

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.

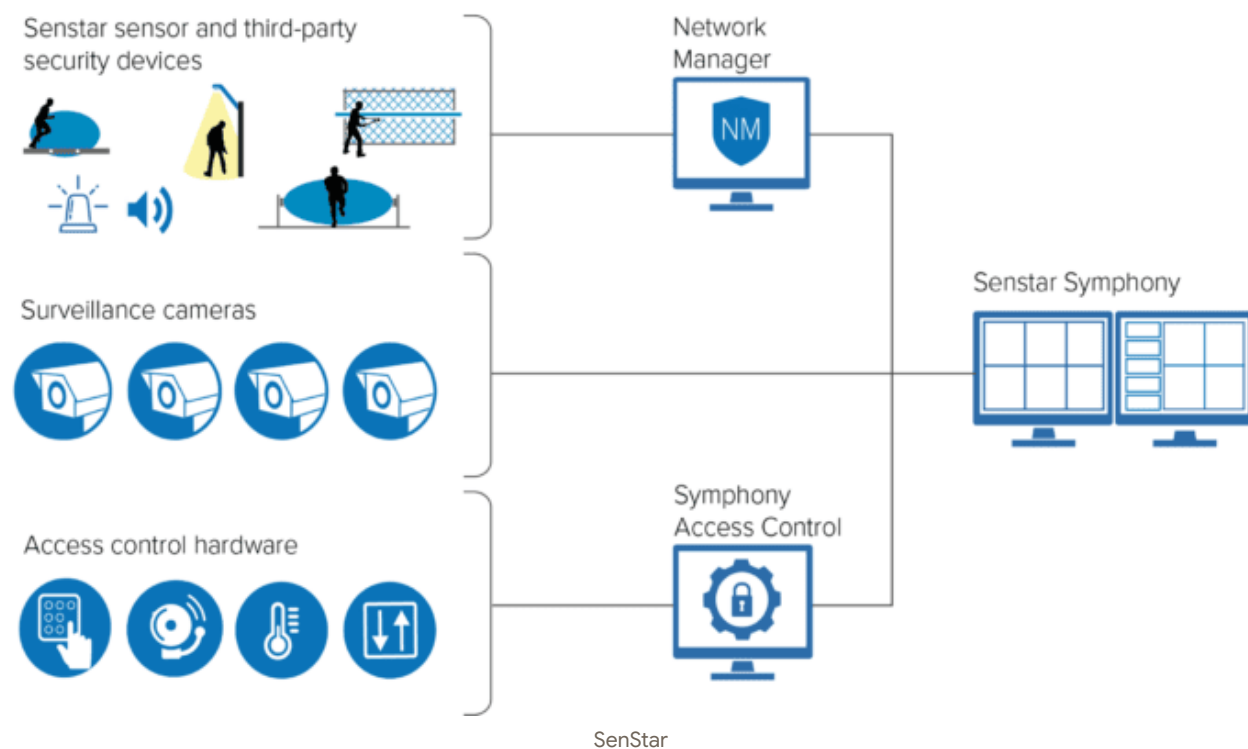
SenStar

Updated 16 August 2026

Einleitung

In dieser Anleitung wird beschrieben, wie man integrieren und konfigurieren das Senstar Video Management System (VMS) in Ihr Sicherheitsmanagement-Framework. Es behandelt die wichtigsten Schritte zur Konfiguration der Geräteanbindung und zur Integration mit Überwachungsplattformen. Ziel ist es, eine nahtlose Ereignisdatenübertragung von Senstar in die GCX-ONE-Plattform zu ermöglichen und eine effektive Alarmierung, Videokorrelation sowie operative Transparenz sicherzustellen.

Das Angebot von Senstar im Bereich Videomanagement umfasst die VMS-Softwareplattform (z. B. die „Senstar Symphony Common Operating Platform“) sowie zugehörige Module für Kameras, Videoanalyse, Zutrittskontrolle und Perimeterüberwachung.



In Ihrer sicheren Umgebung fungiert das Senstar VMS als zentrale Video- und Event-Plattform :

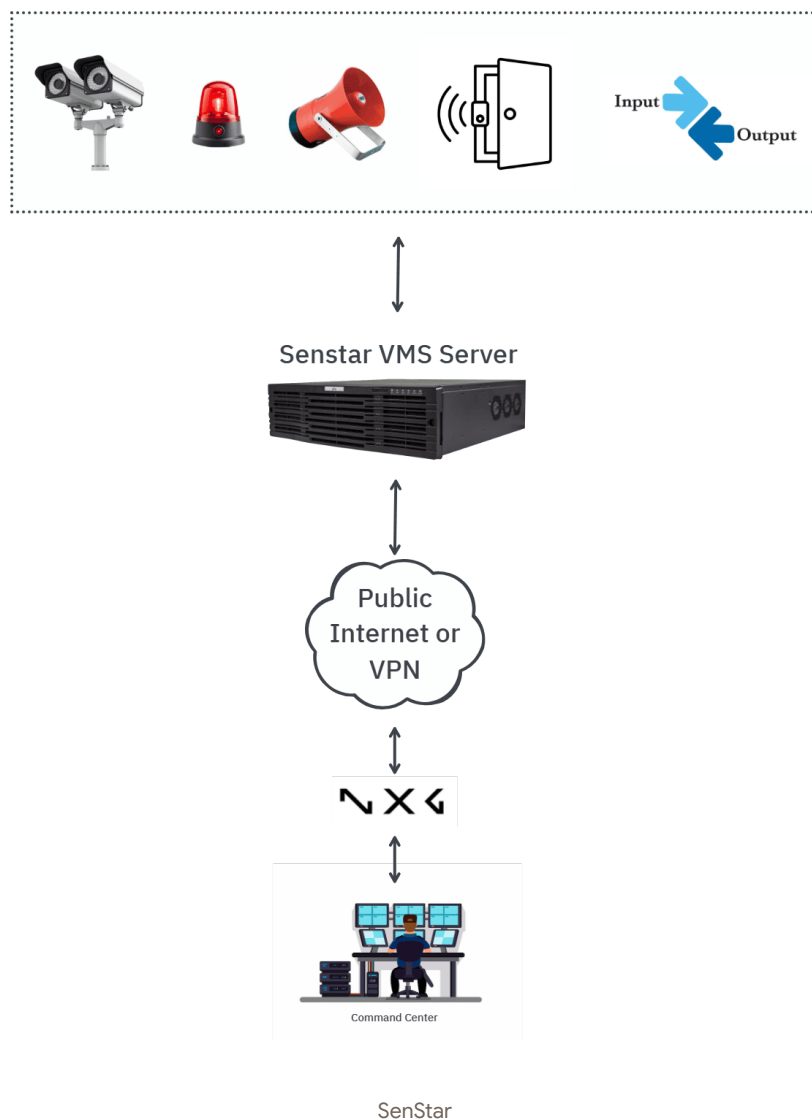
- Es fasst die Videostreams der Kameras auf dem Gelände zusammen.

- Es erfasst Alarmer und Statusmeldungen von Sensoren, Analysesystemen und angeschlossenen E/A-Geräten.
- Es bietet eine einheitliche Benutzeroberfläche für Bediener und lässt sich in externe Plattformen integrieren.

Systemarchitektur

In einer typischen Bereitstellung:

1. Kameras (IP/analog) übertragen ihre Bilder an den Senstar-VMS-Server (vor Ort / Appliance).
2. Vernetzte Sicherheitssensoren leiten E/A-Daten und Telemetriedaten an das VMS oder dessen Sensorintegrationsmodul weiter.
3. Das VMS generiert Ereignisse (z. B. Einbruchserkennung, Sensoralarm, Warnmeldung aus der Videoanalyse), die über API, TCP oder SDK an das zentrale Überwachungssystem weitergeleitet werden.
4. GCX-ONE empfängt diese Ereignisse, filtert Fehlalarme heraus und löst entsprechend Benachrichtigungen an das CMS aus.



SenStar-Konfiguration

Voraussetzungen für die Integration

1. Überprüfen Sie die Senstar-VMS-Version (8.10) und alle erforderlichen Module (z. B. Videomanagement, Analysen).
2. Stellen Sie die Netzwerkverbindung (entweder über einen öffentlichen Netzwerkzugang oder über ein VPN) zwischen dem VMS-Server und der Überwachungsplattform (GCX-ONE) sicher.
3. Stellen Sie sicher, dass der Mobile Bridge API-Dienst läuft. Eine ausführliche Anleitung zur Konfiguration des Senstar-Systems finden Sie hier.

4. Erstellen oder identifizieren Sie ein Integration des Benutzerkontos in Senstar mit ausreichenden Administratorrechten für den Zugriff auf Ereignisströme und Alarme.

SenStar-Konfigurationsanleitung mit GCX-ONE

In der GCX-ONE-Plattform, können Sie sich für die Senstar-VMS-Instanz als Gerät vom Typ „SenStar“-

Diese Konfiguration stellt eine sichere Kommunikationsverbindung zwischen GCX-ONE und dem

Senstar-Videomanagementsystem her und ermöglicht so die Ereignissynchronisation, den Zugriff auf

Videostreams sowie die Steuerung und Überwachung.

Wichtige Konfigurationsparameter

PARAMETER NAME	DESCRIPTION	EXAMPLE VALUE
Device Type	Select SenStar as the device type to enable integration with the Senstar VMS platform.	SenStar
Device Name	A unique name to identify this VMS instance within GCX-ONE. This name will also appear in dashboards and event logs.	Tower01_VMS
Server IP / Hostname	The IP address or hostname of the Senstar VMS server or appliance where the Mobile Bridge is hosted.	192.168.10.25
HTTP/S Port	The Mobile Bridge API port used to access the Senstar API and event listener interface. Default value is 8433.	8433
Enable HTTPS	Toggle this option ON if the Senstar VMS server is configured to support secure HTTPS communication.	true
Username	The username of the integration account with API and event subscription privileges.	integration_admin
Password	The corresponding password for the integration account.	*****
RTSP Port	The Mobile Bridge Video Proxy Port used for live and recorded video streams from connected cameras.	8488

Streaming Key	Encoded authentication token that replaces the plain password when accessing RTSP streams over unsecured protocols.	aHR0cHM6Ly8xOTluMTY4LjEwLj1OjU1NC9zdHJlYW0=
Device Timezone	The timezone of the Senstar VMS server. Ensure that it matches the system timezone configured in GCX-ONE to maintain event timestamp accuracy.	CET (+1:00)

Erstellung von Streaming-Schlüsseln

Die Integration von Senstar VMS erfordert ein Passwort für verschlüsseltes Streaming um sicher auf RTSP-basierte Live- und aufgezeichnete Videostreams zuzugreifen. Dieser Mechanismus erhöht die Sicherheit, indem er verhindert, dass das Passwort im Klartext während der Stream-Authentifizierung offengelegt wird.

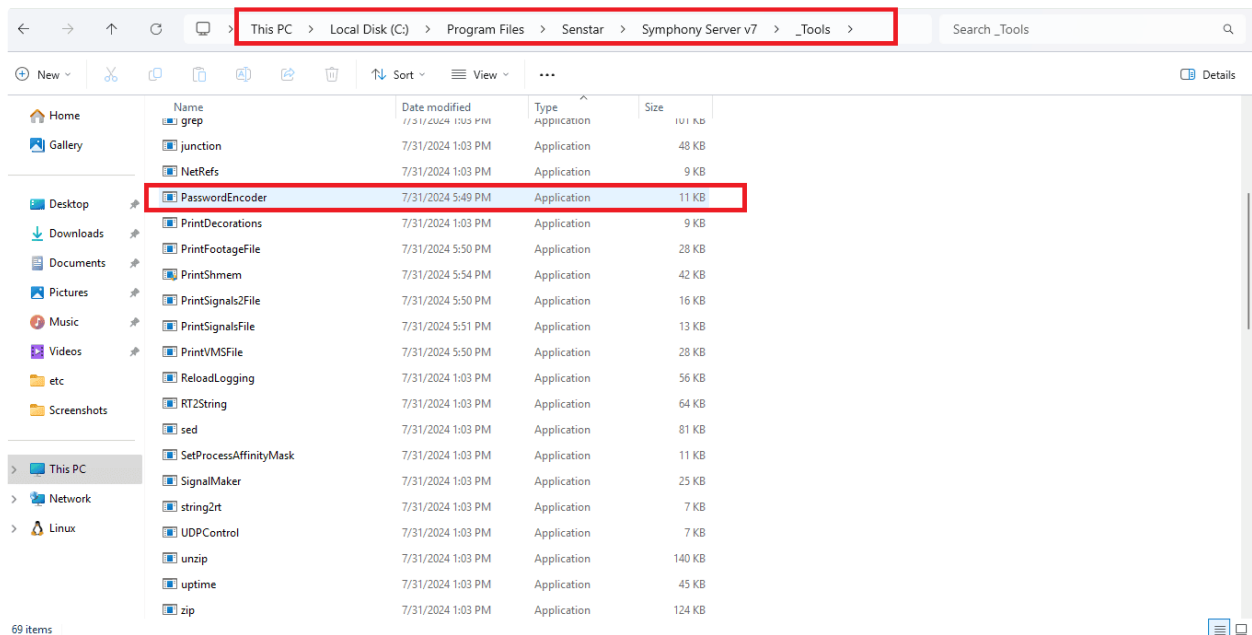
Schritte zur Erzeugung des verschlüsselten Passworts

1. Suchen Sie das Dienstprogramm „Password Encoder“

Das Tool zur Passwortverschlüsselung, PasswordEncoder.exe, wird als Teil des Senstar Symphony Server-Pakets installiert. Es kann nicht separat heruntergeladen werden. Stellen Sie sicher, dass das Senstar Symphony Server auf Ihrem System installiert ist, bevor Sie fortfahren.

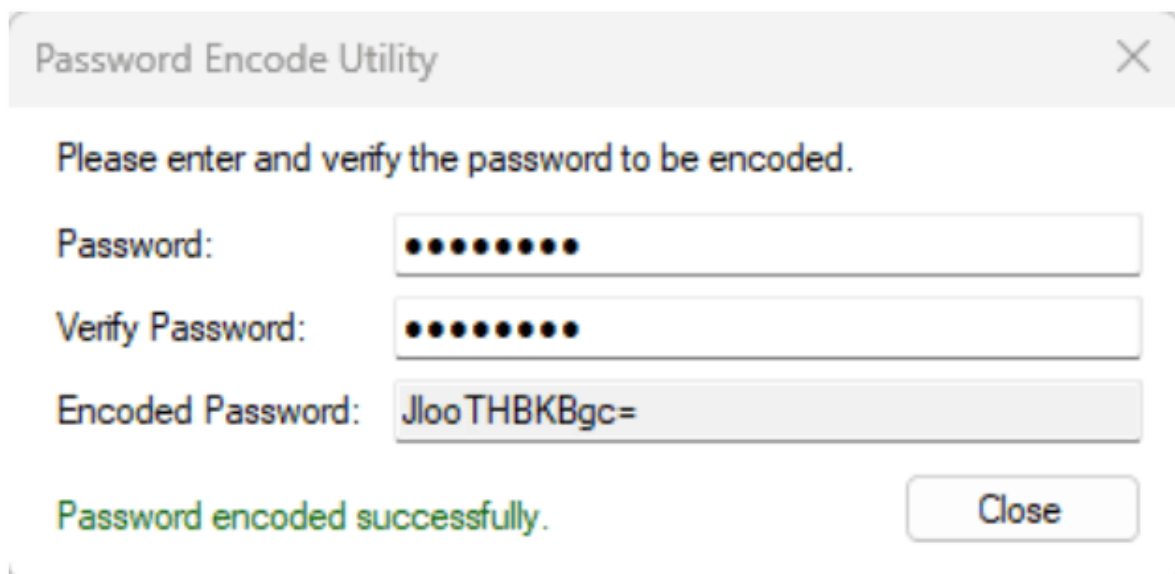
2. Pfad:

1. 3. C:\Programme\Senstar\Symphony Server V7_Tools\PasswordEncoder.exe



SenStar

4. Doppelklick PasswordEncoder.exe um das Encoder-Dienstprogramm zu starten.
5. Geben Sie das Gerätepasswort ein Geben Sie im Dienstprogrammfenster das ursprüngliche (im Klartext) Gerätepasswort ein, das im SenStar VMS konfiguriert ist.
6. Kopieren Sie das verschlüsselte Passwort Sobald das Passwort verschlüsselt ist, kopieren Sie die resultierende Zeichenfolge des verschlüsselten Passworts.



SenStar

7. Fügen Sie den verschlüsselten Passwortwert in das Streaming-Schlüssel Feld innerhalb des

Beispiel für einen Konfigurations-Screenshot

SenStar

SenStar

Konfiguration von Ereignissen und Regeln

Konfiguration von Senstar für Analysen und Systemalarme

Die Senstar VMS Die Plattform bietet eine umfassende Palette an Videoanalyse die Echtzeit-Benachrichtigungen bereitstellen, die zur einheitlichen Überwachung in GCX-ONE integriert werden können.

Zu diesen Analysefunktionen gehören unter anderem Bewegungserkennung, Manipulationserkennung bei Kameras, Kennzeichenerkennung, Objektverfolgung (Personen und Fahrzeuge), Personenzählung im Innen- und Außenbereich sowie fortschrittliche Sensorfusion.

Bevor Sie eine Videoanalyse für eine Kamera aktivieren können, müssen Sie die entsprechende Analyselizenz an das Gerät anschließen und alle erforderlichen Parameter konfigurieren – beispielsweise das Zeichnen von Verarbeitungsmasken oder das Kalibrieren des Kamerabildes. Ausführliche Anweisungen zur Konfiguration dieser Analysen und Systemalarme finden Sie in der offiziellen Senstar-Konfigurationshandbuch bereitgestellt von Senstar: Konfigurationshandbuch Senstar-Funktion „Supported Analytics“

ANALYTICS FEATURE	DESCRIPTION	LICENSING / NOTES
Camera Tampering	Detects when a camera's field of view is obstructed or the camera is repositioned.	Requires analytic license per camera.
Signal Loss (Analog Video)	Monitors analog camera feeds for signal loss (e.g.	solid color or no video).
Indoor People Tracking	Tracks movement of people indoors	counts dwell time
Outdoor People and Vehicle Tracking	Optimized for outdoor environments	tracks people and vehicles under lighting/weather changes.
Left & Removed Item Detection	Detects when an item is left behind or removed within a defined scene.	Use case: object-left detection in public spaces.
Crowd Detection	Estimates number of people in an area; useful for capacity monitoring and alerts when thresholds exceeded.	Often requires advanced license.
License Plate Recognition (ALPR)	Reads and indexes vehicle license plates; integrates with access control or operational workflows.	Region-specific versions available.
Face Recognition	Detects and recognizes faces	triggers events based on known/unknown individuals.

Konfigurationshandbuch für Aktionssätze

Die Konfiguration des Aktionssatzes in Senstar Symphony VMS legt fest, welche Aktionen das System ausführt, wenn bestimmte Regeln oder Ereignisse ausgelöst werden – beispielsweise das Versenden einer Benachrichtigung, das Aktivieren eines externen Geräts oder das Weiterleiten eines Alarms an eine Plattform eines Drittanbieters.

In der Integration der GCX-ONE-Plattform Action Sets spielen eine entscheidende Rolle dabei, sicherzustellen, dass alle Analyse- oder Systemereignisse von Senstar zuverlässig über eine TCP-Verbindung. Sobald Ereignisse und Regeln in Senstar konfiguriert sind, muss ein Aktionssatz erstellt und mit diesen Regeln verknüpft werden, um die Integration abzuschließen.

Voraussetzungen

Bevor Sie Aktionssätze für GCX-ONE konfigurieren:

- In GCX-ONE: Navigieren Sie zu Gerät → Bearbeiten → Eindeutige Referenznummer .

- Die Senstar VMS-Gerät müssen bereits zu GCX-ONE hinzugefügt worden sein und über eine gültige Eindeutige Referenznummer (deviceId) .
- In Senstar sollten Ereignisse und Regeln für die Kameras oder Analysen konfiguriert werden, die Sie überwachen möchten.
- Der Netzwerkzugriff vom Senstar VMS zum GCX-ONE-Cloud-Server muss über den angegebenen TCP-Port ermöglicht werden.

Erstellen eines Aktionssatzes in Senstar

Befolgen Sie die Standardanleitung von Senstar, um ein neues Aktionsset zu erstellen:

1. Öffnen Sie den Senstar Symphony Server Configuration Client.
2. Weiter zu Regeln und Aktionen → Aktionssätze .
3. Klicken Neues Aktionsset .
4. Geben Sie einen aussagekräftigen Namen für das Aktionsset ein (z. B. GCX-ONE_Alarm_Forwarder).
5. Unter Aktionen , klicken Sie auf Aktion hinzufügen → auswählen TCP .

GCX-ONE-spezifische TCP-Konfiguration

Nehmen Sie in der TCP-Nachrichtenkonfiguration die folgenden Einstellungen vor:

PARAMETER	VALUE	DESCRIPTION
Address	18.158.38.178	GCX-ONE TCP alarm receiver endpoint
Port	19232	GCX-ONE TCP listening port
Message (JSON)	(see below)	JSON body containing event metadata

JSON-Format der Nachricht

1. {

```

2  "deviceId": "<<gcx-one device="" id="">>",</gcx-one>
3  "Kamera": "%c",
4  "cameraName": "%e",
5  "Datei": "%f",
6  "RuleName": "%b",
7  „Richtlinie“: „%o“,
8  "metadata": "%md",
9  „AlarmTime“: {
    "Jahr": "%YYYY",
    "Monat": "%MM",
    "date": "%DD",
    "Stunde": "%hh",
    "Minute": "%mm",
    "second": "%ss",
    "ms": "%fff"
17 }
18 }

```

Parameterbeschreibung

FIELD	DESCRIPTION
deviceId	Unique Reference Number of the device registered in GCX-ONE (replace manually).
Camera	Internal camera ID from Senstar.
cameraName	Display name of the camera associated with the rule.
file	File path or name of the captured image or video clip associated with the event.

RuleName	The name of the triggering rule in Senstar.
Policy	The policy name under which the rule is configured.
metadata	Analytical or contextual metadata generated by Senstar (if available).
AlarmTime	Structured timestamp of when the alarm was triggered

Platzhalterreferenz (Senstar-Syntax)

Platzhalter wie %c, %e, %f usw. sind dynamische Variablen, die von Senstar automatisch ersetzt werden, sobald ein Ereignis eintritt:

PLACEHOLDER	VALUE
%c	Camera ID
%e	Camera Name
%f	File Name
%b	Rule Name
%o	Policy Name
%md	Metadata
%YYYY	Year
%MM	Month
%DD	Day
%hh	Hour
%mm	Minute
%ss	Second
%fff	Milliseconds

Prüfung und Verifizierung

1. Lösen Sie eine bekannte Regel in Senstar aus (z. B. einen Bewegungs- oder Analysealarm).
2. Überprüfen Sie in GCX-ONE, ob das entsprechende Ereignis in der Suche nach Videoaktivitäten oder im Alarm-Dashboard auf Geräteebeane angezeigt wird.

3. Falls keine Ereignisse angezeigt werden, überprüfen Sie die Netzwerkverbindungen zu 18.158.38.178:19232 und vergewissern Sie sich, dass das Aktionsset aktiv ist.

Bewährte Verfahren

- Überprüfen Sie vor dem Speichern immer die Verbindung mit dem Befehl „telnet 18.158.38.178 19232“.
- Stellen Sie sicher, dass die Firewall- oder ausgehenden Netzwerkrichtlinien TCP-Datenverkehr zum GCX-ONE-Endpunkt zulassen.
- Vermeiden Sie es, die Syntax der Platzhalter zu ändern – jedes falsche Zeichen führt zu einem Fehler beim Parsen von JSON.
- Verwenden Sie nach Möglichkeit UTC-Zeitstempel, um die Zeitsynchronisation zwischen Senstar und GCX-ONE aufrechtzuerhalten.

Übersicht über die Integrationsfunktionen

Die GCX-ONE-Plattform lässt sich nahtlos in die Senstar Symphony VMS durch eine Kombination aus API-Schnittstellen für Mobile Bridge , RTSP-Streaming und TCP-basierte Alarmweiterleitung . Diese Integration ermöglicht eine einheitliche Verwaltung, Überwachung und Auswertung aller angeschlossenen Kameras und Sensoren innerhalb des Senstar-Ökosystems.

FEATURE	DESCRIPTION	API/PROTOCOL USED	GCX-ONE INTEGRATION STATUS
Device Discovery	Automatically retrieves the list of configured cameras	encoders	and input/output channels from the Senstar VMS.
Live Stream	Provides real-time video streaming from cameras connected to the Senstar VMS for live monitoring.	RTSP	Integrated
Playback Stream	Enables access to recorded or historical footage from Senstar's video archive.	RTSP	Integrated
Timeline Control	Displays the recorded video timeline for each camera	allowing smooth scrubbing and playback control.	Mobile Bridge API

PTZ and Preset Control	Allow pan	tilt	and zoom control of supported cameras
Alarms	Forwards real-time event notifications (analytics	system	or rule-based alarms) to GCX-ONE using Action Sets.

Zusammenfassung

Wenn Sie dieser Anleitung folgen, können Sie Ihre Senstar-VMS-Instanz so konfigurieren, dass

Live-Videobilder und Alarmereignisdaten in Ihr GCX-ONE-Überwachungssystem eingespeist werden.

Diese Integration trägt dazu bei, Videoüberwachung und Sensoralarme zu vereinen, und sorgt für

reaktionsschnellere und ganzheitlichere Überwachungsabläufe.