

Clause de non-responsabilité

Avertissement juridique

Ce guide et son contenu (le « Guide ») sont fournis par NXGEN. Tous les droits sur le Guide et sur la propriété intellectuelle qu'il incorpore — y compris, sans s'y limiter, les marques, noms commerciaux, logos et signes similaires figurant dans ou sur le Guide — sont protégés par la loi. L'ensemble des droits, titres et intérêts relatifs au Guide et aux droits de propriété intellectuelle qui s'y rapportent appartiennent et demeurent à NXGEN et à ses concédants.

Le Guide est fourni gratuitement, « en l'état » et à titre d'information uniquement, sans garantie d'aucune sorte. Il n'est ni destiné ni propre à établir une quelconque relation juridique entre le lecteur et NXGEN ou ses sociétés affiliées, y compris, sans s'y limiter, une quelconque obligation de NXGEN ou de ses sociétés affiliées envers le lecteur.

Les obligations de NXGEN et de ses sociétés affiliées concernant les produits ou services NXGEN achetés par un client sont régies exclusivement par les termes du contrat au titre duquel ces produits ou services ont été achetés.

Pour clarification

Le lecteur assume l'intégralité du risque quant à l'utilisation, aux résultats et aux performances du Guide. Dans toute la mesure permise par la loi applicable, NXGEN décline et exclut toutes garanties, qu'elles soient légales, expresses ou implicites — y compris, sans s'y limiter, les garanties implicites de qualité marchande, d'adéquation à un usage particulier, de titre et de non-contrefaçon des droits de tiers — ainsi que toute responsabilité ou garantie découlant de suggestions, spécifications ou échantillons liés au Guide.

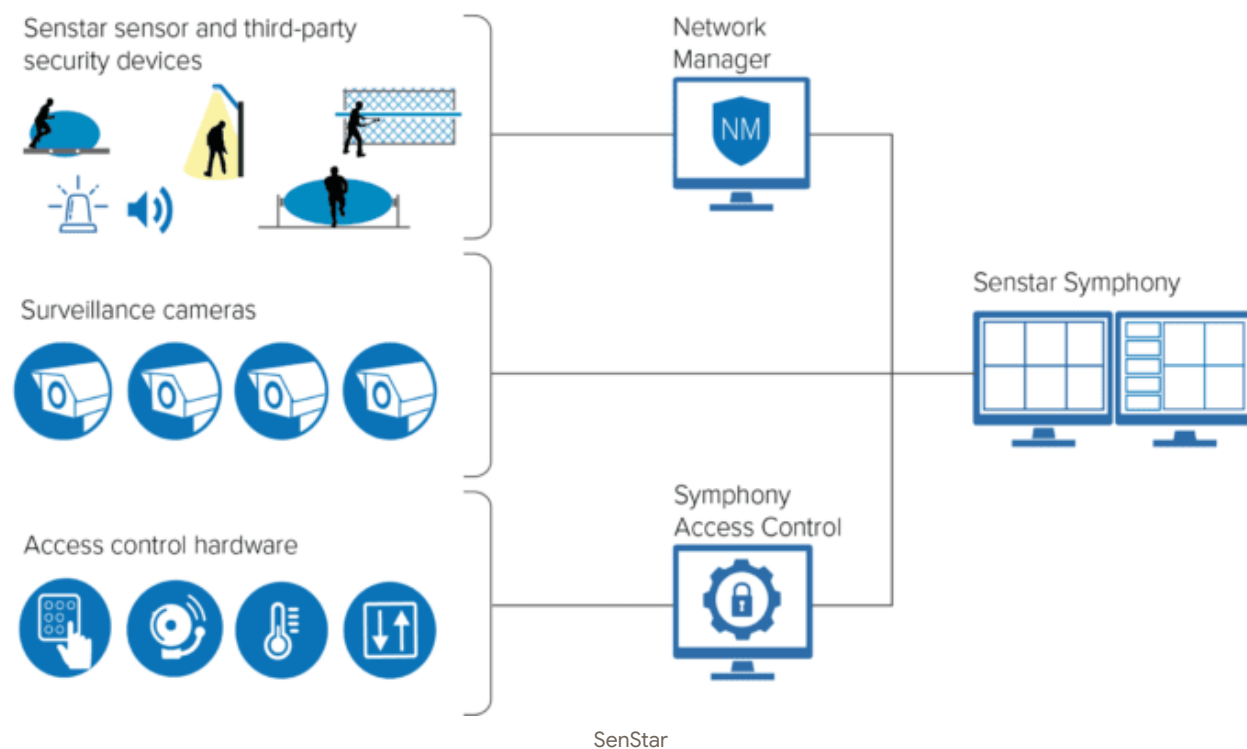
SenStar

Updated 16 August 2026

Introduction

Ce guide explique comment Intégrer et configurer le système de gestion vidéo Senstar (VMS) au sein de votre cadre d'opérations de sécurité. Il couvre les étapes clés pour configurer la connectivité des appareils et l'intégration avec les plateformes de surveillance. L'objectif est de permettre une télémétrie d'événements fluide de Senstar vers la plateforme GCX-ONE et d'assurer une alerte efficace, une corrélation vidéo et une visibilité opérationnelle.

Les offres de gestion vidéo de Senstar incluent la plateforme logicielle VMS (par exemple, Senstar Symphony Common Operating Platform) et des modules de support pour les caméras, l'analyse vidéo, le contrôle d'accès et la détection d'intrusion périmétrique.



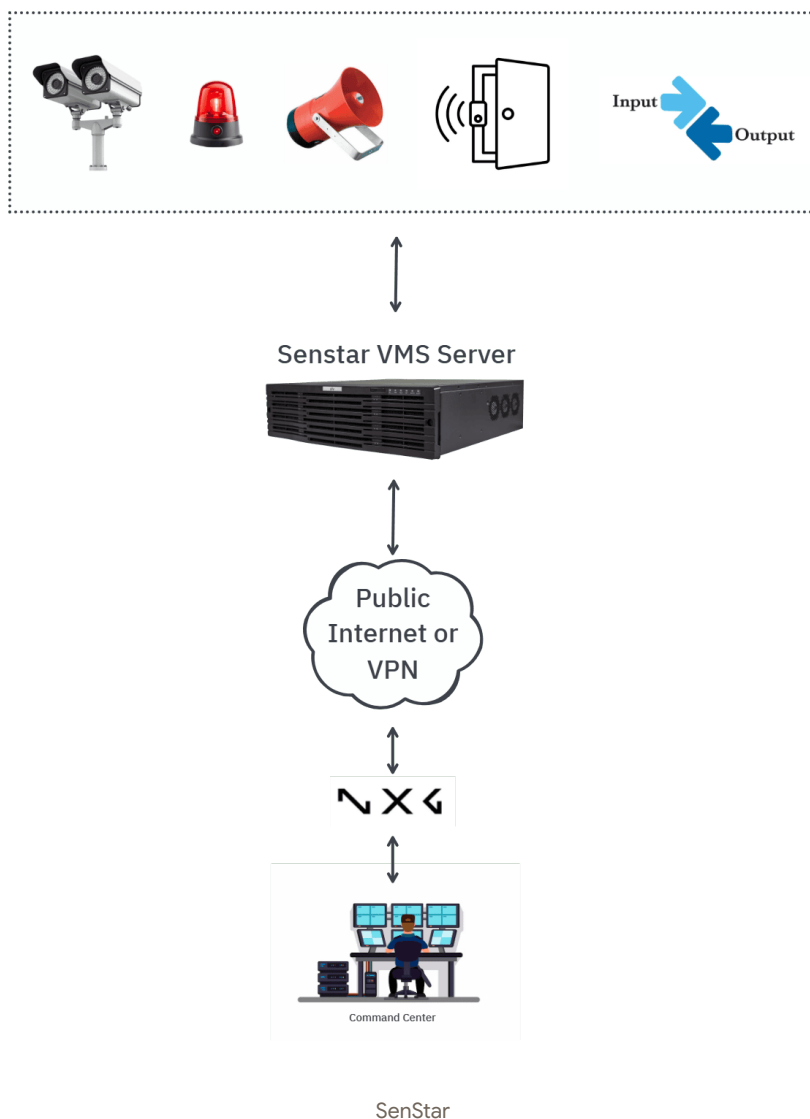
Lorsqu'il est utilisé dans votre environnement sécurisé, le Senstar VMS agit comme le Moteur central de vidéo et d'événements :

- Il agrège les flux vidéo provenant des caméras du site.
- Il collecte les alarmes et l'état des capteurs, des analyses et des E/S connectées.
- Il offre une interface utilisateur unifiée aux opérateurs et s'intègre avec des plateformes externes.

Architecture système

Dans un déploiement typique :

1. Les caméras (IP/analogique) sont diffusées vers le serveur VMS Senstar (sur site / appliance).
2. Des capteurs de sécurité connectés alimentent l'E/S et la télémétrie dans le VMS ou son module d'intégration des capteurs.
3. Le VMS génère des événements (par exemple, détection d'intrusion, alarme de capteur, alerte vidéo analytique) qui sont transmis au système central de surveillance via API, TCP ou SDK.
4. GCX-ONE reçoit ces événements, effectue des filtres de fausses alertes et déclenche des notifications à CMS en conséquence.



SenStar Configuration

Exigences préalables à l'intégration

1. Confirmez la version Senstar VMS (8.10) ainsi que tous les modules nécessaires (par exemple, gestion vidéo, analyses).
2. Assurez la connectivité réseau (accès public ou via VPN) entre le serveur VMS et la plateforme de surveillance (GCX-ONE).
3. Assurez-vous que le service API Mobile Bridge fonctionne. Guide détaillé de configuration du système Senstar disponible [ici](#).

4. Créer ou identifier un Compte utilisateur d'intégration dans Senstar avec suffisamment de privilèges administrateur pour accéder aux flux d'événements et aux alarmes.

Guide de configuration SenStar avec GCX-ONE

Dans le Plateforme GCX-ONE, vous pouvez enregistrer le Instance VMS de Senstar comme dispositif de type « SenStar ». Cette configuration établit un canal de communication sécurisé entre GCX-ONE et le Senstar Video Management System, permettant la synchronisation des événements, l'accès en flux vidéo et le commandement & contrôle.

Paramètres clés de configuration

NOM DU PARAMÈTRE	DESCRIPTION	VALEUR D'EXEMPLE
Type de dispositif	Sélectionnez SenStar comme type d'appareil pour permettre l'intégration avec la plateforme Senstar VMS.	SenStar
Nom de l'appareil	Un nom unique pour identifier cette instance VMS au sein de GCX-ONE. Ce nom apparaîtra également dans les tableaux de bord et les journaux d'événements.	Tower01_VMS
IP serveur / Nom d'hôte	L'adresse IP ou le nom d'hôte du serveur ou de l'appareil VMS Senstar où le Mobile Bridge est hébergé.	192.168.10.25
HTTP/S Port	Le port de l'API Mobile Bridge servait à accéder à l'API Senstar et à l'interface d'écoute des événements. La valeur par défaut est 8433.	8433
Activez HTTPS	Activez cette option si le serveur VMS Senstar est configuré pour supporter une communication HTTPS sécurisée.	Vrai
Nom d'utilisateur	Le nom d'utilisateur du compte d'intégration avec l'API et les privilèges d'abonnement aux événements.	integration_admin
Mot de passe	Le mot de passe correspondant pour le compte d'intégration.	

Porte-retrait RTSP	Le port Proxy Vidéo Mobile Bridge est utilisé pour les flux vidéo en direct et enregistrés depuis des caméras connectées.	8488
Clé de diffusion	Jeton d'authentification codé qui remplace le mot de passe simple lors de l'accès aux flux RTSP via des protocoles non sécurisés.	aHROcHM6Ly8xOTluMTY4LjEwLjI1OjU1NC9zdHJIYW0=
Fuseau horaire de l'appareil	Le fuseau horaire du serveur VMS Senstar. Assurez-vous qu'il correspond au fuseau horaire système configuré dans GCX-ONE pour maintenir la précision des événements.	CET (+1:00)

Génération de clés en streaming

Le Intégration Senstar VMS nécessite un Mot de passe de streaming codé pour accéder de manière sécurisée aux flux vidéo en direct et enregistrés basés sur RTSP. Ce mécanisme améliore la sécurité en évitant l'exposition directe du mot de passe en texte clair lors de l'authentification du flux.

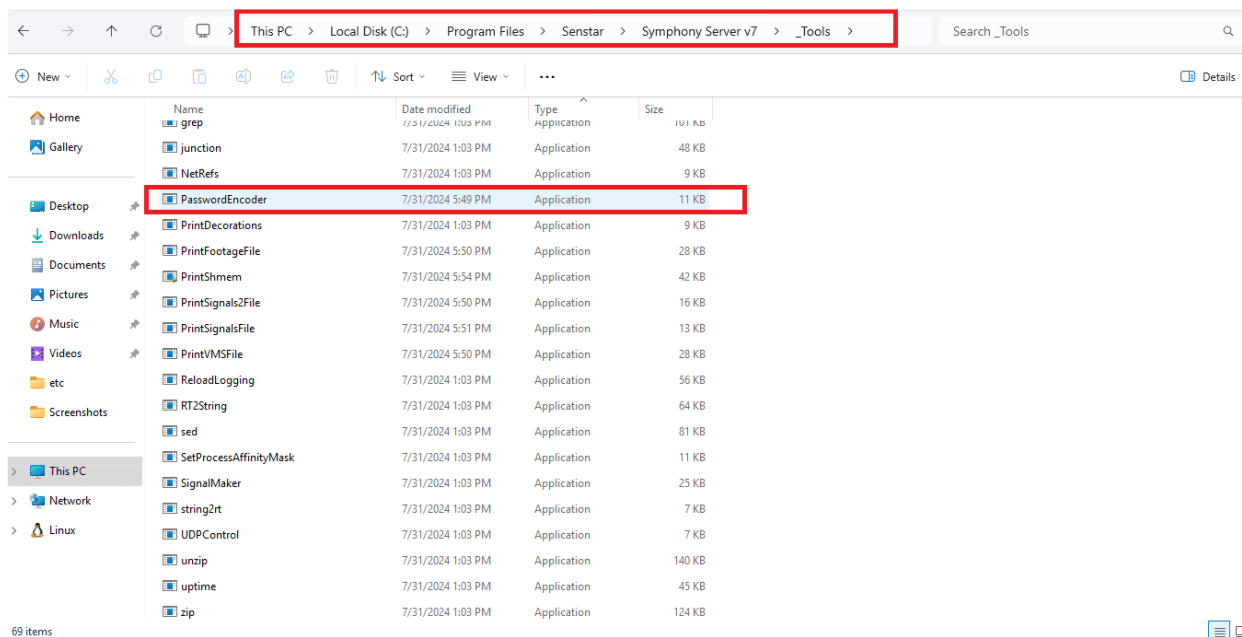
Étapes pour générer le mot de passe codé

1. Localiser l'utilitaire d'encodeur de mot de passe

L'outil de codage de mot de passe, PasswordEncoder.exe, est installé dans le cadre du package Senstar Symphony Server. Il ne peut pas être téléchargé séparément. Assurez-vous que le Serveur symphonique de Senstar est installé sur votre système avant de procéder.

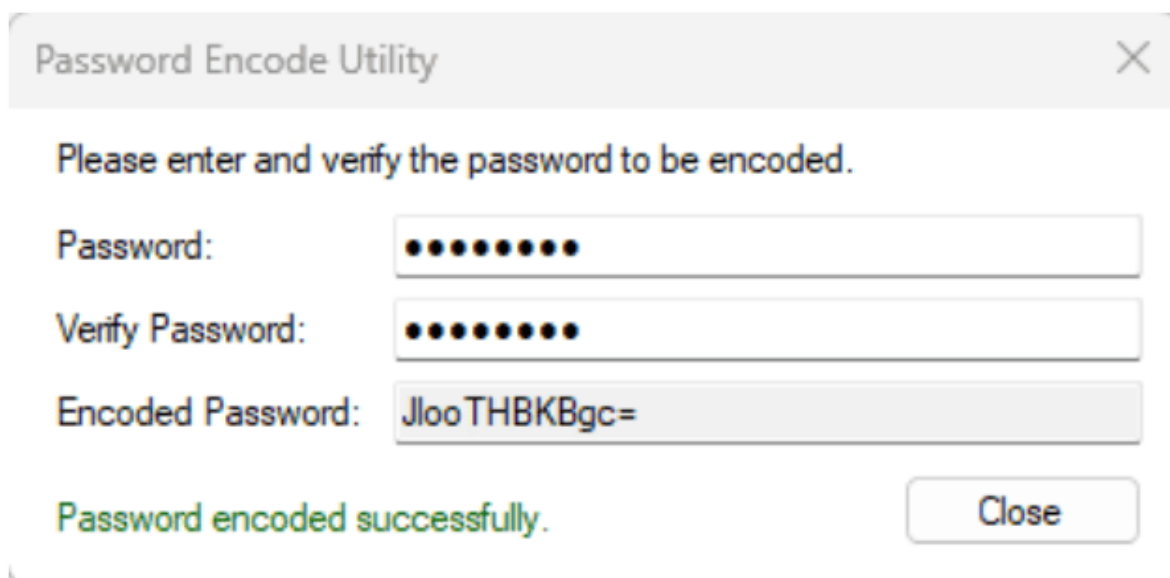
2. Chemin :

3. C:\Program Files\Senstar\Symphony Server V7\Tools\PasswordEncoder.exe



SenStar

4. Double-clic PasswordEncoder.exe pour lancer l'utilitaire encodeur.
5. Saisissez le mot de passe de l'appareil Dans la fenêtre utilitaire, saisissez le mot de passe original (texte brut) de l'appareil configuré dans la VMS Senstar.
6. Copier le mot de passe codé Une fois le mot de passe encodé, copiez la chaîne de mots de passe encodée qui en résulte.



SenStar

7. Collez la valeur du mot de passe codée dans le Clé de diffusion Champ dans le Configuration des appareils GCX-ONE page pour votre instance VMS Senstar.

Exemple de capture d'écran de configuration

SenStar

SenStar

Configuration des événements et des règles

Configuration de Senstar pour l'analyse et les alarmes système

Le Senstar VMS La plateforme propose une suite complète de Analyse vidéo qui fournissent des alertes en temps réel pouvant être intégrées à GCX-ONE pour une surveillance unifiée.

Ces analyses incluent des fonctionnalités telles que la détection de mouvement, la falsification de caméras, la reconnaissance des plaques d'immatriculation, le suivi des objets (personnes et véhicules), le comptage des personnes intérieures et extérieures, et la fusion avancée des capteurs.

Avant de pouvoir activer une analyse vidéo pour une caméra, vous devez assigner les données appropriées Licence analytique à l'appareil et configurer tous les paramètres nécessaires — comme dessiner des masques de traitement ou calibrer la vue de la caméra. Pour des instructions détaillées sur la configuration de ces analyses et alarmes système, veuillez consulter l'officiel Senstar Configuration Guide fourni par Senstar : Guide de configuration

Fonctionnalité d'analyse prise en charge par Senstar

FONCTIONNALITÉ ANALYTIQUE	DESCRIPTION	LICENCES / NOTES
Manipulation de caméra	Détecte lorsque le champ de vision d'une caméra est obstrué ou que la caméra est repositionnée.	Nécessite une licence analytique par caméra.
Perte de signal (vidéo analogique)	Il surveille les flux analogiques des caméras pour détecter la perte de signal (par exemple	couleur unie ou absence de vidéo).
Suivi des personnes en intérieur	Il suit les mouvements des personnes à l'intérieur	compte le temps d'observation
Personnes en extérieur et suivi des véhicules	Optimisé pour les environnements extérieurs	il suit les personnes et les véhicules sous l'éclairage et les changements météorologiques.
Détection d'objets à gauche et supprimés	Détecte lorsqu'un élément est laissé derrière ou retiré dans une scène définie.	Cas d'utilisation : détection de gauche d'objet dans les espaces publics.
Détection de foule	Estime le nombre de personnes dans une zone ; utile pour la surveillance de la capacité et les alertes lorsque les seuils dépassent.	Il faut souvent obtenir une licence avancée.
Reconnaissance des plaques d'immatriculation (ALPR)	Lit et indexe les plaques d'immatriculation des véhicules ; s'intègre avec le contrôle d'accès ou les flux de travail opérationnels.	Des versions spécifiques à chaque région sont disponibles.
Reconnaissance faciale	Détecte et reconnaît les visages	déclenche des événements basés sur des individus connus ou inconnus.

Guide de configuration de l'ensemble d'actions

La configuration de l'ensemble d'actions dans Senstar Symphony VMS définit quelles actions le système effectue lorsque des règles ou événements spécifiques sont déclenchés — par exemple, envoyer une notification, activer un appareil externe ou transférer une alarme vers une plateforme tierce.

Dans le Intégration de la plateforme GCX-ONE , Les ensembles d'actions jouent un rôle clé pour garantir que tous les événements analytiques ou système provenant de Senstar soient transmis de manière fiable à GCX-ONE via un Connexion TCP . Une fois les événements et règles configurés dans Senstar, un ensemble d'actions doit être créé et lié à ces règles pour compléter l'intégration.

Prérequis

Avant de configurer les ensembles d'actions pour GCX-ONE :

- Dans GCX-ONE : naviguer vers Dispositif → Modifier → Numéro de référence unique .
- Le Dispositif VMS Senstar doit déjà être ajouté à GCX-ONE et avoir une validité Numéro de référence unique (deviceId) .
- Les événements et règles doivent être configurés dans Senstar pour les caméras ou les analyses que vous souhaitez surveiller.
- L'accès au réseau doit être autorisé depuis la VMS Senstar au serveur cloud GCX-ONE sur le port TCP spécifié.

Créer un ensemble d'action à Senstar

Suivez la procédure standard de Senstar pour créer un nouvel ensemble d'actions :

1. Client de configuration du serveur Senstar Symphony.
2. Aller à Règles et actions → ensembles d'actions .
3. Click Nouveau jeu d'action .

4. Entrez un nom descriptif pour l'Action Set (par exemple, GCX-ONE_Alarm_Forwarder).
5. Sous Actions , clic Ajouter une action → sélectionner TCP.

Configuration TCP spécifique à GCX-ONE

Dans la configuration du message TCP, appliquez les paramètres suivants :

PARAMÈTRE	VALEUR	DESCRIPTION
Adresse	18.158.38.178	Extrémité du récepteur d'alarme GCX-One TCP
Port	19232	Port d'écoute GCX-One TCP
Message (JSON)	(voir ci-dessous)	Corps JSON contenant les métadonnées d'événements

Message JSON Format

```
1. {  
2   « deviceId » : « <<ID de dispositif GCX-ONE>> »,  
3   « Caméra » : « %c »,  
4   « NomCaméra » : « %e »,  
5   « file » : « %f »,  
6   « NomDeRègle » : « %b »,  
7   « Politique » : « %o »,  
8   « metadata » : « %md »,  
9   « AlarmTime » : {  
    « année » : « %YYYY »,  
    « mois » : « %MM »,  
    « date » : « %DD »,  
    « heure » : « %hh »,
```

```
« minute » : « %mm »,
```

```
« deuxième » : « %ss »,
```

```
« ms » : « %fff »
```

```
17. }
```

```
18. }
```

Description des paramètres

TERRAIN	DESCRIPTION
deviceld	Numéro de référence unique de l'appareil enregistré dans GCX-ONE (remplacez manuellement).
Caméra	Identifiant interne de la caméra de Senstar.
Nom de la caméra	Nom affiché de la caméra associée à la règle.
fichier	Chemin de fichier ou nom de l'image ou du clip vidéo capturé associé à l'événement.
Nom de la règle	Le nom de la règle déclencheuse dans Senstar.
Politique	Le nom de la politique sous lequel la règle est configurée.
Métadonnées	Métadonnées analytiques ou contextuelles générées par Senstar (si disponibles).
AlarmTime	Horodatage structuré du moment où l'alarme a été déclenchée

Référence provisoire (Senstar Syntax)

Les réservoirs tels que %c, %e, %f, etc. sont des variables dynamiques remplacées automatiquement par Senstar lorsqu'un événement se produit :

MARQUEUR	VALEUR
%c	Identification de la caméra
%e	Nom de la caméra
%f	Nom du fichier
%b	Nom de la règle

%o	Nom de la politique
%md	Métadonnées
%OUIAAAAAAAAAAAAAAAAAAAA	Année
%MM	Mois
%DD	Jour
%hh	Heure
%mm	Minute
%ss	Deuxième
%fff	Millisecondes

Tests et vérification

1. Déclenchez une règle connue dans Senstar (par exemple, alerte de mouvement ou d'analytique).
2. Dans GCX-ONE, vérifiez que l'événement correspondant apparaît dans la recherche d'activité vidéo ou dans le tableau de bord d'alarme au niveau de l'appareil.
3. Si aucun événement n'apparaît, confirmez la portée du réseau à 18.158.38.178:19232 et vérifiez que l'Action Set est actif.

Bonnes pratiques

- Testez toujours la connectivité avec le telnet 18.158.38.178 19232 avant de sauvegarder.
- Assurez-vous que les politiques du pare-feu ou du réseau sortant permettent au trafic TCP vers le point d'extrémité GCX-ONE.
- Évitez de modifier la syntaxe des substituts — tout caractère incorrect cassera l'analyse JSON.
- Utilisez des horodatages UTC lorsque possible pour maintenir la synchronisation temporelle entre Senstar et GCX-ONE.

Présentation des fonctionnalités d'intégration

La plateforme GCX-ONE s'intègre parfaitement avec le Senstar Symphony VMS par une combinaison de API de ponts mobiles , RTSP streaming , et Transfert d'alarme basé sur TCP . Cette intégration permet une gestion, une surveillance et des analyses unifiées pour toutes les caméras et capteurs connectés au sein de l'écosystème Senstar.

CARACTÉRISTIQUES	DESCRIPTION	API/PROTOCOLE UTILISÉ	ÉTAT DE L'INTÉGRATION DE GCX-ONE
Découverte des dispositifs	Récupère automatiquement la liste des caméras	encodeurs et canaux d'entrée/sortie configurés depuis le VMS Senstar.	Mobile Bridge API
Diffusion en direct	Fournit un streaming vidéo en temps réel depuis des caméras connectées au Senstar VMS pour une surveillance en direct.	RTSP	Intégré
Flux de lecture	Permet d'accéder à des images enregistrées ou historiques provenant des archives vidéo de Senstar.	RTSP	Intégré
Contrôle de la chronologie	Affiche la timeline vidéo enregistrée pour chaque caméra	permettant un frottement fluide et un contrôle de la lecture.	Mobile Bridge API
PTZ et contrôle pré réglé	Permettre le contrôle de panoramique	d'inclinaison et de zoom des caméras supportées	ainsi que la possibilité de déclencher des pré réglages PTZ prédéfinis.
Alarmes	Transmettre les notifications d'événements en temps réel (analyses	alarmes système ou basées sur des règles) vers GCX-ONE à l'aide des ensembles d'actions.	TCP

Résumé

En suivant ce guide, vous pourrez configurer votre instance VMS Senstar pour alimenter en direct les données vidéo et les événements d'alarme dans votre écosystème de surveillance GCX-ONE.

Cette intégration permet d'unifier la vidéosurveillance, les alarmes capteurs, et rend vos opérations de surveillance plus réactives et globales.