der Zutrittskontrolle usw., finden Sie unter *Eigenschaften der Zutrittskontrolle*.

Türen und Bereiche

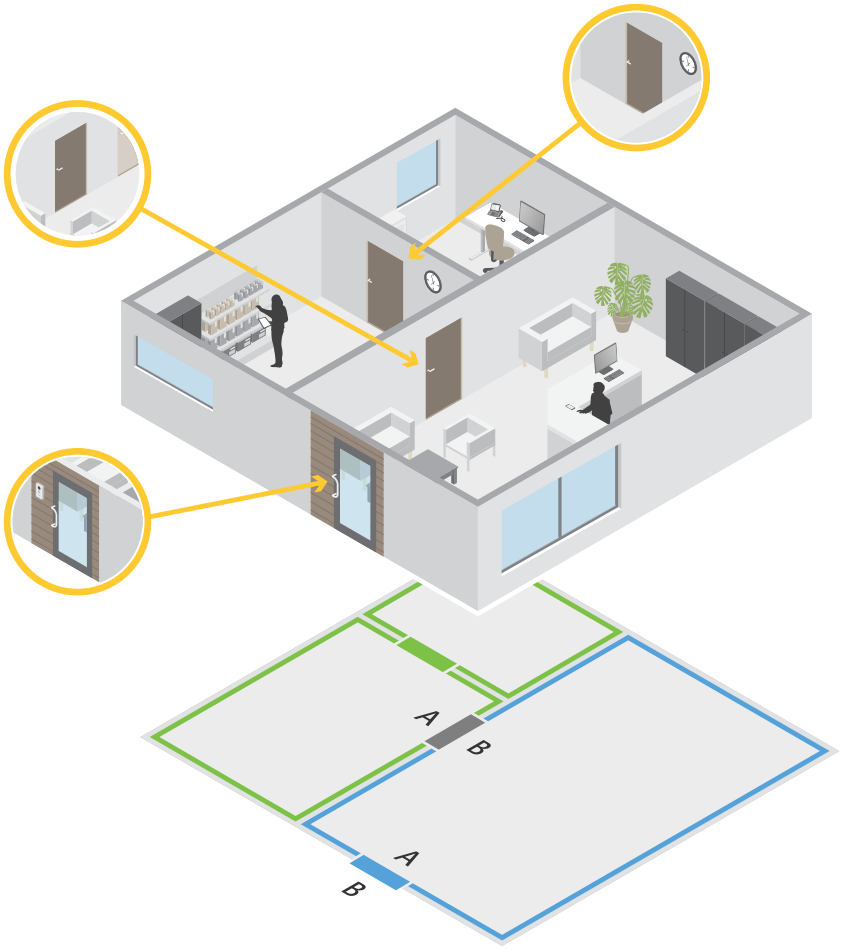
Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**, um einen Überblick zu erhalten und Zugänge und Zonen zu konfigurieren.

Pin Chart	Zeigen Sie das Pin Chart des Controllers an, das einem Zugang zugeordnet ist. Wenn Sie das Pin Chart ausdrucken möchten, klicken Sie auf **Print (Drucken)**.
Identifizierungsprofil	Ändern Sie das Identifizierungsprofil für Zugänge.
Secure Channel	Schalten Sie OSDP Secure Channel für einen bestimmten Leser ein oder aus.

Türen	
Bezeichnung	Der Name des Zugangs.
Tür-Controller	Die Tür-Steuerung, die mit dem Zugang verbunden ist.
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.
Kartenformate und PIN	Zeigt den Typ des Kartenformats oder die PIN-Länge an.

Status	Der Status des Zugangs. • **Online:** Der Zugang ist online und funktioniert normal. • **Leser offline:** Der Leser in der Zugangskonfiguration ist offline. • **Leserfehler:** Der Leser in der Türkonfiguration unterstützt keinen sicheren Kanal oder sicherer Kanal ist für den Leser nicht aktiviert.
Zonen	
Bezeichnung	Der Name der Zone.
Anzahl der Zugänge	Die Anzahl der Zugänge in der Zone.

Beispiel für Zugänge und Zonen



- Es gibt zwei Zonen: eine grüne Zone und eine blaue.
- Es gibt drei Zugänge: einen grünen Zugang, 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.
- Wenn einer Tür-Steuerung keine Zugänge zugewiesen sind und Sie eine neue Version von Axis Optimizer mit einer Tür-Steuerung mit älterer Software 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 Software.

Erstellen einer neuen Zugangskonfiguration zum Hinzufügen einer Tür:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**.
2. Klicken Sie auf **Add door (Zugang hinzufügen)**.
3. Geben Sie einen Namen für den Zugang ein.
4. Wählen Sie im Drop-Down Menü **Controller** eine Tür-Steuerung aus. Der Controller ist ausgegraut, wenn Sie keine weitere Tür hinzufügen können, wenn er offline ist oder HTTPS nicht aktiviert ist.
5. Wählen Sie im Drop-Down Menü **Door type (Zugangsart)** die zu erstellende Zugangsart aus.
6. Klicken Sie auf **Next (Weiter)**, um die Seite zur Zugangskonfiguration aufzurufen.
7. Wählen Sie im Drop-Down Menü **Primary lock (Primäres Schloss)** einen Relay-Port aus.
8. Um zwei Schlösser am Zugang zu konfigurieren, wählen Sie den anderen Relay-Port im Drop-Down Menü **Secondary lock (Sekundäres Schloss)** aus.
9. Wählen Sie ein Identifizierungsprofil aus. Siehe *Identifizierungsprofile, on page 90*.
10. Konfigurieren Sie die Zugangseinstellungen. Siehe *Einstellungen der Tür, on page 78*.
11. Richten Sie einen überwachten Zugang ein. Siehe dazu *Überwachten Zugang hinzufügen, on page 81*.
12. Klicken Sie auf **Save (Speichern)**.

Kopieren einer vorhandenen Zugangskonfiguration zum Hinzufügen eines Zugangs:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**.
2. Klicken Sie auf **Add door (Zugang hinzufügen)**.
3. Geben Sie einen Namen für den Zugang ein.
4. Wählen Sie im Drop-Down Menü **Controller** eine Tür-Steuerung aus.
5. Klicken Sie auf **Next (Weiter)**.
6. 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.
7. Sie können die Einstellungen jederzeit ändern.
8. Klicken Sie auf **Save (Speichern)**.

So bearbeiten Sie einen Zugang:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer**> **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)** > **Doors (Zugänge)**.
2. Wählen Sie einen Zugang in der Liste aus.
3. Klicken Sie auf **Edit (Bearbeiten)**.
4. Ändern Sie die Einstellungen und klicken Sie auf **Save (Speichern)**.

So entfernen Sie einen Zugang:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer**> **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)** > **Doors (Zugänge)**.
2. Wählen Sie einen Zugang in der Liste aus.
3. Klicken Sie auf **Remove (Entfernen)**.
4. **Yes (Ja)** anklicken

Um Ihre Aktualisierung in das VMS zu integrieren, wenn Sie einen Türname hinzufügen, entfernen oder bearbeiten:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **Access control (Zutrittskontrolle)** und klicken Sie auf die Integration der Zutrittskontrolle.
2. Klicken Sie auf **Refresh Configuration (Konfiguration aktualisieren)** auf der Registerkarte **General settings (Allgemeine Einstellungen)**.

Einstellungen der Tür

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**.
2. Wählen Sie den Zugang aus, den Sie bearbeiten möchten.
3. Klicken Sie auf **Edit (Bearbeiten)**.

Zugangszeit (s)	Legen Sie die Anzahl von Sekunden fest, die der Zugang geöffnet bleibt, nachdem Zutritt gewährt wurde. Die Tür bleibt entriegelt, bis sie sich öffnet oder bis die eingestellte Zeit endet. Die Tür verriegelt sich beim Schließen selbst dann, wenn noch Zugangszeit bleibt.
Open-too-long time (sec) (Maximale Öffnungsdauer (s))	Nur gültig, wenn ein Zugangsmonitor konfiguriert ist. Legen Sie fest, wie viele Sekunden die Tür geöffnet bleibt. Wenn die Tür geöffnet ist, wenn die eingestellte Zeit endet, löst sie einen Alarm einer zu lange geöffneten Tür aus. Richten Sie eine Aktionsregel ein, die festlegt, welche Aktion ausgelöst werden soll, wenn die maximale Öffnungsdauer überschritten wird.
Lange Zutrittszeiten (Sekunden)	Legen Sie die Anzahl von Sekunden fest, die der Zugang geöffnet bleibt, nachdem Zutritt gewährt wurde. Der Wert für die lange Zutrittszeit überschreibt die bereits festgelegte Zutrittszeit für Karteninhaber, wenn diese Einstellung aktiviert ist.
Long open-too-long time (sec) (Lange maximale Öffnungsdauer (s))	Nur gültig, wenn ein Zugangsmonitor konfiguriert ist. Legen Sie fest, wie viele Sekunden die Tür geöffnet bleibt. Wenn die Tür geöffnet ist, wenn die eingestellte Zeit endet, löst sie ein Ereignis einer zu lange geöffneten Tür aus. Wenn Sie die Einstellung **Long access time (Lange Zugangszeit)** einschalten, überschreibt der Wert für die lange maximale Öffnungsdauer die bereits festgelegte maximale Öffnungsdauer für Karteninhaber.

Verzögerungszeit bis zum Wiederverriegeln (ms)	Legen Sie die Zeit (in Millisekunden) fest, die die Tür nach dem Öffnen oder Schließen entriegelt bleibt.
Wieder verriegeln	• **After opening (Nach dem Öffnen):** Nur gültig, wenn ein Zugangsmonitor hinzugefügt wurde. • **After closing (Nach dem Schließen):** Nur gültig, wenn ein Zugangsmonitor hinzugefügt wurde.

Sicherheitsstufe der Tür

Sie können einer Tür die folgenden Sicherheitsfunktion hinzufügen:

Zwei-Personen-Regel – Die Zwei-Personen-Regel erfordert, dass zwei Personen gültige Zugangsdaten verwenden, um Zugang zu erhalten.

Double Swipe – Mit dem doppelten Durchziehen kann der Karteninhaber den aktuellen Status einer Tür überschreiben. Beispielsweise kann er damit einen Zugang außerhalb des regulären Zeitplans sperren und entsperren, was bequemer ist, als das Entsperren des Zugangs im System. Die Double-Swipe-Funktion wirkt sich nicht auf einen vorhandenen Zeitplan aus. Wenn etwa ein Zugang zur Schließzeit gemäß Zeitplan verriegelt werden soll und ein Mitarbeiter in die Mittagspause geht, wird der Zugang dennoch gemäß Zeitplan verriegelt.

Sie können die Sicherheitsstufe konfigurieren, während Sie eine neue Tür hinzufügen, oder Sie können die Konfiguration für eine vorhandene Tür durchführen.

So fügen Sie eine **Zwei-Personen-Regel** zu einem vorhandenen Zugang hinzu:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**.
2. Wählen Sie die Tür aus, für die Sie eine Sicherheitsstufe konfigurieren möchten.
3. Klicken Sie auf **Edit (Bearbeiten)**.
4. Klicken Sie auf **Security level (Sicherheitsstufe)**.
5. Aktivieren Sie **Zwei-Personen-Regel**.
6. Klicken Sie auf **Anwenden**.

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

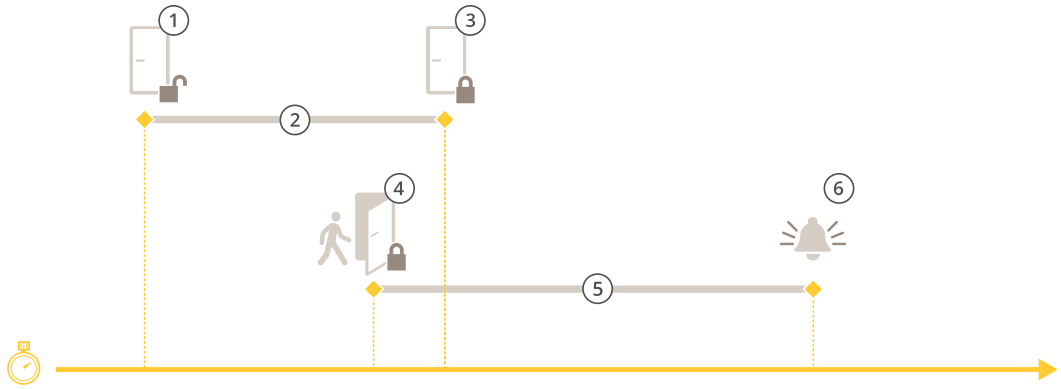
So fügen Sie einem vorhandenen Zugang **Double Swipe** hinzu:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**.
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**.

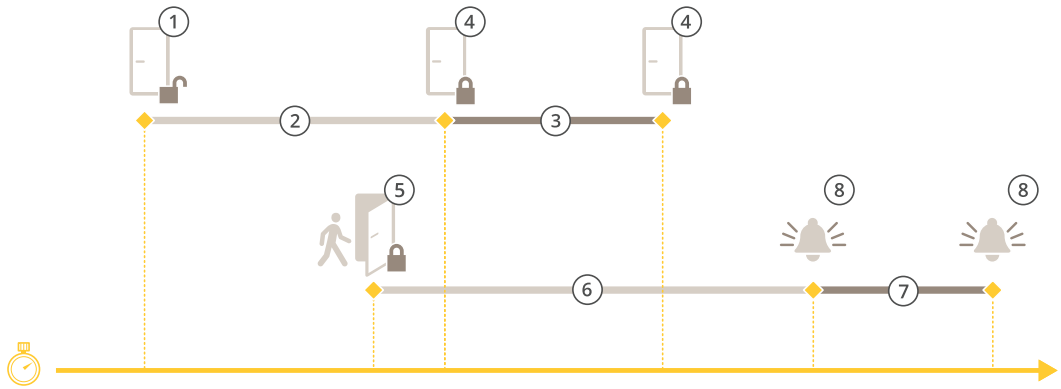
6. Klicken Sie auf **Anwenden**.
7. Wenden Sie **Double Swipe** auf einen Karteninhaber an.
   7.1. Wechseln Sie zu **Cardholder management (Karteninhaberverwaltung)**.
   7.2. Wählen Sie den Karteninhaber aus, den Sie bearbeiten möchten, und klicken Sie auf **Edit (Bearbeiten)**.
   7.3. Klicken Sie auf **Erweitert**.
   7.4. Wählen Sie **Allow double-swipe (Double Swipe zulassen)** aus.
   7.5. Klicken Sie auf **Save (Speichern)**.

Double Swipe	
Zeitüberschreitung (Sekunden)	Timeout ist die maximal zulässige Zeit zwischen dem Durchziehen der Karte oder der Verwendung eines anderen Typs gültiger Zugangsdaten.

Zeitoptionen



1 Zugang gewährt – Schloss entriegelt
2 Zugangszeit
3 Keine Aktion ausgeführt – Schloss verriegelt
4 Aktion ausgeführt (Tür geöffnet) – Schloss verriegelt oder bleibt entriegelt, bis die Tür geschlossen wird
5 Zu lange geöffnet
6 Zu lange geöffnet – Alarm wird ausgelöst



1 Zugang gewährt – Schloss entriegelt
2 Zugangszeit

3 2+3: Lange Zugriffszeit
4 Keine Aktion ausgeführt – Schloss verriegelt
5 Aktion ausgeführt (Tür geöffnet) – Schloss verriegelt oder bleibt entriegelt, bis die Tür geschlossen wird
6 Zu lange geöffnet
7 6+7: Lange maximale Öffnungsdauer
8 Zu lange geöffnet – Alarm wird ausgelöst

Zugangsmonitor hinzufügen

Ein Zugangsmonitor ist ein Zugangspositionsschalter, der den physischen Zustand eines Zugangs überwacht. Sie können Ihrem Zugang wahlweise einen Zugangsmonitor hinzufügen und konfigurieren, wie der Zugangsmonitor angeschlossen ist.

1. Rufen Sie die Seite zur Zugangskonfiguration auf. Siehe *Fügen Sie einen Zugang hinzu, on page 77*
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 dem Netzwerk-Tür-Controller und dem Zugangsmonitor unterbrochen wird, aktivieren Sie **Supervised input (Überwachte Eingänge)**. Siehe *Überwachte Eingänge, on page 86*.

Tür auf, wenn	
Stromkreis geöffnet	Der Schaltkreis des Zugangsmonitors ist ein Öffner-Kontakt. Der Zugangsmonitor gibt bei offenem Schaltkreis an, dass der Zugang geöffnet ist. Der Zugangsmonitor gibt bei geschlossenem Schaltkreis an, dass der Zugang geschlossen ist.
Stromkreis geschlossen	Der Schaltkreis des Zugangsmonitors ist ein Schliesser-Kontakt. Der Zugangsmonitor gibt bei offenem Schaltkreis an, dass der Zugang geschlossen ist. Der Zugangsmonitor gibt bei geschlossenem Schaltkreis an, dass der Zugang offen ist.

Überwachten Zugang hinzufügen

Ein überwachter Zugang ist ein Zugangstyp, dessen geöffneter oder geschlossener Zustand angezeigt werden kann. Dies kann z. B. eine Brandschutztür sein: Diese benötigt kein Schloss, aber Sie müssen wissen, ob sie geöffnet ist.

Ein überwachter Zugang unterscheidet sich von einem normalen Zugang mit Monitor. Ein normaler Zugang mit Monitor unterstützt Schlösser und Kartenleser, erfordert aber eine Tür-Steuerung. Ein überwachter Zugang unterstützt einen Sensor für die Türposition, benötigt aber nur ein netzwerkbasiertes E/A-Relaismodul, das mit einer Tür-Steuerung verbunden ist. Sie können bis zu fünf Sensoren für die Türposition mit einem netzwerkbasierten E/A-Relaismodul verbinden.

Hinweis

Für einen überwachten Zugang brauchen Sie das netzwerkbasierte E/A-Relaismodul AXIS A9210 mit der neuesten Software 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 im VMS zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**.
4. Klicken Sie auf **Add door (Zugang hinzufügen)**.
5. Geben Sie einen Namen ein.
6. Wählen Sie unter **Type (Typ) Monitoring door (Überwachter Zugang)** aus.
7. Wählen Sie unter **Device (Gerät)** Ihr netzwerkbasiertes E/A-Relaismodul aus.
8. Klicken Sie auf **Next (Weiter)**.
9. Klicken Sie unter **Sensors (Sensoren)** auf **Add (Hinzufügen)** und wählen Sie **Door position sensor (Sensor Türposition)** aus.
10. Wählen Sie den E/A, der mit dem Sensor für die Türposition verbunden ist.
11. Klicken Sie auf **Hinzufügen**.

Leser hinzufügen

Sie können eine Tür-Steuerung zum Verwenden von zwei verdrahteten Lesern konfigurieren. Wählen Sie einen Leser für eine oder für beide Seiten eines Zugangs.

Wenn ein benutzerdefiniertes Setup von Kartenformaten oder PIN-Längen auf einen Leser angewendet wird, wird dieses in **Card formats (Kartenformate)** unter **Configuration > Access control > Doors and zones (Konfiguration > Zutrittskontrolle > Zugänge und Zonen)** deutlich angezeigt. Siehe *Türen und Bereiche, on page 75*.

1. Rufen Sie die Seite zur Zugangskonfiguration auf. Siehe *Fügen Sie einen Zugang hinzu, on page 77*.
2. Klicken Sie für eine Seite des Zugangs auf **Add (Hinzufügen)**.
3. Wählen Sie **Card reader (Kartenleser)**.
4. Wählen Sie unter **Reader type (Lesertyp)** die gewünschte Option aus.
5. So verwenden Sie ein benutzerdefiniertes Setup der PIN-Länge für diesen Leser.
   5.1. Klicken Sie auf **Erweitert**.
   5.2. Aktivieren Sie **Custom PIN length (Benutzerdefinierte PIN-Länge)**.
   5.3. Legen Sie Werte für **Min PIN length (Min. PIN-Länge)**, **Max PIN length (Max. PIN-Länge)** und **End of PIN character (Ende des PIN-Zeichens)** fest.
6. So verwenden Sie ein benutzerdefiniertes Kartenformat für diesen Leser.
   6.1. Klicken Sie auf **Erweitert**.
   6.2. Aktivieren Sie **Custom card formats (Benutzerdefinierte Kartenformate)**.
   6.3. Wählen Sie die Kartenformate, die Sie für den Leser verwenden möchten. Wenn bereits ein Kartenformat mit der gleichen Bitlänge verwendet wird, müssen Sie es zuerst deaktivieren. Ein Warnsymbol wird auf dem Client angezeigt, wenn sich das Kartenformat von der konfigurierten Systemkonfiguration unterscheidet.
7. Klicken Sie auf **Hinzufügen**.
8. Um einen Leser zur anderen Türseite hinzuzufügen, dieses Verfahren erneut verwenden.

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.

Wiegand	
LED-Steuerung	Wählen Sie entweder **Single wire (Einzelner Draht)** oder **Dual wire (R/G) (Doppeldraht (R/G))** aus. Leser mit einer dualen LED-Steuerung verwenden verschiedene Adern für die roten und grünen LEDs.
Manipulationsalarm	Wählen Sie aus, wann der Manipulationseingang des Lesers aktiv ist. • **Open circuit (Offener Stromkreis)**: Der Leser übermittelt dem Zugang das Manipulationssignal, wenn der Schaltkreis geöffnet ist. • **Closed circuit (Geschlossener Stromkreis)**: Der Leser übermittelt dem Zugang das Manipulationssignal, wenn der Schaltkreis geschlossen ist.
Tamper debounce time (Entprellzeit)	Legen Sie eine **Tamper debounce time (Entprellzeit Manipulation)** fest, um die Statusänderungen des Manipulationseingangs des Lesers zu ignorieren, bevor er einen neuen stabilen Status annimmt.
Überwachter Eingang	Um ein Ereignis auszulösen, wenn die Verbindung zwischen dem Netzwerk-Zugangscontroller und dem Leser unterbrochen wird, aktivieren Sie dies. Siehe *Überwachte Eingänge, on page 86*.

REX-Gerät hinzufügen

Sie können ein REX-Gerät auf einer oder auf beiden Seiten des Zugangs hinzufügen. Ein REX-Gerät kann ein PIR-Sensor, eine REX-Taste oder eine Druckstange sein.

1. Rufen Sie die Seite zur Zugangskonfiguration auf. Siehe *Fügen Sie einen Zugang hinzu, on page 77*.
2. Klicken Sie für eine Seite des Zugangs auf **Add (Hinzufügen)**.
3. **REX device (REX-Gerät)** auswählen.
4. Wählen Sie den I/O-Port aus, mit dem Sie das REX-Gerät verbinden möchten. Wenn nur ein Port verfügbar ist, wird dieser Port automatisch ausgewählt.
5. Wählen Sie aus, welche **Action (Aktion)** beim Empfang des REX-Signals von der Tür ausgelöst werden soll.
6. Wählen Sie unter **REX active (REX aktiv)** aus, wie die Schaltkreise des Zugangsmonitors angeschlossen sind.
7. Legen Sie eine **Debounce time (ms) (Entprellzeit(ms))** fest, um die Statusänderungen des digitalen Eingangs zu ignorieren, bevor er einen neuen stabilen Status annimmt.

8. Um ein Ereignis auszulösen, wenn die Verbindung zwischen dem Netzwerk-Tür-Controller und dem REX-Gerät unterbrochen wird, aktivieren Sie **Supervised input (Überwachte Eingänge)**. Siehe *Überwachte Eingänge, on page 86*.

Action (Aktion)	
Tür entriegeln	Wählen Sie diese Option aus, um die Tür zu entriegeln, wenn sie das REX-Signal empfängt.
Keine	Wählen Sie diese Option aus, wenn Sie beim Empfang des REX-Signals keine Aktion von der Tür auslösen möchten.

REX aktiv	
Stromkreis geöffnet	Wählen Sie aus, ob der REX-Schaltkreis ein Öffner-Kontakt ist. Das REX-Gerät sendet das Signal, wenn der Schaltkreis geöffnet ist.
Stromkreis geschlossen	Wählen Sie aus, ob der REX-Schaltkreis ein Schliesser-Kontakt ist. Das REX-Gerät sendet das Signal, wenn der Schaltkreis geschlossen ist.

Zone hinzufügen

Eine Zone ist ein bestimmter physischer Bereich mit einer Gruppe von Zugängen. Sie können Zonen erstellen und den Zonen Zugänge hinzufügen. Es gibt zwei Arten von Türen:

- **Perimeter door (Umgrenzungszugang):** Karteninhaber betreten oder verlassen die Zone durch diesen Zugang.
- **Internal door (Interner Zugang):** Ein interner Zugang innerhalb der Zone.

Hinweis

Ein Umgrenzungszugang kann zu zwei Zonen gehören. Ein interner Zugang kann nur zu einer Zone gehören.

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)** > **Zones (Zonen)**.
2. Klicken Sie auf **Add zone (Zone hinzufügen)**.
3. Geben Sie einen Zonennamen ein.
4. Klicken Sie auf **Add door (Zugang hinzufügen)**.
5. Wählen Sie die Türen aus, die Sie der Zone hinzufügen möchten, und klicken Sie auf **Add (Hinzufügen)**.
6. Der Zugang ist standardmäßig ein Umgrenzungszugang. Um das zu ändern, wählen Sie im Aufklappmenü die Option **Internal door (Interner Zugang)** aus.
7. Ein Umgrenzungszugang verwendet standardmäßig die Türseite A als Eingang zur Zone. Um das zu ändern, wählen Sie im Drop-Down Menü die Option **Leave (Verlassen)** aus.
8. Um eine Tür aus der Zone zu entfernen, wählen Sie diese aus und klicken Sie auf **Remove (Entfernen)**.
9. Klicken Sie auf **Save (Speichern)**.

Zum Bearbeiten einer Zone:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)** > **Zones (Zonen)**.
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. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)** > **Zones (Zonen)**.
2. Eine Kamera aus der Liste wählen.
3. Klicken Sie auf **Remove (Entfernen)**.
4. **Yes (Ja)** anklicken

Sicherheitsstufe der Zone

Sie können einer Zone die folgenden Sicherheitsfunktion hinzufügen:

Anti-Passback – Diese Funktion verhindert, dass eine Person die gleichen Zugangsdaten verwenden kann wie jemand, der bereits vor ihr einen Bereich betreten hat. Dadurch wird gewährleistet, dass eine Person den Bereich zuerst verlassen muss, bevor sie ihre Zugangsdaten erneut verwenden kann.

Hinweis

- Für die Anti-Passback-Funktion empfehlen wir den Einsatz von Zugangspositionssensoren an allen Zugängen in der Zone, damit das System registrieren kann, dass ein Benutzer den Zugang nach dem Durchziehen seiner Karte auch wirklich geöffnet hat.
- Wenn eine Tür-Steuerung offline geht, funktioniert Anti-Passback so lange, wie alle Zugänge in der Zone zu derselben Tür-Steuerung gehören. Wenn die Zugänge in der Zone jedoch zu verschiedenen Tür-Steuerungen gehören, die offline gehen, funktioniert Anti-Passback nicht mehr.

Sie können die Sicherheitsstufe konfigurieren, während Sie eine neue Zone hinzufügen, oder Sie können die Konfiguration für eine vorhandene Zone durchführen. So fügen Sie einer vorhandenen Zone eine Sicherheitsstufe hinzu:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**.
2. Wählen Sie die Zone aus, für die Sie eine Sicherheitsstufe konfigurieren möchten.
3. Klicken Sie auf **Edit (Bearbeiten)**.
4. Klicken Sie auf **Security level (Sicherheitsstufe)**.
5. Schalten Sie die Sicherheitsfunktionen ein, die Sie dem Zugang hinzufügen möchten.
6. Klicken Sie auf **Anwenden**.

Anti-Passback	
Log violation only (Soft) (Nur Verstoß protokollieren (Soft))	Verwenden Sie diese Option, um einer zweiten Person den Zutritt mit den gleichen Zugangsdaten wie die erste Person zu gestatten. Diese Option löst lediglich einen Systemalarm aus.

Deny access (Hard) (Zutritt verweigern (Hard))	Verwenden Sie diese Option, um zu verhindern, dass der zweite Benutzer mit den gleichen Zugangsdaten wie die erste Person den Zugang verwendet. Diese Option löst ebenfalls einen Systemalarm aus.
Zeitüberschreitung (Sekunden)	Die Zeitspanne, bis das System einem Benutzer erneut den Zutritt gewährt. Geben Sie 0 ein, wenn Sie keine Zeitüberschreitung verwenden möchten. Für die Zone gilt dann Anti-Passback, bis der Benutzer die Zone verlässt. Verwenden Sie für die Zeitüberschreitung den Wert **0** nur dann zusammen mit **Deny access (Hard) (Zutritt verweigern (Hard))**, wenn alle Zugänge in der Zone auf beiden Seiten über Leser verfügen.

Überwachte Eingänge

Überwachte Eingänge können bei Unterbrechung der Verbindung mit einer Tür-Steuerung ein Ereignis auslösen.

- Verbindung zwischen Tür-Controller und Türmonitor. Siehe *Zugangsmonitor hinzufügen, on page 81*.
- Verbindung zwischen dem Tür-Controller und dem Leser, der Wiegand-Protokolle verwendet. Siehe dazu *Leser hinzufügen, on page 82*.
- Verbindung zwischen Tür-Controller und REX-Gerät. Siehe *REX-Gerät hinzufügen, on page 83*.

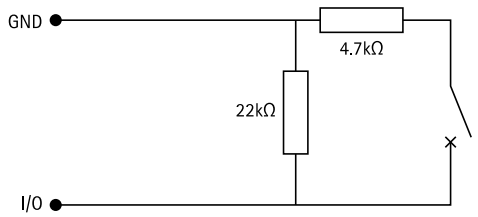
Um überwachte Eingänge zu verwenden:

1. Installieren Sie, wie im Anschlussschaltbild dargestellt, Abschlusswiderstände so nah wie möglich am Peripheriegerät.
2. Gehen Sie zur Konfigurationsseite eines Lesers, eines Zugangsmonitors oder eines REX-Geräts und aktivieren Sie **Supervised input (Überwachte Eingänge)**.
3. Wenn Sie nach dem Schaltplan für eine Parallelschaltung vorgegangen sind, wählen Sie **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Parallelschaltung mit einem parallelen Widerstand (22 KΩ) und einem seriellen Widerstand (4,7 KΩ))**.
4. Wenn Sie nach dem Schaltplan für eine Serienschaltung vorgegangen sind, wählen Sie **Serial first connection (Serienschaltung)** und im Drop-Down Menü **Resistor values (Widerstandswerte)** einen Widerstandswert.

Anschlussschaltbilder

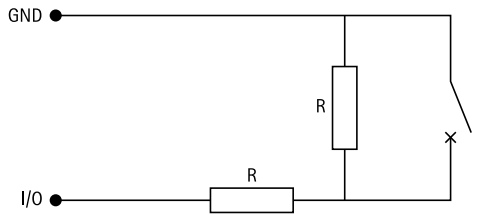
Parallele erste Verbindung

Die Widerstandswerte müssen 4,7 kΩ und 22 kΩ betragen.



Serielle erste Verbindung

Die Widerstandswerte müssen identisch sein und zwischen 1 und 10 kΩ liegen.



Manuelle Aktionen

Sie können die folgenden manuellen Aktionen an Zugängen und Zonen durchführen:

Zurücksetzen – Stellt die konfigurierten Systemregeln wieder her.

Zugang gewähren – Entriegelt 7 Sekunden lang einen Zugang oder eine Zone und sperrt sie dann wieder.

Entriegeln – Hält den Zugang unverschlossen, bis Sie zurücksetzen.

Lock (Sperren) – 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. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Doors and zones (Zugänge und Zonen)**.
2. Wählen Sie den Zugang oder die Zone aus, für die Sie eine manuelle Aktion durchführen möchten.
3. Klicken Sie auf eine der manuellen Aktionen.

Hinweis

Die Tür verbleibt im manuellen Modus – auch als manueller Übersteuerungsmodus bezeichnet –, bis Sie sie wieder auf ihren regulären Zeitplan zurücksetzen.

Kartenformate und PIN

Ein Kartenformat definiert, wie Daten auf einer Karte gespeichert werden. Es handelt sich um eine Übersetzungstabelle zwischen den eingehenden Daten und den validierten Daten im System. Jedes Kartenformat verfügt über einen eigenen Satz an Regeln für die Organisation der gespeicherten Informationen. Durch Definieren eines Kartenformats wird festgelegt, wie das System die Informationen interpretiert, die der Controller vom Kartenlesegerät erhält.

Ihnen stehen vordefinierte, häufig verwendete Kartenformate zur Verfügung, die Sie nach Bedarf verwenden oder bearbeiten können. Außerdem können Sie benutzerdefinierte Kartenformate erstellen.

Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Card formats and PIN (Kartenformate und PIN)**, um Kartenformate zu erstellen, zu bearbeiten oder zu aktivieren. Sie können auch eine PIN konfigurieren.

Die benutzerdefinierten Kartenformate können die folgenden Datenfelder enthalten, die zur Überprüfen von Anmeldedaten verwendet werden.

Kartennummer – Eine Teilmenge der binären Zugangsdaten, die als Dezimal- oder Hexadezimalzahlen codiert ist. Verwenden Sie die Kartennummer, um eine bestimmte Karte oder einen bestimmten Karteninhaber zu identifizieren.

Einrichtungscode – Eine Teilmenge der binären Zugangsdaten, die als Dezimal- oder Hexadezimalzahlen codiert ist. Verwenden Sie den Gebäude-Zugangscode, um einen bestimmten Endkunden oder Standort zu identifizieren.

So erstellen Sie ein Kartenformat:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Card formats and PIN (Kartenformate und PIN)**.

2. **Add card format (Kartenformat hinzufügen)** aufrufen.
3. Geben Sie einen Namen für das Kartenformat ein.
4. Geben Sie im **Feld für die Bitlänge** eine Zahl zwischen 1 und 256 ein.
5. Wählen Sie **Invert bit order (Bit-Reihenfolge invertieren)** aus, falls Sie die Bit-Reihenfolge der vom Kartenleser empfangenen Daten umkehren möchten.
6. Wählen Sie **Invert byte order (Byte-Reihenfolge umkehren)** aus, falls Sie die Byte-Reihenfolge der vom Kartenleser empfangenen Daten umkehren möchten. Diese Option ist nur verfügbar, wenn Sie eine Bitlänge angeben, die man durch acht teilen kann.
7. Wählen Sie die Datenfelder aus und konfigurieren Sie sie so, dass sie im Kartenformat aktiv sind. Entweder **Card number (Kartennummer)** oder **Facility code (Gebäude-Zugangscode)** muss im Kartenformat aktiv sein.
8. Klicken Sie auf **OK**.
9. Um das Kartenformat zu aktivieren, aktivieren Sie das Kontrollkästchen vor dem Namen des Kartenformats.

Hinweis

- Zwei Kartenformate mit der gleichen Bitlänge können nicht gleichzeitig aktiviert sein. Wenn Sie beispielsweise zwei Kartenformate mit 32 Bit definiert haben, kann nur eines davon aktiv sein. Deaktivieren Sie das Kartenformat, um das andere zu aktivieren.
- Kartenformate können nur aktiviert oder deaktiviert werden, wenn der Netzwerk-Tür-Controller im System mit mindestens einem Leser konfiguriert wurde.

ⓘ	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).

So bearbeiten Sie ein Kartenformat:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Card formats and PIN (Kartenformate und PIN)**.
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. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Card formats and PIN (Kartenformate und PIN)**.
2. Wählen Sie ein benutzerdefiniertes Kartenformat aus, klicken Sie auf und dann auf **Yes (Ja)**.

Zurücksetzten eines vordefinierten Kartenformats:

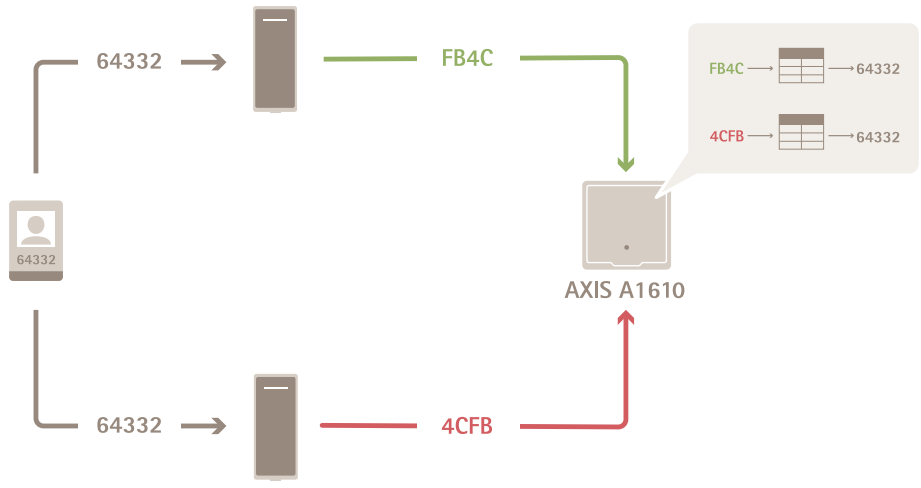
1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Card formats and PIN (Kartenformate und PIN)**.
2. Klicken Sie auf , um ein Kartenformat auf die Standardfeldzuordnung zurückzusetzen.

So konfigurieren Sie die PIN-Länge:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Card formats and PIN (Kartenformate und PIN)**.
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**.

Einstellungen für das Kartenformat

Übersicht



- Die Kartennummer in Dezimalstellen lautet `64332`.
- Ein Leser wandelt die Kartennummer an die Hexadezimalzahl `FB4C` um. Der andere Leser wandelt sie in die Hexadezimalzahl `4CFB` um.
- Der AXIS A1610 Network Door Controller empfängt die Hexadezimalzahl `FB4C` und wandelt sie entsprechend den auf den Leser angewendeten Kartenformateinstellungen in die Dezimalzahl `64332` um.

- Der AXIS A1610 Network Door Controller empfängt die Hexadezimalzahl `4CFB`, ändert sie durch Umkehrung der Byte-Reihenfolge in `FB4C` und wandelt sie entsprechend den auf den Leser angewendeten Kartenformateinstellungen in die Dezimalzahl `64332` um.

Bit-Reihenfolge umkehren

Nach dem Umkehren der Bit-Reihenfolge werden die vom Leser empfangenen Kartendaten Bit für Bit von rechts nach links ausgelesen.



Byte-Reihenfolge umkehren

Eine Gruppe von acht Bits ist ein Byte. Nach dem Umkehren der Byte-Reihenfolge werden die vom Leser empfangenen Kartendaten Byte für Byte von rechts nach links ausgelesen.



26-Bit-Standard-Wiegand-Kartenformat



1 *Führende Parität*
2 *Einrichtungscode*
3 *Kartennummer*
4 *Angehängte Parität*

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.

Identifikationsarten sind Träger der Zugangsdaten, die für die Nutzung eines Zugangs erforderlich sind. Gängige Identifikationsarten sind Tokens, persönliche Identifikationsnummern (PINs), Fingerabdrücke, Gesichtsmasken und REX-Geräte. Eine Identifikationsart kann eine oder mehrere Arten von Informationen enthalten.

Zeitpläne, auch bekannt als **Time profiles (Zeitprofile)**, werden im Management Client erstellt. Informationen zur Einstellung von Zeitprofilen finden Sie unter *Zeitprofile (Erläuterung)*.

Unterstützte Identifikationsarten: Karte, PIN und REX.

Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Identification profiles (Identifizierungsprofile)**.

Ihnen stehen fünf Standard-Identifizierungsprofile zur Verfügung, die Sie nach Bedarf verwenden oder bearbeiten können.

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.

Nummernschild – Karteninhaber müssen mit einem Fahrzeug mit zugelassenem Fahrzeugkennzeichen auf die Kamera zufahren.

So erstellen Sie ein Identifizierungsprofil:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Identification profiles (Identifizierungsprofile)**.
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. Konfigurieren Sie das Identifizierungsprofil für eine Seite des Zugangs.
6. Wiederholen Sie die vorherigen Schritte auf der anderen Seite des Zugangs.
7. Klicken Sie auf **OK**.

So bearbeiten Sie ein Identifizierungsprofil:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Identification profiles (Identifizierungsprofile)**.
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**.

So entfernen Sie ein Identifizierungsprofil:

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Identification profiles (Identifizierungsprofile)**.
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**.

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.

Verschlüsselte Kommunikation

OSDP mit Secure Channel

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 **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Encrypted communication (Verschlüsselte Kommunikation)**.
2. Geben Sie den Hauptverschlüsselungsschlüssel an und klicken Sie auf **OK**.
3. **OSDP Secure Channel** aktivieren. Diese Option ist nur verfügbar, nachdem Sie den Hauptverschlüsselungsschlüssel eingegeben haben.
4. Standardmäßig wird der OSDP Secure Channel-Schlüssel vom Hauptverschlüsselungsschlüssel generiert. So legen Sie den OSDP Secure Channel-Schlüssel manuell fest:
   4.1. Klicken **Sie unter OSDP Secure Channel** (Sicherer Kanal) auf .
   4.2. **Hauptverschlüsselungsschlüssel zum Generieren des Schlüssels für OSDP mit Secure Channel verwenden**entfernen.
   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*.

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.
- 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 53461.

Vorgehensweise

1. Konfigurieren Sie einen Server als Subserver und erstellen Sie die Konfigurationsdatei. Siehe *Die Konfigurationsdatei vom Subserver erstellen, on page 93*.
2. Konfigurieren Sie einen Server als Hauptserver und importieren Sie die Konfigurationsdatei der Subserver. Siehe *Importieren der Konfigurationsdatei auf den Hauptserver, on page 93*.
3. Konfigurieren Sie globale Karteninhaber und Karteninhabergruppen auf dem Hauptserver. Siehe *Karteninhaber hinzufügen, on page 94* und *Gruppe hinzufügen, on page 97*.
4. Auf dem Subserver können Sie die globalen Karteninhaber und Karteninhabergruppen anzeigen und überwachen. Siehe hierzu *Zugriffsverwaltung, on page 93*.

Die Konfigurationsdatei vom Subserver erstellen

1. Wechseln Sie vom Subserver zu **AXIS Optimizer** > **Access Control (Zutrittskontrolle)** > **Multi server (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 **AXIS Optimizer** > **Access Control (Zutrittskontrolle)** > **Multi server (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 **AXIS Optimizer** > **Access Control (Zutrittskontrolle)** > **Multi server (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:

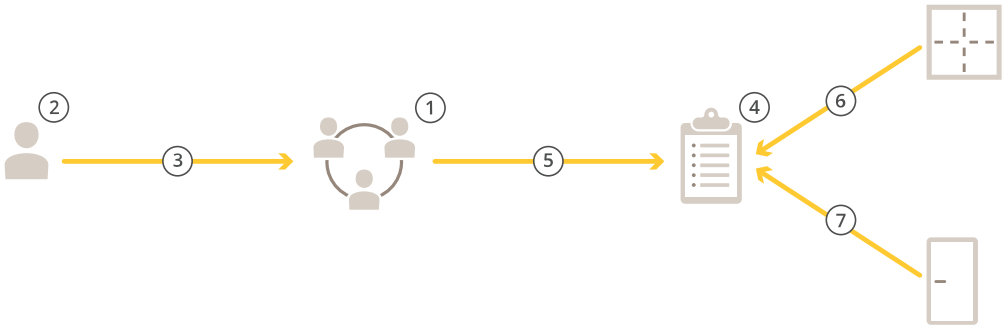
1. Vom Hauptserver:
   1.1. Rufen Sie **Access management (Zugriffsverwaltung)** > **Dashboard** auf.
   1.2. Ändern Sie die globalen Karteninhaber und Gruppen in lokale Karteninhaber und Gruppen.
   1.3. Rufen Sie **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Multi server (Multi-Server)** 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 **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Multi server (Multi-Server)** auf.
   – Klicken Sie auf **Sub server (Subserver)** und dann auf **Revoke server (Server sperren)**.

Zugriffsverwaltung

Auf der Registerkarte „Access Management (Zugriffsverwaltung)“ können Sie die Karteninhaber, Gruppen und Zugangsregeln des Systems konfigurieren und verwalten.

Vorgehensweise bei der Zugriffsverwaltung

Die Struktur der Zugriffsverwaltung ist flexibel. Gehen Sie anhand der Anforderungen der jeweiligen Anwendung vor. Im Folgenden finden Sie ein Beispiel für eine Vorgehensweise:



1. Fügen Sie Gruppen hinzu. Siehe *Gruppe hinzufügen, on page 97*.
2. Fügen Sie Karteninhaber hinzu. Siehe *Karteninhaber hinzufügen, on page 94*.
3. Fügen Sie Karteninhaber und Gruppen hinzu.
4. Fügen Sie Zugangsregeln hinzu. Siehe *Fugen Sie eine Zugangsregel hinzu, on page 98*.
5. Ordnen Sie Zugangsregeln Gruppen zu.
6. Ordnen Sie Zugangsregeln Zonen zu.
7. Ordnen Sie Zugangsregeln Zugänge zu.

Karteninhaber hinzufügen

Ein Karteninhaber ist eine Person mit einer eindeutigen ID, die im System registriert ist. Konfigurieren Sie einen Karteninhaber mit Zugangsdaten, die dem System mitteilen, wer die Person ist und wann und wie der Person die Nutzung von Zugängen gewährt wird.

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Cardholder management (Verwaltung von Karteninhabern)**.
2. Navigieren Sie zu **Cardholders (Karteninhaber)** und klicken Sie dann auf **+ Add (+ Hinzufügen)**.
3. Geben Sie den Vor- und Nachnamen des Karteninhabers ein und klicken Sie auf **Next (Weiter)**.
4. Klicken Sie optional auf **Advanced (Erweitert)** und wählen Sie die gewünschten Optionen aus.
5. Fügen Sie Zugangsdaten für den Karteninhaber hinzu. Siehe *Zugangsdaten hinzufügen, on page 95*
6. Klicken Sie auf **Save (Speichern)**.
7. Fügen Sie den Karteninhabers zu einer Gruppe hinzu.
   7.1. Wählen Sie unter **Groups (Gruppen)** die Gruppe aus, zu der Sie den Karteninhaber hinzufügen möchten, und klicken Sie auf **Edit (Bearbeiten)**.
   7.2. Klicken Sie auf **+ Add (+ Hinzufügen)** und wählen Sie den Karteninhaber aus, den Sie zu der Gruppe hinzufügen möchten. Sie können mehrere Karteninhaber auswählen.
   7.3. Klicken Sie auf **Hinzufügen**.
   7.4. Klicken Sie auf **Save (Speichern)**.

Erweitert	
Lange Zugriffszeit	Wählen Sie diese Option aus, damit für den Karteninhaber eine lange Zutrittszeit und eine lange Dauer für einen zu lange geöffneten Zugang gelten sollen, wenn ein Zugangsmonitor installiert ist.
Karteninhaber suspendieren	Wählen Sie diese Option aus, um den Karteninhaber zu suspendieren.
Allow double-swipe (Double Swipe zulassen)	Auswählen, um einem Karteninhaber zu erlauben, den aktuellen Zustand eines Zugangs außer Kraft zu setzen. Dies kann beispielsweise dazu verwendet werden, eine Tür außerhalb des regulären Zeitplans zu entriegeln.
Vom Lockdown ausgeschlossen	Wählen Sie diese Option aus, um dem Karteninhaber während der Sperrzeit Zugang zu gewähren.
Exempt from anti-passback (Doppelnutzungsausnahme)	Sie können einem Karteninhaber jetzt eine Ausnahme von der Anti-Passback-Regel gewähren. Die Anti-Passback-Funktion verhindert, dass eine Person die gleichen Zugangsdaten verwenden kann wie jemand, der bereits vor ihr einen Bereich betreten hat. Die erste Person muss zunächst den Bereich verlassen, bevor ihre Zugangsdaten erneut verwendet werden können.
Globaler Karteninhaber	Wählen Sie diese Option aus, damit der Karteninhaber auf den Subservern angezeigt und überwacht werden kann. Diese Option ist nur für auf dem Hauptserver erstellte Karteninhaber verfügbar. Siehe .

Zugangsdaten hinzufügen

Sie können einem Karteninhaber die folgenden Arten von Zugangsdaten hinzufügen:

- PIN
- Karte
- Nummernschild
- Mobiltelefon

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**.

Siehe das Beispiel in *Fahrzeugkennzeichen als Zugangsdaten verwenden, on page 96*.

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 eine Zwangs-PIN zum Auslösen eines stillen Alarms zu verwenden, aktivieren Sie **Duress PIN (Zwangs-PIN)** und geben Sie eine Zwangs-PIN ein.
4. Klicken Sie auf **Hinzufügen**.

Eine PIN ist immer gültig. Sie können auch eine Zwangs-PIN konfigurieren, die zwar das Öffnen des Zugangs ermöglicht und dabei einen stillen Alarm im System auslöst.

So fügen Sie einem Karteninhaber Karten-Zugangsdaten hinzu:

1. Klicken Sie unter **Credentials (Zugangsdaten)** auf **+ Add (+ Hinzufügen)** und wählen Sie **Card (Karte)** aus.
2. Um die Kartendaten manuell einzugeben, geben Sie einen Kartennamen, eine Kartennummer und eine Bitlänge ein.

Hinweis

Die Bitlänge ist nur konfigurierbar, wenn Sie ein Kartenformat mit einer bestimmten Bitlänge erstellen, die sich nicht im System befindet.

3. So rufen Sie automatisch die Kartendaten der zuletzt durch den Leser gezogenen Karte ab:
   3.1. Wählen Sie aus dem Ausklappmenü **Select reader (Leser auswählen)** einen Zugangspunkt aus.
   3.2. Ziehen Sie die Karte durch den Leser, der an diesen Zugang angeschlossen ist.
   3.3. Klicken Sie auf **Get last swiped card data from the door's reader(s) (Daten der zuletzt verwendeten Karte vom Leser des Zugangs abrufen)**.
4. Einen Einrichtungscode eingeben. Dieses Feld ist nur verfügbar, wenn Sie **Facility code (Gebäude-Zugangscode)** unter **Access management > Settings (Zugriffsverwaltung > Einstellungen)** aktiviert haben.
5. Legen Sie das Start- und Enddatum für die Zugangsdaten fest.
6. Klicken Sie auf **Hinzufügen**.

Verfallsdatum	
Gültig ab	Legen Sie ein Datum und einen Zeitpunkt für die Gültigkeit der Zugangsdaten fest.
Gültig bis	Wählen Sie eine Option aus dem Drop-Down Menü.

Gültig bis	
Kein Enddatum	Die Zugangsdaten laufen niemals ab.
Datum	Wählen Sie ein Datum und eine Uhrzeit aus, an dem die Zugangsdaten ablaufen.
Von der ersten Verwendung	Wählen Sie aus, wie lange nach der ersten Verwendung die Zugangsdaten ablaufen. Wählen Sie eine Anzahl von Tagen, Monaten, Jahren oder Wiederholungen nach der ersten Verwendung aus.
Von der letzten Verwendung	Wählen Sie aus, wie lange nach der letzten Verwendung die Zugangsdaten ablaufen. Wählen Sie Tage, Monate oder Jahre nach der letzten Verwendung aus.

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 Optimizer hinzu.
2. Legen Sie mithilfe der Funktion **Synchronize with server computer time (Mit Computerzeit des Servers synchronisieren)** Datum und Uhrzeit für die neuen Geräte fest.
3. Aktualisieren Sie die Software der neuen Geräte auf die neueste verfügbare Version.
4. Fügen Sie einen neuen Zugang hinzu, die mit Ihrer Tür-Steuerung verbunden ist. Siehe *Fügen Sie einen Zugang hinzu, on page 77*.
   4.1. Fügen Sie einen Kartenleser hinzu unter **Seite A**. Siehe *Leser hinzufügen, on page 82*.
   4.2. Wählen Sie unter **Türeinstellungen** die Option **AXIS License Plate Verifier** als **Lesertyp** und geben Sie einen Namen für den Leser ein.
   4.3. Fügen Sie optional einen Leser oder ein REX-Gerät auf **Seite B** hinzu.
   4.4. Klicken Sie auf **Ok**.
5. Installieren und aktivieren Sie AXIS License Plate Verifier auf Ihrer Kamera. Siehe das Benutzerhandbuch zu *AXIS License Plate Verifier*.
6. Starten Sie AXIS License Plate Verifier.
7. Konfigurieren Sie AXIS License Plate Verifier.
   7.1. Gehen Sie zu **Konfiguration > Zutrittskontrolle > Verschlüsselte Kommunikation**.
   7.2. Klicken Sie unter **Authentifizierungsschlüssel für externes Peripheriegerät** auf **Authentifizierungsschlüssel anzeigen** und **Schlüssel kopieren**.
   7.3. Öffnen Sie AXIS License Plate Verifier über die Weboberfläche der Kamera.
   7.4. Setup nicht ausführen.
   7.5. **Settings (Einstellungen)** aufrufen.
   7.6. Wählen Sie unter **Zutrittskontrolle** die Option **Sicherer Zugang** as **Typ**.
   7.7. Geben Sie in **IP address (IP-Adresse)** die IP-Adresse für die Tür-Steuerung ein.
   7.8. Fügen Sie in **Authentifizierungsschlüssel** den zuvor kopierten Authentifizierungsschlüssel ein.
   7.9. **Connect (Verbinden)** anklicken.
   7.10. Wählen Sie unter **Door controller name (Tür-Steuerung)** Ihre Tür-Steuerung aus.
   7.11. Wählen Sie unter **Lesername** den Leser aus, den Sie zuvor hinzugefügt haben.
   7.12. Schalten Sie Integration ein.
8. Fügen Sie den Karteninhaber hinzu, dem Sie Zugriff gewähren möchten. Siehe *Karteninhaber hinzufügen, on page 94*.
9. Fügen Sie dem neuen Karteninhaber die Zugangsdaten zum Fahrzeugkennzeichen hinzu. Siehe *Zugangsdaten hinzufügen, on page 95*.
10. Fugen Sie eine Zugangsregel hinzu. Siehe *Fugen Sie eine Zugangsregel hinzu, on page 98*.
    10.1. Einen Zeitplan hinzufügen.
    10.2. Fügen Sie den Karteninhaber hinzu, dem Sie Zugang über das Fahrzeugkennzeichen gewähren möchten.
    10.3. Fügen Sie die Tür dem AXIS License Plate Verifier hinzu.

Gruppe hinzufügen

Gruppen ermöglichen es Ihnen, Karteninhaber und deren Zugangsregeln gemeinsam und effizient zu verwalten.

1. Gehen Sie zu **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Access control (Zutrittskontrolle)** > **Cardholder management (Verwaltung von Karteninhabern)**.
2. Navigieren Sie zu **Groups (Gruppen)** und klicken Sie dann auf **+ Add (+ Hinzufügen)**.
3. Geben Sie einen Namen und optional Initialen für die Gruppe ein.

4. Wählen Sie **Global group (Globale Gruppe)** aus, damit der Karteninhaber auf den Subservern angezeigt und überwacht werden kann. Diese Option ist nur für auf dem Hauptserver erstellte Karteninhaber verfügbar. Siehe *Multiserver BETA, on page 92*.
5. So fügen Sie der Gruppe Karteninhaber hinzu:
   5.1. **+ hinzufügen** anklicken.
   5.2. Wählen Sie die gewünschten Karteninhaber aus und klicken Sie auf **Add (Hinzufügen)**.
6. Klicken Sie auf **Save (Speichern)**.

Fugen 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. Gehen Sie zu **Access control (Zutrittskontrolle)** > **Cardholder management (Karteninhaberverwaltung)**.
2. Klicken Sie unter **Access rule (Zugangsregel)** auf **+ Add (+ Hinzufügen)**.
3. Geben Sie einen Namen für die Regel ein und klicken Sie auf **Next (Weiter)**.
4. Konfigurieren der Karteninhaber und Gruppen:
   4.1. Klicken Sie unter **Cardholders (Karteninhaber)** oder **Groups (Gruppen)** auf **+ Add (+ Hinzufügen)**.
   4.2. Wählen Sie Karteninhaber bzw. Gruppen und klicken Sie auf **Add (Hinzufügen)**.
5. Zugänge und Bereiche konfigurieren:
   5.1. Klicken Sie unter **Doors (Zugänge)** oder **Zones (Zonen)** auf **+ Add (+ Hinzufügen)**.
   5.2. Wählen Sie Zugänge bzw. Zonen und klicken Sie auf **Add (Hinzufügen)**.
6. Konfigurieren der Zeitpläne:
   6.1. Klicken Sie unter **Schedules (Zeitpläne)** auf **+ Add (+ Hinzufügen)**.
   6.2. Wählen Sie einen oder mehrere Zeitpläne aus und klicken Sie auf **Add (Hinzufügen)**.
7. 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.

Zugänge und Zonen manuell entriegeln

Informationen über manuelle Aktionen, wie das manuelle Entsperren eines Zugangs, finden Sie unter *Manuelle Aktionen, on page 87*.

Informationen über manuelle Aktionen, wie das manuelle Entsperren einer Zone, finden Sie unter *Manuelle Aktionen, on page 87*.

Berichte zur Systemkonfiguration exportieren

Sie können Berichte exportieren, die verschiedene Typen von Informationen über das System enthalten. AXIS Optimizer exportiert den Bericht als Datei mit kommagetrennten Werten (CSV) und speichert ihn im Standard-Download-Ordner. So exportieren Sie einen Bericht:

1. Rufen Sie **Reports (Berichte)** > **System configuration (Systemkonfiguration)** auf.
2. Wählen Sie die Berichte aus, die Sie exportieren möchten, und klicken Sie auf **Download**.

Angaben zum Karteninhaber	Dieser Bericht enthält Informationen zu Karteninhabern, Zugangsdaten, Kartenüberprüfung und zur letzten Transaktion.
Zugriff für Karteninhaber	Dieser Bericht enthält die Karteninhaberinformationen und Informationen über die Karteninhabergruppen, Zugangsregeln, Zugänge und Zonen, mit denen der Karteninhaber in Verbindung steht.
Cardholders group access report (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.
Zugriffsregel	Dieser Bericht enthält den Namen der Zugangsregel und Informationen zu den Karteninhabern, Karteninhabergruppen, Zugangsregeln, Zugänge und Zonen, mit denen die Zugangsregel in Verbindung steht.
Zutritt über die Tür	Dieser Bericht enthält den Namen des Zugangs und Informationen zu den Karteninhabern, Karteninhabergruppen, Zugangsregeln und Zonen, mit denen der Zugang in Verbindung steht.
Zonenzugriff	Dieser Bericht enthält den Namen der Zone und Informationen zu den Karteninhabern, Karteninhabergruppen, Zugangsregeln und Zugänge, mit denen die Zone in Verbindung steht.

Berichte über Karteninhaberaktivitäten erstellen

Ein Appellbericht listet die Karteninhaber innerhalb einer bestimmten Zone auf und hilft dabei festzustellen, wer zu einem bestimmten Zeitpunkt anwesend ist.

Ein Musterungsbericht listet Karteninhaber innerhalb einer bestimmten Zone auf und hilft dabei, in Notfällen festzustellen, wer sicher ist und wer vermisst wird. Er unterstützt die Verwaltung von Gebäuden bei der Lokalisierung von Mitarbeitern und Besuchern nach Evakuierungen. Ein Sammelpunkt ist ein ausgewiesener Kartenleser, an dem sich das Personal bei Notfällen meldet und einen Bericht über die Personen am und außerhalb des Standorts erstellt. Das System kennzeichnet Karteninhaber als vermisst, bis sie sich an einem Sammelpunkt melden oder bis jemand sie manuell als sicher kennzeichnet.

Sowohl die Appell- als auch die Musterungsberichte erfordern Zonen zum Tracking der Karteninhaber.

So erstellen Sie einen Appell- oder Musterungsbericht und führen ihn aus:

1. Rufen Sie **Reports (Berichte)** > **Cardholder activity (Karteninhaberaktivitäten)** auf.
2. Klicken Sie auf **+ Add (+ Hinzufügen)** und wählen Sie **Appell / Musterung**.
3. Geben Sie einen Namen für den Bericht ein.
4. Wählen Sie die Zonen aus, die in den Bericht aufgenommen werden sollen.
5. Wählen Sie die Gruppen aus, die Sie in den Bericht aufnehmen möchten.
6. Wenn Sie einen Musterungsbericht wünschen, wählen Sie **Mustering point (Sammelpunkt)** und einen Kartenleser für den Sammelpunkt.

7. Wählen Sie einen Zeitrahmen für den Bericht aus.
8. Klicken Sie auf **Save (Speichern)**.
9. Wählen Sie den Bericht aus und klicken Sie auf **Run (Ausführen)**.

Status des Appellberichts	Beschreibung
Anwesend	Der Karteninhaber hat die angegebene Zone betreten und sie nicht verlassen, bevor Sie den Bericht ausgeführt haben.
Nicht anwesend	Der Karteninhaber hat die angegebene Zone verlassen und sie nicht betreten, bevor Sie den Bericht ausgeführt haben.

Status des Musterungsberichts	Beschreibung
Sicher	Der Karteninhaber hat seine Karte am Sammelpunkt benutzt.
Fehlt	Der Karteninhaber hat seine Karte am Sammelpunkt nicht benutzt.

Zugriffsverwaltungseinstellungen

So passen Sie die Karteninhaberfelder an, die im Zugriffsverwaltungsdashboard verwendet werden:

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Settings (Einstellungen)** > **Custom cardholder fields (Benutzerdefinierte Karteninhaberfelder)**.
2. **+ Add (+ Hinzufügen)** anklicken und eine Bezeichnung eingeben. Sie können bis zu 6 benutzerdefinierte Felder hinzufügen.
3. Klicken Sie auf **Hinzufügen**.

So aktivieren Sie die Verwendung eines Gebäude-Zugangscodes, um Ihr Zutrittssystem zu überprüfen:

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Settings (Einstellungen)** > **Facility code (Gebäude-Zugangscode)**.
2. Wählen Sie **Facility code on (Gebäude-Zugangscode ein)** aus.

Hinweis

Sie müssen beim Konfigurieren von Identifizierungsprofilen außerdem die Option **Include facility code for card validation (Gebäude-Zugangscode in Kartenprüfung einbeziehen)** auswählen. Siehe .

Import und Export

Karteninhaber importieren

Über diese Option können Karteninhaber, Karteninhabergruppen, Zugangsdaten und Bilder von Karteninhabern aus einer CSV-Datei importiert werden. Stellen Sie zum Importieren von Bildern von Karteninhaber sicher, dass der Server Zugriff auf die Bilder hat.

Beim Importieren von Karteninhabern speichert das Zugangsverwaltungssystem automatisch die Systemkonfiguration inklusive sämtlicher Hardwarekonfiguration und löscht alle zuvor gespeicherten.

Optionen importieren	
Neu	Diese Option entfernt vorhandene Karteninhaber und fügt neue Karteninhaber hinzu.
Aktualisieren	Über diese Option werden vorhandene Karteninhaber aktualisiert und neue Karteninhaber hinzugefügt.
Hinzufügen	Diese Option behält vorhandene Karteninhaber bei und fügt neue Karteninhaber hinzu. Kartennummern und Karteninhaber-IDs sind eindeutig und können nur einmal verwendet werden.

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Import and export (Import und Export)**.
2. Klicken Sie auf **Import cardholders (Karteninhaber importieren)**.
3. Wählen Sie **Neu**, **Aktualisieren** oder **Hinzufügen**.
4. Klicken Sie auf **Next (Weiter)**.
5. Klicken Sie auf **Choose a file (Wählen Sie eine Datei)** und rufen Sie die CSV-Datei auf. **Öffnen** anklicken.
6. Geben Sie ein Spaltentrennzeichen ein, wählen Sie einen eindeutigen Bezeichner aus und klicken Sie auf **Next (Weiter)**.
7. Weisen Sie jeder Spalte eine Überschrift zu.
8. Klicken Sie auf **Importieren**.

Einstellungen importieren	
Erste Zeile ist Kopfzeile	Wählen Sie aus, ob die CSV-Datei eine Spaltenüberschrift enthält.
Spaltentrennzeichen	Geben Sie ein Spaltentrennformat für die CSV-Datei ein.
Eindeutiger Bezeichner	Das System identifiziert standardmäßig einen Karteninhaber mit der **Cardholder ID (Karteninhaber-ID)**. Alternativ können Sie dazu den Vor- und Nachnamen oder die E-Mail-Adresse verwenden. Mit der eindeutigen Kennung wird der Import doppelter Personalaufzeichnungen verhindert.
Format der Kartennummer	In der Standardeinstellung ist **Allow both hexadecimal and number (Hexadezimal und Zahl zulassen)** ausgewählt.

Karteninhaber exportieren

Diese Option exportiert die Daten des Karteninhabers im System in eine CSV-Datei.

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Import and export (Import und Export)**.
2. Klicken Sie auf **Export cardholders (Karteninhaber exportieren)**.
3. Wählen Sie einen Download-Speicherort und klicken Sie auf **Save (Speichern)**.

AXIS Optimizer aktualisiert die Karteninhaberfotos in `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos`, wenn die Konfiguration geändert wird.

Import rückgängig machen

Beim Import von Karteninhabern wird die Konfiguration des Systems automatisch gespeichert. Über **Undo import (Import rückgängig machen)** werden die Daten des Karteninhabers und die Hardwarekonfiguration auf die Voreinstellungen vor dem letzten Import des Karteninhabers zurückgesetzt.

1. Klicken Sie auf der Registerkarte **Access management (Zugriffsverwaltung)** auf **Import and export (Import und Export)**.
2. Klicken Sie auf **Undo import (Import rückgängig machen)**.
3. **Yes (Ja)** anklicken

Sichern und Wiederherstellen

Jede Nacht werden automatische Datensicherungen durchgeführt. Die drei neuesten Sicherungsdateien werden unter C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\backup gespeichert. Zur Wiederherstellung dieser Dateien:

1. Verschieben Sie die Sicherungsdatei nach C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\restore.
2. Starten Sie AXIS Secure Entry mit einer der folgenden Methoden neu:
   - Starten Sie das MSC-Programm (Dienste), suchen Sie „AXIS Optimizer Secure Entry Service" und starten Sie neu.
   - Starten Sie Ihren Computer neu.
3. Führen Sie das Installationsprogramm für den AXIS Optimizer auf dem Rechner des Ereignis-Servers erneut aus.

Zutrittsverwaltung in Smart Client

Über den Smart Client können Bediener Vorgänge im Zusammenhang mit Ihrem Zutrittssystem ausführen. Die meisten Funktionen der Zutrittskontrolle, wie beispielsweise die manuelle Tür-Steuerung, sind im Smart Client verfügbar. Weitere Informationen zu diesen Funktionen finden Sie unter *Verwendung der Zutrittskontrolle in Smart Client*.

Sie können die Zugriffsrechte auch direkt im Smart Client verwalten. Die folgenden Funktionen, die im Client für die Verwaltung enthalten sind, stehen auch im Smart Client zur Verfügung:

- Karteninhaberverwaltung
- Allgemeine Einstellungen
- Benutzerdefinierte Felder für Karteninhaber
- Einrichtungscode
- E-Mail-Vorlagen
- Ausweisvorlagen BETA

So zeigen Sie die Registerkarte „Axis Zutrittsverwaltung" im SMART Client an:

1. Installieren Sie AXIS Optimizer auf dem Smart-Client-Rechner.
2. Aktivieren Sie eine Zugangslizenz, falls noch keine aktiviert wurde. Informationen zur Aktivierung einer Zugangslizenz finden Sie unter *Zugangslizenzen aktivieren, on page 74*.
3. Stellen Sie sicher, dass der angemeldete Benutzer über Zutrittsverwaltungsberechtigungen verfügt; siehe *Einstellungen für die Rolle „AXIS Secure Entry", on page 102*.

Einstellungen für die Rolle „AXIS Secure Entry"

1. Wechseln Sie im Management Client zu **Site Navigation** > **Security** > **Roles** (Standortnavigation > Sicherheit > Rollen).

2. Wählen Sie eine bestimmte Rolle im System aus.
3. Wählen Sie **AXIS Optimizer**.
4. Erweitern Sie die Liste und klicken Sie auf **Access control (Zutrittskontrolle)**.
5. Wählen Sie **Read (Lesen)**, um die Sicherheitseinstellungen für die Zutrittskontrolle aufzurufen.
6. Klicken Sie auf die Funktion, für die die Rolle eine Berechtigung erhalten soll, und wählen Sie **Grant (Zuweisen)**.
   - **Access control configuration (Zutrittskontrollkonfiguration):** Dadurch erhält die Rolle „Operator" Bediener) Zugriff auf alle Funktionen auf der Registerkarte „Configuration" (Konfiguration).
   - **Access management (Zutrittsverwaltung):** Dadurch erhält die Rolle „Operator" (Bediener) Zugriff auf alle Funktionen auf der Registerkarte „Access Management" (Zutrittsverwaltung).

Systemverwaltung und Sicherheitskontrollen

Anpassen des Funktionszugriffs für Bediener

Rolleneinstellungen

Voreingestellt hat ein Bediener Zugriff auf alle Funktionen von AXIS Optimizer im Smart Client, wenn er auch im VMS Zugriff auf das Gerät hat. Im Management Client kann jedoch über Role Settings (Rolleneinstellungen) konfiguriert werden, auf welche Funktionen ein Bediener Zugriff hat.

Rolleneinstellungen konfigurieren

Aktivieren Sie **Role settings (Rolleneinstellungen)**:

1. Wechseln Sie im Management Client zu **Site Navigation > Security > AXIS Optimizer Security (Standortnavigation > Sicherheit > AXIS Optimizer Security)**.

Hinweis

Sie können die Rolleneinstellungen nicht mehr deaktivieren, sobald Sie sie aktiviert haben. Die Einstellung ist permanent.

2. Wählen Sie **Turn on role settings (Rolleneinstellungen aktivieren)**.
3. Starten Sie den Management Client neu.

Konfigurieren Sie unter **Role settings** die Rolleneinstellungen:

1. Wechseln Sie im Management Client zu **Site Navigation > Security > Roles (Standortnavigation > Sicherheit > Rollen)**.
2. Wählen Sie eine Rolle aus, und wechseln Sie zu **Overall security (Gesamtsicherheit)**.
3. Klicken Sie auf **AXIS Optimizer Security**.
4. Wählen Sie aus, auf welche Funktionen die Rolle zugreifen darf oder nicht.
   - **Full control (Volle Kontrolle)**Gibt dem Bediener den vollen Zugriff auf alle Funktionen des AXIS Optimizer.
   - **Edit (not applicable) (Bearbeiten (nicht zutreffend))**Eine VMS-Funktion, die nicht auf die Rolleneinstellungen von AXIS Optimizer anwendbar ist.
   - **Auf AXIS Optimizer im Management-Client zugreifen**Die Bedienerrolle kann alle Verwaltungsfunktionen von AXIS Optimizer im Management Client nutzen.
   - **Sicherheit von AXIS Optimizer verwalten**Die Bedienerrolle kann die Einstellungen in **Site Navigation (Standortnavigation) > Security (Sicherheit) > AXIS Optimizer Security** ändern.
   - **Steuerungen von dynamischen Kameras durch einen Bediener**Die Bedienerrolle hat Zugriff auf alle vorinstallierten Funktionen, die das System auf einem Gerät findet.
   - **Steuerung des fernsteuerbaren Fokus durch einen Bediener**Die Bedienerrolle kann den Fernfokus für Fixed-Dome-Kameras festlegen.
   - **PTZ operator controls (PTZ-Bedienelemente)**Die Bedienerrolle erhält Zugriff auf bestimmte PTZ-Bedienelemente: Fokussteuerung, PTZ-Voreinstellungen, Bedienelemente für Autotracking 2, Waschen und SpeedDry/Wischer-Taste.
   - **Temperature spot measurement control (Punktbasierte Temperaturmessung)**Die Bedienerrolle kann die Punkttemperatur der AXIS Q2901-E messen.
   - **Steuerung der Lautsprecher durch einen Bediener**Die Bedienerrolle erhält im Smart Client Zugriff auf alle Funktionen des Lautsprecher-Managers.
   - **Access visitor management (Zugang zur Besucherverwaltung)**Die Bedienerrolle erhält Zugriff auf alle mit der Besucherverwaltung verknüpften Informationen, z. B. Anrufannahme und Öffnen einer Tür in der Live-Ansicht.

- **Access call history (Zugriff auf Anrufverlauf)**Die Bedienerrolle kann auf den Anrufverlauf einer IP-Türsprechanlage zugreifen. Um diese Einstellungen zu nutzen, müssen Sie den **Access visitor management (Zugriff auf die Besucherverwaltung)** erlauben.
- **Erweiterte Suchfunktionen**Bei Auswahl von **„Deny"** wird im Smart Client die Registrierkarte „AXIS License Plate Verifier" ausgeblendet. Außerdem können Sie bei der zentralisierten Suche nicht die Suche nach Fahrzeugen und Containern verwenden.
- **Steuerung der Entzerrungsansicht**Die Bedienerrolle kann sich in den Entzerrungsansichten bewegen.
- **Home-Position einer Entzerrungsansicht bearbeiten**Die Bedienerrolle kann die Home-Position einer Kamera bearbeiten.
- **Webseite**Die Bedienerrolle kann eine Ansicht mit einem Web-Browser erstellen.
- **Dashboard für Axis Insights**
  Die Bedienerrolle erhält Zugriff auf das Axis Insights-Dashboard.

5. Klicken Sie auf **Save (Speichern)**.
6. Starten Sie alle ausgeführten Smart Clients in Ihrem Systems neu.

Geräteverwaltung

AXIS Device Manager Extend

Mit AXIS Optimizer können Sie mithilfe von AXIS Device Manager Extend Geräte an mehreren Standorten verwalten. Durch das Einrichten von Edge-Hosts auf Aufzeichnungsservern kann sich AXIS Device Manager Extend mit Ihren Geräten im VMS verbinden. Dadurch lassen sich über eine einzige Benutzeroberfläche Informationen zur Gewährleistung einfach überprüfen und auf mehreren Geräten und an mehreren Standorten die Software aktualisieren.

Weitere Informationen zu AXIS Device Manager Extend finden Sie im *Benutzerhandbuch*.

Hinweis

Anforderungen

- Melden Sie sich in Ihrem *MyAxis-Konto* an.
- Die Aufzeichnungsserver müssen über einen Internetzugang verfügen.
- Wird nur bei Geräten mit AXIS OS 6.50 unterstützt. Weitere Informationen zu den unterstützten Geräten finden Sie in den *häufig gestellten Fragen (FAQ)*.

Edge-Host installieren

Der Edge-Host ist ein am Standort verwalteter Dienst, über den AXIS Device Manager Extend mit Ihren lokalen Geräten im VMS kommunizieren kann.

Der Edge-Host und der Desktop-Client müssen installiert werden, damit AXIS Device Manager Extend im VMS verwendet werden kann. Sowohl der Edge-Host als auch der Desktop-Client sind im Installationsprogramm des AXIS Device Manager Extend enthalten.

1. Laden Sie den *Installationsassistenten* von AXIS Device Manager Extend herunter.
   Der Edge-Host muss auf den Aufzeichnungsservern vom VMS installiert werden.
2. Führen Sie das Installationsprogramm auf dem Aufzeichnungsserver aus und installieren Sie nur den Edge-Host.

Weitere Informationen zu offenen Netzwerkports und anderen Voraussetzungen finden Sie im *Benutzerhandbuch zu Axis Device Manager Extend*.

Den Edge-Host beanspruchen und Geräte synchronisieren



1. Öffnen Sie den Management Client.
2. Gehen Sie zu **Standortnavigation > AXIS Optimizer > Systemübersicht**.
3. Wählen Sie und melden Sie sich bei MyAxis an.
4. Klicken Sie auf eine Kachel mit einem Aufzeichnungsserver mit installiertem Edge-Host, der bereit ist, beansprucht zu werden.
5. Erstellen auf der Seitenleiste eine neue Organisation oder wählen Sie eine zuvor erstellte Organisation.
6. Klicken Sie auf den Edge Host und beanspruchen Sie diesen.
7. Warten Sie, bis die Seite neu geladen wurde, und klicken Sie auf **Synchronisieren**.
   Alle Axis Geräte auf dem Aufzeichnungsserver werden nun dem Edge-Host hinzugefügt und gehören der von Ihnen ausgewählten Organisation an.

Hinweis

AXIS Device Manager Extend muss auf die Axis Hardware im VMS zugreifen können. Weitere Informationen zu unterstützten Geräten finden Sie unter *Fehlerbehebung beim Hinzufügen von Geräten zum Edge-Host, on page 107*.

8. Wenn Sie einem Aufzeichnungsserver neue Geräte hinzufügen oder Geräteinformationen ändern, müssen Sie zum Synchronisieren der Änderungen mit dem AXIS Device Manager Extend Schritt 7 erneut durchführen.
9. Wiederholen Sie die Schritte 4 bis 7 für alle Aufzeichnungsserver mit Geräten, die Sie zum hinzufügen AXIS Device Manager Extend.

Edge-Host-Status

In der **Systemübersicht** wird für jeden Aufzeichnungsserver angezeigt, ob der Edge-Host bereits installiert oder beansprucht wurde. Sie können zum Filtern der Ansicht die Option **Geräte anzeigen, für die eine Edge-Host-Aktion erforderlich ist** aktivieren.

- – Auf dem Aufzeichnungsserver wurde kein Edge-Host erkannt.
  - Wenn kein Edge-Host installiert wurde, laden Sie den Edge-Host herunter und installieren Sie diesen auf dem Aufzeichnungsserver. Siehe *Edge-Host installieren, on page 105*.
  - Wenn Edge-Host installiert ist, müssen Sie sich beim MyAxis-Konto anmelden, um den Edge-Host erkennen zu können.
- – Der Edge-Host wurde installiert, aber nicht beansprucht. Beanspruchen Sie den Edge-Host, indem Sie eine neue Organisation erstellen oder eine zuvor erstellte Organisation wählen. Siehe *Den Edge-Host beanspruchen und Geräte synchronisieren, on page 106*.
- – Der Edge-Host wurde installiert und beansprucht, ist aber nicht erreichbar. Überprüfen Sie, ob der Aufzeichnungsserver über einen Internetzugang verfügt.
- – Der Edge-Host wird synchronisiert.

-  – Der Edge-Host muss synchronisiert werden. Möglicherweise wurden dem Edge-Host neue Geräte in der VMS hinzugefügt oder Geräteinformationen aktualisiert, die synchronisiert werden müssen.

Konfiguration von Geräten mithilfe von AXIS Device Manager Extend

Nach der Synchronisierung der Geräte mit dem Edge-Host können die Geräte in AXIS Device Manager Extend konfiguriert werden. Dazu können Sie jeden mit dem Internet verbundenen PC nutzen.

Hinweis

Wenn Sie auch Geräte über eine Remote-Verbindung verwalten möchten, müssen Sie den *Fernzugriff auf jedem Edge-Host aktivieren*.

1. Installieren und öffnen Sie die *Desktop-Anwendung von AXIS Device Manager Extend*.
2. Wählen Sie die Organisation, die für die Beanspruchung des Edge-Hosts verwendet wurde.
3. Die synchronisierten Geräte finden Sie unter einem Standort mit demselben Namen wie der des VMS-Aufzeichnungsservers.

Fehlerbehebung beim Hinzufügen von Geräten zum Edge-Host

Wenn Sie Probleme beim Hinzufügen von Geräten zum Edge-Host haben, gehen Sie wie folgt vor:

- AXIS Optimizer fügt das VMS nur aktivierte Hardware hinzu.
- Stellen Sie sicher, dass die Verbindung mit der Hardware in VMS nicht beschädigt ist.
- Stellen Sie sicher, dass das Gerät über AXIS OS 6.50 oder höher verfügt.
- Stellen Sie sicher, dass das Gerät auf Digest-Authentifizierung eingestellt ist. AXIS Device Management unterstützt standardmäßig keine Basisauthentifizierung.
- Versuchen Sie, Geräte direkt aus der Anwendung AXIS Device Manager Extend hinzuzufügen.
- Erfassen Sie Protokolle von AXIS Device Manager Extend und wenden Sie sich an den Axis Support.
  1. Gehen Sie auf dem Aufzeichnungsserver, auf dem die Kamera installiert ist, in die Anwendung AXIS Device Manager Extend zu dem spezifischen Standort.
  2. Gehen Sie auf **Einstellungen** und klicken Sie auf **Standortprotokoll herunterladen**.

AXIS Site Designer Import

In AXIS Optimizer können Sie Ihr AXIS Site Designer Designprojekt importieren und die Konfiguration in einem einfachen Importvorgang auf Ihr VMS anwenden. Verwenden Sie *AXIS Site Designer*, um Ihr System zu entwerfen und zu konfigurieren. Sobald Ihr Projekt fertiggestellt ist, können Sie die Einstellungen für alle Kameras und andere Geräte aus AXIS Site Designer mit AXIS Optimizer in Management Client importieren.

Weitere Informationen zu AXIS Site Designer finden Sie im *Benutzerhandbuch*.

Hinweis

Anforderungen

- VMS-Version 2020 R2 oder höher

Designprojekt importieren



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

In AXIS Site Designer

1. Erstellen Sie ein Projekt und konfigurieren Sie die Geräte.
2. Erstellen Sie nach Abschluss des Projekts einen Code oder laden Sie die Einstellungsdatei herunter.

Hinweis

Wenn Sie Aktualisierungen an Ihrem Designprojekt vornehmen, müssen Sie einen neuen Code erstellen oder eine neue Einstellungsdatei herunterladen.

In Management Client

1. Stellen Sie sicher, dass relevante Geräte zu Ihrer VMS hinzugefügt werden.
2. Wechseln Sie zu **Site Navigation > AXIS Optimizer > Import design project (Standortnavigation > AXIS Optimizer > Designprojekt importieren)**.
3. Es wird eine Schritt-für-Schritt-Anleitung geöffnet. Wählen Sie das zu importierende Projekt aus, indem Sie entweder den Zugangscode eingeben oder die Einstellungsdatei des Projekts wählen. Klicken Sie auf **Next (Weiter)**.
4. In **Project overview (Projektübersicht)** finden Sie Informationen darüber, wie viele Geräte im AXIS Site Designer-Projekt und wie viele Geräte im VMS gefunden werden. Klicken Sie auf **Next (Weiter)**.
5. Im nächsten Schritt werden die Geräte der VMS den Geräten des AXIS Site Designer zugeordnet. Geräte mit nur einer möglichen Zuordnung werden automatisch ausgewählt. Es werden nur Geräte importiert, die zugeordnet sind. Wenn Sie mit der Zuordnung fertig sind, klicken Sie auf **Next (Weiter)**.
6. Die Einstellungen für alle zugeordneten Geräte werden importiert und auf Ihre VMS angewendet. Dies kann je nach Größe des Designprojekts mehrere Minuten dauern. Klicken Sie auf **Next (Weiter)**.
7. In **Results of import (Importergebnissen)** finden Sie Details zu den verschiedenen Schritten des Importvorgangs. Wenn manche Einstellungen nicht importiert werden konnten, beheben Sie die Probleme und führen Sie den Import erneut aus. Klicken Sie auf **Export... (Exportieren...)**, wenn Sie die Ergebnisliste als Datei speichern möchten. Klicken Sie auf **Done (Fertig)**, um die Schritt-für-Schritt-Anleitung zu schließen.

Importierte Einstellungen

Nur Geräte, die mit der VMS und dem Designprojekt übereinstimmen, sind Teil des Imports. Die folgenden Einstellungen werden importiert und für alle Gerätetypen auf die VMS angewendet:

- Beim Designprojekt verwendeter Gerätename
- Beim Designprojekt verwendete Gerätebeschreibung
- Einstellungen für Geolocation, wenn das Gerät auf einem Lageplan platziert ist

Wenn es sich um ein videofähiges Gerät handelt, werden auch die folgenden Einstellungen angewendet:

- Ein oder zwei in der VMS konfigurierte Videostreams (Auflösung, Bildrate, Codec, Komprimierung und Zipstream-Einstellungen)
  - Videostream 1 ist für die Live-Ansicht und Aufzeichnung konfiguriert.
  - Videostream 2 ist für die Aufzeichnung konfiguriert, wenn sich die Videostreameinstellungen des Designprojekts zwischen Live-Ansicht und Aufzeichnung unterscheiden.
- Regeln für die Bewegungserkennung oder kontinuierliche Aufzeichnung werden gemäß dem Designprojekt eingerichtet. Die integrierte Bewegungserkennung des VMS wird verwendet, Zeitprofile für die Regeln werden erstellt und auf den Aufzeichnungsservern werden Speicherprofile für verschiedene Aufbewahrungszeiten erstellt.
- Das Mikrofon ist gemäß den Audioeinstellungen des Designprojekts ein- oder ausgeschaltet.

Einschränkungen

Es gibt Einschränkungen im VMS, wenn es um den Import von AXIS Site Designer Designprojekten geht.

- Die Standardregel für Bewegungsaufzeichnungen im VMS kann die durch den Import erstellten Aufzeichnungsregeln außer Kraft setzen. Widersprüchliche Regeln deaktivieren oder betroffene Geräte von den Regeln ausschließen.
- Aufzeichnungsschätzungen können für durch Bewegung ausgelösten Aufzeichnungen des VMS ungenau sein.
- Grundrisse werden in der aktuellen Version nicht unterstützt.
- Wenn sowohl bewegungsgesteuerte Aufzeichnungen als auch kontinuierliche Aufzeichnungen gleichzeitig im Designprojekt konfiguriert sind, werden nur die Stream-Einstellungen der bewegungsgesteuerten Aufzeichnungseinstellungen verwendet.
- Sie können im VMS keine Mindestbildrate für Zipstream konfigurieren.

Kontenverwaltung

Mit der Kontoverwaltung können Sie die Konten und Kennwörter auf allen von XProtect verwendeten Axis Geräten verwalten.

Gemäß den Axis Richtlinien sollten Sie kein Root-Konto verwenden, um eine Verbindung zu Geräten herzustellen. Mit der Kontoverwaltung können Sie ein XProtect-Dienstkonto erstellen. Für jedes Gerät werden eindeutige 16-stellige Kennwörter erstellt. Geräte, die bereits über das XProtect-Konto verfügen, erhalten neue Kennwörter.

Herstellung einer Verbindung zu Geräten mit dem XProtect-Dienstkonto

1. Rufen Sie **Site Navigation > AXIS Optimizer > Account management (Standortnavigation > Axis Optimizer > Kontenverwaltung)** auf.
   Die Grafik zeigt, wie viele Geräte online sind, wie viele davon über das XProtect-Dienstkonto verfügen und wie viele nicht über das XProtect-Dienstkonto verfügen.
2. Klicken Sie auf **Show device details (Gerätedetails anzeigen)**, um weitere Informationen zu den Geräten anzuzeigen. Geräte, die online sind, werden oben in der Liste angezeigt. Sie können bestimmte Geräte auswählen, für die Kennwörter generiert werden sollen. Wenn keine ausgewählt sind, erhalten alle Geräte, die online sind, neue Kennwörter. Klicken Sie auf **OK**.

Hinweis

Kennwörter werden im Klartext zwischen dem Aufzeichnungsserver und dem Axis Gerät gesendet, wenn Sie in der Hardwarekonfiguration HTTP auswählen. Wir empfehlen Ihnen, HTTPS einzustellen, um die Kommunikation zwischen dem VMS und Ihrem Gerät zu sichern.

3. Klicken Sie auf **Generate passwords (Kennwörter erstellen)**. Das generierte Kennwort enthält einen zufälligen Text aus 16 ASCII-Zeichen, der zwischen 32 und 126 liegt.
   Klicken Sie auf **Show device details (Gerätedetails anzeigen)**, um Live-Statusaktualisierungen des Prozesses anzuzeigen. Während des Vorgangs sehen Sie eine kurze Unterbrechung der aktiven Live-Ansichten und ausstehenden Aufzeichnungen.
4. Geräte, die online sind, erhalten das XProtect-Dienstkonto und neue Kennwörter. Geräte, die online sind und bereits über das XProtect-Dienstkonto verfügen, erhalten nur neue Kennwörter.

Axis Ereignisse

Die Ereignisfunktion von Axis bietet eine Übersicht über die verfügbaren Ereignisse für Axis Geräte in Ihrem VMS. Sie können Ereignisse auf einem bestimmten Gerät testen, Details zu den Ereignissen anzeigen und Ereignissen zu mehreren Geräten hinzufügen.

Unter **Site Navigation (Standortnavigation)** rufen Sie **Rules and Events > Axis events (Regeln und Ereignisse > Axis Ereignisse)** auf. Im Fenster **Configuration (Konfiguration)** wird eine Liste aller verfügbaren Ereignisse angezeigt. Sie können erkennen, welche Ereignisse in Ihrem System aktiv sind und welche nicht.

Für jedes Ereignis wird der Name der Geräte angezeigt, zu denen das Ereignis hinzugefügt wurde. Außerdem werden der Ereignisanzeigename, der Status des Ereignisses und der letzte Zeitpunkt angezeigt, an dem das Ereignis ausgelöst wurde.

Hinweis

Anforderungen

- VMS-Version 2023 R2 oder höher.

Ein Ereignis für mehrere Geräte einrichten

1. Rufen Sie **Configuration (Konfiguration)** auf und wählen Sie ein Ereignis aus.
2. Klicken Sie auf **Add devices** .
3. Das Fenster **Add devices (Geräte hinzufügen)** zeigt eine Liste der Geräte an, zu denen das Ereignis hinzugefügt werden kann. Wählen Sie eines oder mehrere dieser Geräte aus und klicken Sie auf **Add devices (Geräte hinzufügen)**.

Um ein Ereignis von einem Gerät zu entfernen, klicken Sie auf **Remove (Entfernen)**.

Informationen zu Ereignissen

In Axis Ereignissen können Sie das letzte bekannte Auftreten, den Status von Ereignissen sowie Echtzeitaktualisierungen auf der Benutzeroberfläche anzeigen. Hierfür müssen Sie im Management Client die Vorhaltezeit festlegen.

1. Rufen Sie **Tools > Options > Alarm and Events > Event retention (Tools > Optionen > Alarm und Ereignisse > Ereignisaufbewahrung)** auf.
2. Legen Sie die Vorhaltezeit für die gesamte Ereignisgruppe des Geräts oder für bestimmte Ereignisse in der Gruppe fest.

Metadaten und Suche

Metadaten und die Suche geben eine Übersicht über alle Geräte, die Sie im VMS hinzugefügt haben, über deren Metadaten-Funktionen und die Axis Suchkategorien, die für Ihre Bediener sichtbar sind.

Metadaten und die Suche ermöglichen das Einschalten bestimmter Funktionen für diese Geräte. Sie können also Ereignisdaten, Analysedaten und zusammengeführte Daten für mehrere Geräte aktivieren und auch die von Ihren Geräten unterstützten Analysefunktionen anzeigen. Mit Axis Suchkategorien können Sie die Suchoptionen für alle Bediener steuern, um die verfügbaren Analysefunktionen in Ihrem VMS wiederzugeben. Die Unterstützung für Suchkategorien und Filter unterscheidet sich je nach Kameramodell und installierter Analyseanwendung.

Einstellungen für die Metadaten konfigurieren

1. Rufen Sie **Management Client** > **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Metadata and search (Metadaten und Suche)** auf.
   - **Ereignisdaten**: Schalten Sie das VMS ein, um Ereignisdaten vom Gerät abzurufen. Dies ist für mehrere Funktionen von AXIS Optimizer erforderlich.
   - **Analysedaten**: Schalten Sie diese Funktion ein, um die forensische Suche zu verwenden und in der Live-Ansicht und der Wiedergabe Umgrenzungsfelder anzuzeigen.
   - **Analytics features (Analysefunktionen)**: Zeigen Sie die Videoanalysefunktionen an, die Ihr Gerät derzeit unterstützt, z. B. den Objekttyp (Personen, Fahrzeuge) und die Objektfarbe. Durch das Aktualisieren der Gerätesoftware können weitere Analysefunktionen verfügbar werden.
   - **Consolidated metadata (Zusammengeführte Metadaten)**: Schalten Sie diese Funktion ein, um eine schnellere forensische Suche durchzuführen und die Ladezeiten in Axis Insights zu verkürzen.

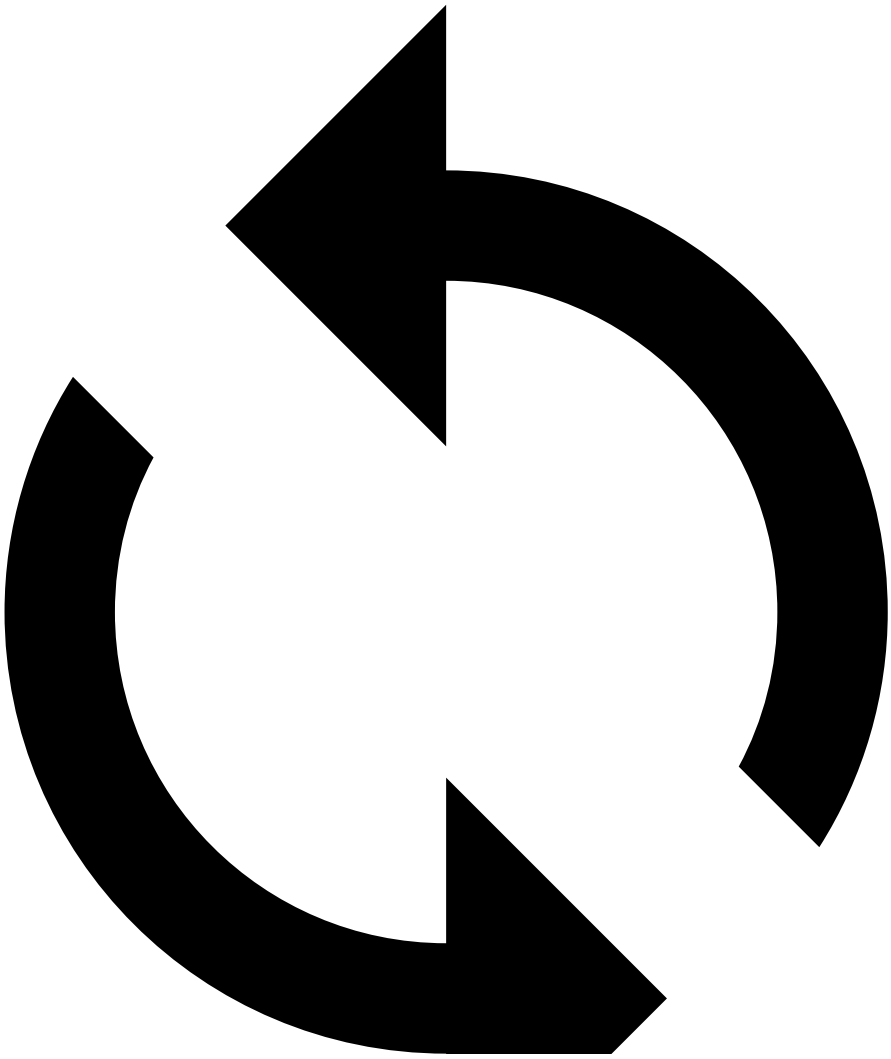
Hinweis

Anforderungen für zusammengeführte Metadaten

- Axis Geräte mit Versionen von AXIS OS 11.10 oder höher.

Einschränkungen für zusammengeführte Metadaten

- Umgrenzungsfelder in der Live-Ansicht und der Aufzeichnerung und die VMS-integrierten Suchoptionen sind nicht verfügbar.

– 
: Klicken Sie hier, um die Konfiguration Ihres Geräts neu zu laden, wenn Sie Änderungen daran vornehmen.

Axis Suchkategorien konfigurieren

1. Rufen Sie **Management Client** > **Site Navigation (Standortnavigation)** > **AXIS Optimizer** > **Metadata and search (Metadaten und Suche)** auf.
2. Aktivieren Sie die zu verwendenden Suchkategorien im Dialogfeld **Axis search categories (Axis Suchkategorien)**:
   - Forensische Suche
   - Fahrzeugsuche
   - Suche nach Geschwindigkeit im Bereich
   - Containersuche
3. Wählen Sie in jeder Suchkategorie anwendbare Filter aus.

Hinweis

Anforderungen an Axis Suchkategorien

- AXIS Optimizer Version 5.3 oder höher im SMART Client.

Cybersicherheit

Cybersicherheit trägt zu einem erfolgreichen Produktlebenszyklus bei, bei dem Risiken auf ein Minimum reduziert werden. Ausführliche Informationen und Dokumente zu unserer Cybersicherheitsstrategie finden Sie auf *axis.com/about-axis/cybersecurity*. Befolgen Sie die nachstehenden Richtlinien zur Cybersicherheit, um Sicherheitsbenachrichtigungen von Axis zu erhalten und Ihr Produkt für eine sichere Benutzung und Außerbetriebnahme zu konfigurieren.

Unter *Axis Trust Center* finden Sie Informationen darüber, wie Axis die Einhaltung von Sicherheitsvorschriften, Transparenz, Datenschutz und den Schutz der Privatsphäre implementiert.

Schwachstellen-Management

Axis ist eine *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)*. Um das Risiko einer Gefährdung für Sie so gering wie möglich zu halten, halten wir uns bei der Erkennung und Behebung von Sicherheitslücken in unseren Geräten, unserer Software und unseren Diensten an die Branchenstandards. Weitere Informationen zu unseren Richtlinien zur Verwaltung von Sicherheitslücken oder zur Meldung einer Schwachstelle finden Sie unter *axis.com/vulnerability-management*.

Sicherheitsbenachrichtigungen

Sicherheitsbenachrichtigungs-E-Mails von Axis können Sie auf *axis.com/security-notification-service* abonnieren. Wir informieren Sie über Schwachstellen, geben entsprechende Sicherheitshinweise und benachrichtigen Sie zu anderen sicherheitsrelevanten Themen für Ihr Axis Produkt.

Sicherer Produktlebenszyklus

Axis minimiert Risiken über die gesamte Lebensdauer unserer Produkte hinweg durch eine sichere Verwaltung des Lebenszyklus. Nutzen Sie unsere Sicherheitsrichtlinien unter *help.axis.com*, um Ihre Axis Produkte sicherer zu konfigurieren und zum Betrieb zu nutzen und um Informationen zu folgenden Themen zu erhalten:

Sichere Erstnutzung – Axis Produkte sind standardmäßig mit einem hohen Sicherheitsniveau in der Konfiguration vorkonfiguriert, um von Anfang an eine sichere Inbetriebnahme und verschlüsselte Kommunikation zu gewährleisten.

Bestimmungsgemäßer Gebrauch und häufige Fehler bei der Konfiguration – Unsere Anleitungen enthalten Informationen zur bestimmungsgemäßen Verwendung von Axis Produkten, einschließlich häufiger sicherheitsrelevanter Fehlbedienungen und Fehler bei der Konfiguration, die vermieden werden sollten.

Sicherheitslücken und Transparenz in der Lieferkette verwalten – Mit jeder Softwareversion wird auf *axis.com* eine Software-Bestellliste (SBOM) veröffentlicht, um Sicherheitslücken offenzulegen und die Transparenz in der Lieferkette zu verbessern.

Stilllegung und die sichere Löschung von Daten – Um ein Produkt am Ende seines Lebenszyklus sicher außer Betrieb zu nehmen, setzen Sie es auf die Werkseinstellungen zurück. Dadurch werden Ihre Konfigurationen, gespeicherten Daten und vertraulichen Informationen gelöscht.

Hardening Guide

Als integraler Bestandteil Ihrer VMS-Infrastruktur erfordert AXIS Optimizer bestimmte Konfigurationen, um eine sichere Umgebung zu gewährleisten. Die Verwendung dieser empfohlenen Einstellungen ist zum Schutz Ihrer Gerätekennwörter und privaten Daten sowie zur Vermeidung eines unbefugten Zugriffs auf Ihr System unerlässlich.

- Verwenden Sie zum Hinzufügen von Geräten zu Ihrem VMS immer HTTPS.
- Aktivieren Sie die Verschlüsselung zwischen den Clients und Servern des VMS.
- Aktivieren Sie die verschlüsselte Speicherung im VMS.
- Prüfen Sie alle VMS-Rollen und stellen Sie sicher, dass diese ausschließlich die unbedingt erforderlichen Berechtigungen besitzen.

Benötigen Sie Hilfe?

FAQ

Frage	Antwort
Wie aktualisiere ich AXIS Optimizer, wenn der Client-PC keinen Internetzugang hat?	Veröffentlichen Sie die neue Version auf dem VMS Management-Server (siehe *Automatisches Aktualisieren des Systems, on page 10*).
Muss ich vor dem Upgrade auf eine neuere Version von AXIS Optimizer die Einstellungen sichern?	Nein, ein Backup ist nicht erforderlich. Beim Upgrade auf eine neuerer Version ändert sich nichts.
Wenn ich über 30 Client-PCs mit AXIS Optimizer habe, muss ich diese dann einzeln aktualisieren?	Sie können die Clients einzeln aktualisieren. Sie können das Upgrade auch automatisch durchführen, indem Sie eine lokale Version von AXIS Optimizer Version in Ihrem System veröffentlichen (siehe *Automatisches Aktualisieren des Systems, on page 10*).
Kann ich im AXIS Optimizer jedes Plugin separat aktivieren oder deaktivieren?	Nein, aber sie nehmen keine Ressourcen ein, wenn Sie diese nicht aktiv nutzen.
Welche Ports verwendet AXIS Optimizer?	Die Ports 80 und 443 sind beide für die Kommunikation mit axis.com erforderlich, damit Ihr System Informationen über neue Versionen erhalten und Aktualisierungen herunterladen kann. Die Ports 53459 und 53461 werden für eingehenden Datenaustausch (TCP) geöffnet, wenn Sie AXIS Optimizer über AXIS Secure Entry installieren.

Fehlerbehebung

Wenn Sie technische Probleme haben, aktivieren Sie die Debug-Protokollierung, reproduzieren Sie das Problem und teilen Sie diese Protokolle mit dem Axis Support. Sie können die Debug-Protokollierung im Management Client oder Smart Client einschalten.

In Management Client:

1. Gehen Sie auf **Site Navigation** > **Basics** > **AXIS Optimizer** (Standortnavigation > Grundlegendes > AXIS Optimizer).
2. Wählen Sie **Turn on debug logging** (Debug-Protokoll aktivieren).
3. Klicken Sie auf **Save report** (Bericht speichern), um die Protokolle auf Ihrem Gerät zu speichern.

In Smart Client:

1. Wechseln Sie zu **Settings**> **Axis general options** (Einstellungen > Allgemeine Axis Optionen).
2. Wählen Sie **Turn on debug logging** (Debug-Protokoll aktivieren).
3. Klicken Sie auf **Save report** (Bericht speichern), um die Protokolle auf Ihrem Gerät zu speichern.

Support

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

Tipps und Tricks

Webseite in eine Ansicht des Smart Client hinzufügen

Mit AXIS Optimizer lassen sich fast alle Webseiten direkt im Smart Client anzeigen, nicht nur HTML-Seiten. Diese Webansicht wird von einer modernen Browser-Engine betrieben und ist mit den meisten Webseiten kompatibel. Dies ist nützlich, wenn Sie beispielsweise über den Smart Client auf AXIS Body Worn Manager zugreifen oder ein Dashboard von AXIS Store Reporter in Ihrer Live-Ansicht anzeigen möchten.

1. Klicken Sie im Smart Client auf **Setup**.
2. Rufen Sie **Views (Ansichten)** auf.
3. Neue Ansicht erstellen oder eine vorhandene auswählen.
4. Gehen Sie zu **Systemübersicht > AXIS Optimizer**.
5. Klicken Sie auf **Web view (Webansicht)** und ziehen Sie diese in die Ansicht.
6. Geben Sie eine Adresse ein und klicken Sie auf **OK**.
7. Klicken Sie auf **Setup**.

Videoexport mit eingebetteten Suchfunktionen

Videos im XProtect-Format exportieren

Um Videos mit integrierten AXIS Optimizer Suchfunktionen und/oder Axis Entzerrungsfähigkeiten anzuzeigen, müssen Sie die Videos im XProtect-Format exportieren. Dies ist zum z. B. hilfreich bei einem Videoexport zu Demozwecken.

Hinweis

Bei AXIS Optimizer Version 5.3 oder späteren Versionen beginnen Sie mit Schritt 3.

1. Gehen Sie im Smart Client zu **Einstellungen** > **Axis Suchoptionen**.
2. Aktivieren Sie die Option **Include search plugins in exports (Export mit Such-Plugins)**.
3. Wählen Sie **XProtect format (XProtect-Format)** bei der Erstellung des Exports in Smart Client.

Exportsperrung auf empfangenden Computern aufheben

Um den Export auf einem anderen Computer erfolgreich zu verwenden, stellen Sie sicher, dass die Blockierung des Datei-Archivs für den Export aufgehoben wird.

1. Klicken Sie auf dem empfangenden Computer mit der rechten Maustaste auf die Exportdatei (Zip-Datei) und wählen Sie **Properties (Eigenschaften)**.
2. Klicken Sie unter **General (Allgemein)** auf **Unblock (Blockierung aufheben)** > **OK**.
3. Extrahieren Sie den Export und öffnen Sie die Datei „SmartClient-Player.exe“.

Exportierte AXIS Dewarp-Ansicht wiedergeben

1. Öffnen Sie das exportierte Projekt.
2. Wählen Sie die Ansicht aus, die die Axis-Dewarped-Ansicht enthält.

T10134385_de

2026-09 (M61.2)

© 2021 – 2026 Axis Communications AB