



ARCANES
VIDEO TECHNOLOGY



CONFIGURATION DU SYSTÈME

Version 7.0

août 2023

Ce document décrit la configuration des systèmes VXCORE avec l'image d'installation officielle.

Table des matières

1	Pré-requis.....	4
1.1	Définitions courantes.....	4
1.2	Caméras et flux vidéo compatibles.....	4
2	Configuration des modèles de caméras.....	7
2.1	Création automatique d'un modèle de caméra.....	8
2.1.1	Détection / configuration ONVIF.....	8
2.1.2	Détection / configuration ARP.....	9
2.2	Création modèle de caméras constructeur.....	11
2.3	Configuration / Personnalisation des modèles de caméras.....	12
2.3.1	Options propriétaires.....	13
2.3.2	Proxy / Flux Vidéo.....	14
2.3.3	Configuration des modes vidéo.....	14
2.3.4	Contrôle PTZ et driver.....	15
3	Configuration d'une caméra.....	16
3.1	Assistant de configuration.....	16
3.1.1	Configuration de l'analyse vidéo.....	17
3.1.2	Configuration système automatique.....	18
3.2	Configuration avancée.....	19
3.3	Zones réactives.....	21
3.4	Inventaire.....	22
4	Configuration des flux vidéo.....	23
5	Analyse vidéo.....	25
5.1	Analyse vidéo 1 - principale.....	26
5.1.1	Détection de mouvement simple.....	26
5.1.2	Détection de mouvement avancée.....	26
5.1.3	Détection de mouvement IA.....	27
5.1.4	Configuration de l'analyse.....	27
5.2	Analyse vidéo 2 - secondaire.....	31
5.2.1	Reconnaissance des plaques d'immatriculations.....	31
6	Alarmes / détections.....	33
6.1	Limitation des événements d'alarmes.....	34
6.2	Options générales.....	35
6.3	Alarme analyse vidéo simple.....	37
6.4	Alarme analyse vidéo avancée.....	39
6.5	Alarme analyse vidéo IA.....	42
6.6	Alarme réseau (FTP).....	44
6.7	Alarme réseau (HTTP/S).....	45
6.8	Scénario d'alarmes.....	46
6.9	Alarme centralisée (VPN).....	47
7	Messages audio.....	49
8	Programmation.....	51
8.1	Programmation des événements systèmes.....	51
8.2	Configuration des calendriers.....	51
8.3	Configuration des rondes PTZ.....	52
8.3.1	Ronde PTZ active.....	52
8.3.2	Ronde PTZ home.....	53
8.4	Configuration des commandes I/O.....	53
8.4.1	Configuration des périphériques de contrôle I/O.....	53
8.4.2	Configuration des commandes.....	54

8.5 Configuration des actions.....	55
9 Agents de sécurité et Supervision.....	56
9.1 Agents de sécurité.....	56
9.2 Agents de supervision.....	60
10 Gestion des comptes / rôles.....	61
10.1 Description des comptes.....	61
10.2 Rôles.....	62
10.3 Administrateur système maintenance.....	63
10.4 Administrateur système vidéo.....	63
10.5 Utilisateur du système.....	66
11 Journaux systèmes.....	69

1 Pré-requis

1.1 Définitions courantes

Codec vidéo

Algorithme de compression/décompression des images vidéo. Le choix du codec et de l'algorithme vont déterminer les performances d'encodage/décodage et la taille ou le débit du flux vidéo.

Exemples de codecs vidéo : MJPEG, H.264, MPEG4, etc

Protocole de transport vidéo

Méthode de transmission des images vidéo sur le réseau IP. Les codecs vidéo ne sont pas tous compatibles avec les mêmes protocoles de transport.

Exemples de protocole de transport : HTTP, RTSP over TCP, RTSP over UDP, etc

Conteneur vidéo ou format de fichier

Méthode d'écriture et de lecture des données vidéo dans un fichier informatique. Les codecs vidéo ne sont pas tous compatibles avec les mêmes conteneur de fichier.

Exemples de conteneur vidéo : avi, mp4, mov, etc

1.2 Caméras et flux vidéo compatibles

Le système peut gérer jusqu'à 3 flux vidéo par caméra IP avec codec identique ou différent, en utilisant les protocoles HTTP / HTTPS / RTSP (UDP/TCP).

Flux vidéo MJPEG

Les flux vidéo MJPEG ne nécessitent pas de configuration particulière pour fonctionner directement avec le système. Ces anciens flux vidéo sont déconseillés car ils sont extrêmement gourmand en bande passante et stockage vidéo.

Flux vidéo H.265/H.264/MPEG4

Les flux vidéo H.265/H.264/MPEG4 nécessitent un paramétrage de base pour qu'ils puissent fonctionner correctement dans le système.

Entêtes de configuration des images

Les caméras devront être configuré pour une diffusion vidéo continue et non pour une diffusion à la demande en session unique (comme avec une "Webcam" IP).

La plupart des caméras IP du marché sont déjà configurées en ce sens et ne nécessiteront aucune intervention. Mais il existe malheureusement toujours des exceptions chez les constructeurs.

Concrètement, chaque bloc d'image devra intégrer les entêtes de configuration des images : SPS (Sequence Parameter Set) et PPS (Picture Parameter Set). Ce format de stream vidéo est appelé « **Annex B byte-stream** ».

Ces entêtes permettront à un système externe d'afficher les images correctement, en lisant directement dans le flux vidéo les paramètres de décodage des images (par exemple : la résolution et le frame rate vidéo).

Paramètres Intra-Frame

Pour obtenir une réactivité et un affichage optimal des flux vidéo, vous devez configurer vos caméras et les flux vidéo avec l'insertion d'une image de référence toutes les secondes (paramètres Intra-Frame ou taille de GOP).

Si votre modèle de caméra ne permet pas de configurer directement le temps d'insertion des Intra-Frame et vous demande une longueur de GOV : vous devez renseigner une taille de GOV qui sera égale au frame-rate de votre flux vidéo (exemple : flux vidéo à 23 images/seconde = GOV de 23 = 1 Intra-Frame par seconde).

Stream settings

Video settings for stream 1 [Viewing Window](#)

MPEG-4

H.264

Frame size: 1280x1024 ▼

Maximum frame rate: 25 fps ▼

Intra frame period: 1 S ▼

Video quality

Constant bit rate:

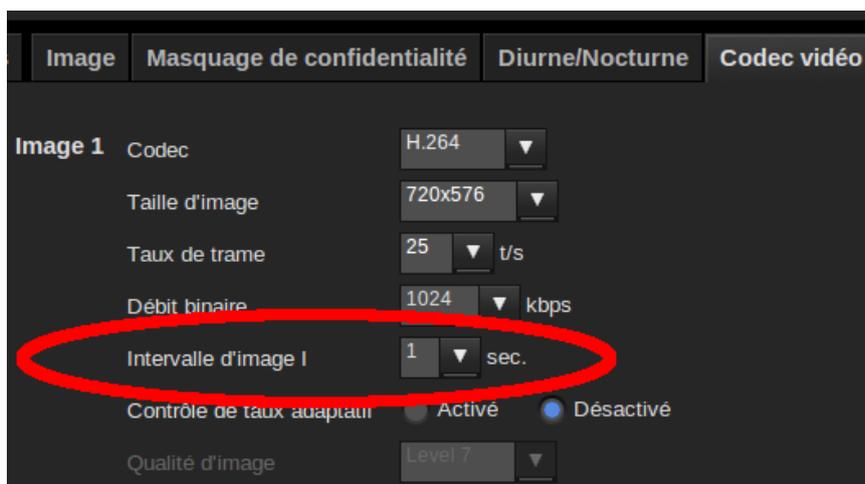
Bit rate restriction: Average Upper

Target bit rate: 4 Mbps ▼

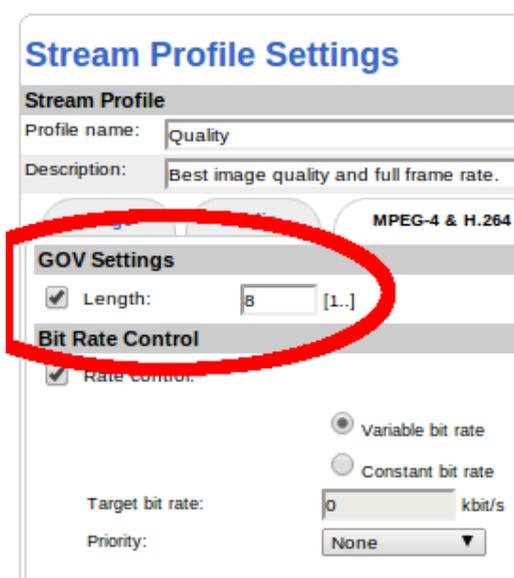
Policy: Frame rate priority

Fixed quality: Good ▼

Configuration Intra-Frame pour caméra VIVOTEK



Configuration Intra-Frame pour caméra SONY



Configuration Intra-Frame pour caméra AXIS

2 Configuration des modèles de caméras

Le système utilise une méthode ouverte d'intégration des caméras IP qui lui permet de gérer simplement et efficacement la plupart des modèles du marché.

Important : VXCORE est une solution qui s'installe derrière un parc caméra déjà configuré (adresse IP, flux vidéo, réglages d'images, etc).

Le système n'intègre pas de module de réglage de paramètres propre à chaque constructeur de caméra IP, il est avant tout un enregistreur de flux vidéo.

Une caméra est configurée via la création d'un "modèle" qui précise les flux vidéo qui seront ouverts et traités par le système. VXCORE peut gérer jusqu'à 3 flux vidéo H.265/H.264/MPEG4/MJPEG par caméra, via de multiples protocoles réseaux (HTTP, HTTPS, RTSP, etc).

Chaque flux vidéo sera dé-multiplexé et synchronisé dans la mémoire interne du système, appelée "Proxy Vidéo". Cette technologie permet de n'ouvrir qu'un seul flux vidéo par caméra et de le rediffuser sans limite aux utilisateurs (les limites seront fixées par les capacités de traitement du serveur et la bande passante disponible sur le réseau).

VXCORE sera aussi capable d'enregistrer en simultané les trois flux vidéo pour optimiser la consultation.

Exemple de configuration du Proxy Vidéo d'une caméra IP :

- Vidéo 1 - Flux vidéo H.265 : 1920x1080 - 25 img/s - 2.10 Mbits/s
- Vidéo 2 - Flux vidéo H.264 : 640x480 - 15 img/s - 0.13 Mbits/s
- Vidéo 3 - Flux vidéo MJPEG : 352x288 - 25 img/s - 2.47 Mbits/s

Tous les flux vidéo gérés par le système pourront être automatiquement affectés pour la visualisation via des accès réseau particuliers, comme sur le réseau local (LAN) ou les accès distant par Internet (WAN).

Exemple de configuration pour la visualisation des flux vidéo :

• **Visualisation flux vidéo via réseau LAN**

Flux vidéo 1 - H.265 : 1920x1080 - 25 img/s

• **Visualisation flux vidéo via réseau WAN (Internet)**

Flux vidéo 3 - MJPEG : 352x288 - 8 img/s

• **Visualisation flux vidéo via réseau MOBILE (smartphone)**

Flux vidéo 3 - MJPEG : 352x288 - 3 img/s

• **Visualisation flux vidéo pour mur d'images et/ou analyse vidéo**

Flux vidéo 2 - H.264 : 640x480 - 8 img/s

Le système ne dispose d'aucune limite de gestion en terme de flux vidéo, que ce soit par la taille/résolution d'image (exemple : vidéo Full HD 1920x1080), par le débit d'image (exemple : vidéo à 60 images/seconde) ou par la bande passante (exemple : flux vidéo MJPEG 8 Mégapixels à 50 Mbits/seconde).

Les limites seront fixées par les capacité de traitement et les ressources du serveur, comme pour la rediffusion des flux vidéo.

*Remarque : de manière générale pour optimiser les ressources du serveur et des caméras, il est recommandé de n'ouvrir que **deux flux vidéo par caméra** : un flux vidéo haute définition (4K/FULL-HD) et un flux vidéo basse définition (type VGA).*

Le système dispose d'une fonctionnalité de **transcoding vidéo** permettant de créer un flux vidéo supplémentaire à la demande, pour la consultation en très bas débit par exemple.

Avant d'ajouter une caméra dans le système et de pouvoir la visualiser ou l'enregistrer, vous devez d'abord créer un modèle de caméra.

Pour ajouter un modèle de caméra, vous pouvez utiliser le module d'auto-détection des caméras ou créer directement votre modèle dans la section configuration > Caméras > Configuration des modèles de caméras.

Un modèle de caméra rassemble toute la configuration nécessaire pour la gestion des flux vidéo ou des options spécifiques constructeurs comme le contrôle PTZ.

Le système dispose d'une fonctionnalité d'import/export des modèles de caméras ou la gestion d'un inventaire, vous permettant de constituer une base commune à plusieurs systèmes.

2.1 Création automatique d'un modèle de caméra

Pour détecter automatiquement un modèle de caméra, vous pouvez utiliser la fonctionnalité de recherche en cliquant sur le bouton « Configurer une nouvelle caméra » ou sur l'onglet « Rechercher des caméras ».

Il existe deux modes de recherche et configuration des modèles de caméras : **ONVIF** et **ARP**

Avant de lancer une recherche de caméras, vous pouvez également choisir l'interface réseau pour le scan, si votre système dispose de plusieurs cartes Ethernet (par défaut eth0).

2.1.1 Détection / configuration ONVIF

La méthode ONVIF permet d'utiliser le protocole standard de communication des caméras récentes.

La détection/configuration des caméras ONVIF va utiliser les méthodes du profil ONVIF-S : `getSystemDateAndTime`, `getDeviceInformation`, `getProfiles`, `getNodes`, `getVideoSources`, `getStreamUri`, `getServices`.

Si la caméra n'est pas complètement compatible vous ne pourrez pas utiliser cette méthode de configuration.

Pour les anciens modèles, utilisez plutôt la méthode de configuration ARP ou la création d'un modèle de caméra personnalisé.

Configuration des caméras		Rechercher des caméras réseau		Configuration des modèles de caméras		Inventaire	
Q Rechercher des caméras réseau [ARP]		Q Rechercher des caméras réseau [ONVIF]					
-	unknown	192.168.0.245	44:19:b6:68:7f:c6				
▶	DS-2CD2432F-IW	192.168.0.237	00:95:69:0a:a4:3c	+			
-	unknown	192.168.0.240	44:19:b6:68:80:00				
▶	AXIS M1065-LW	192.168.0.15	ac:cc:8e:fc:bb:2d				
-	unknown	192.168.0.244	44:19:b6:68:7f:93				
▶	AXIS M2026-LE-MKII	192.168.0.10	ac:cc:8e:fa:01:62				
▶	VIVOTEK CC9381-HV	192.168.0.233	00:02:d1:89:30:2d				
▶	HIKVISION DS-2CD2442FWD-IW	192.168.0.235	10:a4:be:de:2c:1c				
▶	2N-IPVERSO	192.168.0.200	7c:1e:b3:03:34:e3				
▶	DAHUA IPC-HDBW4431F-AS	192.168.0.236	e0:50:8b:fc:97:e9				

Après avoir fait un scan des caméras ONVIF, cliquez ensuite sur le bouton « Ajouter » pour afficher l'interface de création du modèle de caméra.

Vous devez ensuite renseigner un nom d'utilisateur et un mot de passe pour communiquer avec la caméra avec le protocole ONVIF.

Si vous ne renseignez pas bien vos identifiants ou si la caméra n'est pas compatible ONVIF, le système vous affichera une erreur.

Remarque : attention avec certains modèles de caméras, il est nécessaire de créer un utilisateur/compte spécifique pour utiliser le protocole ONVIF ou encore de l'activer dans la caméra avant de pouvoir l'utiliser.

Cliquez ensuite sur le bouton « Rechercher les flux vidéo » pour interroger automatiquement la caméra avec le protocole ONVIF.

Si la caméra est bien compatible, le système vous affichera les informations systèmes comme son numéro de série, sa version de firmware encore les flux vidéo configurés.

Vous devez ensuite choisir quels flux vidéo vous souhaitez affecter au proxy vidéo interne de VXCORE : video1, video2 et video3.

Le système va ensuite créer un modèle de caméra spécifique ONVIF qui pourra être modifié et personnalisé au besoin.

Après validation, votre caméra sera ajoutée dans le système, et vous serez redirigé vers l'assistant de configuration caméra, pour une activation rapide des paramètres de base. Si vous souhaitez régler plus de paramètres, cliquez sur le bouton « Configuration avancée » situé en bas.

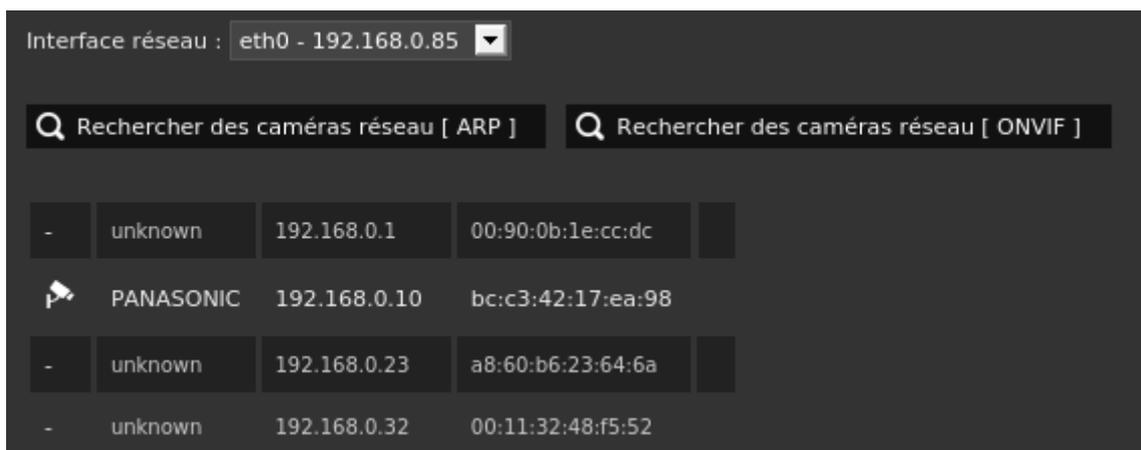
2.1.2 Détection / configuration ARP

La méthode ARP permet d'identifier les caméras sur le réseau par leur adresse Mac (utile pour les anciens modèles de caméras).

Si une caméra est reconnue par le système, il vous suffira de cliquer sur le bouton « Ajouter » pour afficher l'interface de configuration.

Vous devez ensuite saisir un identifiant et un mot de passe pour communiquer avec la caméra.

Le système va utiliser automatiquement les deux flux vidéo de la caméra : un flux vidéo haute définition (enregistrement/visualisation) et un flux vidéo basse définition (analyse vidéo, consultation à distance, transcodage vidéo, etc).



Remarque : la méthode ARP est avant tout un scan réseau, il affichera toutes les adresses IP présentes sur le réseau.

2.2 Création modèle de caméras constructeur

Si la méthode de détection ONVIF ou ARP ne fonctionnent pas correctement, vous devez créer un modèle de caméra personnalisé.

Pour simplifier la configuration, vous pouvez utiliser un modèle existant « constructeur caméra » que vous pourrez ensuite personnaliser.

Pour utiliser un modèle constructeur, cliquez sur le bouton « Personnaliser un modèle constructeur » et sélectionnez un fabricant dans la liste proposée.

The screenshot shows a configuration page titled "Caméras / Modèles". At the top, there are two fields: "Constructeur :" with a dropdown menu set to "AXIS / RTSP Dual Stream", and "Nom du modèle de caméra :" with a text input field containing "AXIS P3925-R". Below this is a section titled "PROXY VIDÉO". Underneath, there are three sections labeled "Video 1", "Video 2", and "Video 3". Each section contains the following fields: "Codec vidéo / Protocole:" (dropdown menu set to "VIDEO @ RTSP over TCP"), "Port vidéo:" (text input field), "Désactivé:" (checkbox), and "Adresse du flux vidéo:" (text input field). For Video 1, the address is "/axis-media/media.amp?videocodec=h264&streamprofile=Quality&audio=1&videopsen". For Video 2, the address is "/axis-media/media.amp?videocodec=h264&streamprofile=Bandwidth&videopsenabled". For Video 3, the address is empty and the codec dropdown is set to "-- sélectionnez --". At the bottom of the form, there are two buttons: "✓ Appliquer" and "◀ Retour".

Personnalisation d'un modèle constructeur

Important : ces modèles constructeurs sont avant tout utiles pour retrouver les adresses des flux vidéo des constructeurs de caméras. Vous devez les choisir et les personnaliser en fonction de vos propres caméras et surtout de leur configuration effective.

2.3 Configuration / Personnalisation des modèles de caméras

Les modèles de caméras sont avant tous des liens vers des adresses de flux vidéo. Vous devez donc bien renseigner les différentes adresses, et ne pas oublier de configurer les flux vidéo des caméras (résolution d'image, codec, bande passante, etc).

Tous les modèles de caméras pourront être personnalisés, que ce soit des modèles automatiques créés avec le protocole ONVIF, ou des modèles créés à partir d'un modèle constructeur exemple.

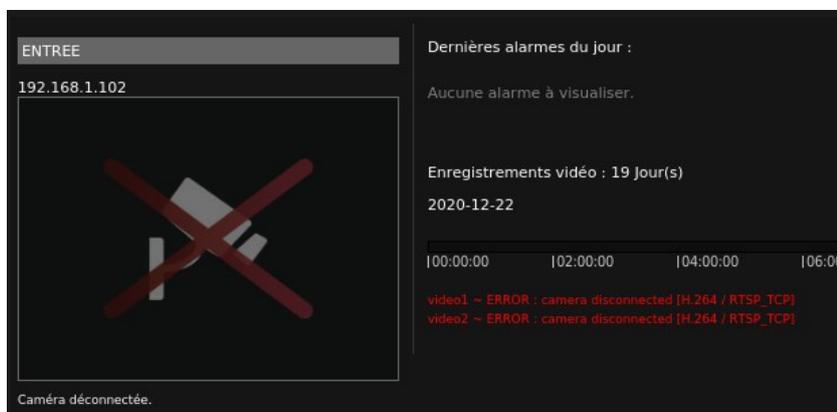
Remarque : lorsque vous changez la configuration d'un modèle de caméra, cela affectera toutes les caméras qui seront liées à ce modèle.

Un modèle de caméra est identifié par un code constructeur et un nom de modèle (exemple : AXIS M1065-LW).

Exemples d'erreurs courantes :

- Choix d'un modèle de caméra H.264 pour une caméra uniquement MJPEG/MPEG4 et inversement
- Activation du flux vidéo2 ou vidéo3 alors que la caméra ne le supporte pas (flux vidéo inexistant ou non configuré, caméra pas assez puissante pour traiter du multi-flux, etc)
- Incohérence de configuration du codec : flux vidéo H.264 configuré dans le modèle et flux vidéo MPEG4 configuré dans la caméra

Après avoir configuré un modèle de caméra et créer une caméra IP, vous pourrez voir dans le tableau de bord les éventuelles erreurs de flux vidéo :



Remarque : si vous modifiez les ports d'accès au flux vidéo (par exemple : port HTTP 8080 au lieu du port 80 par défaut), vous devez vous assurer que le système puisse effectivement accéder au nouveau port de la caméra.

2.3.1 Options propriétaires

Selon le modèle de votre caméra, vous pouvez activer des fonctionnalités propriétaires supplémentaires qui ont été spécialement intégré dans le système, comme les drivers PTZ pour contrôler les caméras dômes.



Contrôle PTZ applicatif optimisé : pilotage temps réel avec vecteur de déplacement

Driver PTZ

Un driver PTZ est un module spécialement développé pour le contrôle des caméras dômes motorisées. Selon le modèle, il sera possible de déplacer la caméra PTZ en mode Joystick/vecteur, en clic dans l'image ou encore de sélectionner des zones pour zoomer automatiquement.

Un driver générique ONVIF Profil-S est également disponible pour utiliser le protocole de communication standard des caméras.

Consultez le chapitre « Contrôle PTZ et drivers » pour plus de détails sur les drivers PTZ

Contrôle PTZ applicatif optimisé

Cette option permettra d'activer un mode de contrôle PTZ rapide et optimisé dans les applications en utilisant le protocole PTZ natif des caméras compatibles. Le contrôle PTZ pourra se faire instantanément avec un Joystick physique ou virtuel connecté au PC d'exploitation. Les vitesses de motorisation des caméras n'étant pas toute identiques, vous pouvez ajuster les vitesses Pan/Tilt/Zoom pour normaliser les contrôle entre les modèles de caméras.

Remarque : cette option ne sera disponible que si le driver PTZ sélectionné intègre un pilotage natif (exemple : AXIS / HIK / HANWHA / etc).

Fisheye / 360 Dewarping

Permet d'activer le Dewarping des caméras Fisheye/360 et de naviguer/zoomer dans l'image à 360 degré. Attention cette option n'est compatible qu'avec les caméras fixées au plafond à la verticale (et non murale). Pour un autre mode d'installation, vous devez configurer le dewarping directement dans l'interface de la caméra au niveau des flux vidéo.

2.3.2 Proxy / Flux Vidéo

La configuration du Proxy Vidéo va déterminer quels flux vidéo seront ouverts entre la caméra et le serveur VXCORE (jusqu'à 3 flux vidéo simultanés par caméra).

*Remarque : de manière générale pour optimiser les ressources du serveur et des caméras, il est recommandé de n'ouvrir que **deux flux vidéo par caméra** : un flux vidéo haute définition (4K/FULL-HD) et un flux vidéo basse définition (VGA). Le transcodage vidéo temps réel permettra de créer un flux vidéo supplémentaire pour la consultation très bas débit sur mobile.*

Consultez les documentations constructeurs de vos modèles de caméras pour connaître précisément les adresses des flux vidéo et les protocoles supportés.

Codec vidéo / Protocole

Définit le codec vidéo et le transport du flux vidéo entre la caméra et le serveur. Les protocoles de transport vidéo peuvent être différents selon le choix du codec vidéo (MJPEG ou H.264).

Utilisez de préférence le protocole standard VIDEO@RTSP/TCP compatible avec la plupart des caméras récentes (attention flux vidéo non chiffré).

Port vidéo

Permet de définir un port vidéo différent selon la configuration de la caméra. Si non spécifié, VXCORE utilisera les ports par défaut des protocoles de transport : HTTP (80), HTTPS (443), RTSP (554).

Adresse du flux vidéo

Renseigne l'adresse absolue du flux vidéo, commençant par un slash et pouvant contenir différents paramètres. Consultez la documentation de votre caméra pour connaître précisément les adresses et les paramètres des flux vidéo.

Désactivé

Cette option permet de désactiver la gestion du flux vidéo, comme s'il n'était pas configuré, mais tout en conservant la configuration.

Important : le système maintiendra ouvert en permanence tous les flux vidéo configurés. Votre architecture réseau/serveur doit donc être dimensionné en ce sens.

Il existe une option « **Flux vidéo à la demande** » sur certains systèmes, qui permet de n'ouvrir les flux vidéo que si un utilisateur le demande explicitement (consultation Live via logiciel PC ou application Mobile).

Dans ce mode de configuration, l'enregistrement ou l'analyse vidéo de la caméra ne fonctionneront que lorsque les flux vidéo seront consultés par un utilisateur. Le système coupera automatiquement les flux vidéo de la caméra si plus personne ne les visualise.

2.3.3 Configuration des modes vidéo

Il est possible de configurer directement les flux vidéo dans le modèle de caméra.

Grâce à ce paramétrage, le système configurera automatiquement les modes vidéo associés pour toutes les nouvelles caméras de même modèle ajoutées dans le système.

Ce paramétrage automatique pourra être ensuite adapté manuellement pour chaque caméra.

Remarque : le paramétrage automatique des flux vidéo n'interviendra que lors de la création d'une nouvelle caméra. Si vous modifiez les modes vidéo d'un modèle de caméra, cela n'affectera pas les réglages des caméras déjà configurées.

2.3.4 Contrôle PTZ et driver

VXCore intègre des fonctionnalités spécifiques pour la gestion des caméras PTZ.

Un driver PTZ est un microcode propriétaire spécialement développé pour une famille de caméra d'un constructeur. Il permettra de disposer de fonctionnalités supplémentaires pour piloter les caméras dômes motorisées compatibles.

Ces drivers PTZ ont été spécialement développés nativement à partir des documents officiels et des API constructeurs. Tous les constructeurs de caméras ne disposent pas des mêmes fonctionnalités de contrôle PTZ.

Pour activer les fonctionnalités PTZ d'une caméra, il suffit de sélectionner le bon driver dans le modèle de caméra. Le système se chargera alors de convertir les actions utilisateurs en commandes PTZ compatibles et de les transmettre à la caméra.

Important : pour contrôler et configurer les caméras PTZ, le système doit disposer d'un compte d'accès caméra avec permissions administrateur. L'identifiant et le mot de passe d'accès doivent être configurés correctement dans les paramètres de la caméra.

Chaque driver PTZ disposera de ses fonctionnalités en fonction du modèle de caméra (consultez les documentations constructeurs pour vérifier les possibilités).

Gestion des presets

Permet la création, la modification, la suppression et l'appel des positions "presets" de la caméra PTZ.

Déplacement PTZ continu

Déplace la caméra PTZ en mode joystick en restant appuyé pour piloter dans une direction (relâchement du bouton, arrêt des mouvements de la caméra)

Déplacement PTZ relatif

Déplace la caméra PTZ avec des mouvements simples à partir de la position relative actuelle : left, right, top, left, upleft, upright, topleft, topright, tele, wide, ...

Zoom min/max

Repositionne le zoom de la caméra au minimum ou au maximum (clic droit dans la vidéo = zoom minimum).

Centrer sur clic

Repositionne la caméra PTZ et centre la vue en fonction d'un clic utilisateur dans la vidéo.

Zoom sur zone

Repositionne la caméra PTZ et zoom sur une zone de l'image en fonction d'une sélection dans la vidéo.

*Important : pour obtenir de bons résultats d'exploitations, notamment sur la latence du contrôle PTZ, il sera **nécessaire d'activer le contrôle PTZ applicatif optimisé**.*

*Lorsque ce mode de contrôle n'est pas actif, toutes les requêtes PTZ vont transiter par le serveur et seront relayées vers la caméra : on considère plutôt cette méthode comme du « **repositionnement** » de caméra (contrôle PTZ difficilement exploitable pour du suivi en temps réel, en milieu urbain par exemple).*

3 Configuration d'une caméra

Après avoir configuré un modèle de caméra, vous pourrez maintenant ajouter une caméra dans le système.

Il existe deux modes de configuration :

- **un mode simple** avec assistant de configuration
- **un mode avancé** pour accéder à toutes les options

3.1 Assistant de configuration

L'assistant de configuration des caméras regroupera tous les éléments essentiels pour créer une configuration rapide et fonctionnelle.

Si vous avez ajouté une caméra avec la fonctionnalité de détection/recherche automatique, vous serez immédiatement redirigé sur cette interface.

Vous pouvez basculer à tout moment sur l'interface de configuration avancée en cliquant sur le bouton situé en bas.

Caméras / Assistant de configuration

Nom identifiant: ENTREE

Pas d'analyse vidéo | Analyse vidéo simple | Analyse vidéo avancée | Analyse vidéo IA (0 / 0)

Plan serré (gros objets) | Plan normal | Plan large (petits objets) | Paramètres personnalisés

Trafic/Activité faible | Trafic/Activité normal | Trafic/Activité dense

Configuration système automatique:

- Configurer automatiquement les flux vidéo
- Activer l'enregistrement vidéo
- Configurer automatiquement l'alarme associée

(*) Cochez ces options pour configurer automatiquement ou restaurer les fonctionnalités

Contrôle PTZ: OFF / Désactivé

✓ Appliquer | ⚙️ Configuration avancée | ⬅️ Retour

Assistant de configuration d'une caméra

Nom identifiant

Nom utilisé pour identifier la caméra dans le système. Évitez les accents et les caractères spéciaux qui peuvent parfois poser des problèmes d'encodage et d'affichage avec les smartphones. Si vous choisissez de configurer une alarme automatique, elle portera le même nom.

3.1.1 Configuration de l'analyse vidéo

Le système intègre des fonctionnalités d'analyse vidéo natives : détection de mouvement simple, détection de mouvement avancée SMART (couleurs, directions, comportement) ou détection d'objets SMART/IA (Deep Learning : détection des classes d'objets de type humains, voitures, vélo, animaux, etc).

Choix du type d'algorithme d'analyse vidéo

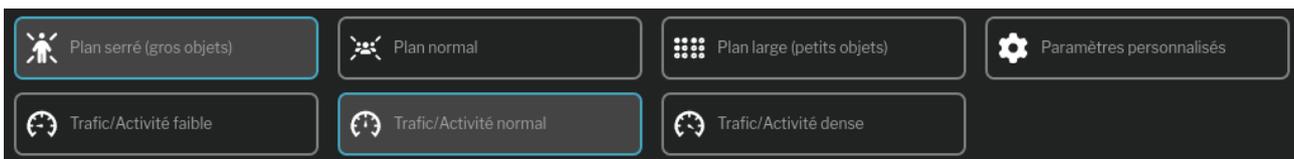
Pour chaque caméra, vous pouvez choisir d'activer l'analyse vidéo simple, avancée ou IA. Les algorithmes avancés et IA nécessiteront des licences supplémentaires.



Si vous ne souhaitez pas d'analyse vidéo sur la caméra ou tout désactiver : cliquez sur le bouton « Pas d'analyse vidéo ».

Profils de scène/trafic

Ces paramètres sont communs à tous les algorithmes d'analyse vidéo : simple, avancé ou IA. Vous le retrouverez dans l'interface de l'assistant de configuration ou dans la configuration avancée.



Les boutons permettent de pré-régler l'analyse vidéo sur un profil adapté en fonction du placement de la caméra et du plan qui sera filmé.

Ces profils de réglages vont grandement optimiser l'analyse vidéo, en ajustant automatiquement la résolution et le débit des images qui seront analysés, et ce pour chaque caméra. Avec de bons réglages, les économies en ressources de calculs pourront être significatives, ce qui vous permettra de rajouter encore plus de caméras sur votre serveur.

***** Consultez le chapitre de l'analyse vidéo pour la description de ces options *****

3.1.2 Configuration système automatique

Ces options permettent de configurer automatiquement des éléments du système : ne les cochez pas si vous ne souhaitez pas de configuration. Vous pouvez également utiliser ces options pour restaurer une configuration valide.

Configurer automatiquement les flux vidéo

Cette option permet d'attribuer automatiquement les flux vidéo des caméras. Le flux vidéo Haute définition VIDEO1 sera assigné en visualisation qualité optimale LAN, le flux vidéo Basse définition VIDEO2 sera assigné en visualisation qualité réduite WEB et MOBILE.

Remarque : si vous avez activé le transcodage vidéo, le flux vidéo VIDEO4 sera automatiquement assigné en qualité réduite WEB et MOBILE.

Activer l'enregistrement vidéo

Cette option permet d'activer les flux VIDEO1 et VIDEO2 pour l'enregistrement vidéo. Si la caméra a été programmée pour l'enregistrement vidéo continu ou sur alarme, elle sera immédiatement enregistrée.

Remarque : le flux vidéo VIDEO2 est enregistré afin d'optimiser les générations des vignettes d'alarmes, de l'analyse vidéo intelligente et de la consultation à distance des enregistrements. Il permet également de disposer d'un backup de l'enregistrement, au cas où le flux vidéo Haute définition VIDEO1 ne serait pas disponible, en erreur ou corrompu.

Configurer automatiquement l'alarme associée

Cette option permet de créer/configurer une alarme directement liée avec la caméra pour la détection de mouvement (simple, avancée ou IA). L'alarme sera créée avec le même nom identifiant que la caméra.

Remarque : l'alarme permet avant tout de créer un historique d'un évènement particulier et pour envoyer des notifications d'alertes, elle n'est pas nécessaire pour activer un enregistrement vidéo sur alarme/détection. L'analyse vidéo intelligente autorise à elle seule d'activer ce type d'enregistrement.

Contrôle PTZ

Cette option permet d'activer ou désactiver explicitement le contrôle PTZ de la caméra. Ce réglage sera prioritaire quelque soit la configuration définie dans le modèle de caméra. Vous pouvez donc forcer un driver PTZ particulier, ou explicitement désactiver le contrôle PTZ en sélectionnant l'option « OFF ». L'option par défaut « automatique » permet de récupérer la configuration du modèle de caméra. Si vous sélectionnez un modèle/driver qui est compatible avec le contrôle PTZ applicatif optimisé, il sera automatiquement activé.

3.2 Configuration avancée

La configuration avancée vous permettra d'accéder à tous les paramètres de la caméra. Si vous avez utilisé un modèle de caméra automatique, les adresses IP/port et identifiants ont été renseignés par le système.

Paramètres de base

Nom identifiant

Nom utilisé pour identifier la caméra dans le système. Évitez les accents et les caractères spéciaux qui peuvent parfois poser des problèmes d'encodage et d'affichage avec les anciens navigateurs Web.

Modèle de caméra

Choix du modèle de caméra précédemment créé dans le système. Le modèle de caméra déterminera quels flux vidéo seront gérés entre la caméra et le système.

Adresse IP / Hostname

Adresse IP statique de la caméra ou l'encodeur IP, elle peut être locale ou distante. Si vous spécifiez un "hostname" statique ou dynamique (exemple : dyndns.org), le système renseignera et mettra à jour automatiquement le champ de l'adresse IP (requête DNS).

Port de connexion

Port par défaut de contrôle de la caméra ou l'encodeur IP (en général son interface Web).

Remarque : ce port ne concerne que l'interface de contrôle de la caméra, ce n'est pas le port d'acquisition des flux vidéo (qui sont configurés dans le modèle de caméra).

Authentification

Définit le nom d'utilisateur et le mot de passe pour accéder aux informations de la caméra : flux vidéo, contrôle PTZ, commandes CGI, etc.

Flux vidéo

Les modes vidéo permettent de définir les flux vidéo qui seront utilisés en fonction de l'environnement réseau et de l'application utilisée.

Consultez la section « Modes vidéo » pour de plus amples informations sur la gestion des flux vidéo des caméras.

Vous pourrez utiliser le bouton spécial "Appliquer la configuration à toutes les caméras du même modèle" pour copier votre configuration sur l'ensemble des caméras du même modèle.

Audio

VXCORE peut gérer les flux audio des caméras compatibles, afin de pouvoir écouter le son en direct dans les applications PC/Mobile.

Afin d'activer le décodage de l'audio Live, il sera nécessaire de spécifier le format/encodage du flux audio de la caméra. Les formats audio supportés seront les codecs AAC et G.711/PCM (8 Khz ALAW ou MULAW).

*Important : pour permettre le décodage de l'audio, il sera nécessaire de configurer la caméra pour que l'audio soit bien activé au bon format sur le flux vidéo principal du système **VIDEO1**. Il sera également nécessaire de configurer le format de transport **RTSP** dans le proxy vidéo système **VIDEO1**.*

Onvif

Cet onglet n'apparaîtra que si vous avez créé un modèle de caméra en utilisant la méthode ONVIF et une caméra compatible.

Grace au protocole ONVIF vous pourrez directement modifier certains réglages des flux vidéo de la caméra, comme la résolution d'image ou encore le débit (fps/bitrate).

Pour afficher les options de configuration, cliquez sur le bouton « Afficher la configuration des flux vidéo de la caméra ».

Le système vous affichera les informations détaillées de la caméra, comme le modèle, numéro de série et firmware installé.

Pour chaque flux vidéo de la caméra, vous pourrez choisir son affectation dans le système : vidéo1, vidéo2 ou vidéo3.

A droite de chaque flux vidéo, vous pouvez cliquer sur l'icône de configuration pour configurer le flux vidéo de la caméra.

En fonction du modèle de caméra, vous pourrez modifier la résolution du flux vidéo, son débit d'image FPS ou encore son bitrate (en fonction des valeurs min/max supportées).

Après vos réglages, vous pouvez appliquer les changements en cliquant sur le bouton « Modifier la configuration ».

Vous pouvez aussi vérifier vos changements ou revenir à la configuration sauvegardée dans la caméra en cliquant sur le bouton « Recharger la configuration ».

Caméras / Caméra IP

CAMÉRA ONVIF MODES VIDÉO AUDIO ANALYSE VIDÉO 1 ANALYSE VIDÉO 2

🔍 Afficher la configuration des flux vidéo de la caméra

HIKVISION DS-2CD2332-1 / serial DS-2CD2332-I20140904CCWR477268053 / firmware V5.2.0 build 140721

Affectations des flux vidéo

H264 ~ 1920x1080 @ 25 FPS [VideoSource_1:Profile_1] → video 1 ⚙️

H264 ~ 704x576 @ 15 FPS [VideoSource_1:Profile_2] → video 2 ⚙️

video2 -- Configuration du flux vidéo

Encodage: H264 @ Main

Resolution: 704x576

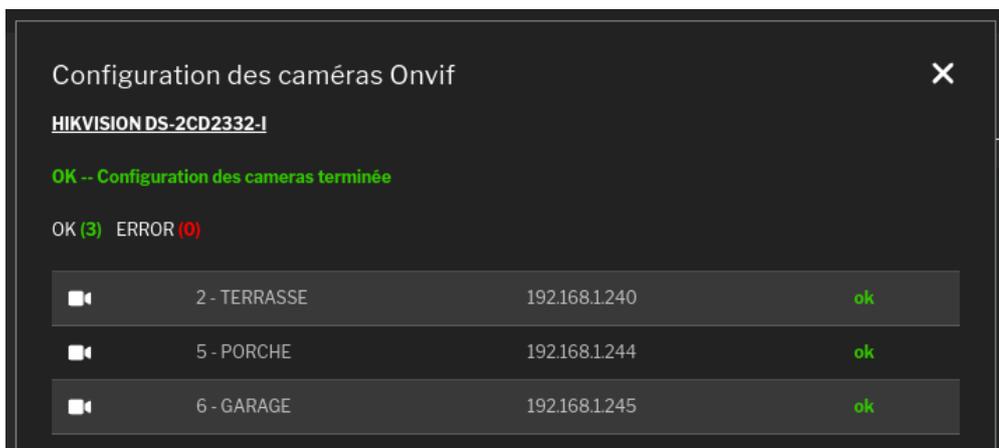
FPS: 15

Bitrate (kbps): 768 [min 32 - 8192 max]

⚙️ Modifier la configuration de la caméra 🔄 Recharger la configuration de la caméra ⏪ Annuler

⚙️ Appliquer la configuration sur toutes les caméras

Si vous souhaitez appliquer la même configuration sur l'ensemble des caméras du même modèle, cliquez sur le bouton « Appliquer la configuration sur toutes les caméras ». Une fenêtre popup spécifique s'affichera en indiquera l'état de la configuration automatique de chaque caméra (ok ou erreur).



Analyse vidéo

VXCORE peut activer deux algorithmes d'analyse vidéo pour chaque caméra du système :

- Analyse vidéo 1 : détection de mouvement simple, avancée ou IA
- Analyse vidéo 2 : reconnaissance des plaques d'immatriculation

***** Consultez le chapitre de l'analyse vidéo pour la description de ces options *****

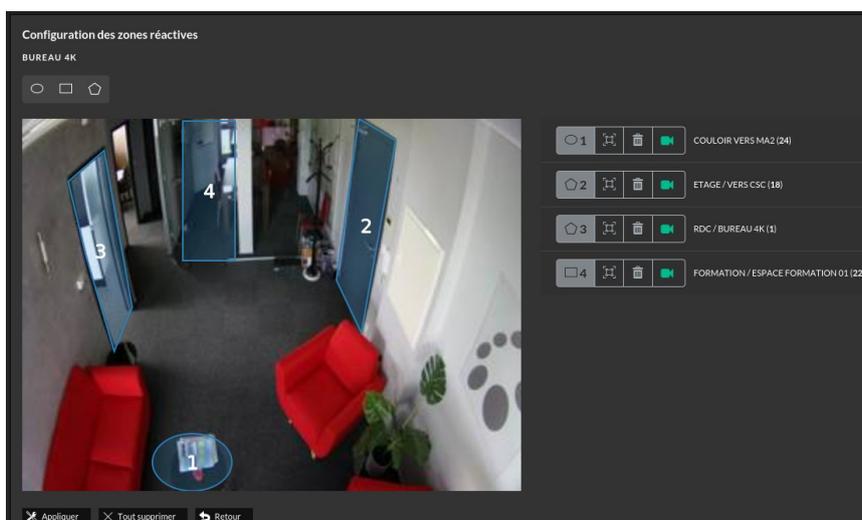
3.3 Zones réactives

Les zones réactives permettront d'afficher des zones cliquables directement dans la vidéo pour naviguer entre les caméras (Live et/ou enregistrement). Le changement de vue sera instantané pour faciliter les investigations ou le suivi de personnes ou d'évènement en temps réel.

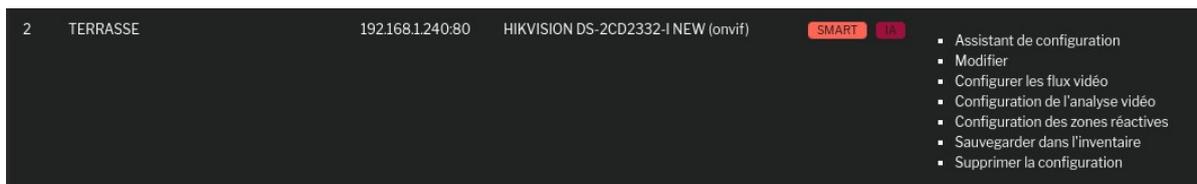
Les caméras seront donc organisées selon leur zones géographique et leur point de vue réel.

Plusieurs formes réactives seront possibles pour une intégration parfaite dans les détails de l'image (ellipse, rectangle, polygone ...).

Vous pouvez configurer jusqu'à 8 zones par caméra.



Pour configurer les zones réactives d'une caméra, cliquez sur le bouton des options avancés situé à droite de la caméra, puis cliquez sur « Configuration des zones réactives ».



Choisissez une forme et dessinez la directement dans l'image, puis affectez-y une caméra.

3.4 Inventaire

L'inventaire est une fonctionnalité permettant de sauvegarder/restaurer des configurations complètes de caméras.

Les caméras pourront facilement être ajoutées, supprimées ou interchangées de la configuration. L'inventaire pourra être exporté et importé entre plusieurs systèmes VXCORE pour créer une liste globale des modèles de caméras.

Caméras / Inventaire				
Caméra - PORTIQUE VOITURES	192.168.0.25	VXCORE VXCORE PORTIQUE VOITURE	2023-03-17 08:08:18	×
Caméra - M2M	51.255.82.38	RELAYCAM M2M PORTAIL	2022-12-18 08:50:40	×
Caméra - RUE INTERPHONE	192.168.0.25	VXCORE RUE INTERPHONE	2022-09-20 07:46:52	×
Caméra - TRAFIC	192.168.0.25	VXCORE TRAFIC	2022-09-20 07:44:08	×
Caméra - CENTRE VILLE 2	192.168.0.25	VXCORE CENTRE VILLE 2	2022-09-20 07:44:03	×
Caméra - CENTRE VILLE 1	192.168.0.25	VXCORE CENTRE VILLE 1	2022-09-20 07:43:56	×
Caméra - AXIS M1065-LW	192.168.1.232	AXIS RTSP Dual Stream	2022-06-14 09:27:12	×

Une caméra exportée dans l'inventaire sera prête à l'emploi en incluant l'adresse IP, le port, le modèle de caméra, la configuration des flux vidéo et les identifiants de connexion.

La configuration de l'analyse vidéo et des alarmes ne sera pas sauvegardée, car ces réglages sont spécifiques à l'installation et au point de vue de la caméra.

Remarque : si vous utilisez l'assistant de configuration pour ajouter votre caméra dans le système, les flux vidéo seront reconfigurés automatiquement (notamment en fonction de l'activation de la fonctionnalité de transcodage vidéo).

4 Configuration des flux vidéo

VXCORE permet une configuration souple et précise de la diffusion des flux vidéo en provenance des caméras ou des encodeurs IP. Vous pourrez régler les modes vidéo d'une caméra soit directement dans l'interface de configuration des paramètres, soit en utilisant la liste complète du menu "Modes vidéo" (Options avancées).

Comme expliqué précédemment, le système peut gérer jusqu'à 3 flux vidéo par caméra, via de multiples codecs (H.265, H.264, MPEG4, MJPEG) et protocoles réseaux (HTTP, HTTPS, RTSP, etc).

Chaque flux vidéo sera dé-multiplexé et synchronisé dans la mémoire du système, appelée "Proxy Vidéo". Cette technologie n'ouvre qu'un seul flux vidéo sur la caméra et permet de le rediffuser sans limite aux utilisateurs (les limites seront fixées par les capacité de traitement du serveur et le dimensionnement réseau).

Lorsque les différents flux vidéo des caméras ont été correctement configurés, il est alors possible de spécifier dans quels cas ils seront utilisés.

Important : saut réglage spécifique, le système maintiendra ouvert en permanence tous les flux vidéo configurés. Votre architecture réseau doit donc être dimensionnée en ce sens.

*Il existe une option « **Flux vidéo a la demande** » sur certains systèmes, qui permet de n'ouvrir les flux vidéo que si un utilisateur le demande explicitement (consultation Live via logiciel PC ou application Mobile).*

Enregistrement des caméras

Les flux vidéo qui seront cochés seront automatiquement enregistrés par le système. Il sera possible d'enregistrer les 3 flux vidéo simultanément.

Il est recommandé d'enregistrer le flux vidéo principal Haute qualité (video1) et un flux en Basse qualité (video2).

Le flux vidéo basse qualité sera utilisé pour optimiser les recherches intelligentes dans les enregistrements vidéo, pour la générations des vignettes intelligentes à la demande et pour optimiser la consultation des enregistrements vidéo à distance. Il permettra également de disposer d'une sauvegarde de la donnée d'enregistrement vidéo, au cas ou le flux vidéo Haute définition se serait pas disponible, en erreur ou corrompu.

Il n'existe aucune limitation sur la charge de l'enregistrement, que ce soit par la taille de l'image (résolution), le débit d'image (Frame rate) ou le débit de données (bande passante). Les limitations seront fixées par les capacités physiques du serveur et surtout par les performances de la chaine de stockage (type de disques dur, configuration RAID, performances I/O des contrôleurs, etc).

Visualisation qualité optimale (LAN)

Spécifie les flux vidéo qui seront utilisés sur le réseau local (LAN), avec une bande passante maximale.

Visualisation qualité réduite (WAN)

Spécifie les flux vidéo qui seront utilisés sur le réseau distant (WAN), avec une bande passante minimale (consultation distante avec un PC).

Visualisation qualité mobile

Spécifie les flux vidéo qui seront utilisés pour les terminaux "mobile" (type smartphone), avec une bande passante minimale (type réseau 3G/4G).

Écrans de visualisation

Spécifie les flux vidéo qui seront utilisés pour la diffusion vidéo sur les écrans vidéo et les murs d'images. En configuration par défaut, les flux vidéo seront sélectionnés automatiquement en fonction de la taille des écrans vidéo.

Le système détectera automatiquement la connexion réseau des utilisateurs : réseau local (LAN), réseau distant (WAN) ou mobile. Cette détection s'opère à partir de la configuration des interfaces réseau du système et du type de terminal utilisé (Web, Application, Smartphone, etc).

Le système pré-sélectionnera ensuite un flux vidéo qui sera adapté à la connexion réseau de l'utilisateur : un flux vidéo en qualité optimale pour les accès en réseau local (LAN) ou un flux vidéo en qualité réduite pour les accès distants (WAN) ou encore un flux vidéo adapté à la consultation sur un smartphone connecté en 3G/4G.

Remarque : Si aucun flux de visualisation n'est configuré pour une caméra, le système sélectionnera le premier flux vidéo disponible pour tous les scénarios de visualisation

5 Analyse vidéo

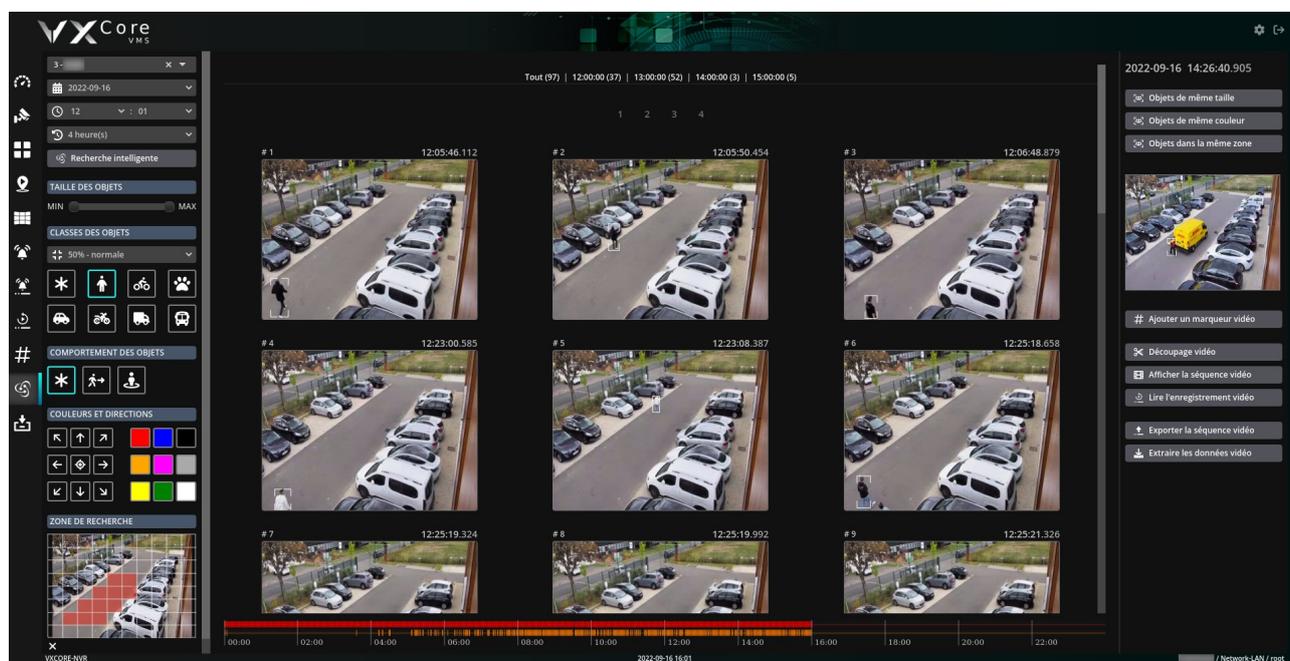
Le système dispose de plusieurs fonctionnalités d'analyse vidéo, qui serviront à créer des alarmes intelligentes ou encore à rechercher des événements précis dans les enregistrements vidéo (sans devoir tout visionner).

Exemple d'alarmes intelligentes : détection multi-zones avec filtre sur taille d'objets, détection périmétrique multi-scénarios, plaques d'immatriculations avec whitelist/blacklist, etc).

Remarque : selon le type d'analyse vidéo intelligente, vous devez disposer d'une ou plusieurs licences supplémentaires « VXSMART » ou « VXIA ».

L'analyse vidéo permettra d'activer plusieurs fonctionnalités du système :

- Enregistrement vidéo sur détection d'activité/mouvement dans la vidéo
- Visualisation active sur détection d'activité/mouvement dans la vidéo
- Alarmes intelligentes avec du filtrage précis (taille et type d'objets, couleurs, directions, etc)
- Recherches intelligentes pour retrouver des événements rapidement (filtres cumulatifs)



Module de recherche avancé « Smart Analytics » avec IA (humains, voitures, vélo, etc)

Important : les algorithmes d'analyse vidéo sont des assistants pour filtrer les mouvements dans les images des caméras. Ce n'est pas une solution fiable à 100% pour configurer une remontée d'événements critiques comme avec un système d'alarme et des détecteurs physiques (qui ne sont pas fiables non plus à 100%).

L'analyse d'image, aussi évoluée soit-elle, ne remplacera jamais le contrôle humain.

L'analyse vidéo est avant tout utile pour pré-filtrer la grande quantité de données vidéo et accélérer les recherches.

5.1 Analyse vidéo 1 - principale

L'analyse vidéo principale (ou analyse vidéo 1) sera toujours affectée aux algorithmes internes de VXCORE pour la détection intelligente des objets. Ces algorithmes sont natifs et n'utilisent pas les fonctionnalités des caméras, ils sont donc compatibles avec tous les modèles de caméras gérés par le système.

Le principe de l'analyse vidéo intelligente est de détecter, analyser, classifier et enregistrer tous les mouvements de la scène sous la forme de métadonnées. Ces métadonnées apporteront beaucoup de fonctionnalités très intéressantes comme la recherche intelligente instantané d'objets/événements précis en utilisant plusieurs filtres cumulatifs.

Cet algorithme pourra être configuré de trois manières : soit en **détection simple**, soit en **détection avancée** (licence VXSMART nécessaire), soit en **détection IA** (licence VXIA nécessaire).

5.1.1 Détection de mouvement simple

(ne nécessite pas de licence supplémentaire)

La détection simple sera principalement utilisée en détection intérieure sans besoin précis. Il sera possible de rechercher/filtrer les objets en mouvement selon leur taille et une ou plusieurs zones de détection.

L'algorithme de détection simple est principalement utilisé pour des scènes de caméras intérieures courantes (type pièce, bureau, couloir, etc). Cet algorithme ne sera pas adapté pour des scènes extérieures complexes avec fortes variations de luminosité ou des caméras très grand angles.



5.1.2 Détection de mouvement avancée

(nécessite une licence VXSMART supplémentaire)

La détection avancée sera bien plus efficace pour l'analyse vidéo, notamment sur des environnements extérieurs complexes et des caméras très grands angles (surveillance périphérique).

L'algorithme sera plus précis dans la résolution d'analyse/fps et capable de compenser les fortes variations de luminosité (soleil, nuages, intempéries, etc).

Les métadonnées permettront des recherches plus évoluées comme le comportement des objets (mouvement, stagnation, apparus/disparus), le sens de direction/déplacement ou encore les couleurs dominantes.



Remarque : la détection de mouvement avancée nécessitera environ 15% de ressources CPU en plus par rapport à la détection de mouvement simple.

5.1.3 Détection de mouvement IA

(nécessite une licence VXIA supplémentaire)

La détection IA est une extension de la détection de mouvement avancée, en y rajoutant une étape de reconnaissance d'objet.

Ce traitement sera capable d'identifier les types d'objets suivants : personnes, visages, vélos, animaux (chats, chiens, chevaux, moutons, oiseaux, vaches), bagages (valises, sacs), voitures, camions/utilitaires, motos/scooters, bus.

Chaque objet sera classé selon son type et son score de « confiance » entre 20 et 100%. Ce score correspond au pourcentage de pertinence de reconnaissance de l'objet (par exemple : objet de type voiture reconnu avec un score de 79%).



Cette valeur de confiance/score sera très importante, car elle permettra de régler la fiabilité des alarmes ou des recherches intelligentes.

Remarque : la détection IA nécessitera une grande puissance de traitement, surtout si vous l'utilisez sur plusieurs dizaines de caméras (l'installation d'un GPU compatible est fortement conseillé, consultez les documentations d'installation et d'administration du système pour plus de détails).

5.1.4 Configuration de l'analyse

Choix du type d'algorithme d'analyse vidéo

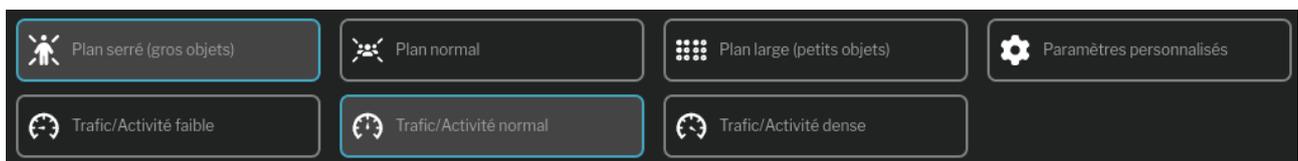
Pour chaque caméra, vous pouvez choisir d'activer l'analyse vidéo simple, avancée ou IA. Les algorithmes avancés et IA nécessiteront des licences supplémentaires.



Si vous ne souhaitez pas activer d'analyse vidéo sur la caméra ou bien tout désactiver : cliquez sur le bouton « Pas d'analyse vidéo ».

Profils de scène/trafic

Ces paramètres sont communs à tous les algorithmes d'analyse vidéo : simple, avancé ou IA. Vous les retrouverez dans l'interface de l'assistant de configuration ou bien dans l'interface de configuration avancée.



Ces boutons permettent de pré-régler l'analyse vidéo en choisissant un profil adapté en fonction du placement de la caméra et du plan réel qui sera filmé.

Ces profils de réglages vont grandement optimiser l'analyse vidéo, en ajustant automatiquement la résolution et le débit des images, et ce pour chaque caméra. Avec de bons

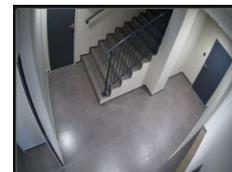
réglages, les économies en ressources de calculs pourront être significatives, ce qui vous permettra de rajouter encore plus de caméras sur votre serveur (ou de ne pas faire surcharger le serveur).

Choix du type de scène

Permet d'ajuster la résolution de l'analyse vidéo (avec une grande résolution d'image : de très petits objets pourront être détectés, mais cela consommera plus de ressources)

Plan serré

Pour détecter des gros objets comme des véhicules dans une rue ou un objectif de caméra très serré ou zoomé, comme dans un couloir



Plan normal

Pour détecter des objets de tailles normales, comme des personnes dans une pièce, un bureau, une entrée, etc



Plan large

Pour détecter de très petits objets lointains sur des caméras très grand angles ou des vues intérieures/extérieures très larges



Paramètres personnalisés

Pour configurer manuellement l'analyse vidéo (avec l'interface de configuration avancée)

Choix du type de trafic/activité

Permet d'ajuster le débit des images de l'analyse vidéo (avec un débit important d'images : des objets très rapides pourront être détectés et tracés efficacement, mais cela consommera plus de ressources). Remarque : ces profils ne sont pas disponibles pour l'analyse vidéo simple.

Trafic/activité faible

Pour des caméras intérieures avec peu de mouvements rapides, comme des personnes qui se déplacent dans des pièces, des couloirs, etc

Trafic/activité normale

Pour des caméras intérieures/extérieures avec des objets mixtes et des vitesses variables, comme des personnes et des véhicules qui se déplacent sur des parkings, des accès de bâtiments, des entrepôts, etc

Trafic/activité dense

Pour des caméras extérieures avec beaucoup de trafic et des objets en déplacements rapides, comme des caméras urbaines, routes, croisements, etc

Paramètres personnalisés

Pour configurer manuellement l'analyse vidéo (avec l'interface de configuration avancée)

Remarque : utilisez les valeurs par défaut si vous ne savez pas quel profil choisir.

Paramètres de l'analyse vidéo

Flux vidéo d'analyse

Permet de forcer le flux vidéo qui sera utilisé pour l'analyse vidéo. De manière générale il est préférable de ne jamais utiliser un flux vidéo supérieur à 800x600 pixels (ressources CPU décodage/analyse trop importante).

Remarque : en mode automatique, le système va rechercher et choisir le flux vidéo qui sera le plus adapté pour l'analyse (résolution maximale 1000 pixels). Si toutefois aucun flux vidéo n'est disponible, le système affichera un message d'erreur dans le tableau de bord pour avertir d'un problème de configuration. Si vous ne disposez que d'un flux vidéo de résolution supérieure à 1000 pixels, l'analyse vidéo ne sera pas fonctionnelle en mode automatique, et vous devrez explicitement forcer le flux vidéo d'analyse en le sélectionnant.

Sensibilité (*) uniquement en mode avancé

Permet de définir la sensibilité d'analyse vidéo de 50% à 90%. Une sensibilité de 75% sera efficace dans la plupart des cas. Si votre caméra est en noir et blanc ou que la scène est très large avec des petits objets, il sera nécessaire d'augmenter la sensibilité.

Ce paramètre sera réglé automatiquement si vous utilisez un profil de scène.

Taille des formes/pixels (*) uniquement en mode avancé

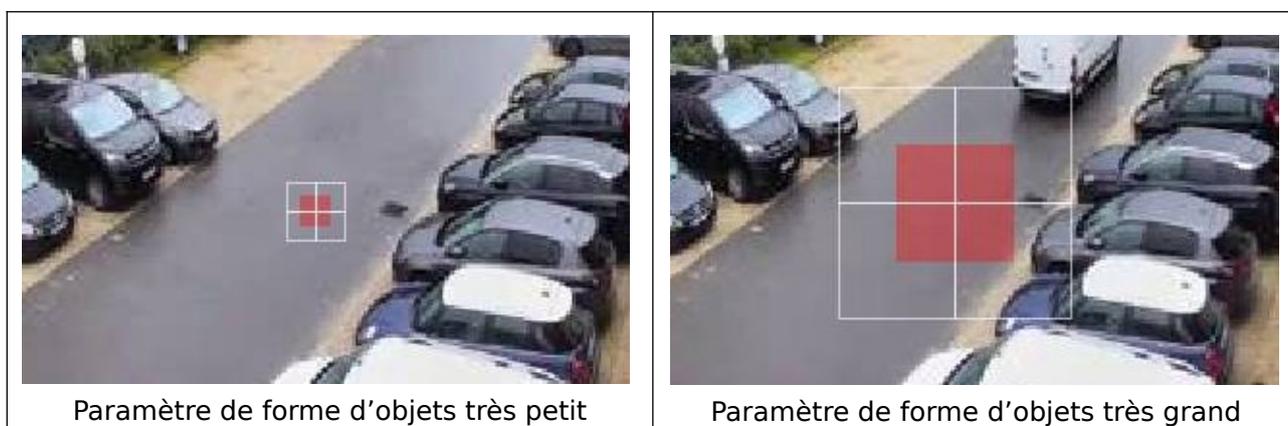
Permet de définir la taille des objets optimale par rapport au type de scène. L'algorithme va détecter les variations des pixels et regrouper ces formes en objets en fonction de ce paramètre.

Ce paramètre sera réglé automatiquement si vous utilisez un profil de scène.

Si vous souhaitez détecter des objets petits, comme par exemple dans un plan très large ou une caméra grand angle, utilisez un réglage petit (~5/10).

Au contraire, si vous disposez d'un plan serré et que les objets sont très grand, utilisez un réglage haut (~20/30). Dans la majorité des cas, un réglage de 10 sera tout a fait adapté.

Remarque : vous pouvez vérifier la valeur du réglage de taille de forme/objet dans l'image de prévisualisation. Le quadrillage blanc et le carré rouge situé au centre représente l'objet de référence qui va permettre ce regroupement de pixel (taille minimale des objets à détecter).



Désactiver temporairement l'analyse si variation d'image trop importante

Cette option permet de stopper l'analyse vidéo pour éviter des détections d'objets intempestifs qui serait provoqué par un changement brutal de la scène (par exemple : mouvement/repositionnement de caméra PTZ, activation filtre IR pour passage en mode jour/nuit, etc). Un réglage de 50% signifie que l'analyse sera stoppée si plus de la moitié de l'image apparait subitement en mouvement.

L'analyse vidéo restera désactivée tant que l'image n'aura pas retrouvé la stabilité nécessaire (environ 3~5 secondes).

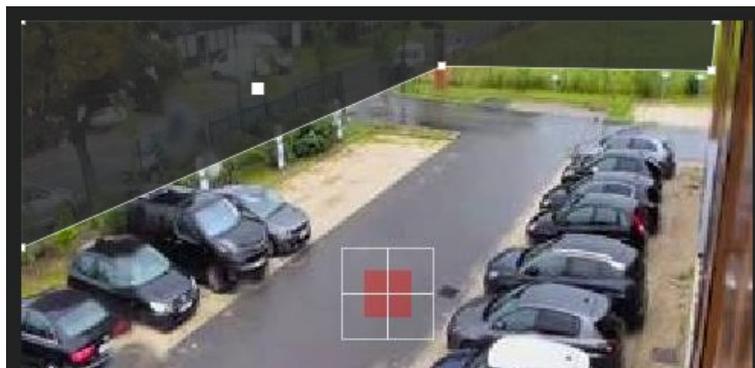
Zone de masquage

Ce paramètre est très important : il permet d'exclure une zone de l'analyse vidéo pour optimiser le traitement.

Par exemple, vous pouvez exclure une route à fort passage, des arbres en mouvements réguliers, une fenêtre avec reflets lumineux, des zones publiques interdites, etc

Vous pouvez dessiner la zone de masquage directement dans l'image de prévisualisation située en bas (plusieurs points pour dessiner une forme de type polygone). Tous les pixels contenus dans cette zone seront définitivement exclus de l'analyse vidéo (forme de couleur gris foncé).

Cette zone d'exclusion sera très utile pour optimiser l'analyses vidéo IA, très consommatrice en ressources : la reconnaissance d'objet ne se déclenchera pas systématiquement sur toute l'image, mais uniquement sur les zones d'intérêts.



Remarque : la zone de masquage affectera également la configuration des alarmes, les notifications d'alertes et la recherche intelligente (aucun objet ne sera jamais détecté dans cette zone).

5.2 Analyse vidéo 2 - secondaire

L'analyse vidéo secondaire (ou analyse vidéo 2) est utilisée pour activer d'autres algorithmes intelligents externes, comme la reconnaissance des plaques d'immatriculations.

La différence avec l'analyse vidéo 1 principale est que le traitement sera fait par un système externe (caméra intelligente type LPR/IA ou logiciel d'analyse vidéo tierce).

Les données d'analyses seront donc transmises en temps réel au serveur VXCORE (« push »), qui se chargera de les traiter et les stocker en associant la bonne caméra / source vidéo. L'analyse vidéo secondaire nécessitera donc la sélection d'un driver compatible pour convertir les données entrantes.

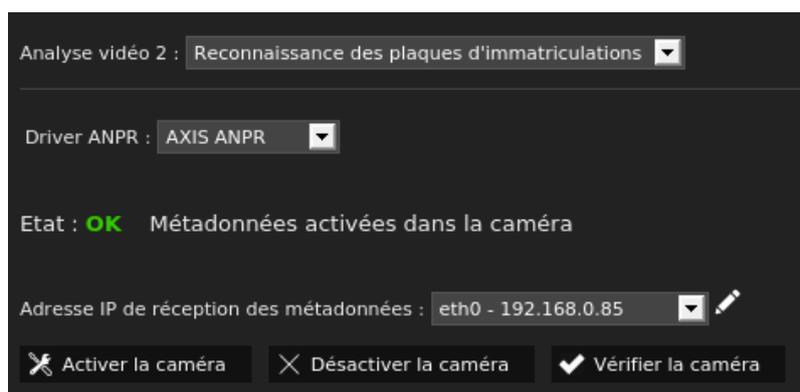
Remarque : pour activer l'analyse vidéo secondaire, il est également nécessaire de disposer d'une licence supplémentaire « VXSMART ».

5.2.1 Reconnaissance des plaques d'immatriculations

La détection des plaques d'immatriculations n'est pas un algorithme d'analyse interne, il va réceptionner/enregistrer les données d'un autre système d'analyse externe (type caméra intelligente LPR ou unité de calcul indépendante).

Pour configurer l'envoi/réception des métadonnées de plaques d'immatriculation, il sera nécessaire de choisir une caméra ou un logiciel compatible avec le système (driver ANPR).

Un driver ANPR permettra de configurer automatiquement la caméra associée pour qu'elle puisse envoyer automatiquement les informations des plaques au serveur VXCORE.



La seule chose que vous devrez configurer est l'adresse IP ou la caméra ANPR doit envoyer ses données, c'est à dire l'adresse IP du serveur VXCORE (située sur la bonne classe réseau).

Si votre serveur dispose de plusieurs interfaces réseaux, une liste déroulante apparaîtra pour faciliter ce choix.

Vous pouvez également cliquer sur l'icône d'édition située à droite de la liste pour renseigner manuellement une adresse IP (dans le cas d'une redirection NAT ou d'un adressage réseau spécifique).

Si le driver ANPR sélectionné est compatible avec la configuration automatique de la caméra, vous pourrez utiliser les boutons de configuration. Sinon, vous devez configurer manuellement la caméra ou le logiciel externe pour envoyer les données au bon format (JSON) et sur la bonne adresse IP (VXCORE).

Activer la caméra

Utilisez ce bouton pour activer l'envoi des métadonnées dans la caméra LPR

Désactiver la caméra

Utilisez ce bouton pour désactiver l'envoi des métadonnées dans la caméra LPR

Vérifiez la caméra

Utilisez ce bouton pour vérifiez l'état de configuration la caméra LPR

Remarque : si vous modifiez manuellement la configuration de la caméra LPR, vérifiez toujours que l'envoi des métadonnées est bien actif en cliquant sur le bouton « Vérifiez la caméra » dans l'interface de VXCORE.

6 Alarmes / détections

VXCORE intègre beaucoup de fonctionnalités permettant de générer et de centraliser les évènements d'alarmes.

Les alarmes peuvent provenir d'algorithmes de détection d'images simples ou complexes, ou encore d'appareils physiques connectés au réseau IP (détecteur IR, barrière infrarouge, etc).



Photo d'une détection de mouvement du journal des alarmes

Une alarme permettra une multitude de fonctionnalités :

- Galerie d'image visuelle des déclenchements d'alarmes (journal des alarmes)
- Génération de mini séquences vidéo d'alarmes
- Enregistrement vidéo ou visualisation active sur alarme
- Recherche et positionnement simplifié dans les enregistrements vidéo
- Déclenchement d'actions systèmes (exemple : ouverture/fermeture de contacts secs)
- Déplacement automatique des caméras PTZ
- Envoi d'alertes email avec pièces jointes (photos, vidéos)

Le système permet de créer plusieurs types d'alarmes, correspondant à la majorité des besoins pouvant être rencontrés :

- Alarme par analyse vidéo (mode simple ou avancée)
- Alarme réseau par FTP
- Alarme réseau par HTTP
- Alarme scénario
- Alarme centralisée (VPN)

Pour chaque caméra, il sera possible de configurer plusieurs alarmes de même type ou de type différents. Par exemple, sur la même caméra :

- une alarme IA de détection de personne
- une alarme FTP configurée dans la caméra pour réceptionner l'état I/O du contact de la porte
- une alarme HTTP configurée dans un boîtier externe type IPX800 pour réceptionner l'état I/O d'une sonnette extérieure

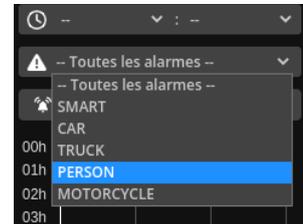
Tag / Types d'alarmes

Lors de la génération d'un évènement d'alarme, un tag automatique sera enregistré, ce qui permettra de retrouver des catégories plus rapidement.

Ces tags seront être de type : personnes, visages, audio, intrusion, fire, anpr, etc

Ils seront ajoutés sur les alarmes en fonction du type d'alarme configuré et des éventuels algorithmes d'analyses (comme l'IA ou la reconnaissance de plaques d'immatriculations).

Dans l'interface du journal des alarmes, un nouveau menu de filtrage s'affichera à gauche, permettant de filtrer selon le type des alarmes (seuls les types disponibles s'afficheront).



6.1 Limitation des évènements d'alarmes

Les évènements alarmes sont avant tout utiles pour déclencher un scénario automatisé ou notifier des utilisateurs (par exemple : une personne devant une porte, un visage devant un visiophone, un véhicule en sens interdit, une ouverture de barrière, un affichage dynamique sur le mur d'image, etc).

A la différence de la recherche intelligente, une alarme va générer une photo et/ou une séquence vidéo qui sera stockée dans un journal historique et conservée par le système.

L'alarme sera donc par définition beaucoup plus consommatrice en ressources que la recherche intelligente notamment en I/O (analyse du scénario, déclenchement, extraction/encodage JPG de la photo, activation des actions, enregistrement dans la base de données et dans le volume de stockage, etc).

Concrètement, si vous n'avez pas besoin d'être alerté par une notification sur votre smartphone ou de configurer des actions automatique, vous n'avez probablement pas besoin d'activer des alarmes. Les caméras peuvent être enregistrées sur détection de mouvement sans avoir à configurer des alarmes : c'est l'analyse vidéo qui sera utilisée pour déterminer s'il faut enregistrer ou non les données « hors mouvements ».

Sur un système de plus d'une centaines de caméras, dans un milieu urbain ou un centre commercial par exemple, il serait peu efficace de configurer des alarmes « automatiques » pour stocker une image quasiment toutes les secondes « lorsqu'il y a du mouvement ». Il y aura effectivement du mouvement constant sur toutes les caméras et le système va générer des vignettes d'alarmes en continu, qui seront enregistrées dans les disques de stockage du serveur et vite saturer l'espace disque à la place de données plus importantes. Ces alarmes ne sont d'aucunes utilités, car elles ne seront jamais consultées en totalité (trop de données), et seront au final supprimées automatiquement par le système.

Dans ce cas précis, il sera beaucoup plus efficace d'utiliser la recherche intelligente pour retrouver des évènements et afficher des galeries d'images à la volée.

Une bonne approche sera de configurer des alarmes utiles qui ne seront activées que la nuit dans un calendrier (par exemple : alarmes de type anti-intrusion avec lien télésurveillance).

L'utilisation de l'IA permettra également d'obtenir des alarmes plus fiables, notamment insensible aux variations de lumières, et de configurer des scénarios précis (exemple : maraudage, intrusion zones périmétriques, etc).

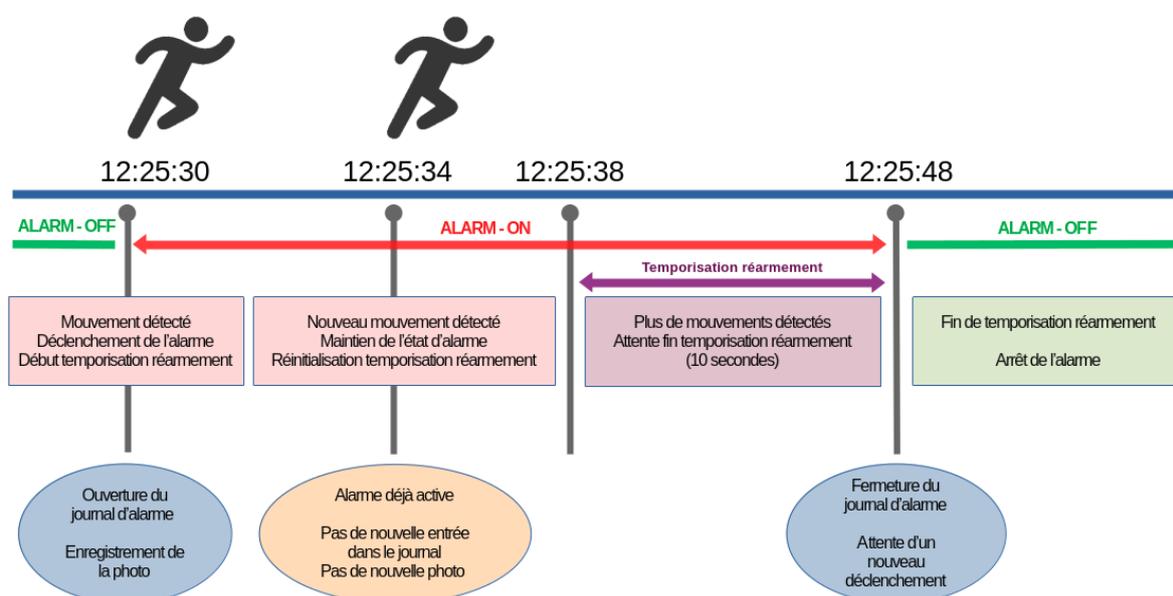
6.2 Options générales

Chaque alarme pourra être configurée de manière indépendante, avec des options pouvant influencer sur son comportement (plages horaires, journalisation, association images/vidéo, évènements, etc).

Période de maintien forcée / réarmement

La période de maintien forcée permet de configurer la valeur minimale d'activation d'une alarme (temporisation). Une alarme en état "ON" ne se désactivera pas avant cette période. Si un nouveau signal d'alarme est réceptionné par le système pendant cette période, la temporisation actuelle sera automatiquement remise à zéro, sans déclencher une nouvelle journalisation (donc le stockage d'une nouvelle photo et/ou vidéo).

La période de maintien forcée affecte directement les valeurs "post-alarme" des enregistrements vidéo programmés sur alarme. Tant qu'une alarme reste active, toutes les caméras qui lui sont associées seront maintenues en enregistrement.



Fonctionnement du déclenchement d'une alarme et de la temporisation de réarmement

Remarque : un réglage de cette valeur trop bas (inférieure à 10 secondes) pourrait générer un nombre important de photos d'alarmes et provoquer une saturation du stockage ou des ressources du serveur s'il n'a pas été dimensionné correctement (exemple : transcodage de photos en qualité 4K sur un serveur type Intel Atom).

Caméra associée

La caméra associée permet au système de lier automatiquement un point de vue caméra aux évènements d'alarmes. Une caméra n'est pas forcément liée à une seule alarme, il est possible de l'associer à plusieurs alarmes.

Une caméra associée à une alarme permettra d'activer plusieurs fonctionnalités du système :

Ouverture de la caméra "live"

En cas d'alarme, un bouton permettra à l'utilisateur de visualiser directement la caméra associée.

Sélection de l'enregistrement vidéo de la caméra

Le système positionnera automatiquement la lecture des enregistrements vidéo de la caméra associée.

Enregistrement vidéo sur alarme

La caméra associée pourra être configurée en enregistrement sur alarme. La caméra sera enregistrée ou non, en fonction de l'état de toutes ces alarmes associées. Le temps d'enregistrement "post-alarme" dépendra aussi du réglage et de l'état de toutes les alarmes associées.

Galerie d'image

Une galerie d'image sera générée automatiquement pour tous les déclenchements d'alarmes.

Séquences vidéo d'alarmes

Le système sera capable de générer des mini-séquences vidéo permettant d'accélérer et fiabiliser les levées de doutes des déclenchements d'alarmes.

Remarque : si vous utilisez l'assistant de configuration caméra, le système va automatiquement créer l'alarme associée à la caméra (exemple : caméra entrée => alarme entrée).

Horaires d'activation

Chaque alarme peut être configurée sur une ou plusieurs plage horaire. Par défaut, une alarme est activée en permanence 24h/24. Pour configurer une nouvelle plage horaire, vous devez avoir préalablement ajouter des calendriers dans le système.

Consultez la section "Programmation/Gestion des calendriers" de ce manuel pour plus de détails sur la configuration des calendriers.

Journal des alarmes

Le journal des alarmes est une fonctionnalité très importante. Elle permet une journalisation efficace des évènements d'alarmes, tout en conservant des informations très utiles :

- Date et heure de chaque évènement d'alarme
- Date, heure et utilisateur ayant fait la levée de doute de l'alarme
- Photo du déclenchement d'alarme, facilitant la levée de doute
- Mini-séquence vidéo extraite des enregistrements vidéo, facilitant la levée de doute

La journalisation des alarmes permettra aussi un positionnement plus efficace dans la lecture ou la recherche des enregistrements vidéo.

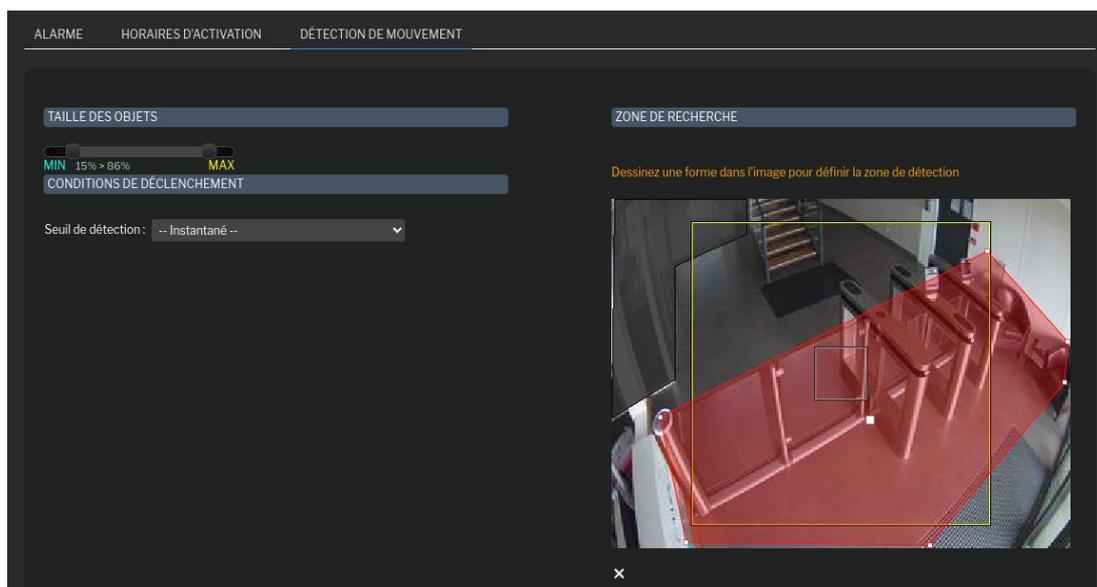
En mode automatique, la durée du journal sera réglée sur la rétention des enregistrements vidéo de la caméra associée (exemple : si la caméra ne dispose que de 3 jours d'enregistrement vidéo, l'historique du journal des alarmes sera aussi de 3 jours).

6.3 Alarme analyse vidéo simple

Ce type d'alarme permet d'activer une détection d'activité en utilisant l'analyse vidéo simple de la caméra (qui devra bien être activée dans la configuration de la caméra).

Pour configurer une alarme par détection de mouvement, sélectionnez simplement la caméra associée pour l'analyse. Il sera aussi possible de créer plusieurs alarmes associées à la même caméra (par exemple pour une caméra grand angle : alarme porte gauche et alarme porte droite).

Pour configurer la détection de mouvement, cliquez sur l'onglet « Détection de mouvement ».



Exemple de configuration zone de détection et taille Min/Max

Taille des objets

Ce réglage permet de filtrer les objets selon une taille minimale (carré bleu) et une taille maximale (carré jaune). Seuls les objets qui seront dans cette intervalle déclencheront l'alarme. Si les tailles min/max sont configurées, alors tous les objets déclencheront l'alarme, quelque soit leur taille (Min 0% - Max 100%).

Seuil de détection

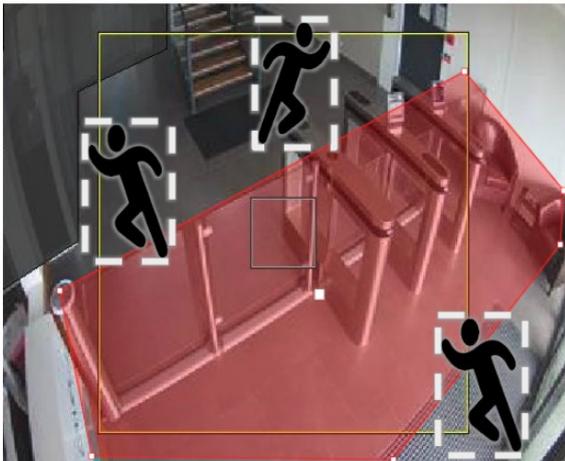
Ce réglage permet d'ajouter une temporisation sur le déclenchement de l'alarme. L'alarme ne se déclenche que si les mouvements sont persistants dans la zone. Ce paramètre permet de fiabiliser les alarmes en éliminant les objets « flash » comme une variation de lumière ou un passage bref devant la caméra (oiseau, etc).

Par exemple, cela peut être utile pour configurer une alarme sur une porte située dans une zone de passage : l'alarme ne se déclenche pas dès qu'une personne passe devant, mais seulement si elle reste devant la porte pendant le temps de temporisation défini.

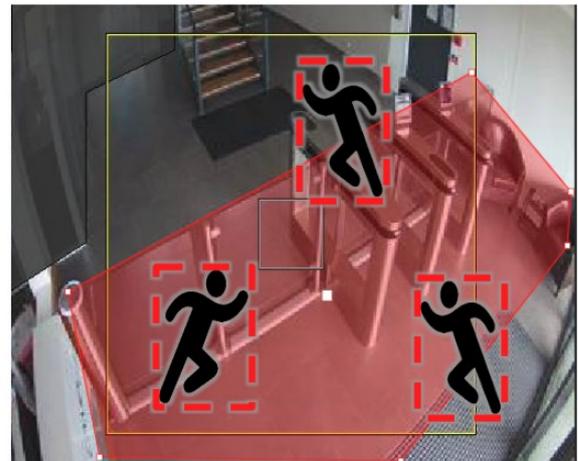
Zone de détection

Vous pourrez dessiner directement dans l'image pour créer la zone de détection de l'alarme (dessin de type points/polygones de **couleur rouge**). Cliquez dans l'image pour ajouter des nouveaux points dans la zone. Vous pouvez déplacer chaque point en cliquant dessus et le déplaçant. Faites un clic droit sur un point pour le supprimer. Cliquez sur la croix située sous l'image pour tout supprimer et recommencer. Si vous ne dessinez pas de zone, toute l'image sera utilisé pour le déclenchement.

Il sera important de créer une zone de détection cohérente, ou la position des objets en fonction de leurs coordonnées pourront réellement être calculés. Pour qu'un objet soit détecté dans une zone, la moitié des coordonnées d'extrémités ou les coordonnées de son centre devront être dedans (bounding box).



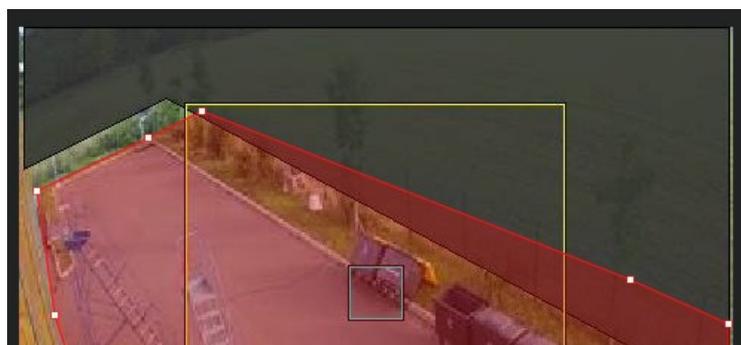
OBJETS NON DÉTECTÉS DANS LA ZONE



OBJETS DÉTECTÉS DANS LA ZONE

Zone de masquage

Comme expliqué précédemment, la zone de masquage sera configurée directement dans les paramètres d'analyse vidéo de la caméra. Cette zone sera visible dans l'image de prévisualisation avec une **couleur grise foncé**.



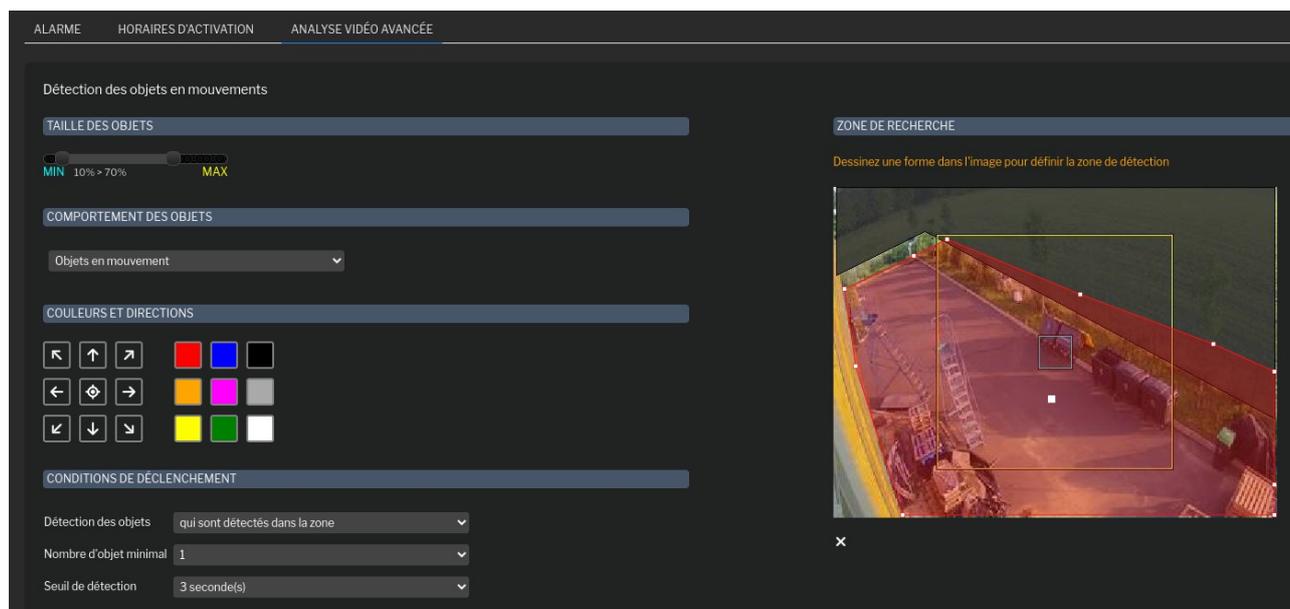
La zone de masquage affectera toutes les alarmes : aucun mouvement n'y sera jamais détecté, même si vous dessinez explicitement une zone de détection par dessus.

6.4 Alarme analyse vidéo avancée

Ce type d'alarme permet d'activer une détection en utilisant l'analyse vidéo avancé de la caméra (qui devra bien être activée dans la configuration de la caméra).

L'alarme se comportera comme un filtre intelligent, en analysant simultanément plusieurs critères sur les profils des objets et en vérifiant des conditions sur leur comportement (direction, couleur, zone, etc).

Pour configurer les paramètres du filtre de l'alarme, cliquez sur l'onglet « Analyse vidéo avancée ».



Les paramètres de l'alarme seront cumulatifs : tous les critères devront être remplis pour déclencher l'alarme. Par exemple : taille objet 10%-70% > en mouvement > de couleur rouge > direction droite vers gauche > situé dans la zone de détection.

Taille des objets

Ce réglage permet de filtrer les objets selon une taille minimale (carré bleu) et une taille maximale (carré jaune). Seuls les objets qui seront dans cette intervalle déclencheront l'alarme. Si les tailles min/max sont configurées, alors tous les objets déclencheront l'alarme, quelque soit leur taille (Min 0% - Max 100%).

Comportement des objets

Permet de spécifier quels types objets seront analysés dans l'alarme : soit tous les objets, soit seulement les objets en mouvements, soit seulement les objets statiques/apparus/disparus. Ces attributs sont calculés grâce à un masque de mouvement directement généré par l'analyse vidéo.

Ce masque va automatiquement s'adapter lors de chaque image analysée. Si un objet en mouvement s'immobilise dans l'image, il sera d'abord détecté « en mouvement », puis « immobile ». Si le filtre d'alarme a été configuré sur « immobile » alors le déclenchement n'interviendra que lorsque l'objet sera identifié avec cet attribut.

En fonction du type de scène, notamment avec des objets trop rapides ou « flash », il est possible que l'analyse vidéo n'ait pas le temps de calculer les attributs de mouvements. L'objet restera donc en état de mouvement « inconnu », qui sera seulement détecté quand le réglage du filtre sera configuré sur « Tous les objets ».

Directions

Permet de déterminer une ou plusieurs directions des objets dans l'alarme : seuls les objets correspondant seront analysés. Au moins une direction sélectionnée devra correspondre. Par défaut, tous les objets seront pris en compte. Pour calculer et tracer efficacement les déplacements et les directions, les objets devront être détecté plusieurs fois (pendant plus d'une seconde).

Attention : le calcul des directions nécessite un suivi des objets « persistants » et ne peut pas s'opérer sur des objets trop rapides avec des paramètres d'analyses non adaptés.

Par exemple, si vous avez configuré un profil d'analyse vidéo « trafic/activité faible » dans les paramètres de la caméra, et que la scène filme une route à fort trafic avec des véhicules très rapides, le système ne disposera pas d'assez d'images pour calculer les déplacements et les directions.

Ce critère ne pourrait donc pas être pertinent dans la configuration d'une alarme fiable.

Couleurs dominantes

Permet de déterminer une ou plusieurs couleurs dominantes des objets dans l'alarme : seuls les objets correspondant seront analysés. Au moins une couleur sélectionnée devra correspondre. Par défaut, tous les objets seront pris en compte.

Attention : le calcul de la couleur dominante est directement dépendant de la qualité d'image et de l'objectif de la caméra.

Ce critère ne pourrait donc pas être pertinent dans la configuration d'une alarme fiable.

Détection des objets

Permet de spécifier le comportement des objets par rapport à la zone afin de déclencher l'alarme :

- qui sont dans la zone
- qui sont en dehors de la zone
- qui entrent dans la zone (détectés d'abord en dehors de la zone, puis dedans)
- qui sortent de la zone (détectés d'abord dans la zone, puis en dehors)
- qui traversent la zone (détectés d'abord en dehors de la zone, puis dedans et a nouveau en dehors)

Attention : le calcul de la position des objets par rapport à la zone nécessite un suivi des objets « persistants » et ne peut pas s'opérer avec des paramètres d'analyses non adaptés (comme un profil de trafic/activité faible).

Nombre d'objet total dans la zone

Permet de spécifier le nombre d'objet minimal qui correspond aux critères de détection de la zone (par défaut 1). Cette option peut être utile pour de la détection d'attroupement d'objets. Par exemple : 2 personnes ou plus présentes simultanément en dehors de la zone.

Seuil de détection

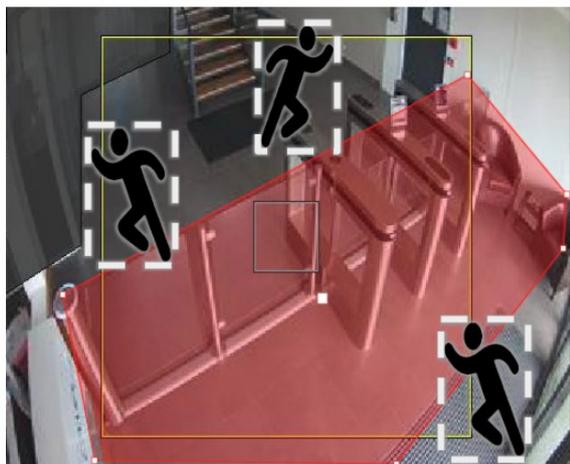
Ce réglage permet d'ajouter une temporisation sur le déclenchement de l'alarme. L'alarme ne se déclenchera que si les mouvements sont persistants dans la zone. Ce paramètre permet de fiabiliser les alarmes en éliminant les objets « flash » comme une variation de lumière ou un passage bref devant la caméra (oiseau, etc).

Par exemple, cela peut être utile pour configurer une alarme sur une porte située dans une zone de passage : l'alarme ne se déclenchera pas dès qu'une personne passe devant, mais seulement si elle reste devant la porte pendant le temps de temporisation défini.

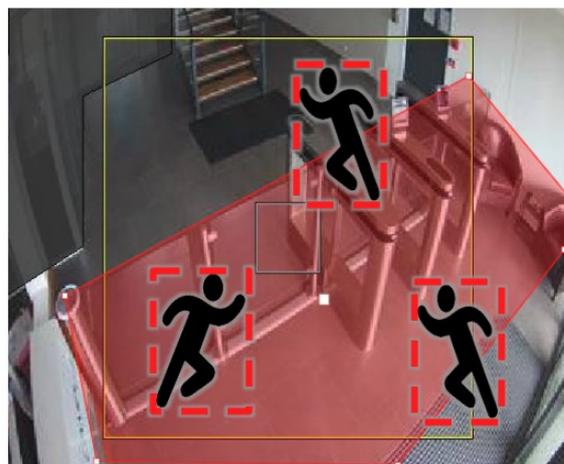
Zone de détection

Vous pourrez dessiner directement dans l'image pour créer la zone de détection de l'alarme (dessin de type points/polygones de **couleur rouge**). Cliquez dans l'image pour ajouter des nouveaux points dans la zone. Vous pouvez déplacer chaque point en cliquant dessus et le déplaçant. Faites un clic droit sur un point pour le supprimer. Cliquez sur la croix située sous l'image pour tout supprimer et recommencer. Si vous ne dessinez pas de zone, toute l'image sera utilisé pour le déclenchement.

Il sera important de créer une zone de détection cohérente, ou la position des objets en fonction de leurs coordonnées pourront réellement être calculés. Pour qu'un objet soit détecté dans une zone, la moitié des coordonnées d'extrémités ou les coordonnées de son centre devront être dedans (bounding box).



OBJETS NON DÉTECTÉS DANS LA ZONE



OBJETS DÉTECTÉS DANS LA ZONE

Zone de masquage

Comme expliqué précédemment, la zone de masquage sera configurée directement dans les paramètres d'analyse vidéo de la caméra. Cette zone sera visible dans l'image de prévisualisation avec une **couleur grise foncé**.



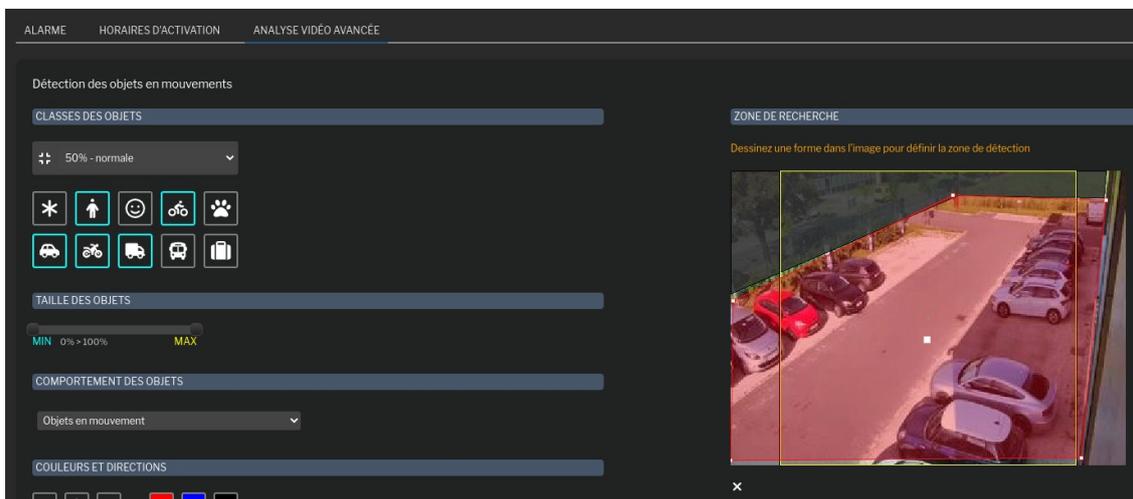
La zone de masquage affectera toutes les alarmes : aucun mouvement n'y sera jamais détecté, même si vous dessinez explicitement une zone de détection par dessus.

6.5 Alarme analyse vidéo IA

Ce type d'alarme permet d'activer une détection en utilisant l'analyse vidéo avancé de la caméra et des paramètres supplémentaires pour filtrer selon le type d'objet avec l'IA (qui devra bien être activée dans la configuration de la caméra).

L'alarme se comportera comme un filtre intelligent, en analysant simultanément plusieurs critères sur les profils des objets, en vérifiant des conditions sur leur comportement (direction, couleur, zone, etc) et également en fonction de leur classe/confiance (personne, voiture, etc).

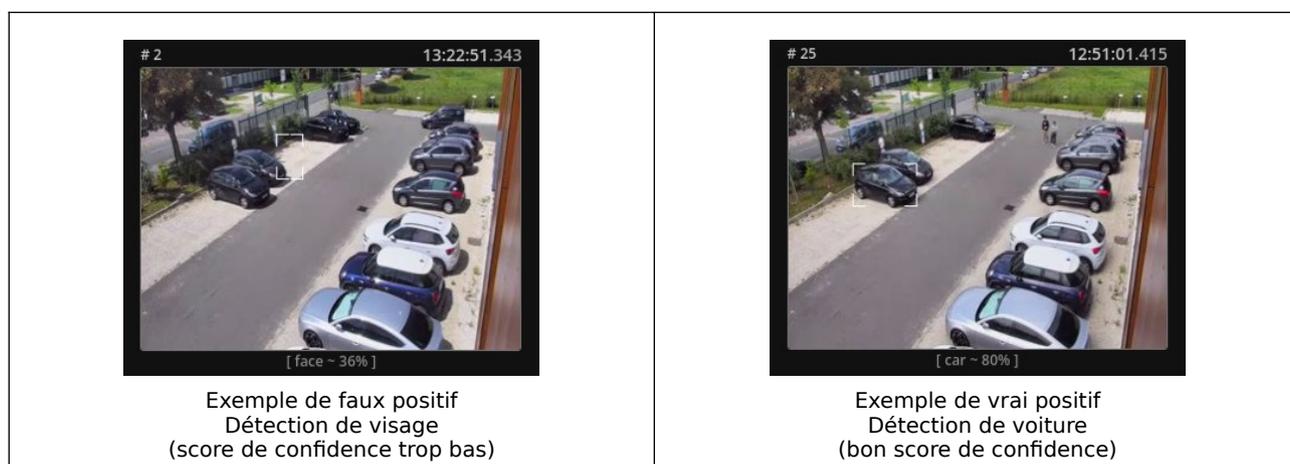
Pour configurer les paramètres du filtre de l'alarme, cliquez sur l'onglet « Analyse vidéo avancée ».



Classes des objets et Score de détection

Dans une alarme avancée IA, un filtre supplémentaire permettra de choisir les classes d'objets qui déclencheront l'alarme. Si vous sélectionnez plusieurs classes d'objets, alors l'alarme se déclenchera si au moins une des classes est détectée (ou plusieurs en même temps).

Le paramètre de réglage du score de la confiance est très important : il permettra de fiabiliser la détection d'objet. Chaque objet sera classé selon son type et son score de « confiance » entre 20 et 100%. Ce score correspond au pourcentage de pertinence de reconnaissance de l'objet (par exemple : objet de type voiture reconnu avec un score de 79%). Les objets sélectionnés qui n'auront pas un score de confiance supérieur ou égal à la valeur configurée ne seront pas pris en compte.



Remarque : le score de confiance est directement lié au placement et à la qualité d'image de la caméra. Pour vous aider à configurer l'alarme IA, vous pouvez utiliser le module de recherche intelligent pour voir et tester les différentes valeurs/score des classes d'objets que vous souhaitez détecter.

Comportement des objets / Couleurs / Directions / Zone ...

Les autres paramètres/filtres seront les mêmes que pour une alarme par détection avancée, consultez le chapitre dédié pour la description de toutes les options.

Remarque : si vous avez activé l'algorithme de détection des visages en plus de l'algorithme de détection des objets intégré, attention au réglage de la confiance/pertinence.

Chaque algorithme dispose de son propre calcul du score de confiance des objets et il ne sera pas normalisé. Il pourrait donc y avoir des alarmes indésirables si vous renseignez un score de confiance commun pour des classes d'objets qui sont issus de deux algorithmes différents (comme la détection des personnes et la détection des visages).

Par exemple : l'algorithme de détection des personnes sera fiable à partir de 70% de confiance, alors que l'algorithme de détection des visages le sera à partir de 95%.

Dans ce cas, il est conseillé de créer deux alarmes distinctes : une alarme pour la détection des personnes et une alarme pour la détection des visages (chacune avec son réglage de confiance adapté).

6.6 Alarme réseau (FTP)

Une alarme réseau FTP est utilisée pour réceptionner un signal d'alarme ou une image envoyée par une caméra ou un encodeur IP via le réseau et le protocole FTP. Ce type d'alarme est déconseillé du fait que le protocole FTP n'est pas sécurisé (authentification et mot de passe non chiffré sur le réseau).

Un compte FTP virtuel sera créé sur le serveur VXCORE pour réceptionner une image JPEG envoyée par la caméra. Cette transmission d'image sera utilisée pour déclencher l'alarme du système.

Chaque caméra disposera de son propre compte FTP pour envoyer ces images. Les images JPEG envoyées par les caméras pourront être stockées ou non dans le journal des alarmes du système.

Remarque : le système ne configure pas les alarmes FTP dans les caméras. Vous devez configurer manuellement toutes vos caméras pour qu'elles envoient leurs images d'alarmes sur le bon compte FTP du serveur.

Par défaut, l'identifiant et le mot de passe du compte FTP sont identiques (exemple : login "alarm1" / password "alarm1"), mais il est fortement conseillé de changer le mot de passe pour des raisons de sécurité.

Attention : le firewall et le port FTP doivent être ouverts pour réceptionner des alarmes FTP

Type : Alarme réseau (FTP)

Nom de l'alarme : TEST FTP

Caméra associée : MAISON (MAISON) (*)

Temps d'activation minimal : 3 seconde(s)

(*) : Lecture de l'enregistrement et archive de photo dans le journal

FTP Username : alarm5

FTP Password : alarm5

Configuration d'une alarme FTP

Dans la configuration de l'alarme FTP, vous pourrez choisir d'activer la journalisation de la photo JPEG qui sera envoyée par la caméra.

Il est également possible de laisser le système extraire une photo des enregistrements de la caméra associée. Dans ce cas précis, l'upload de l'image par FTP ne servira que pour déclencher le signal d'alarme et non stocker l'image de la caméra.

Si l'upload FTP de la caméra n'est pas instantané, vous pouvez éventuellement forcer un recalage de la date et heure de l'alarme (par exemple : -3 secondes).

Important : ne configurez jamais vos caméras pour qu'elles envoient plusieurs images de suite sur le compte FTP. Le système utilisera seulement la première image pour déclencher l'alarme et la journalisation. Vous pouvez même provoquer des surcharges du réseau, de la caméra ou du serveur si vous configurez un envoi d'images consécutifs avec un frame rate trop élevé.

6.7 Alarme réseau (HTTP/S)

Une alarme réseau HTTP est utilisée pour réceptionner un signal d'alarme envoyé par une caméra ou un encodeur IP via le réseau et les protocoles HTTP/HTTPS.

Lors de la création d'une alarme HTTP, le système créera une ou deux URL d'accès afin de réceptionner les signaux des caméras ou périphériques IP (notification simple, sans upload d'image ou de données).

Il suffira de configurer cette URL avec le chemin d'accès complet (protocole et adresse IP) dans la caméra.

A chaque fois que ce lien sera appelé, le système déclenchera l'alarme associée.

Exemple / ALARM HTTP URL - ON :

`http://192.168.0.99/cgi-bin/alarm?id=0ea4a618770474a2efa310131396e2c0`

Il est possible de configurer deux méthodes d'alarmes HTTP : soit une alarme avec un timer, soit une alarme avec une action directe ON/OFF.

Si vous sélectionnez une temporisation dans l'option "Temps d'activation minimal", l'alarme restera en état ON pendant le temps minimal configuré, avant de repasser automatiquement en état OFF (si aucun nouveau signal réceptionné entre temps).

Si vous sélectionnez la valeur "CGI ON/OFF control" dans la même liste d'option, le système générera deux liens d'accès : un pour l'état ON et un pour l'état OFF.

Dans ce mode, vous aurez donc deux liens à configurer dans la caméra ou dans le périphérique IP : un pour activer l'alarme et un pour la désactiver.

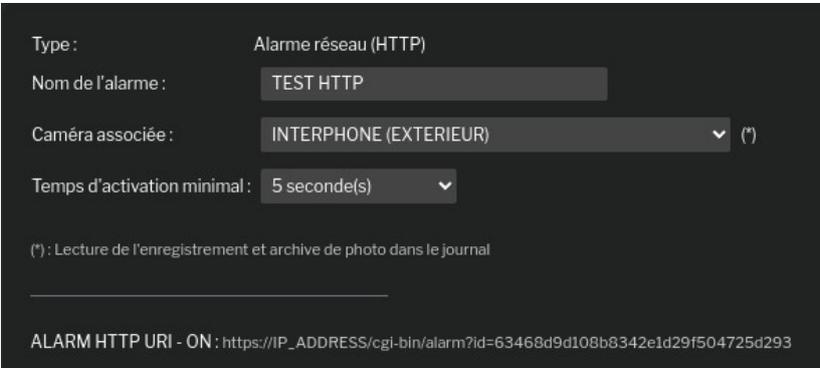
Ce mode est très utile pour répliquer précisément les états de contacts secs d'une caméra ou d'un périphérique IP : tant que le signal OFF n'a pas été transmis, l'alarme restera active dans le système. Exemple d'application : contact ouverture porte, contact de mise en/hors surveillance, etc.

Exemple / ALARM HTTP URL - ON :

`http://192.168.0.99/cgi-bin/alarm?id=0ea4a618770474a2efa310131396e2c0&alarmctrl=on`

Exemple / ALARM HTTP URL - OFF :

`http://192.168.0.99/cgi-bin/alarm?id=0ea4a618770474a2efa310131396e2c0&alarmctrl=off`



The screenshot shows a configuration window for a network alarm. The fields are as follows:

Type :	Alarme réseau (HTTP)
Nom de l'alarme :	TEST HTTP
Caméra associée :	INTERPHONE (EXTERIEUR) (*)
Temps d'activation minimal :	5 seconde(s)

(*) : Lecture de l'enregistrement et archive de photo dans le journal

ALARM HTTP URI - ON : `https://IP_ADDRESS/cgi-bin/alarm?id=63468d9d108b8342e1d29f504725d293`

Configuration d'une alarme HTTP avec contrôle ON seul (PULSE MODE)

Dans la configuration de l'alarme HTTP, vous pourrez choisir d'activer la journalisation d'une image qui sera extraire directement des enregistrements de la caméra associée. Il vous sera également possible de retarder la prise de photo et de recalculer la date et heure du journal.

Remarque : consultez la documentation API / Génération d'une alarme HTTP pour tous les détails sur les paramètres et les possibilités de ces types d'alarmes.

6.8 Scénario d'alarmes

Un scénario d'alarme permet de créer une alarme virtuelle composée de plusieurs alarmes. Cette alarme aura la particularité de ne se déclencher que lorsqu'un scénario spécifique sera détecté.

Une alarme scénario reprend les mêmes caractéristiques qu'une alarme réseau, elle peut aussi être associée à une caméra pour créer un journal et une galerie d'image et se configure également sur agenda.

L'alarme scénario sera ensuite composée de plusieurs scénarios d'alarmes qui seront inspectés en fonction de la configuration.

Un scénario d'alarme peut être activé en fonction des comparaisons logiques "ET" (AND) et "OU" (OR) :

OU - une seule alarme doit être activée

ET - toutes les alarmes doivent être activées

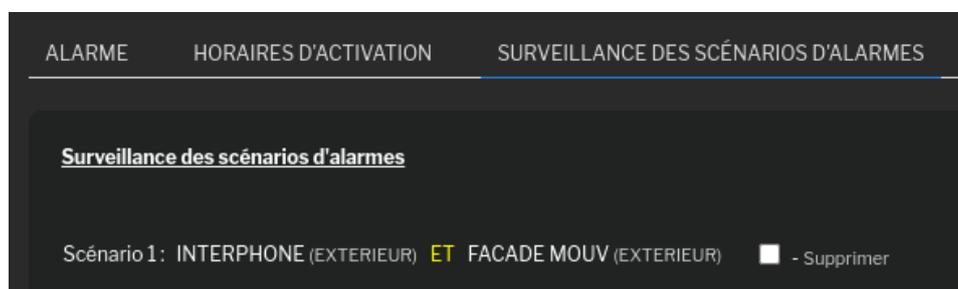
Par exemple : déclenchement d'un scénario d'alarme SI { "Alarme Porte d'entrée" ET "Alarme Hall d'entrée" }

Si l'alarme comprends plusieurs scénarios, son déclenchement sera aussi fonction des comparaisons logiques "ET" (AND) et "OU" (OR) :

OU - un seul scénario d'alarme doit être activé

ET - tous les scénarios d'alarme doivent être activés

Par exemple : déclenchement de l'alarme SI { "scénario d'alarme 1" OU "scénario d'alarme 2" }

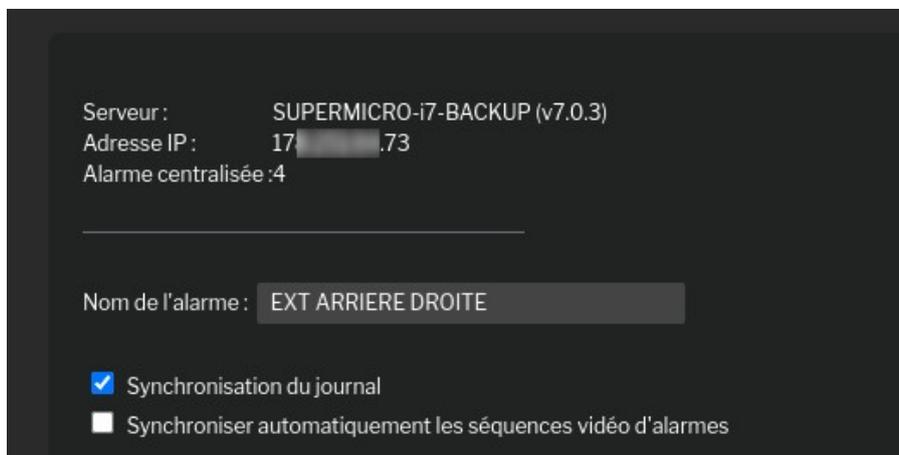


Le temps d'activation d'une alarme scénario est automatique et dépend directement de l'ensemble des alarmes associées. L'alarme scénario ne se désactivera que lorsque toutes ces alarmes associées seront à l'état OFF.

6.9 Alarme centralisée (VPN)

Ce type d'alarme est une alarme configurée sur un serveur de centralisation VXCORE-CORPORATE ou VXCORE-ENTERPRISE.

Cette alarme sera directement reliée à une autre alarme, située sur un autre système vidéo (connecté en local ou a distance). A chaque fois que l'alarme se déclenchera sur le système vidéo, elle sera automatiquement activée sur le serveur central.



The screenshot shows a configuration window for a centralized alarm. It displays the following information:

- Serveur : SUPERMICRO-i7-BACKUP (v7.0.3)
- Adresse IP : 17[redacted].73
- Alarme centralisée : 4
- Nom de l'alarme : EXT ARRIERE DROITE
- Synchronisation du journal
- Synchroniser automatiquement les séquences vidéo d'alarmes

Nom de l'alarme

Permet de spécifier le nom identifiant de l'alarme

Synchronisation du journal

Permet d'activer le journal de l'alarme sur le serveur central. Lorsque cette option est active, le système synchronisera automatiquement la photo de l'alarme et éventuellement la séquence vidéo associée.

Le journal des alarmes d'un serveur central est totalement indépendant et consolidé avec l'ensemble des historiques des alarmes de tous les systèmes vidéo connectés. Le stockage du serveur central doit donc être dimensionné pour accueillir l'ensemble des données de journalisation des systèmes clients.

Il existe une option globale pour limiter la journalisation des événements dans l'administration du système (section administration/accès externes/VPN).

Synchroniser automatiquement les séquences vidéo d'alarmes

L'option de synchronisation des séquences vidéo d'alarme permet au serveur central de télécharger et stocker automatiquement la séquence vidéo des événements d'alarmes (vidéo de 5 à 15 secondes).

La durée des séquences vidéo d'alarmes est paramétrable dans les options vidéo de l'interface d'administration du système.

Remarque : pour que la synchronisation des séquences vidéo soit effective, le système vidéo doit disposer d'une bande passante suffisante, supérieure à 128 kbit/sec. Le téléchargement des séquences vidéo sera limité à une exécution de 45 secondes avant d'échouer.

Dans la consultation du journal des alarmes d'un serveur de centralisation, il peut y avoir plusieurs états pour les séquences vidéo d'alarmes.

Séquence vidéo OK

Vous verrez apparaître l'état "VIDEO SEQUENCE" en dessous de la vidéo, avec les détails du fichier vidéo téléchargé (taille, résolution, débit, etc). La séquence vidéo a bien été synchronisée et est bien stockée sur le serveur central.



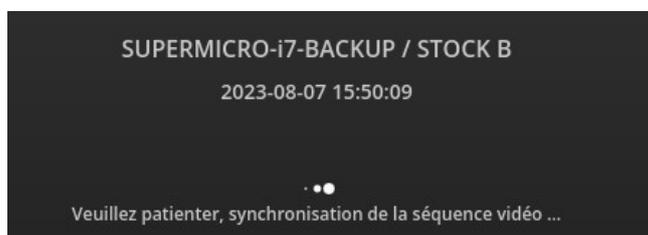
Séquence vidéo d'alarme disponible sur le serveur central

Remarque : si vous disposez de la permission d'exportation vidéo, vous pouvez cliquer sur le bouton « Sauvegarder la séquence vidéo » pour la transformer en fichier vidéo téléchargeable.

Séquence vidéo en cours de synchronisation

Lorsque la séquence vidéo n'existe pas sur le serveur central et que vous la consultez pour la première fois, le système va automatiquement la synchroniser du système vidéo qui héberge l'alarme.

La séquence vidéo s'affichera automatiquement quand elle sera synchronisée. Si vous ne disposez pas d'assez de bande passante ou que le réseau tombe en timeout, un message d'erreur s'affichera.



Pas de séquence vidéo

Si aucune séquence vidéo pour cette alarme n'est disponible sur le serveur, vous verrez apparaître l'état "VIDEO PLAYBACK" en dessous de la vidéo. Le système tentera de lire directement la séquence vidéo sur le système vidéo client qui héberge l'alarme.

Les causes d'une non-synchronisation des séquences vidéo peuvent être multiples : manque de bande passante, déconnexion du client VPN, flux vidéo sélectionné trop gros, etc.



Pas de séquence vidéo d'alarme disponible sur le serveur central, playback direct sur le système vidéo client

7 Messages audio

VXCORE dispose d'une fonctionnalité de diffusion audio (locale ou multi-site) permettant de transformer chaque serveur vidéo en haut-parleur IP.

Les utilisateurs pourront diffuser des messages audio manuellement via l'interface d'exploitation ou automatiquement via des agents / actions systèmes.

Remarque : pour diffuser des messages audio avec le serveur, la sortie audio doit avoir été activée via l'interface d'administration du système.

Pour ajouter des messages audio, vous pouvez soit importer un fichier audio, soit utiliser la fonctionnalité d'enregistrement directe du logiciel d'exploitation PC (la durée des messages audio est limitée à 45 secondes).

Importation de fichier audio

Pour importer un nouveau fichier audio, cliquez sur le bouton « Ajouter », sélectionnez un fichier sur votre PC, puis cliquez sur le bouton « Importer un fichier audio ».

Les fichiers audio compatibles seront au format wav/mp4/mp3, le système remontrera une erreur si le format n'est pas supporté.

Enregistrement de message audio

Pour enregistrer un message audio directement avec le logiciel d'exploitation PC, cliquez sur le bouton « Ajouter », puis utilisez les boutons situés dans la section « Enregistrer un message audio ».

Démarrer l'enregistrement audio

Cliquez sur ce bouton pour démarrer l'enregistrement audio, en utilisant l'entrée son par défaut de votre PC (entrée micro). Vous pouvez changer l'entrée son par défaut de votre PC en utilisant le tableau de bord de réglage audio de votre système d'exploitation.

Stopper l'enregistrement audio

Cliquez sur ce bouton pour stopper l'enregistrement audio en cours.

Écouter l'enregistrement audio

Cliquez sur ce bouton pour écouter le message audio que vous venez d'enregistrer. Si vous souhaitez recommencer l'enregistrement, cliquez à nouveau sur le bouton « Démarrer l'enregistrement audio ».

Envoyez le fichier audio sur le serveur

Utilisez ce bouton pour transférer le message audio que vous venez d'enregistrer sur votre PC vers le serveur VXCORE. Il apparaîtra ensuite dans la liste des messages audio du système.

Messages audio			
service-bell_daniel_simion	00:00:01.64	0.01 MB	☰
Wolf	00:00:04.45	0.04 MB	☰
Scary_Demon_Haunting-Adam_Webb-97651262	00:00:45.02	0.36 MB	☰
survivor-eye-of-the-tiger	00:00:45.02	0.36 MB	☰
+ Ajouter			

Liste des messages audio importés ou enregistrés

Paramètres des messages audio

Pour chaque message audio, vous pouvez sélectionner un nom identifiant et une catégorie.

Le nom identifiant sera affiché dans l'interface pour repérer les messages dans l'interface de diffusion audio.

La catégorie permettra de classer les sons selon leur utilisation : soit en diffusion directe via l'interface utilisateur, soit en diffusion système automatique, soit les deux.

Par exemple : le message audio « warning » pourra être diffusé manuellement par les utilisateurs, mais le message audio « info » ne pourra être diffusé qu'automatiquement par une action système à une heure fixe.

8 Programmation

VXCORE permet une programmation très précise des processus systèmes. Ces processus doivent être programmés dans l'agenda système.

8.1 Programmation des évènements systèmes

Liste des processus programmables :

- Enregistrement permanent

Définit une plage d'enregistrement des caméras en continu.

- Enregistrement sur alarme

Définit une plage d'enregistrement des caméras sur alarme.

- Ronde PTZ

Définit une plage de fonctionnement pour une ou plusieurs ronds PTZ.

- Action système

Définit un horaire d'activation d'une action système.

Remarque : le système dispose d'une option globale pour activer l'enregistrement vidéo (continu ou sur alarme) directement dans l'interface d'administration.

Pour permettre la programmation d'un évènement d'enregistrement de caméra, il sera nécessaire d'avoir préalablement configuré les modes vidéo d'enregistrement.

De la même manière, pour programmer un évènement d'enregistrement sur alarme, les caméras doivent avoir été liées à des alarmes (caméra associée).

Un évènement d'enregistrement permanent ou continu sera toujours prioritaire sur un enregistrement sur alarme.

Chaque administrateur pourra configurer ses propres évènements systèmes.

Vous pouvez cliquer directement sur la pastille rouge ou verte située à gauche de chaque évènement système pour l'activer ou le désactiver.

8.2 Configuration des calendriers

Le système dispose d'une gestion de calendrier unifiée pour l'ensemble du système.

Un même calendrier pourra être utilisé dans plusieurs éléments de la configuration :

- Programmation des évènements systèmes (enregistrement des caméras, ronds, actions)

- Horaires d'activation des alarmes

- Horaires de connexion autorisés des comptes utilisateurs

Nom	Horaire	Lu	Ma	Me	Je	Ve	Sa	Di
Par défaut	24h/24	x	x	x	x	x	x	x
JOUR	06h00 - 21h00	x	x	x	x	x	x	...
NUIT	20h00 - 06h00	x	x	x	x	x	x	...

+ Ajouter

La modification d'un calendrier affectera tous les éléments de configuration où il a été utilisé.

8.3 Configuration des rondes PTZ

Un processus de ronde PTZ est un cycle de plusieurs positions "preset" d'une caméra PTZ. Ce cycle pourra être dynamiquement contrôlé en fonction des événements d'alarmes.

Avant de configurer des rondes PTZ, vous devez donc avoir préalablement configuré des presets dans vos caméras PTZ (via l'interface de contrôle PTZ utilisateur).

Il existe deux types de rondes PTZ dans le système :

- Ronde active

Ronde en mouvement continu, qui va appeler chaque preset PTZ configuré et marquer un temps de pause pré-défini.

- Ronde home

Ronde en attente sur une position pré-définie "home", déplacement uniquement en cas d'alarme associée.

Lorsqu'une ronde PTZ est en fonctionnement, le système la placera automatiquement en pause lorsqu'un utilisateur repositionnera la caméra en utilisant l'interface de contrôle PTZ. Le temps de pause avant la reprise automatique de la ronde est paramétrable.

Il est possible d'associer des déclenchements d'alarmes à chaque position "preset" des rondes PTZ. Le système ajustera alors le comportement de la ronde en fonction des déclenchements d'alarmes.

Remarque : vous pouvez utiliser l'option « Désactiver temporairement l'analyse vidéo » dans la configuration de la caméra pour ne pas déclencher d'alarmes lorsque la caméra PTZ sera en mouvement.

8.3.1 Ronde PTZ active

Une ronde PTZ active est un cycle permanent : la caméra sera positionnée sur chaque preset PTZ configuré et marquera le temps de pause pré-défini (cycle).

En cas de contrôle utilisateur de la caméra PTZ, la ronde sera automatiquement placée en pause. Elle reprendra ensuite la ou elle s'était arrêtée.

En cas d'association des positions de la ronde avec des événements d'alarmes, le comportement deviendra dynamique :

Comportement hors alarme

La ronde se positionnera sur chaque preset configuré en marquant le temps de pause défini.

Comportement si déclenchement d'alarme

La ronde se placera automatiquement sur le preset associé à l'alarme et y stationnera tant que l'alarme restera active.

Dans le cas d'un nouveau déclenchement d'alarme, la ronde sera repositionnée, et ainsi de suite.

Remise à zéro

Ce n'est que lorsque toutes les alarmes associées seront revenues à l'état OFF que la ronde poursuivra son cycle initial.

8.3.2 Ronde PTZ home

Une ronde PTZ home est utilisée pour forcer une position preset/home par défaut. La caméra ne sera repositionnée par le système qu'en cas de déclenchement d'alarme, avant de revenir sur sa position home.

En cas de contrôle utilisateur de la caméra PTZ, le processus de ronde sera automatiquement mis en pause. Après la période de reprise automatique, le système repositionnera à nouveau la caméra sur la position "home".

Le comportement deviendra dynamique en fonction des événements d'alarmes associés :

Comportement hors alarme

La ronde stationnera sur la position "home" configurée (position numéro 1).

Comportement si déclenchement d'alarme

La ronde se placera automatiquement sur le preset associé à l'alarme et y stationnera tant que l'alarme restera active.

Dans le cas d'un nouveau déclenchement d'alarme, la ronde sera repositionnée, et ainsi de suite.

Remise à zéro

Ce n'est que lorsque toutes les alarmes associées seront revenues à l'état OFF que la ronde stationnera à nouveau sur la position "home".

8.4 Configuration des commandes I/O

VXCORE intègre une interface de configuration de commandes externes qui permettra d'ajouter des boutons personnalisables dans l'interface du système. Ces boutons seront accessibles avec le logiciel d'exploitation PC et sur les applications mobiles (iOS/Android).

Il sera alors possible de piloter tout type d'équipements I/O connectés sur le réseau pour interagir avec l'environnement extérieur (lumières, gâches de portes, barrières, sirènes ...).

Les boutons de contrôles pourront être affichés de manière globale ou filtrés par groupes de caméras, et en fonction des droits d'accès utilisateurs.

Chaque bouton de contrôle sera liée à une commande ou une action spécifique vers un périphérique de gestion de contacts secs I/O ou tout autre type d'équipement compatible connecté sur le réseau. Ces commandes I/O seront envoyées via des requêtes Web standard HTTP/HTTPS (GET ou POST).

Remarque : pour activer les actions et les boutons I/O, la permission adéquate devra être configurée dans les paramètres des comptes admin/user.

8.4.1 Configuration des périphériques de contrôle I/O

Avant de configurer des commandes, vous devez renseigner les différents équipements I/O disponibles sur le réseau.

Un équipement réseau sera configuré avec les éléments suivants :

- un nom identifiant
- une adresse IP / port de connexion

- un protocole / méthode de communication Web (HTTP/HTTPS/GET/POST/JSON)
- un identifiant / mot de passe de connexion si nécessaire

Remarque : les équipements réseau I/O ne seront pas supervisés par le système. Si un équipement est déconnecté, les commandes remonteront une simple erreur de communication.

8.4.2 Configuration des commandes

Après avoir configuré les différents périphériques de contrôle, vous pourrez créer et associer des commandes I/O personnalisées.

The screenshot displays the 'Gestion des commandes I/O' configuration page. It features a dark-themed interface with several tabs at the top: 'Programmation du système', 'Configuration des calendriers', 'Configuration des rondes PTZ', 'Gestion des commandes I/O', and 'Configuration des actions'. The main content area is titled 'Commande I/O' and contains the following fields:

- Nom :** LUMIERE
- Périphérique I/O :** IPX800
- Contrôle :** manuel
- URI - ON :** /api/xdevices.json?key=ealRiedweremoodyeft&SetR=01
- URI - OFF :** /api/xdevices.json?key=ealRiedweremoodyeft&ClearR=01

An 'Appliquer' button is located below the URI fields. Underneath, there is a section titled 'Affectation caméras' with a '+ -- Ajouter une caméra --' dropdown menu. Two cameras are listed below: 'CAFE' and 'CUISINE', each with a small 'X' icon to its right, indicating they are assigned to the command.

Configuration d'une commande I/O pour contrôler une lumière avec un module IPX800

Le nom identifiant sera utilisé pour repérer les boutons d'actions dans l'interface du système.

Il existe 2 types de contrôle : **manuel** ou **automatique** avec temporisation

En mode manuel, vous disposerez de deux boutons dans l'interface : ON et OFF.

En mode automatique, nous ne disposerez que d'un seul bouton dans l'interface : TOOGLE

Par exemple : le mode manuel vous permettra de gérer manuellement l'allumage/extinction d'une lumière et le mode automatique vous permettra d'activer automatiquement une gâche électrique pendant 3 secondes.

Les affectations caméras permettent de lier les différents boutons dans l'interface, en fonction des droits d'accès caméras.

Par défaut, si aucune caméra n'est affectée, le bouton apparaîtra partout de manière globale, quelque soit la caméra sélectionnée.

Si au contraire, une ou plusieurs caméras sont affectées à la commande, le bouton de contrôle n'apparaîtra que lors de la visualisation de ces caméras.

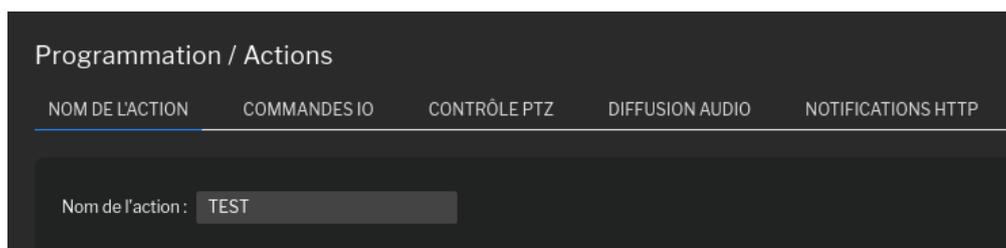
Remarque : si le protocole POST/JSON a été configuré dans le périphérique I/O, deux champs de saisies supplémentaires « REQUEST CONTENT » apparaitront dans les commandes I/O. Ils seront utilisés pour transmettre des données au format JSON au périphérique I/O (Requête POST avec « Content-Type: application/json »).

8.5 Configuration des actions

Une action système est un évènement qui permet de regrouper plusieurs interactions :

- Commandes I/O
- Contrôle PTZ
- Diffusion audio
- Notifications HTTP

Avant de configurer une action, vous devez avoir préalablement configuré les interactions possibles (Commandes IO, sortie/serveurs audio, presets PTZ, etc).



Une action système pourra être utilisée de deux manières :

- soit dans un agent de sécurité
- soit en programmation dans l'agenda système (sur horaire)

Remarque : si vous souhaitez repositionner vos caméras PTZ sur alarme/détection, nous vous conseillons d'utiliser la fonctionnalité des rondes PTZ plutôt que des agents avec actions.

En cas de programmation complexe avec beaucoup d'alarmes, le comportement du repositionnement PTZ avec des agents risque de devenir totalement imprévisible.

9 Agents de sécurité et Supervision

Un agent est un processus système qui va surveiller ou superviser un ensemble d'éléments pour éventuellement alerter ou effectuer des actions précises.

Il existe deux type d'agents :

- Agent de sécurité

Permet de surveiller un groupe d'alarmes, afin d'envoyer des alertes emails avec les images des déclenchements en pièce jointe, de diffuser des messages audio, d'envoyer des images séquences vidéo sur le réseau et de faire des actions.

- Agent de supervision

Permet de surveiller un groupe d'éléments de la configuration, afin d'envoyer des alertes emails en cas de connexion/déconnexions, détection d'erreurs, etc.

Important : afin que le système puisse envoyer des alertes emails aux utilisateurs, vous devez renseigner dans chaque compte utilisateur une ou plusieurs adresses email.

Les agents pourront être activés et désactivés manuellement directement dans le tableau de bord du système ou via l'application Mobile.

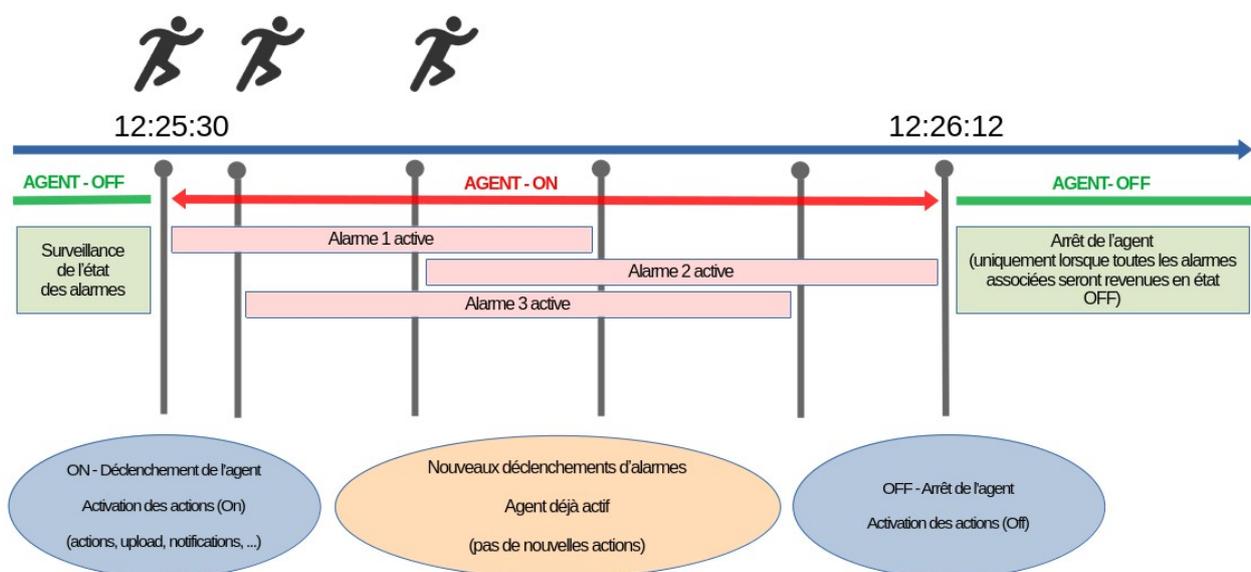
9.1 Agents de sécurité

Un agent de sécurité est un processus spécial qui va superviser une ou plusieurs alarmes et faire des actions en cas de déclenchements : Commandes I/O, Actions, Diffusion audio, Notifications HTTP, Alertes Email, Upload FTP, etc.

Toutes les actions des agents de sécurité seront enregistrées dans un journal système spécifique.

Comportement de l'agent de sécurité :

- **Activation** : si une ou plusieurs alarmes en surveillance se déclenchent (état On)
- **Désactivation** : lorsque l'ensemble des alarmes en surveillance sont désactivées (état Off)



Paramètres de l'agent

Nom de l'agent

Définit le nom identifiant de l'agent de sécurité virtuel.

Alarme maître

Définit une alarme "maître" qui contrôlera le déclenchement général de l'agent. L'agent ne se déclenchera pas tant que l'alarme principale ne sera pas dans l'état attendu (ON ou OFF).

Cette fonctionnalité permettra de désactiver un agent manuellement avec un clavier digicode par exemple, en configurant préalablement une alarme API HTTP/S avec des contacts secs de mise en/hors surveillance.

Surveillance des alarmes

Spécifie l'ensemble des alarmes qui seront supervisées par l'agent.

Horaires d'activations

Permet de programmer l'agent selon un/des calendriers, afin de ne l'activer que sur certaines plages horaires.

Vous devez d'abord programmer des calendriers avant de les configurer dans les agents.

Commandes I/O

Activation des différentes commandes I/O des périphériques programmés dans le système. Il est possible d'activer des commandes sur activation et/ou désactivation de l'agent.

Actions

Permet de définir les actions qui seront déclenchées par l'agent en cas d'alarme détectée (activation de contacts secs, de commandes CGI/IO ou déplacements des caméras PTZ).

Vous devez d'abord programmer des actions avant de les configurer dans les agents.

Diffusion audio

Permet de diffuser automatiquement un message audio système ou personnalisé en cas de déclenchement d'alarme.

Les messages pourront être diffusés sur la sortie son locale du serveur ou sur l'ensemble des systèmes vidéo connectés sur un serveur central.

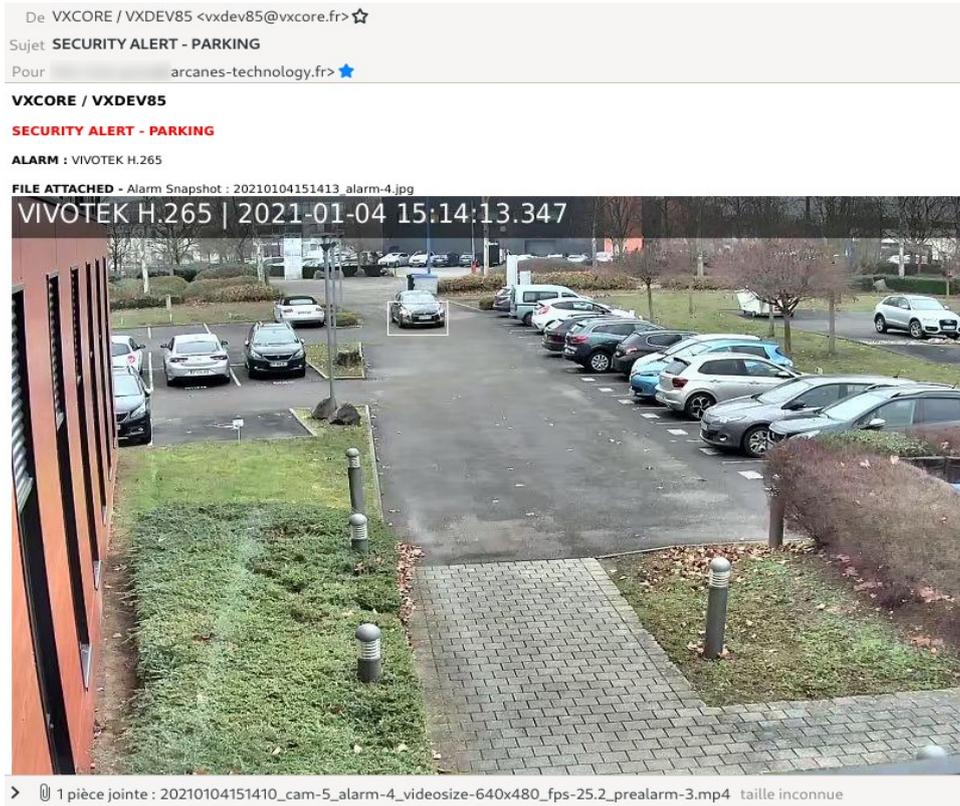
Notifications HTTP/S

Ces liens Web seront appelés automatiquement lors de l'activation ou la désactivation de l'agent. Ces liens seront au format GET et utiliseront le protocole http ou https.

Alertes emails

Permet de spécifier les utilisateurs vers lesquelles l'agent enverra des alertes emails. Chaque utilisateur doit avoir préalablement renseigné dans les paramètres de son compte une ou plusieurs adresses email. Les alertes emails pourront être envoyées au format texte ou HTML (plus lisible).

La fréquence maximum des envois permet de limiter l'envoi des alertes emails au tant imparti, pour ne pas saturer les boîtes mail des destinataires.



Email d'alerte avec photo et vidéo de l'alarme

Upload FTP

Active l'envoi des médias du déclenchement d'alarme sur un serveur FTP accessible au réseau (images JPEG et/ou séquences vidéo au format H.264 (mp4) ou MPEG4 (avi)).

L'envoi par FTP supporte l'authentification anonyme ou via compte utilisateur, le changement de répertoire distant, l'ajout d'un préfixe texte aux fichiers et le mode passif.

Attachement / Upload des médias

Ces médias seront utilisés dans les alertes emails et dans l'upload FTP : pour chaque déclenchement d'alarme, le système pourra extraire les photos et les vidéos associées.

Les photos seront extraites au format JPEG et éventuellement redimensionnée pour accélérer l'envoi et faciliter la consultation dans les emails.

Les séquences vidéos peuvent être générées au format H.264 (mp4) ou MPEG4 (avi).

Format des séquences vidéo

Le système génère des mini-séquences vidéo à partir des enregistrements vidéo des caméras (séquences vidéo de 15 secondes en résolution 640x480).

Format de fichier des séquences :

`${DATETIME}_cam-${IDCAMERA}_alarm-${IDALARM}_videosize-${RESOLUTION}_fps-${FPS}_prealarm-${PREALARMTIME}`

- `${DATETIME}` : date et heure de la séquence vidéo extraite (au format YYYYMMDDHHMMSS)
- `${IDCAMERA}` : identifiant de la caméra utilisée pour créer la séquence vidéo.

- $\{IDALARM\}$: identifiant de l'alarme associée au déclenchement initial.
- $\{RESOLUTION\}$: identifiant de l'alarme associée au déclenchement initial.
- $\{FPS\}$: valeur du frame rate de la séquence vidéo extraite.
- $\{PREALARMTIME\}$: valeur de pré-alarme de la séquence vidéo extraite (en secondes).

Remarque : la date et heure réelle de début de la séquence vidéo se situe avant la valeur de pré-alarme.

$VIDEO_DATETIME = \{DATETIME\} - \{PREALARMTIME\}$

Exemple de séquence vidéo :

20210104151410_cam-5_alarm-4_videosize-640x480_fps-25.2_prealarm-3.mp4

Contrôle utilisateur

Vous pourrez également configurer le contrôle utilisateur : chaque agent pourra être activé/désactivé par un de vos utilisateurs, mais il ne pourra en aucun cas modifier sa configuration.

Les agents pourront être activés et désactivés directement dans le compte utilisateur, en utilisant l'application PC et/ou l'application Mobile.

9.2 Agents de supervision

Un agent de supervision système est un processus qui surveille un ou plusieurs éléments et envoi des alertes emails aux utilisateurs en cas de connexion/déconnexion ou d'erreurs détecté.

Il existe deux types d'agents de supervision :

- Connexion/déconnexion des caméras

Une alerte email sera envoyée en cas de connexion/déconnexion des caméras

- Connexion/déconnexion des clients VPN (sur un serveur central)

Une alerte email sera envoyée en cas de connexion/déconnexion des systèmes vidéo

Pour configurer un nouvel agent, renseignez simplement un nom identifiant, un type d'agent, les éléments à superviser et les utilisateurs à avertir.

Paramètres de l'agent

Type de supervision

Défini le type de supervision système

Nom de l'agent

Défini le nom identifiant de l'agent de supervision

Période de supervision

Permet de régler la période de supervision, afin de temporiser les alertes emails dans le cas de connexions/déconnexions intempestives.

Par exemple : un réglage de 5 min signifie qu'aucune alerte email ne sera envoyée tant que la caméra n'est pas déconnectée depuis 5 min. Si au contraire la caméra se reconnecte dans cette intervalle de temps, l'alerting sera annulé.

Supervision

Cochez dans cette liste les éléments que vous souhaitez superviser.

Horaires d'activations

Permet de programmer l'agent selon un/des calendriers, afin de ne l'activer que sur certaines plages horaires. Vous devez d'abord programmer des calendriers avant de les configurer dans les agents.

Alertes emails

Permet de spécifier à quels utilisateurs l'agent enverra les alertes emails. Chaque utilisateur doit avoir préalablement renseigné dans les paramètres de son compte une ou plusieurs adresses email.

Contrôle utilisateur

Vous pourrez également configurer le contrôle utilisateur : chaque agent pourra être activé/désactivé par un de vos utilisateurs, mais il ne pourra en aucun cas modifier sa configuration. Les agents pourront être activés et désactivés directement dans le compte utilisateur, en utilisant l'application PC et/ou l'application Mobile.

10 Gestion des comptes / rôles

Le système permet de définir des rôles et des comptes utilisateurs. Les possibilités dépendront de la version de l'OS utilisée.

10.1 Types de comptes

Le système dispose de 3 espaces distincts d'utilisation et de configuration :

- Espace d'administration système

Configuration et administration de l'OS (réseau, stockage, VPN, ...).

- Espace de configuration vidéo

Configuration du système vidéo (caméras, alarmes, PTZ, ...).

- Espace d'utilisation

Utilisation du système vidéo (visualisation caméras et alarmes, consultation des enregistrements, ...).

Le système dispose de 4 types d'utilisateurs :

- Administrateur "root" ou Super-utilisateur
- Administrateur maintenance
- Administrateur vidéo
- Utilisateur

Droits d'accès au système, en fonction du type d'utilisateur

	Espace d'administration	Espace de configuration	Espace d'utilisation
Super-utilisateur « root »	oui	oui	oui
Administrateur maintenance	oui	-	-
Administrateur vidéo	(selon permissions)	oui	oui
Utilisateur	-	-	oui

Le système permet de rajouter de multiples droits d'accès pour les administrateurs vidéo et les utilisateurs, permettant de bien segmenter les actions permises ou non.

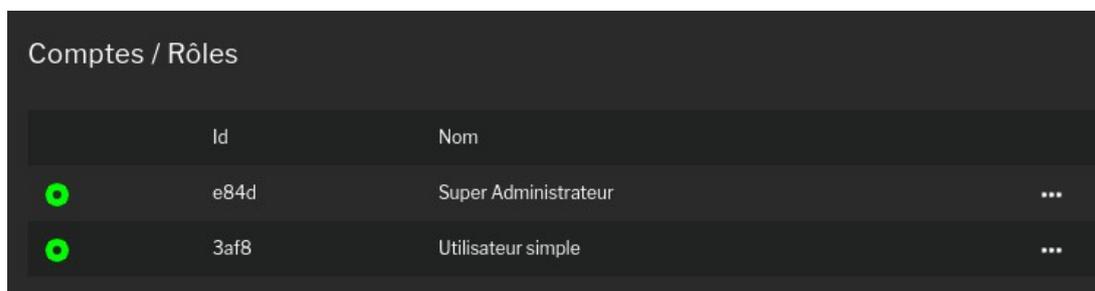
L'interface sera "construite" de manière dynamique en fonction des droits d'accès et du type d'utilisateur, en ajoutant ou supprimant des menus ou des boutons. Il sera alors possible d'afficher aux utilisateurs une interface très simple aussi bien qu'une interface très complète.

Remarque : un utilisateur ne peut par définition rien créer ni configurer. Un utilisateur dispose toujours d'un administrateur "père" qui lui attribuera les droits et lui configurera son interface.

10.2 Rôles

A la différence d'un compte utilisateur ou administrateur, un rôle définit uniquement un ensemble de permissions et droits d'accès, sans aucune information personnelle (identifiant, mot de passe, email, ...)

Un rôle pourra donc être lié à un compte utilisateur, afin de lui affecter des permissions automatiquement par héritage. Par conséquent, si vous modifiez un rôle, tous les comptes utilisateurs liés seront affectés par les changements.



	Id	Nom	
●	e84d	Super Administrateur	...
●	3af8	Utilisateur simple	...

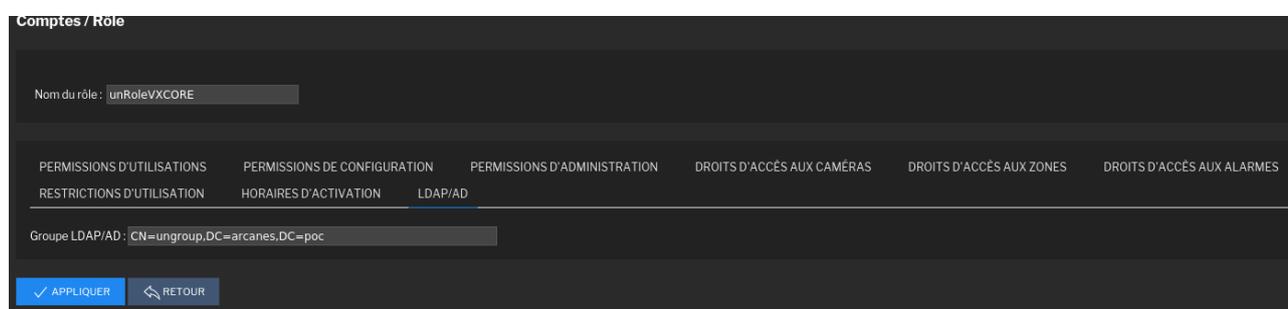
La configuration d'un rôle permet de sélectionner les mêmes permissions et droits d'accès qu'un compte utilisateur ou administrateur : vous pourrez donc lui affecter des caméras, des alarmes, des systèmes vidéo, des écrans, etc

Cela sera très utile pour dissocier totalement les informations de certains comptes (authentification des utilisateurs) et leurs permissions (droits d'accès groupés).

Un compte utilisateur ou administrateur pourra donc disposer d'un droit ou d'une permission :

- soit par un rôle lié (permission héritée)
- soit par la configuration de son compte (permission directe)

Si vous avez configuré un serveur LDAP/Active Directory dans les paramètres d'administration du système, un rôle vous permettra également de lier un groupe LDAP/AD. Si un utilisateur LDAP n'est lié à aucun rôle, il ne pourra pas se connecter au système (compte automatiquement désactivé).



Comptes / Rôle

Nom du rôle : unRoleVXCORE

PERMISSIONS D'UTILISATIONS PERMISSIONS DE CONFIGURATION PERMISSIONS D'ADMINISTRATION DROITS D'ACCÈS AUX CAMÉRAS DROITS D'ACCÈS AUX ZONES DROITS D'ACCÈS AUX ALARMES

RESTRICTIONS D'UTILISATION HORAIRES D'ACTIVATION LDAP/AD

Groupe LDAP/AD : CN=ungroup,DC=arcanes,DC=poc

✓ APPLIQUER ↩ RETOUR

Consultez la documentation Administration du système pour plus de détails sur les possibilités LDAP/AD.

10.3 Administrateur système maintenance

Un administrateur système maintenance est un utilisateur spécial qui n'aura accès qu'à l'espace administrateur du compte root (sauf quelques éléments critiques).

Cet administrateur doit être utilisé pour donner un accès à l'administration du système sans permettre la moindre visualisation ou configuration des caméras ou du système vidéo.

Pour ajouter un administrateur de maintenance, renseignez simplement un login identifiant, un mot de passe, la langue d'utilisation et éventuellement une date et heure d'expiration du compte.

10.4 Administrateur système vidéo

Un administrateur système vidéo est un utilisateur qui a accès à la configuration et la visualisation, et éventuellement à certains éléments d'administration du système.

Un compte administrateur vidéo pourra être créé selon de multitudes de droits d'accès.

Paramètres du compte

Identifiant du compte

Identifiant ou login du compte administrateur, il doit être unique et il sera impossible de le changer ultérieurement.

Rôle

Permet de lier un rôle existant pour hériter de permissions ou droits d'accès groupées.

Mot de passe du compte

Mot de passe du compte administrateur.

La force du mot de passe dépendra de la stratégie globale de sécurité du système : mot de passe faible (8 caractères minimum) ou mot de passe fort selon les recommandations de l'ANSSI (12 caractères minimum : au moins une lettre minuscule, au moins une lettre majuscule, au moins un chiffre, au moins un caractère spécial).

Nom de l'utilisateur

Non complet de l'administrateur.

Email de l'utilisateur

Adresses email de l'administrateur pour les notifications d'alertes (max 2 adresses, séparées par un espace).

Date d'expiration

Permet de créer un compte administrateur temporaire (format de date et heure : yyyy-mm-jj hh:mm:ss).

Langage

Langue du compte administrateur.

Définition des permissions du compte

Défini la liste des permissions du compte administrateur.

Droits d'accès caméras

Défini la liste des caméras autorisées en visualisation et configuration.

Droits d'accès aux zones

Défini la liste des caméras autorisées en visualisation et configuration, en fonction des zones configurés. Toutes les caméras d'une zone sélectionnée seront automatiquement ajoutés aux permissions du compte.

Droits d'accès alarmes

Défini la liste des alarmes autorisées en visualisation et configuration. Vous pouvez cocher l'option spéciale « Droits d'accès automatique aux alarmes » afin de d'activer automatiquement les droits d'accès aux alarmes associées aux caméras du compte.

Droits d'accès écrans vidéo

Défini la liste des des écrans vidéo autorisés à contrôler et configurer.

Droits d'accès aux serveur vidéo

Seulement pour les serveurs de centralisation : liste des permissions autorisées vers les caméras/alarmes des systèmes vidéo NVR.

Cochez un système vidéo pour activer tous les droits d'accès aux caméras/alarmes, ou cochez explicitement chaque caméra/alarme du système vidéo pour restreindre les droits.

L'option spéciale "Droits d'accès à tous les clients VPN, caméras et alarmes" permet au système d'attribuer automatiquement tous les droits d'accès aux caméras/alarmes de tous les systèmes vidéo NVR connectés.

Permissions d'administration

Ces permissions permettront de donner accès a des éléments d'administration du système, normalement réservés au super-utilisateur root : Licence, Réseau, Stockage, Système, Extensions, Maintenance.

Si vous cochez les permissions « Gestion des administrateurs » ou « Gestion des rôles », le compte administrateur aura la possibilité de configurer les comptes ou les rôles comme le super-utilisateur root.

Redirections réseau externes

Seulement pour les serveurs de centralisation : liste des permissions autorisées vers les redirections réseaux externes configurées dans le système.

Horaires d'activation

Permet de définir les horaires d'activation du compte administrateur, en sélectionnant un ou plusieurs calendriers préalablement configurés.

Restrictions d'utilisation

Espace maximal de stockage des exportations

Spécifie la taille maximale de l'espace de stockage qui sera allouée à l'utilisateur pour l'exportation des vidéos. Si non spécifié, l'utilisateur pourra utiliser tout l'espace disponible dans le périphérique.

Nombre maximal d'utilisateurs

Spécifie le nombre maximal d'utilisateur que l'administrateur pourra créer. Si non spécifié, l'administrateur pourra créer autant d'utilisateur qu'il le souhaite.

10.5 Utilisateur du système

Un utilisateur n'aura aucun droit de configuration du système vidéo. Dans VXCore, un utilisateur ne peut par définition rien créer ni configurer.

Un utilisateur dispose toujours d'un administrateur "père" qui lui attribue les droits et lui configure son interface (création des plans, des modèles de visualisation, etc).

Paramètres du compte

Identifiant du compte

Identifiant ou login du compte utilisateur, il doit être unique et il sera impossible de le changer ultérieurement.

Rôle

Permet de lier un rôle existant pour hériter de permissions ou droits d'accès groupées.

Mot de passe du compte

Mot de passe du compte utilisateur. La force du mot de passe dépendra de la stratégie globale de sécurité du système : mot de passe faible (8 caractères minimum) ou mot de passe fort selon les recommandations de l'ANSSI (12 caractères minimum : au moins une lettre minuscule, au moins une lettre majuscule, au moins un chiffre, au moins un caractère spécial).

Nom de l'utilisateur

Non complet de l'utilisateur.

Email de l'utilisateur

Adresses email de l'utilisateur pour les notifications d'alertes (max 2 adresses, séparées par un espace).

Date d'expiration

Permet de créer un compte utilisateur temporaire (format de date et heure : yyyy-mm-jj hh:mm:ss).

Options de l'interface

Langage

Langue du compte utilisateur.

Page par défaut

Permet de spécifier la première page visible après le login de l'utilisateur.

Authentification automatique

Permet de gérer une clé de connexion automatique pour l'utilisateur directement lors de la création du compte.

Définition des permissions du compte

Définit la liste des permissions du compte utilisateur.

Droits d'accès caméras

Défini la liste des caméras autorisées en visualisation et configuration.

Droits d'accès aux zones

Défini la liste des caméras autorisées en visualisation et configuration, en fonction des zones configurés. Toutes les caméras d'une zone sélectionnée seront automatiquement ajoutés aux permissions du compte.

Droits d'accès alarmes

Défini la liste des alarmes autorisées en visualisation et configuration. Vous pouvez cocher l'option spéciale « Droits d'accès automatique aux alarmes » afin de d'activer automatiquement les droits d'accès aux alarmes associées aux caméras du compte.

Droits d'accès écrans vidéo

Défini la liste des des écrans vidéo autorisés à contrôler et configurer.

Droits d'accès aux systèmes vidéo

Seulement pour les serveurs de centralisation : liste des permissions autorisées vers les caméras/alarmes des systèmes vidéo clients.

Cochez un système vidéo pour activer tous les droits d'accès aux caméras/alarmes, ou cochez explicitement chaque caméra/alarme du système vidéo pour restreindre les droits.

L'option spéciale "Droits d'accès à tous les clients VPN, caméras et alarmes" permet au système d'attribuer automatiquement tous les droits d'accès aux caméras/alarmes de tous les systèmes vidéo NVR connectés.

Horaires d'activation

Permet de définir les horaires d'activation du compte administrateur, en sélectionnant un ou plusieurs calendriers préalablement configurés.

Restrictions d'utilisation

Ne pas modifier son mot de passe

Interdit et désactive l'interface de modification du mot de passe de l'utilisateur.

Ne pas modifier ses informations personnelles

Interdit et désactive l'interface de modification des informations personnelles du compte de l'utilisateur (nom complet, email, etc).

Ne pas modifier ses options du compte

Interdit et désactive l'interface de modification des options du compte de l'utilisateur.

Gestion de l'authentification automatique

Interdit et désactive l'interface de gestion de l'authentification automatique de l'utilisateur.

Pas de tableau de bord

Permet de masquer le tableau de bord pour alléger l'interface du compte utilisateur.

Pas de vues multiples

Permet de masquer les vues multiples pour alléger l'interface du compte utilisateur.

Pas de supervision d'alarme

Permet de masquer la supervision des alarmes pour alléger l'interface du compte utilisateur.

Espace maximal de stockage des exportations

Spécifie la taille maximale de l'espace de stockage qui sera allouée à l'utilisateur pour l'exportation des vidéos. Si non spécifié, l'utilisateur pourra utiliser tout l'espace disponible dans le périphérique.

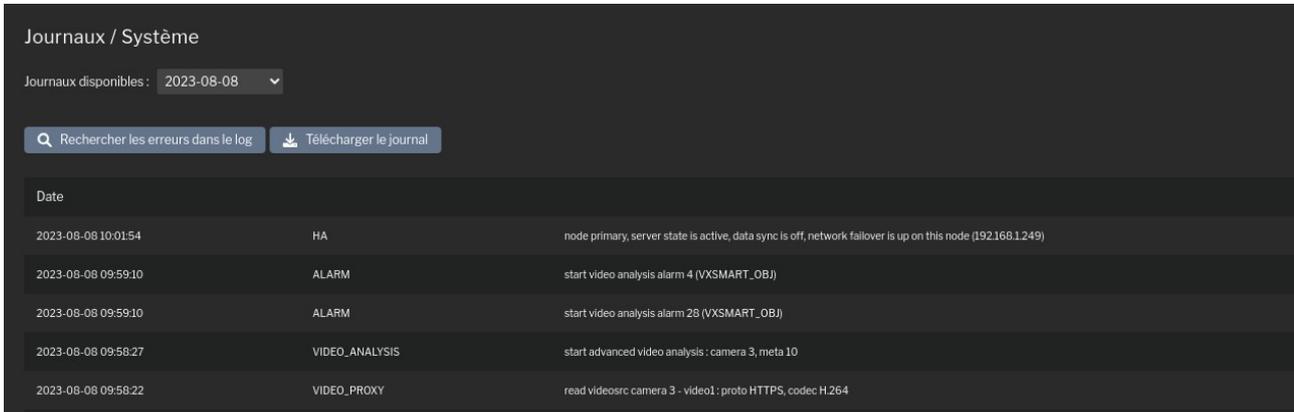
Temps d'exportation maximal

Spécifie un temps d'exportation maximal autorisé pour l'utilisateur.

11 Journaux systèmes

VXCORE dispose d'un système de journalisation de plusieurs événements liés au système ou à la configuration vidéo. Chaque journal sera conservé pour une durée fixe, qui sera configurée dans les paramètres systèmes.

Selon les paramètres de votre compte, vous aurez accès aux journaux de connexion de vos utilisateurs ou encore de l'ensemble du système.



Journaux / Système

Journaux disponibles : 2023-08-08

Rechercher les erreurs dans le log Télécharger le journal

Date		
2023-08-08 10:01:54	HA	node primary, server state is active, data sync is off, network failover is up on this node (192.168.1.249)
2023-08-08 09:59:10	ALARM	start video analysis alarm 4 (VXSMART_OBJ)
2023-08-08 09:59:10	ALARM	start video analysis alarm 28 (VXSMART_OBJ)
2023-08-08 09:58:27	VIDEO_ANALYSIS	start advanced video analysis : camera 3, meta 10
2023-08-08 09:58:22	VIDEO_PROXY	read videosrc camera 3 - video1 : proto HTTPS, codec H.264

Interface de consultation des journaux du système

Consultez la documentation « Administration du système » pour plus de détails sur les journaux disponibles.