

Haftungsausschluss

Rechtlicher Hinweis

Dieser Leitfaden und seine Inhalte (der „Leitfaden“) werden von NXGEN bereitgestellt. Alle Rechte am Leitfaden und am darin verkörperten geistigen Eigentum — einschließlich, aber nicht beschränkt auf Marken, Handelsnamen, Logos und ähnliche Kennzeichen im oder am Leitfaden — sind gesetzlich geschützt. Sämtliche Rechte, Ansprüche und Anteile am Leitfaden und an damit verbundenen Schutzrechten verbleiben bei NXGEN und seinen Lizenzgebern.

Der Leitfaden wird unentgeltlich, „wie besehen“ und ausschließlich zu Informationszwecken bereitgestellt, ohne jegliche Gewährleistung. Er ist weder dazu bestimmt noch geeignet, ein Rechtsverhältnis zwischen dem Leser und NXGEN oder seinen verbundenen Unternehmen zu begründen, einschließlich, aber nicht beschränkt auf Verpflichtungen von NXGEN oder seinen verbundenen Unternehmen gegenüber dem Leser.

Die Verpflichtungen von NXGEN und seinen verbundenen Unternehmen in Bezug auf von einem Kunden erworbene NXGEN-Produkte oder -Dienstleistungen richten sich ausschließlich nach den Bedingungen des Vertrags, unter dem diese Produkte oder Dienstleistungen erworben wurden.

Zur Klarstellung

Der Leser trägt das gesamte Risiko hinsichtlich der Nutzung, der Ergebnisse und der Leistung des Leitfadens. Soweit gesetzlich zulässig, schließt NXGEN alle Gewährleistungen aus, ob gesetzlich, ausdrücklich oder stillschweigend — einschließlich, aber nicht beschränkt auf stillschweigende Gewährleistungen der Marktgängigkeit, der Eignung für einen bestimmten Zweck, des Rechtsbestands und der Nichtverletzung von Rechten Dritter — sowie jegliche Haftung oder Gewährleistung aus Vorschlägen, Spezifikationen oder Mustern im Zusammenhang mit dem Leitfaden.

Avigilon

Updated 11 August 2026

Zusammenfassung

Diese Dokumentation bietet eine umfassende Anleitung zur Integration Avigilon Video Management System (VMS) mit der GC-X-ONE Plattform für verbesserte Videoüberwachung und -analyse.

Zweck: Konfigurieren Sie das Avigilon Video Management System (VMS) für eine nahtlose Integration mit der GC-X-ONE-Plattform für verbesserte Videoüberwachung und -analyse.

Ergebnis: Erweiterte Funktionalität mit Analyse, Benutzerverwaltung und Alarmkonfiguration, die durch die GC-X-ONE-Integration robuste Verwaltungs- und Überwachungsfunktionen ermöglicht.

Zielgruppe: Systemadministratoren / IT-Experten / Außendiensttechniker.

Voraussetzungen

Bevor Sie mit der Integration beginnen, stellen Sie sicher, dass Folgendes verfügbar ist:

- Avigilon ACC-Client-Software
- ACC 7 Web Endpoint Service
- IT-Team, das für die Einrichtung der Portweiterleitung auf seiner Firewall oder seinem Router verantwortlich ist
- Administratorzugriff auf das Avigilon-System

Avigilon-Konfiguration

Geräteprofil

- Typ: Videomanagementsystem (VMS)

- Entdeckung: WebAPI-Endpunkt
- Ereignisse: Bewegungserkennung, Analyseereignisse, Alarmauslöser
- Ports: Benutzerdefiniert (konfiguriert über Portweiterleitung)
- Bekannte Macken: Erfordert die Installation von WebAPI Endpoint für die externe Kommunikation.
Für den GC-X-ONE-Zugriff ist die Einrichtung einer Benutzergruppe erforderlich. Für die Ereigniserkennung ist eine Analysekonfiguration auf Kameraebene erforderlich.
- Live: Unterstützt
- Analyse: Unterstützt (Bewegungserkennung, Objekterkennung)
- Alarmverwaltung: Unterstützt
- Benutzerverwaltung: Unterstützt
- PTZ-Steuerung: Unterstützt

Avigilon-Konfigurationshandbuch mit GC-X-ONE

Schritt 1 – Installieren Sie wesentliche Softwarekomponenten

Installieren Sie den WebAPI-Endpunkt

Wenn Sie über Avigilon VMS verfügen, installieren Sie den WebAPI-Endpunkt, indem Sie den Anweisungen im Avigilon WebAPI-Endpunkt-Schnellstarthandbuch folgen. Dieser Endpunkt erleichtert die Kommunikation zwischen dem VMS und externen Anwendungen.

Stellen Sie die Zugänglichkeit des ACC-Servers sicher

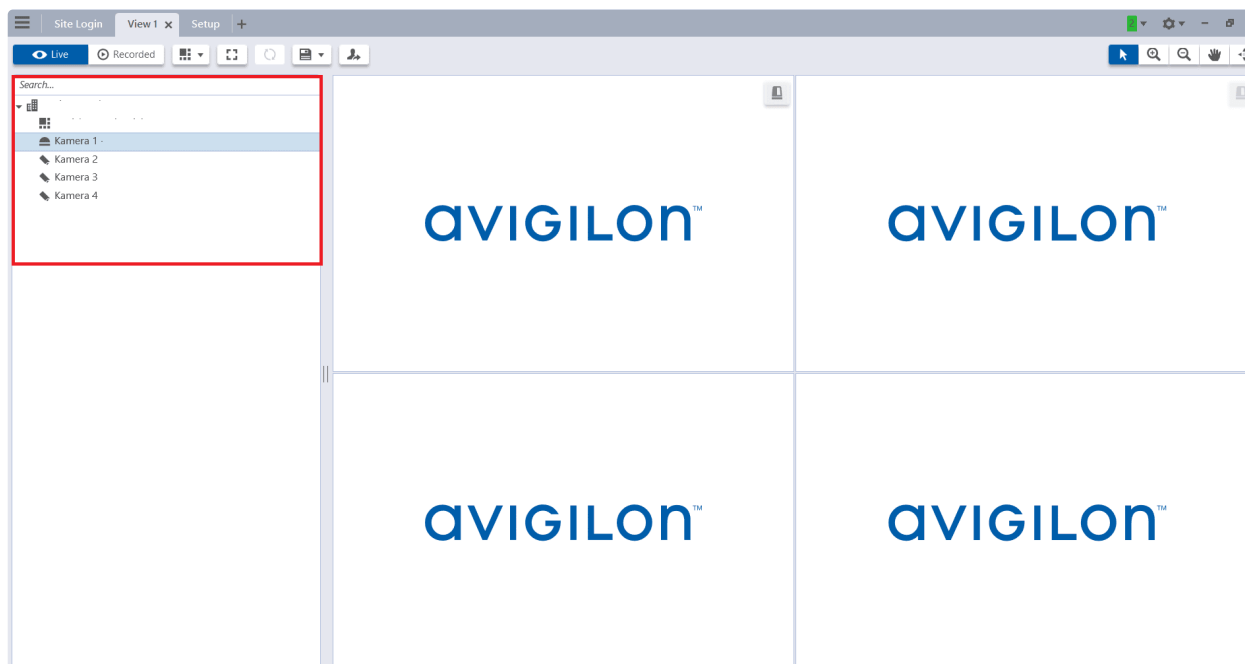
Bestätigen Sie, dass der ACC-Server (Avigilon Control Center) ordnungsgemäß installiert und betriebsbereit ist. Der ACC-Server kommuniziert über den konfigurierten Server-Port mit der Außenwelt und stellt so sicher, dass das VMS bei Bedarf Daten senden und empfangen kann.

Erwartetes Ergebnis: WebAPI-Endpunkt installiert und ACC-Server zugänglich.

Schritt 2 – Melden Sie sich beim Avigilon ACC Client an

UI-Pfad: ACC-Client → Anmelden

Suchen Sie im ACC-Client-Anmeldebildschirm das Feld, um die IP-Adresse des Geräts in die Suchleiste einzugeben. Geben Sie Ihren Benutzernamen und Ihr Passwort für den ACC-Client ein.



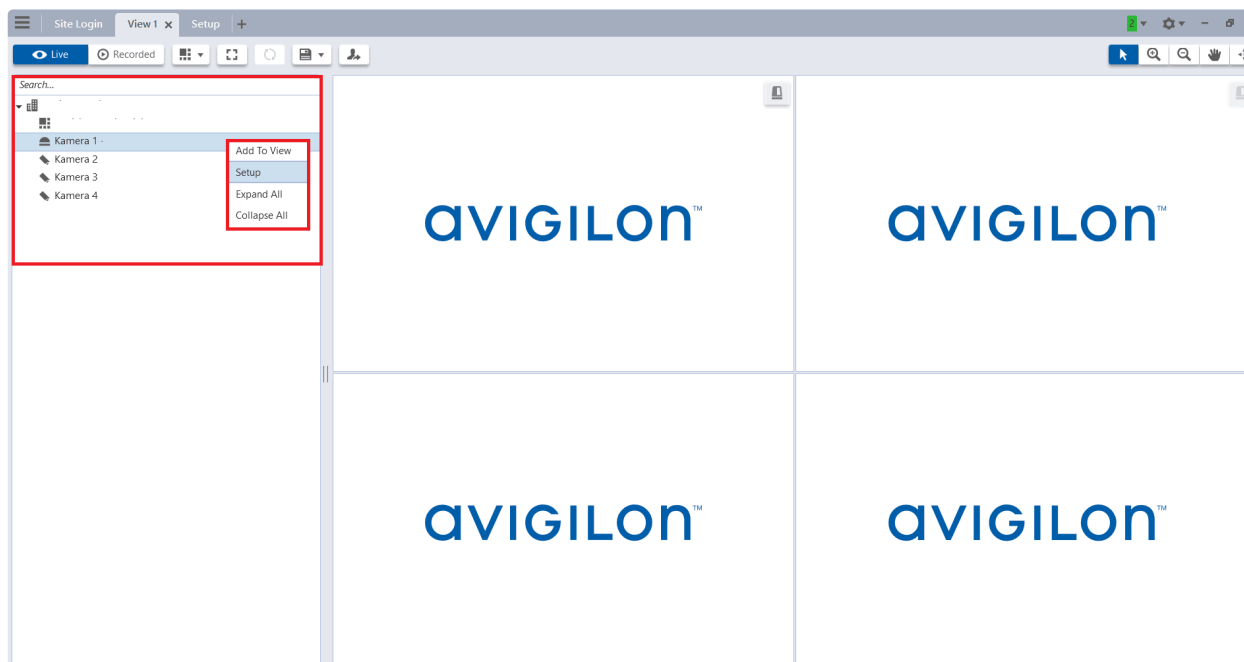
Eine Avigilon-Client-Ansicht mit links hervorgehobenem Kamerabaum und vier leeren Fenstern mit dem Avigilon-Schriftzug.

Erwartetes Ergebnis: Erfolgreich beim ACC-Client angemeldet.

Schritt 3 – Navigieren Sie zur Kamerakonfiguration

UI-Pfad: ACC Client → Kameraauswahl

Sobald Sie angemeldet sind, navigieren Sie über die Client-Schnittstelle zu der spezifischen Kamera oder dem Gerät, die Sie konfigurieren müssen.

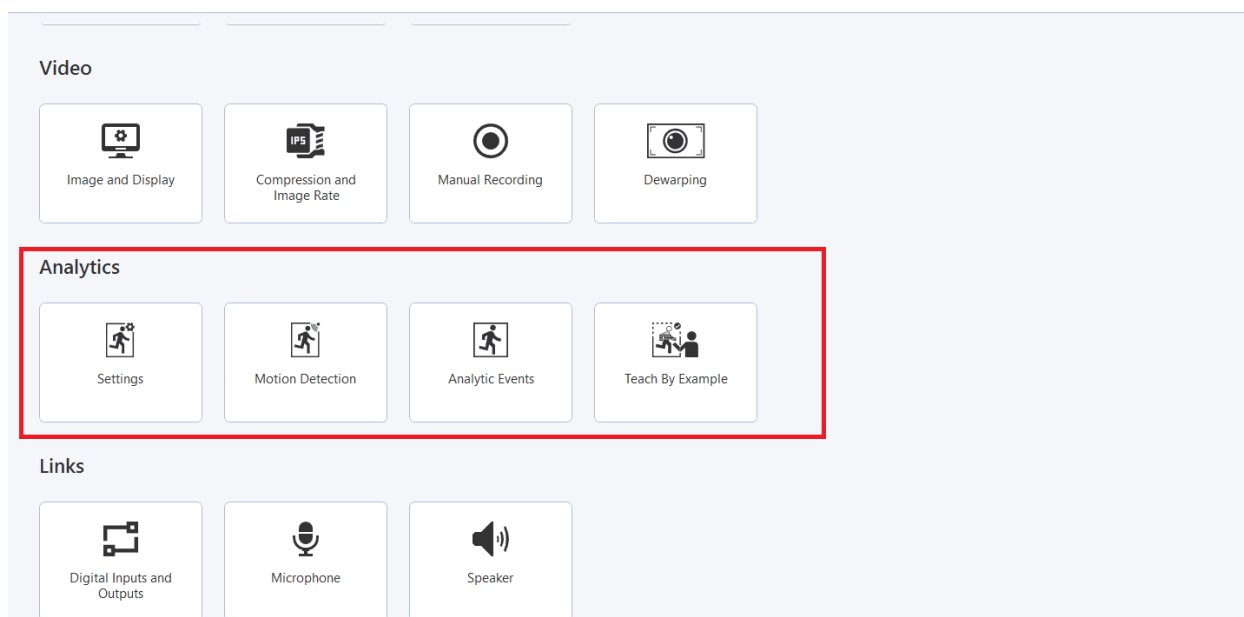


Erwartetes Ergebnis: Kameraschnittstelle zur Konfiguration zugänglich.

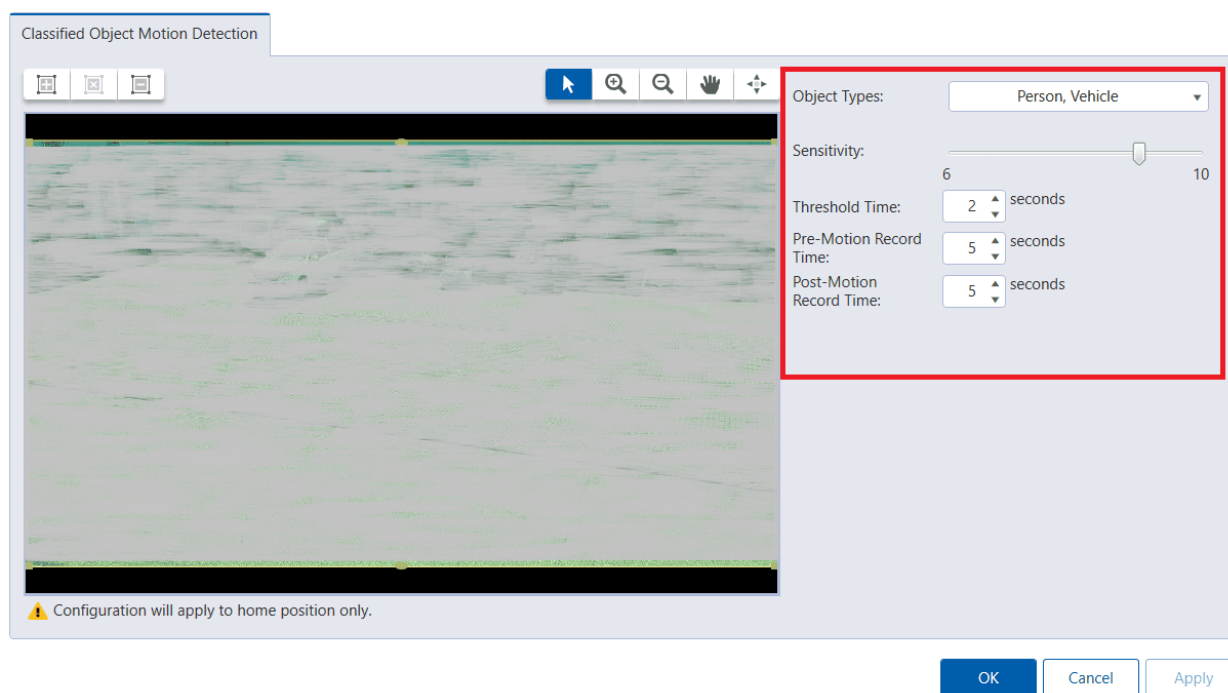
Schritt 4 – Kamera-Setup aufrufen

UI-Pfad: Kamera → Rechtsklick → Setup

- Klicken Sie mit der rechten Maustaste auf die Kamera, die Sie konfigurieren möchten
- Klicken Sie im angezeigten Kontextmenü auf Setup
- Dadurch wird die Konfigurationsseite der Kamera geöffnet



Das Einstellungsmenü einer Kamera mit hervorgehobener Gruppe Analytics – Einstellungen, Bewegungserkennung, Analyseereignisse und Teach by Example – zwischen den Gruppen Video und Links.



Erwartetes Ergebnis: Kamerakonfigurationsseite geöffnet.

Schritt 5 – Bewegungserkennungsanalyse konfigurieren

UI-Pfad: Kamera-Setup → Analyse → Bewegungserkennung

Wählen und konfigurieren Sie die Art der Analyse. Nachdem Sie den gewünschten Analysetyp ausgewählt haben, können Sie verschiedene Einstellungen und Parameter speziell für diesen Typ anpassen.

Konfigurieren Sie die Bewegungserkennungsparameter:

- Objekttypen: Objekttypen auswählen (Person, Fahrzeug)
- Empfindlichkeit: Empfindlichkeitsstufe einstellen (empfohlen 8–10)
- Schwellenwertzeit: Minstdauer festlegen (empfohlen 2 Sekunden)
- Aufnahmezeit vor der Bewegung: Stellen Sie die Aufnahmezeit vor dem Ereignis ein (empfohlen 10 Sekunden)
- Post-Motion-Aufnahmezeit: Stellen Sie die Aufnahmezeit nach dem Ereignis ein (empfohlen 10 Sekunden)

Analytics Events:

Event is enabled

Object Types:

Activity: ☐

Threshold Time:

Sensitivity:

Number of Objects:

Timeout:

+

 Add

+

 Edit

✖

 Delete

OK

Cancel

Apply

Erwartetes Ergebnis: Bewegungserkennungsanalyse konfiguriert.

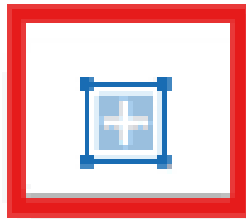
Schritt 6 – Analyseereignisse konfigurieren

UI-Pfad: Kamera-Setup → Analysen → Analyseereignisse

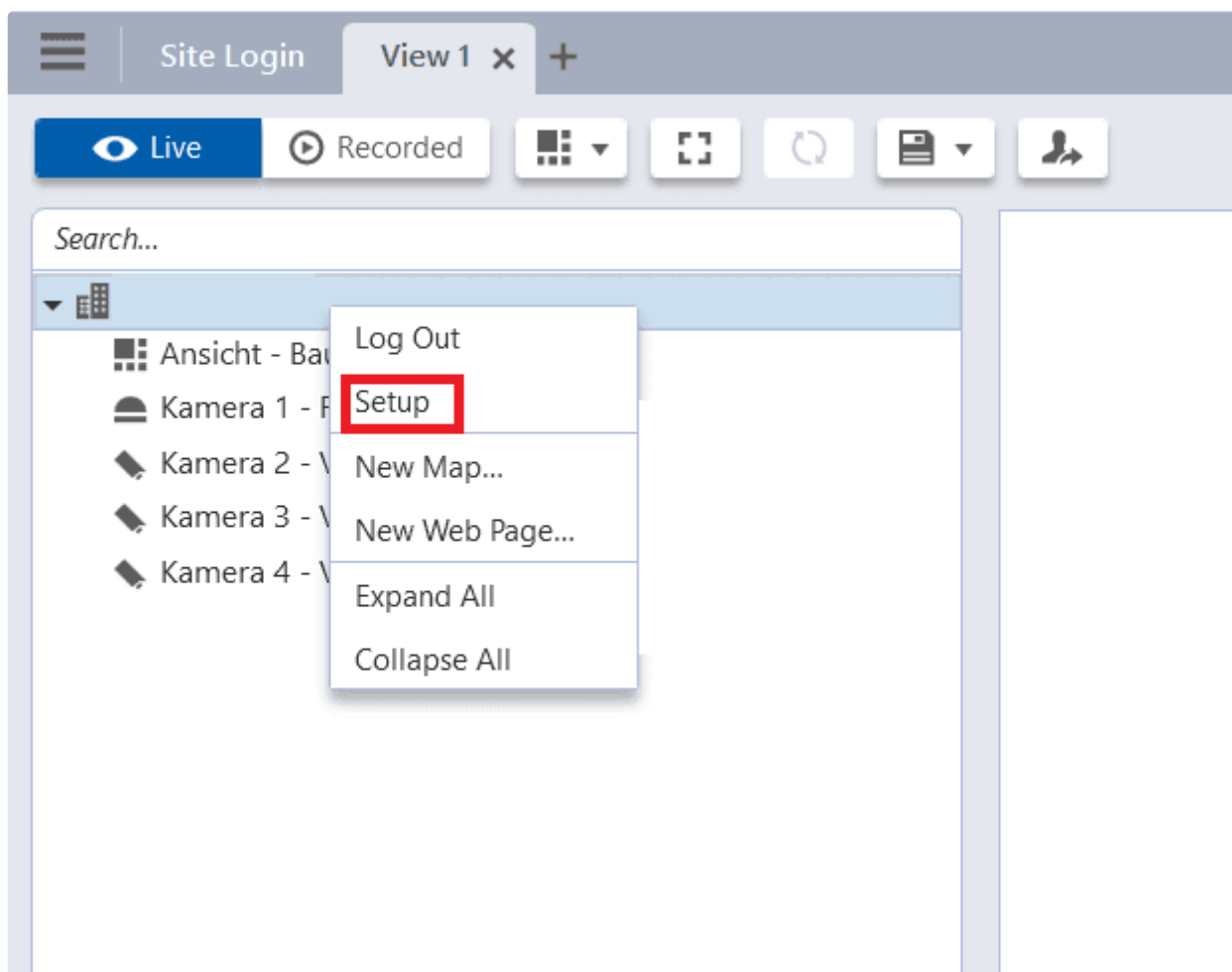
Analytics verarbeitet den Video-Feed in Echtzeit, um bestimmte Aktivitäten oder Bedingungen zu erkennen und darauf zu reagieren.

- Klicken Sie auf die Schaltfläche Hinzufügen
- Definieren Sie Ihr Interessengebiet, indem Sie auf das Symbol oben links auf dem Bildschirm klicken

Add/Edit Analytics Events



Add Exclusion Area



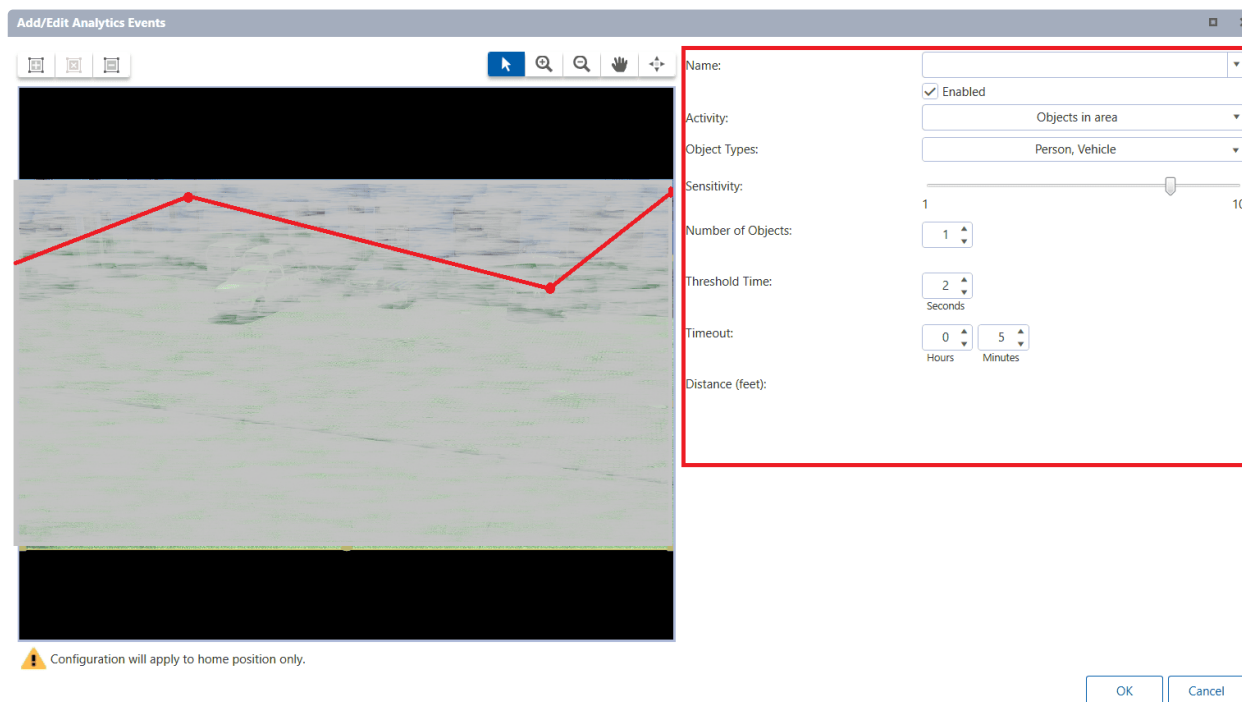
Ein Standortbaum mit geöffnetem Kontextmenü; Setup ist hervorgehoben, darunter New Map, New Web Page, Expand All und Collapse All.

Konfigurieren Sie Ereignisparameter

Nachdem Sie den Interessenbereich hinzugefügt haben, richten Sie Folgendes ein:

- Kontrollkästchen „Aktiviert“: Aktivieren Sie diese Option, um das Analyseereignis zu aktivieren
- Aktivität: Wählen Sie die Art der Aktivität aus, die innerhalb der definierten Zone überwacht werden soll
- Objekttypen: Geben Sie an, welche Arten von Objekten das System erkennen soll
- Empfindlichkeit: Empfindlichkeitsstufe einstellen (empfohlen 8–10)
- Schwellenwertzeit: Minstdauer festlegen (empfohlen 2 Sekunden)

- Anzahl der Objekte: Geben Sie die Anzahl der Objekte an, die zum Auslösen des Ereignisses erforderlich sind
- Timeout: Wartezeit vor dem Zurücksetzen festlegen (empfohlen 10 Sekunden)
- Entfernung (Fuß): Legen Sie die Mindestentfernung fest, die ein Objekt zurücklegen muss



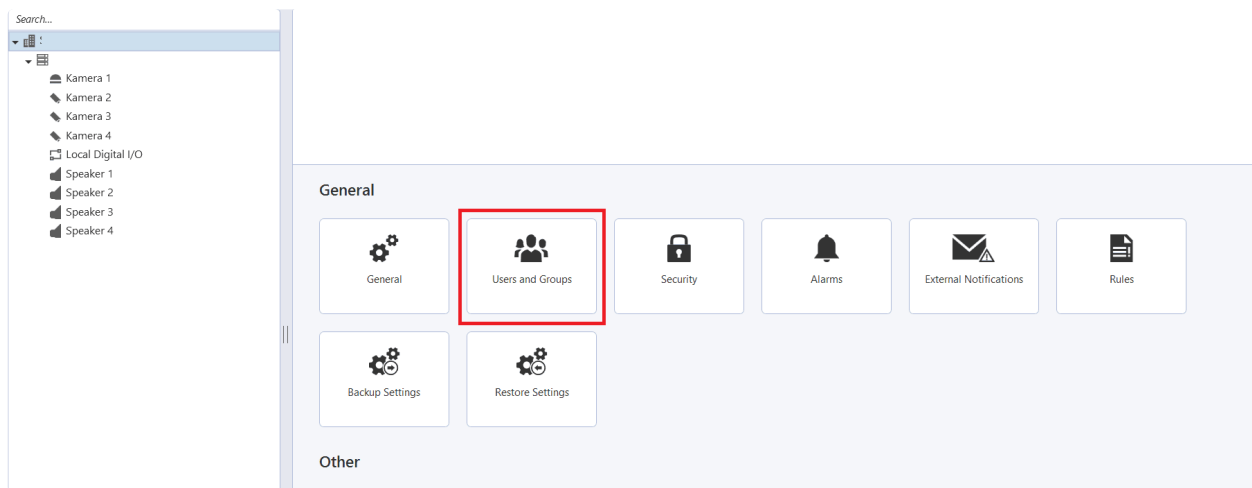
Der Dialog Add/Edit Analytics Events mit einer rot eingezeichneten Erkennungszone über dem Kamerabild und hervorgehobenem Einstellungsbereich: Aktivität, Objekttypen, Empfindlichkeit, Objektanzahl, Schwellenzeit und Timeout.

Erwartetes Ergebnis: Analyseereignisse, konfiguriert mit Interessenbereich.

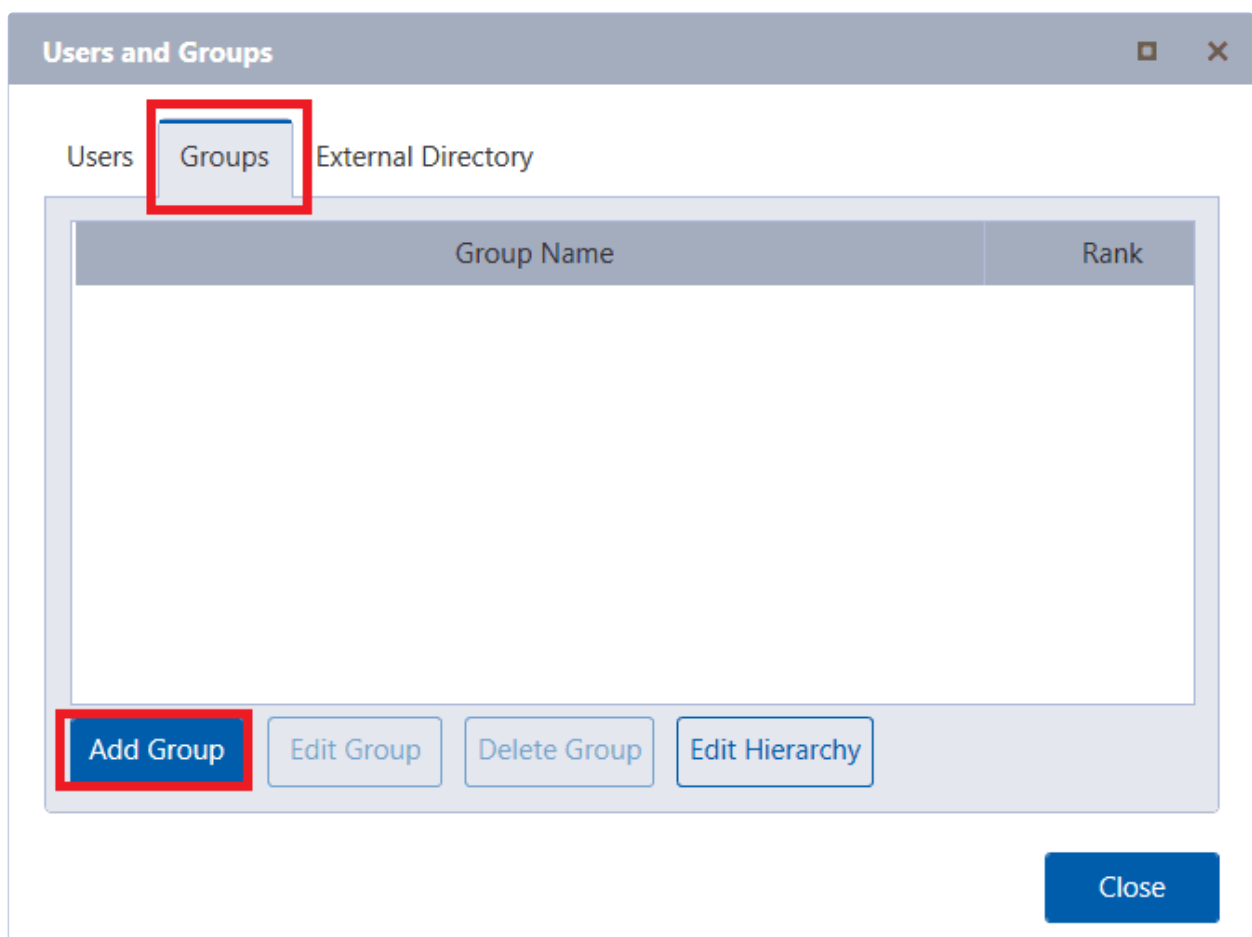
Schritt 7 – Benutzergruppe für GC-X-ONE einrichten

UI-Pfad: Site → Rechtsklick → Setup → Benutzer und Gruppen

- Klicken Sie mit der rechten Maustaste auf die Site, die Sie konfigurieren möchten
- Klicken Sie im erscheinenden Kontextmenü auf „Setup“
- Dadurch wird die Konfigurationsseite der Site geöffnet



- Navigieren zu Benutzer und Gruppen



Das Fenster Users and Groups mit hervorgehobener Registerkarte Groups und Schaltfläche Add Group, darunter eine leere Gruppenliste.

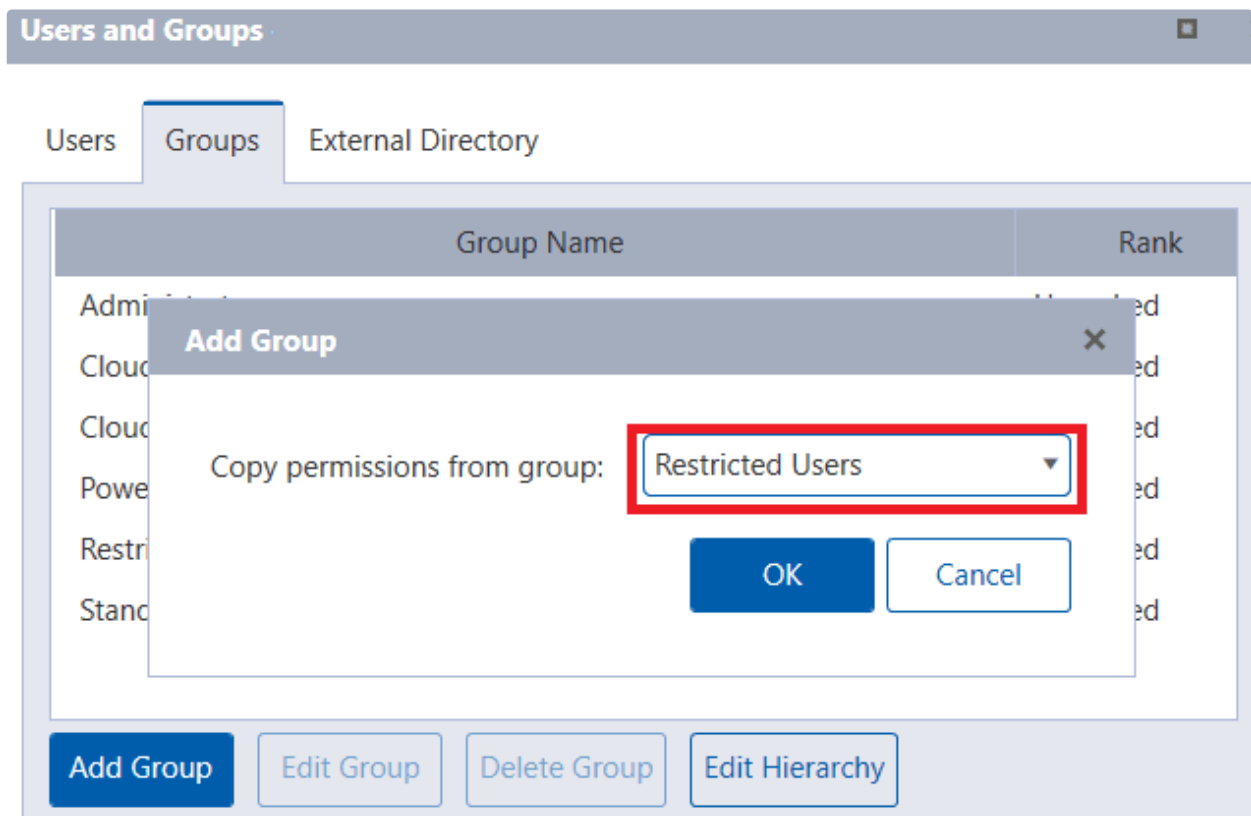
Erwartetes Ergebnis: Benutzer- und Gruppenkonfiguration, auf die zugegriffen wurde.

Schritt 8 – Benutzergruppe erstellen

UI-Pfad: Gruppen → Hinzufügen

Navigieren zu Gruppen und klicken Sie dann auf Gruppe hinzufügen . Wenn Sie dazu aufgefordert

werden, legen Sie fest Berechtigungen aus der Gruppe kopieren zu Eingeschränkte Benutzer .



Edit Group

Group

Members

Name:

Rank:

Unranked

Min Password Strength:

Weak

Strong

Two-Factor Authentication:

☐ Required

Emergency Privilege Override:

☐ Enabled

Group Privileges:

☒ View live images

☒ Use PTZ controls

☒ Lock PTZ controls

☐ Trigger manual recording

☒ Trigger digital outputs

☒ Broadcast to speakers

☒ Receive live events with identifying feature

☒ View high-resolution images

Access Rights:

Search...

☒

☒ Ansicht -

☒ Kamera 1

☒ Kamera 2

☒ Kamera 3

☒ Kamera 4

Enable Dual Authorization

Dual Authorization: Off

OK

Cancel

Erwartetes Ergebnis: Neue Benutzergruppe erstellt.

Schritt 9 – Gruppeneinstellungen konfigurieren

Konfigurieren Sie im Dialogfeld „Gruppe bearbeiten“ die folgenden Details:

Name: Verwendung NXGEN oder NXG im Feld „Name“ (empfohlen).

Gruppenrechte – Live-Bilder anzeigen:

- PTZ-Steuerung verwenden
- PTZ-Steuerung sperren
- Digitale Ausgänge auslösen
- Übertragung an Lautsprecher

- Empfangen Sie Live-Events mit Erkennungsmerkmalen
- Hochauflösende Bilder anzeigen

Gruppenberechtigungen – Aufgezeichnete Bilder anzeigen:

- Bilder exportieren
- Bilder anzeigen, die vor dem Anmelden aufgezeichnet wurden
- Lizenzierte Suche zur Identifizierung von Merkmalen

Gruppenberechtigungen – Karten anzeigen:

- Karten verwalten
- Benutzersitzungen verwalten
- Mikrofone hören

Erwartetes Ergebnis: Gruppenrechte konfiguriert.

Schritt 10 – Kameras zur Gruppe hinzufügen

Im Zugriffsrechte Markieren Sie im Abschnitt des Dialogfelds „Gruppe bearbeiten“ alle Kameras, die auf der GC-X-ONE-Plattform angezeigt werden sollen. Klicken Sie OK , um die Änderungen zu speichern.

Edit Group

Group

Members

Name:

Rank:

Unranked

Min Password Strength:

Weak

Strong

Two-Factor Authentication:

☐ Required

Emergency Privilege Override:

☐ Enabled

Group Privileges:

☒ View recorded images

☒ Export images

☒ View images recorded before login

☐ Archive images

☐ Create teach markers

☒ Licensed search for identifying features

☐ Add to face watch lists from recorded v

☐ Manage saved views

Access Rights:

Search...

☒  Ansicht -

☒  Kamera 1

☒  Kamera 2

☒  Kamera 3

☒  Kamera 4

Enable Dual Authorization

Dual Authorization: Off

OK

Cancel

Der Dialog Edit Group mit hervorgehobener Liste Group Privileges – Bilder exportieren, vor der Anmeldung aufgezeichnete Bilder ansehen, archivieren und weitere – daneben die für die Gruppe zugänglichen Kameras.

Edit Group

Group

Members

Name:

Rank:

Unranked

Min Password Strength:

Weak

Strong

Two-Factor Authentication:

☐ Required

Emergency Privilege Override:

☐ Enabled

Group Privileges:

☐ Manage saved views

☒ View Maps

☒ Manage maps

☐ Manage web pages

☐ Manage virtual matrix monitors

☐ Initiate collaboration sessions

☒ Manage user sessions

☒ Listen to microphones

Access Rights:

Search...

☒ Stadt Overath

☒ Ansicht -

☒ Kamera 1

☒ Kamera 2

☒ Kamera 3

☒ Kamera 4

Enable Dual Authorization

Dual Authorization: Off

OK

Cancel

Der Bereich General der Registerkarte Setup mit hervorgehobener Kachel Alarms, neben General, Users and Groups, Security, External Notifications und Rules.

Erwartetes Ergebnis: Der Benutzergruppe zugewiesene Kameras.

<https://docs.nxgen.cloud/de/gcxone/devices/avigilon>

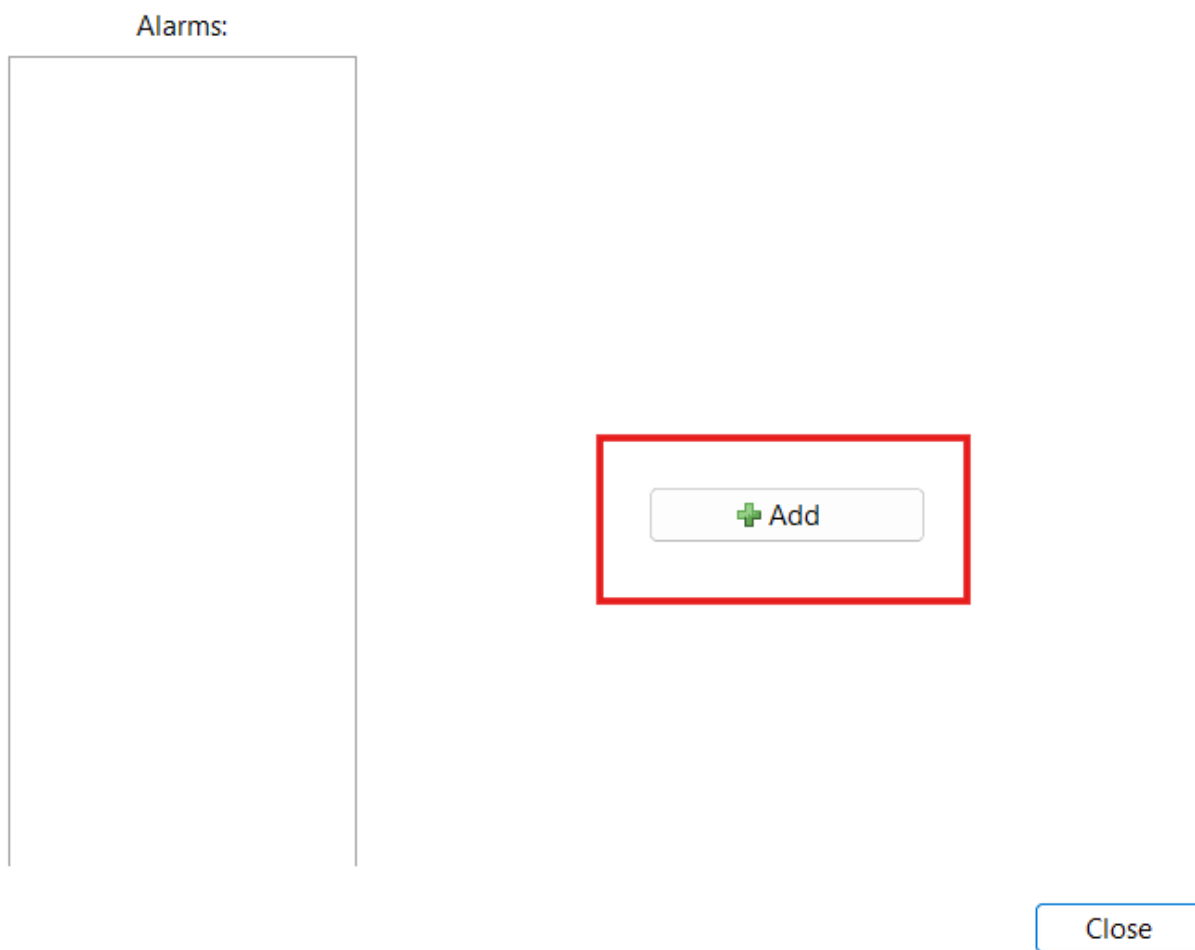
17 / 28

Schritt 11 – Alarme konfigurieren

UI-Pfad: Setup → Alarme

Kehren Sie zur Setup-Seite vom vorherigen Schritt zurück und navigieren Sie zu Alarme . Klicken Sie

Hinzufügen , um einen neuen Alarm zu erstellen.



Eine leere Alarmliste mit daneben hervorgehobener Schaltfläche Add.

Select Alarm Trigger Source

Alarm Trigger Source:

Search...

▼ [Icon] E

☒ [Icon] Kamera

☐ [Icon] Kamera

☒ [Icon] Kamera

☐ [Icon] Kamera 4

☐ Speaker 1

☐ Speaker 2

☐ Speaker 3

☐ Speaker 4

☐ Auto-acknowledge alarm when motion stops

Dropdown Menu:

- Motion Detection
- Video Analytics Event
- Digital Input Activation
- License Plate Watch list Match
- POS Transaction Exception
- Device Error
- System Error
- External Software Event
- Face Watch List Match

[← Previous](#)

➡ Next

Cancel

Erwartetes Ergebnis: Alarmkonfigurationsseite aufgerufen.

Schritt 12 – Alarmauslöserquelle festlegen

Legen Sie die Alarmauslösesequelle im Dropdown-Menü fest. Zu den verfügbaren Optionen gehören:

- Bewegungserkennung
- Videoanalyse-Ereignis
- Aktivierung des digitalen Eingangs
- Übereinstimmung der Nummernschild-Beobachtungsliste
- POS-Transaktionsausnahme
- Gerätefehler

- Legen Sie die Aufnahmedauer fest
- Klicken Weiter

Add Alarm

Select Alarm Recipients

Select the users that will be notified when this alarm is triggered:

User/Group	First Name	Last Name	Wait Time
------------	------------	-----------	-----------

Add Recipients...
Remove Recipients

☐ Play sound when alarm is triggered:
Alarm 1.wav

Previous
Next
Cancel

Erwartetes Ergebnis: Alarmaufzeichnungseinstellungen konfiguriert.

Schritt 14 – Alarmempfänger konfigurieren

UI-Pfad: Alarmempfänger → Empfänger hinzufügen

- Alarmempfänger auswählen
- Klicken Sie auf Empfänger hinzufügen und stellen Sie sicher, dass Sie die Benutzergruppe auswählen, die Sie zuvor konfiguriert haben (NXGEN/NXG).

Select Alarm Recipients

Select Users

Search...

Select	User/Group	First Name	Last Name
☐			
☒	 NXGEN		
☐			
☐			
☐			
☐			
☐			
☐			
☐			

Add
Cancel

- Klicken Weiter

Erwartetes Ergebnis: Alarmempfänger konfiguriert.

Schritt 15 – Alarmkonfiguration abschließen

- Wählen Sie den NXGEN-Benutzer/die NXGEN-Gruppe wie konfiguriert aus
- Klicken Hinzufügen
- Wählen Sie die Dauer aus, die erforderlich ist, um den Empfänger zu benachrichtigen, wenn ein Alarm ausgelöst wird

Add Alarm

Select Alarm Recipients

Select the users that will be notified when this alarm is triggered:

User/Group	First Name	Last Name	Wait Time
NXGEN			0 h 0 m
			0 h 0 m

Add Recipients...
Remove Recipients

☐ Play sound when alarm is triggered: Alarm 1.wav

Previous
Next
Cancel

- Vergiss das nicht Speichern die Änderungen

Erwartetes Ergebnis: Alarmkonfiguration abgeschlossen und gespeichert.

Schritt 16 – Gerät in GC-X-ONE konfigurieren

UI-Pfad: GC-X-ONE → Site → Konfigurations-App → Geräte

Navigieren Sie in der GC-X-ONE-Konfigurations-App zu der Site, zu der Sie das Gerät hinzufügen möchten. Auswählen Avigilon als Gerätetyp und füllen Sie die folgenden Felder aus:

- Name
- IP-Adresse oder Hostname

- Benutzername
- Passwort
- RTSP-Port (Standard: 554)
- Steuerport (Standard: 443)
- Server-Port
- HTTPs-Port (Standard: 443)
- Seriennummer
- Geräte-ID
- Zeitzone

Optionale Einstellungen:

- Audio aktivieren

Hinweis: Audio ist in ACC standardmäßig deaktiviert. Um es zu aktivieren: (1) Öffnen Sie die ACC-Einstellungen und aktivieren Sie den Lautsprecher, und (2) weisen Sie die Kamera diesem Lautsprecher zu. Beide Schritte sind erforderlich – durch alleiniges Aktivieren der Audioumschaltung in GCXONE wird Audio nicht aktiviert.

- Site Pulse-Konfiguration
- Ereignisabfrage
- Heatmap-Maske konfigurieren
- Periodischer Gesundheitscheck (Standard: 30 Tage)

Add Alarm

Select Alarm Recipients

Select the users that will be notified when this alarm is triggered:

User/Group	First Name	Last Name	Wait Time
 NXGEN			0 h 0 m
			0 h 0 m

Add Recipients...

Remove Recipients

☐ Play sound when alarm is triggered: Alarm 1.wav 

Previous

Next

Cancel

Add Device

Avigilon

Name

IP Address Or Host Name

User Name

127.0.0.1

admin

Password

RTSP Port

Control Port

Password

554

443

Server Port

HTTPs Port

Serial Number

Server Port

443

Serial Number

Device Id

Device Id

☒ Enable Audio

☐ Site Pulse Configuration

Timezone

☐ Event Polling

☐ Configure Heatmap Mask

☐ Periodic Health Check

30 days

Schritt 17 – Integration überprüfen

Sobald alle Details ausgefüllt sind, klicken Sie auf Entdecken . Sie sollten die entdeckten Sensoren sehen.

Erwartetes Ergebnis: Sensoren erfolgreich in GC-X-ONE entdeckt.

Verifizierungsprüfungen:

- Überprüfen Sie, ob der WebAPI-Endpunkt funktionsfähig ist
- Testen Sie den Benutzergruppenzugriff und die Berechtigungen
- Bestätigen Sie, dass Analysen geeignete Ereignisse generieren
- Alarmbenachrichtigungen testen

- Überprüfen Sie den Kamerazugriff über die konfigurierte Benutzergruppe

Erwartetes Ergebnis: Vollständige Avigilon-Integration mit der GC-X-ONE-Plattform.

Fehlerbehebung

WebAPI-Endpunktprobleme

- Überprüfen Sie, ob der WebAPI-Endpunkt ordnungsgemäß installiert ist
- Überprüfen Sie die Konfiguration der Portweiterleitung
- Stellen Sie sicher, dass der ACC-Server von außen zugänglich ist

Benutzerzugriffsprobleme

- Überprüfen Sie, ob die Benutzergruppenberechtigungen korrekt konfiguriert sind
- Überprüfen Sie die Kamerazuweisungen zur Benutzergruppe
- Stellen Sie sicher, dass die richtigen Berechtigungen gewährt werden

Analytics funktioniert nicht

- Empfindlichkeitseinstellungen prüfen (empfohlen 8–10)
- Überprüfen Sie, ob der Interessenbereich richtig definiert ist
- Bestätigen Sie die Einstellungen für Schwellenwertzeit und Timeout

Probleme mit der Alarmkonfiguration

- Überprüfen Sie, ob die Alarmauslösequellen richtig ausgewählt sind
- Überprüfen Sie, ob die Empfängerkonfiguration mit der Benutzergruppe übereinstimmt
- Stellen Sie sicher, dass die Aufnahmeeinstellungen richtig konfiguriert sind

Notizen

- Die Installation von WebAPI Endpoint ist für die externe Kommunikation obligatorisch
- Für den GC-X-ONE-Zugriff ist die Einrichtung einer Benutzergruppe erforderlich
- Analytics-Konfiguration auf Kameraebene für die Ereigniserkennung erforderlich
- Empfohlene Einstellungen: Empfindlichkeit 8–10, Schwellenwertzeit 2 Sekunden, Timeout 10 Sekunden
- Voralarm- und Nachbewegungsaufzeichnung mit 10 Sekunden empfohlen
- Korrekte Einrichtung der Portweiterleitung durch das IT-Team erforderlich