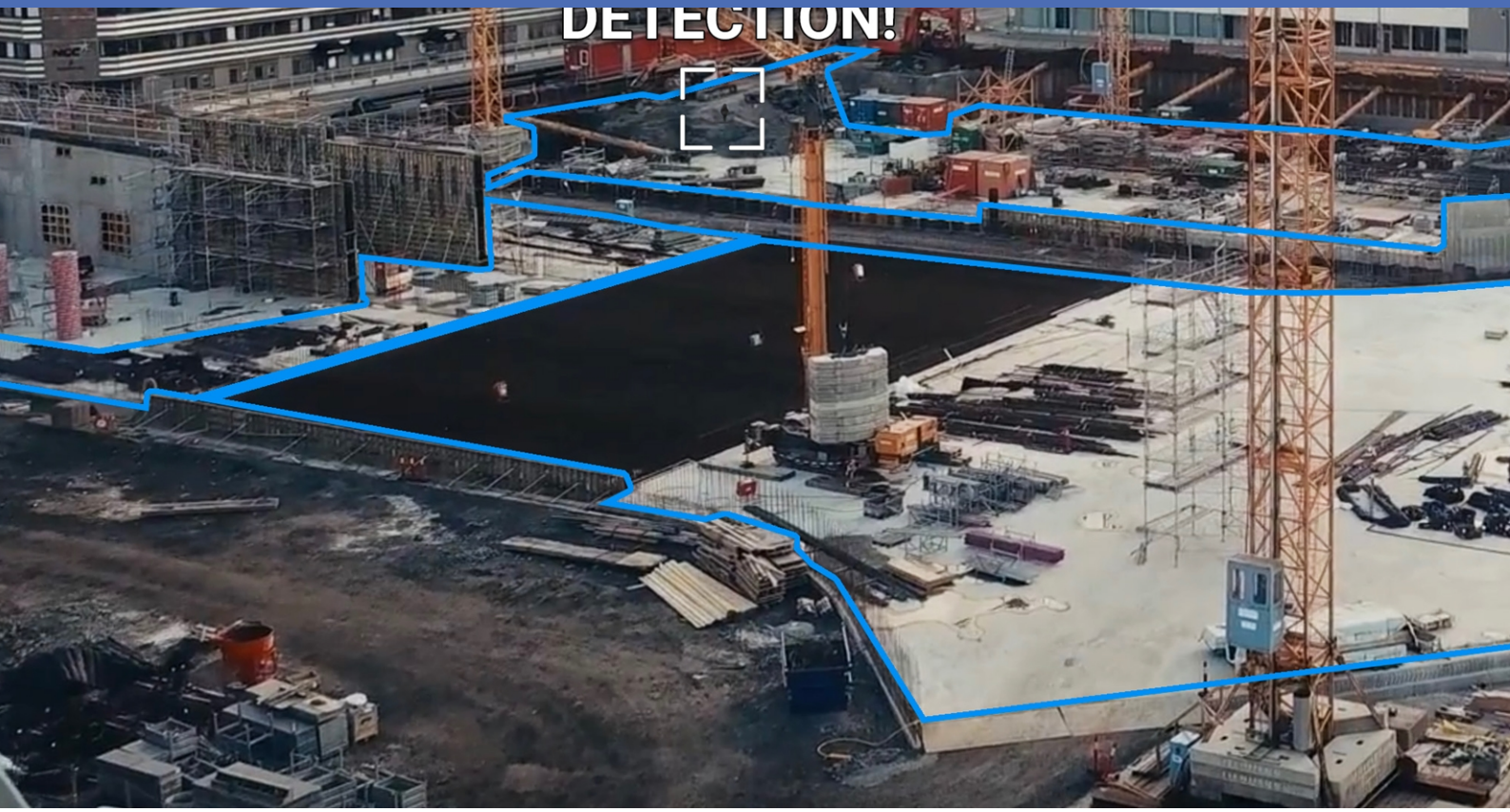
Guide

Irisity IRIS AI Analytics - Intrusion Detection



BeyondHumanVision

MOBOTIX

V1.09_16/03/2023, Code de commande : Mx-APP-IRIS-C-INT

Table des matières

Table des matières **2**

Avant de commencer **3**
Support 4
Consignes de sécurité 4
Mentions légales 5

À propos de Irisity IRIS AI Analytics - Intrusion Detection **7**
Smart Data Interface vers MxManagementCenter 7

Spécifications techniques **9**

Licences des Apps certifiées **11**
Activation des licences des applications certifiées dans MxManagementCenter 11
Gestion des licences dans MxManagementCenter 16

Exigences relatives à la caméra, à l'image et à la scène **18**
Dépannage 19

Activation de l'interface de l'App certifiée **21**

Configuration de Irisity IRIS AI Analytics - Intrusion Detection **23**
Détection d'intrusion IRIS 23
Détection des effractions IRIS 24
Zones d'alarme 25
Superpositions visuelles 27
Sauvegarde de la configuration 28

MxMessageSystem **29**
Qu'est-ce que MxMessageSystem ? 29
Informations sur les messages MxMessages 29

MxMessageSystem : traitement des événements d'application générés automatiquement **30**
Vérification des événements d'application générés automatiquement 30
Gestion des actions - Configuration d'un groupe d'actions 31
Paramètres d'action - Configuration des enregistrements de la caméra 33

MxMessageSystem : traitement des métadonnées transmises par les applications **35**
Métadonnées transférées dans le MxMessageSystem 35
Créer un événement de message personnalisé 37
Exemples de noms de message et de valeurs de filtre de Irisity IRIS AI Analytics - Intrusion Detection 39

1

Avant de commencer

Support 4
Consignes de sécurité 4
Mentions légales 5

Support

Si vous avez besoin d'une assistance technique, contactez votre concessionnaire MOBOTIX. Si votre concessionnaire ne peut pas vous aider, il contactera le canal d'assistance afin d'obtenir une réponse le plus rapidement possible.

Si vous disposez d'un accès Internet, vous pouvez ouvrir le service d'assistance MOBOTIX pour obtenir des informations supplémentaires et des mises à jour logicielles. Rendez-vous sur :

www.mobotix.com/fr > Support > Centre d'assistance

Consignes de sécurité

- Ce produit ne doit pas être utilisé dans des endroits exposés à des risques d'explosion.
- N'utilisez pas ce produit dans un environnement poussiéreux.
- Protégez ce produit de l'humidité ou de l'eau qui pourrait pénétrer dans le boîtier.
- Installez ce produit comme indiqué dans ce document. Une installation inappropriée pourrait endommager la caméra !
- Cet équipement n'est pas adapté à une utilisation dans des endroits où des enfants sont susceptibles d'être présents.
- Lorsque vous utilisez un adaptateur de classe I, le cordon d'alimentation doit être branché à une prise de courant avec mise à la terre appropriée.
- Afin de se conformer aux exigences de la norme EN 50130-4 concernant l'alimentation des systèmes d'alarme pour le fonctionnement du système 24 h/24, 7 j/7, il est fortement recommandé d'utiliser un onduleur pour protéger l'alimentation de ce produit.
- Cet équipement doit être connecté uniquement aux réseaux PoE sans être acheminé vers d'autres réseaux.

Mentions légales

Questions juridiques relatives aux enregistrements vidéo et audio

Lors de l'utilisation de produits MOBOTIX AG, vous êtes tenu de vous conformer à l'ensemble des réglementations relatives à la protection des données qui s'appliquent à la surveillance vidéo et audio. Selon la législation nationale et le site d'installation des caméras, l'enregistrement de données vidéo et audio peut être soumis à une documentation spéciale, voire être interdit. Tous les utilisateurs de produits MOBOTIX sont donc tenus de s'informer des réglementations applicables et de s'y conformer. MOBOTIX AG décline toute responsabilité en cas d'utilisation illicite de ses produits.

Déclaration de conformité

Les produits de MOBOTIX AG sont certifiés conformément aux réglementations applicables de l'UE et d'autres pays. Vous trouverez les déclarations de conformité des produits de MOBOTIX AG sur le site www.-mobotix.com, sous **Support > Download Center > Marketing & Documentation > Certificates & Declarations of Conformity (Support > Centre de téléchargement > Marketing et Documentation > Certificats et déclarations de conformité)**.

Déclaration RoHS

Les produits de MOBOTIX AG sont entièrement conformes aux restrictions de l'Union européenne relatives à l'utilisation de certaines substances dangereuses dans les équipements électriques et électroniques (directive RoHS 2011/65/CE), dans la mesure où ils sont soumis à ces réglementations (pour la déclaration RoHS de MOBOTIX, voir www.mobotix.com, **Support > Download Center > Marketing & Documentation > Brochures & Guides > Certificates (Support > Centre de téléchargement > Marketing & Documentation > Brochures & Guides > Certificats)**).

Mise au rebut

Les produits électriques et électroniques contiennent de nombreux matériaux précieux. Pour cette raison, nous vous recommandons de mettre au rebut les produits MOBOTIX en fin de vie conformément à l'ensemble des exigences et réglementations légales en vigueur (ou de déposer ces produits dans un centre de collecte municipal). Les produits MOBOTIX ne doivent pas être jetés avec les ordures ménagères ! Si le produit contient une batterie, mettez-la au rebut séparément (le cas échéant, les manuels des produits correspondants contiennent des instructions spécifiques).

Exclusion de responsabilité

MOBOTIX AG décline toute responsabilité en cas de dommages résultant d'une utilisation inappropriée ou du non-respect des manuels ou règles et réglementations applicables. Nos conditions générales s'appliquent. Vous pouvez télécharger la version actuelle des **Conditions générales** sur notre site Web à l'adresse www.-mobotix.com en cliquant sur le lien correspondant au bas de chaque page.

À propos de Irisity IRIS AI Analytics - Intrusion Detection

Détecter l'activité humaine dans les zones armées

Irisity IRIS AI Analytics - Intrusion Detection déclenche des alarmes en cas d'intrusion dans des zones interdites. L'algorithme permet de détecter précisément l'activité humaine sur de longues distances et dans des zones étendues. L'application offre une précision pouvant atteindre 99 %. L'application peut être testée gratuitement pendant 30 jours et peut être activée pour une durée illimitée. Les détections de présence humaine comprennent également des véhicules tels que des vélos, des voitures et des camions, même en cas de mauvais temps et de mauvais éclairage.

- Détecte la présence d'objets dans les zones de détection définies par l'utilisateur
- Conçu pour une détection fiable des personnes et des véhicules couvrant uniquement de petites parties du champ de vision
- Réduction maximale des fausses alarmes en filtrant les mouvements non critiques (arbres, nuages, etc.)
- Détection simultanée sur un ou plusieurs capteurs d'image
- Événements MOBOTIX via MxMessageSystem
- Recherche d'événements consolidée via l'interface Smart Data MxManagementCenter et/ou MOBOTIX HUB

ATTENTION! Cette application ne prend pas en charge les modules de capteurs thermiques ECO.

Smart Data Interface vers MxManagementCenter

Cette application dispose d'une Smart Data Interface vers MxManagementCenter.

Grâce à Smart Data System MOBOTIX, les données de transaction sont associées aux enregistrements vidéo effectués au moment de la transaction. La source Smart Data peut être des applications MOBOTIX certifiées (aucune licence requise) ou des sources Smart Data générales (licence requise) comme les systèmes POS ou les systèmes de reconnaissance de plaques d'immatriculation.

Smart Data System MxManagementCenter vous permet de trouver et d'analyser rapidement toute activité suspecte. Smart Data Bar et Smart Data View permettent de rechercher et d'analyser les transactions. La Smart Data Bar fournit un aperçu direct des transactions les plus récentes (des dernières 24 heures), ce qui la rend particulièrement pratique pour toute vérification et recherche.

AVIS! Pour plus d'informations sur l'utilisation de Smart Data System, consultez l'aide en ligne correspondant au logiciel de la caméra et MxManagementCenter.

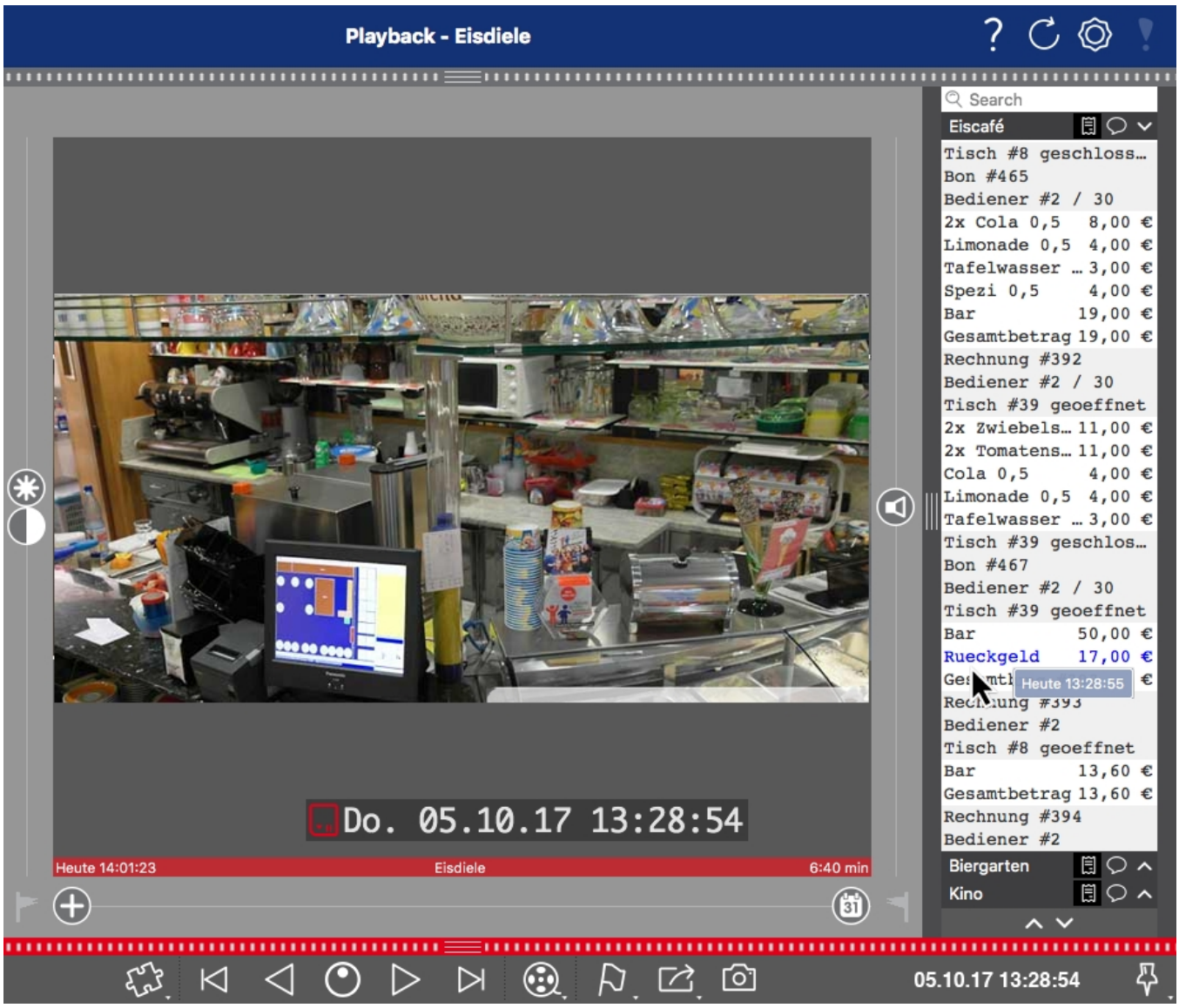


Fig. 1: : Smart Data Bar dans MxManagementCenter (exemple : Système POS)

Spécifications techniques

Informations sur le produit

Nom du produit	Irisity IRIS AI Analytics - Intrusion Detection
Code de commande	Mx-APP-IRIS-C-INT
Caméras MOBOTIX prises en charge	Mx-M73A, Mx-S74A
Micrologiciel minimum pour la caméra	V7.3.0.x
MxManagementCenter Intégration	■ min. MxMC v2.5.3 ■ Configuration : licence Advanced Config requise ■ Recherche : licence interface Smart Data incluse

Fonctionnalités du produit

Fonctionnalités de l'application	■ Détecte la présence d'objets dans les zones de détection définies par l'utilisateur ■ Conçu pour une détection fiable des personnes et des véhicules couvrant uniquement de petites parties du champ de vision ■ Réduction maximale des fausses alarmes en filtrant les mouvements non critiques (arbres, nuages, etc.) ■ Détection simultanée sur un ou plusieurs capteurs d'image ■ Événements MOBOTIX via MxMessageSystem ■ Recherche d'événements consolidée via l'interface Smart Data MxManagementCenter et/ou MOBOTIX HUB
Nombre maximal de zones de reconnaissance	20
Formats des métadonnées/statistiques	JSON
Licence d'essai	Licence d'essai de 30 jours préinstallée
MxMessageSystem pris en charge	Oui

Événements MOBOTIX	Oui
Événements ONVIF	Oui (événement de message générique)

Exigences relatives à la scène

Hauteur minimale de l'objet	20 px / ~6 % de la hauteur d'image (analyse actuellement bloquée sur une résolution de 640 x 360)
Hauteur de montage de la caméra	min. 2 m (en considérant que les exigences relatives à la scène entre 5 et 20 m sont optimales)
Angle vertical maximal	180°
Angle horizontal maximal	180°
Angle d'inclinaison maximal	Inclinaison vers le bas uniquement : pas de limite

Caractéristiques techniques de l'application

Application synchrone/ asynchrone	Asynchrone
Précision	> 99 % (en tenant compte des exigences relatives à la scène)
Nombre d'images traitées par seconde	Typ. 10 ips
Temps de détection	~2 sec

Licences des Apps certifiées

Les licences suivantes sont disponibles pour Irisity IRIS AI Analytics - Intrusion Detection :

- **Licence d'essai de 30 jours** préinstallée
- **Licence commerciale permanente**

La période d'utilisation commence par l'activation de l'interface de l'App certifiée (voir)

AVIS! Pour acheter ou renouveler une licence, contactez votre partenaire MOBOTIX.

AVIS! Les applications sont généralement préinstallées avec le micrologiciel. Dans de rares cas, les applications doivent être téléchargées depuis le site Web et installées. Dans ce cas, consultez **www.mobotix.com/fr > Support > Centre de téléchargement > Marketing & Documentation**, téléchargez et installez l'application.

Activation des licences des applications certifiées dans MxManagementCenter

Après la période d'essai, les licences commerciales doivent être activées pour être utilisées avec une clé de licence valide.

Activation en ligne

Après avoir reçu les ID d'activation, activez-les dans MxMC comme suit :

1. Sélectionnez **Window (Fenêtre) > Camera App Licenses (Licences d'applications de caméra)**.
2. Sélectionnez la caméra sur laquelle vous souhaitez utiliser la licence et cliquez sur **Select (Sélectionner)**.

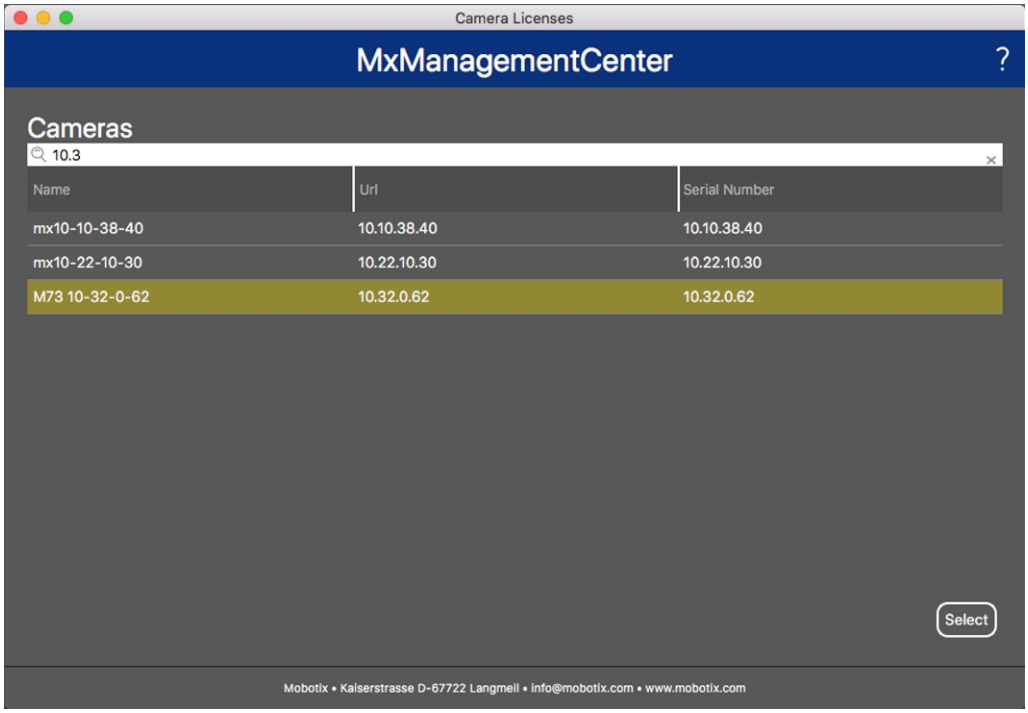


Fig. 2: Vue d'ensemble des licences d'applications de caméra dans MxManagementCenter

AVIS! Si nécessaire, modifiez l'heure définie sur la caméra.

1. Une vue d'ensemble des licences installées sur la caméra peut s'afficher. Cliquez sur **Activate License (Activer la licence)**.

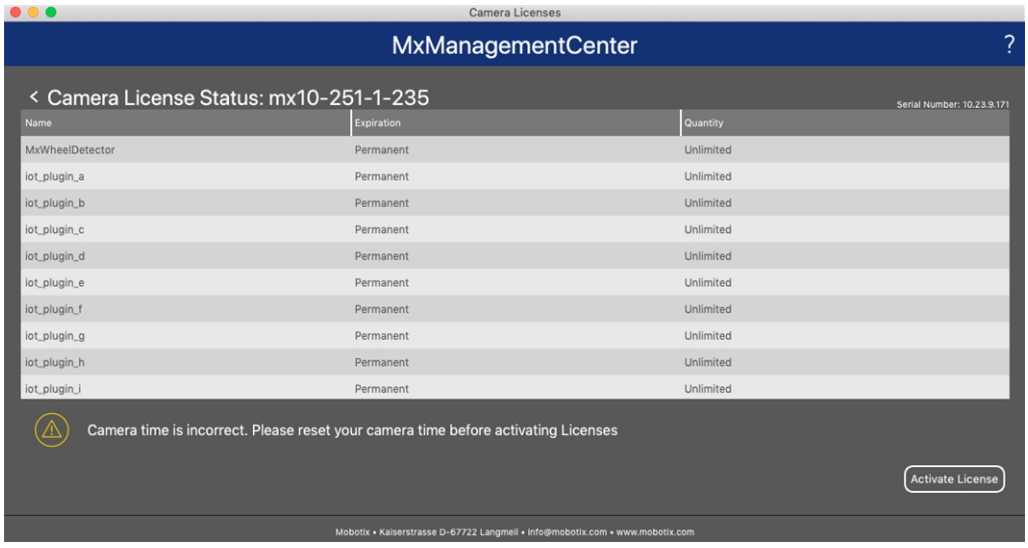


Fig. 3: Vue d'ensemble des licences installées sur la caméra

AVIS! Si nécessaire, modifiez l'heure définie sur la caméra.

2. Saisissez un ID d'activation valide et spécifiez le nombre de licences à installer sur cet ordinateur.
3. Si vous souhaitez obtenir une licence pour un autre produit, cliquez sur . Dans la nouvelle ligne, saisissez l'ID d'activation approprié et le nombre de licences souhaité.
4. Pour supprimer une ligne, cliquez sur .
5. Lorsque vous avez saisi tous les ID d'activation, cliquez sur **Activate License Online (Activer la licence en ligne)**. Lors de l'activation, **MxMC** se connecte au serveur de licences. Une connexion Internet est nécessaire.

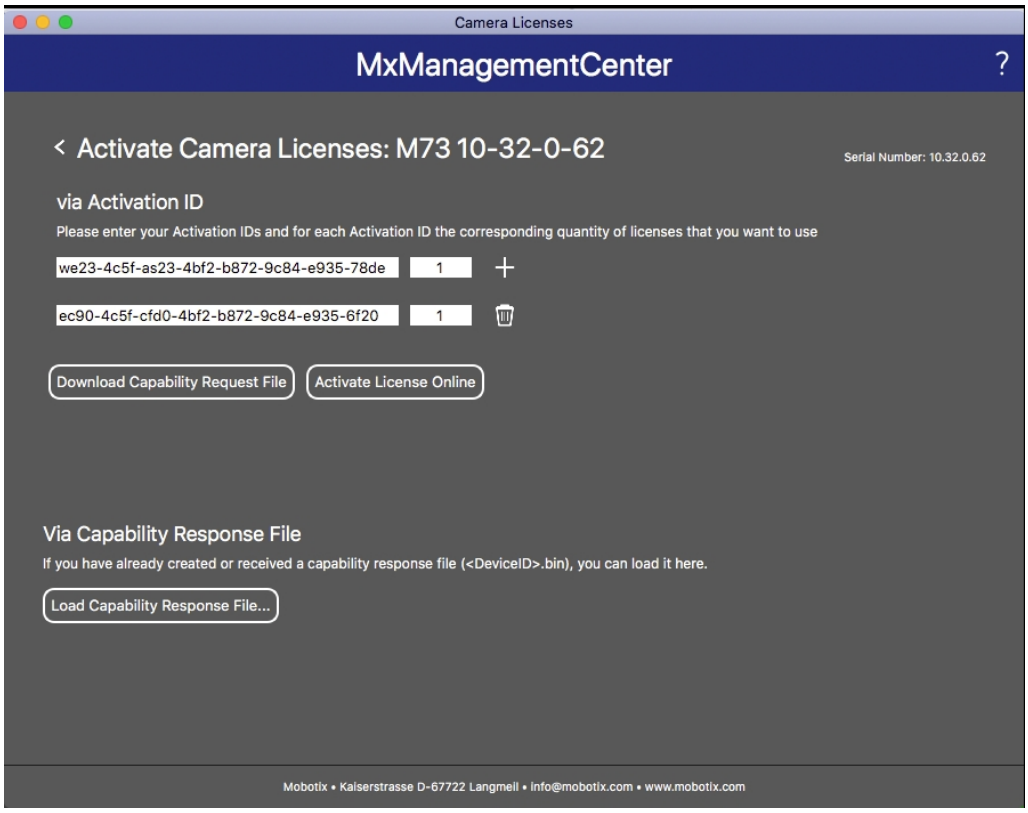


Fig. 4: Ajouter des licences

Activation réussie

Une fois l'activation effectuée, une nouvelle connexion est requise pour appliquer les modifications. Vous pouvez également revenir à la gestion des licences.

Échec de l'activation (absence de connexion Internet)

S'il est impossible de se connecter au serveur de licences, par exemple en raison d'une absence de connexion Internet, les applications peuvent également être activées hors ligne. (Voir Activation hors ligne, p. 13).

Activation hors ligne

Pour l'activation hors ligne, le partenaire ou l'installateur auprès duquel vous avez acheté les licences peut générer une réponse de capacité (fichier .bin) sur le serveur de licences pour activer ses licences.

1. Sélectionnez **Window (Fenêtre) > Camera App Licenses (Licences d'applications de caméra)**.
2. Sélectionnez la caméra sur laquelle vous souhaitez utiliser la licence et cliquez sur **Select (Sélectionner)**.

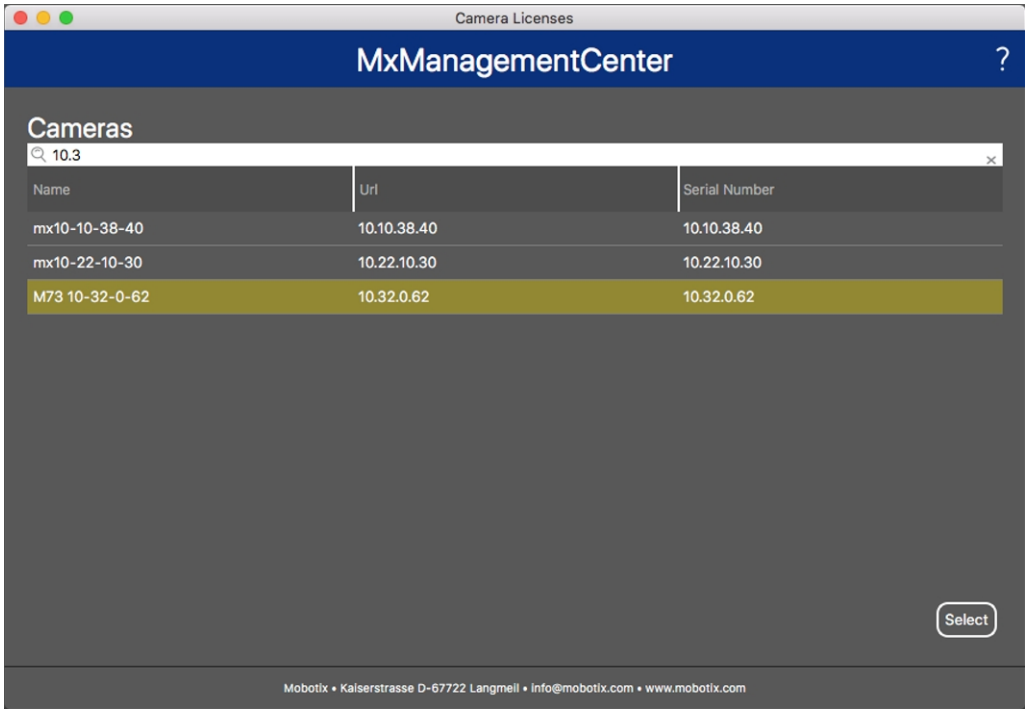


Fig. 5: Vue d'ensemble des licences d'applications de caméra dans MxManagementCenter

AVIS! Si nécessaire, modifiez l'heure définie sur la caméra.

3. Une vue d'ensemble des licences installées sur la caméra peut s'afficher. Cliquez sur **Activate License (Activer la licence)**.

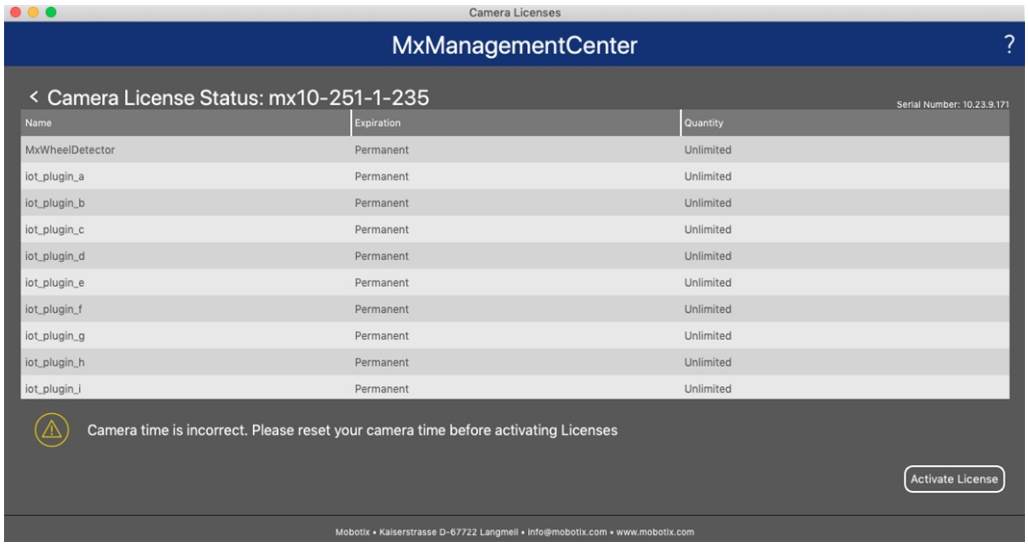


Fig. 6: Vue d'ensemble des licences installées sur la caméra

AVIS! Si nécessaire, modifiez l'heure définie sur la caméra.

4. Saisissez un ID d'activation valide et spécifiez le nombre de licences à installer sur cet ordinateur.
5. Si vous souhaitez obtenir une licence pour un autre produit, cliquez sur . Dans la nouvelle ligne, saisissez l'**ID d'activation** approprié et le nombre de licences souhaité.
6. Si nécessaire, cliquez sur pour supprimer une ligne.
7. Lorsque vous avez saisi tous les ID d'activation, cliquez sur **Download Capability Request File (.lic) (Télécharger le fichier de demande de capacité (.lic))** et envoyez le fichier à votre partenaire ou installateur.

AVIS! Ce fichier permet au partenaire/à l'installateur auprès duquel vous avez acheté les licences de générer un fichier de réponse de capacité (.bin) sur le serveur de licences.

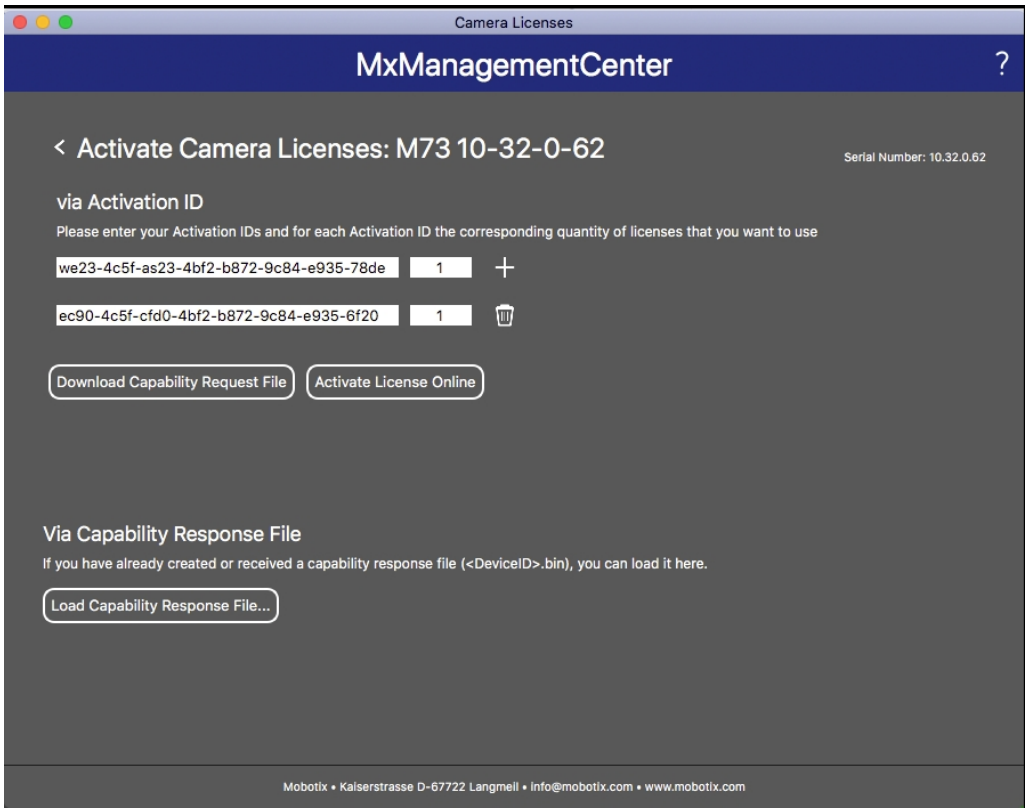


Fig. 7: Ajouter des licences

8. Cliquez sur Load Capability Response File (Charger le fichier de réponse de capacité) et suivez les instructions.

Activation réussie

Une fois l'activation effectuée, une nouvelle connexion est requise pour appliquer les modifications. Vous pouvez également revenir à la gestion des licences.

Gestion des licences dans MxManagementCenter

Dans MxManagementCenter, vous pouvez gérer facilement toutes les licences activées pour une caméra.

1. Sélectionnez **Window (Fenêtre) > Camera App Licenses (Licences d'applications de caméra)**.
2. Sélectionnez la caméra sur laquelle vous souhaitez utiliser la licence et cliquez sur **Select (Sélectionner)**.

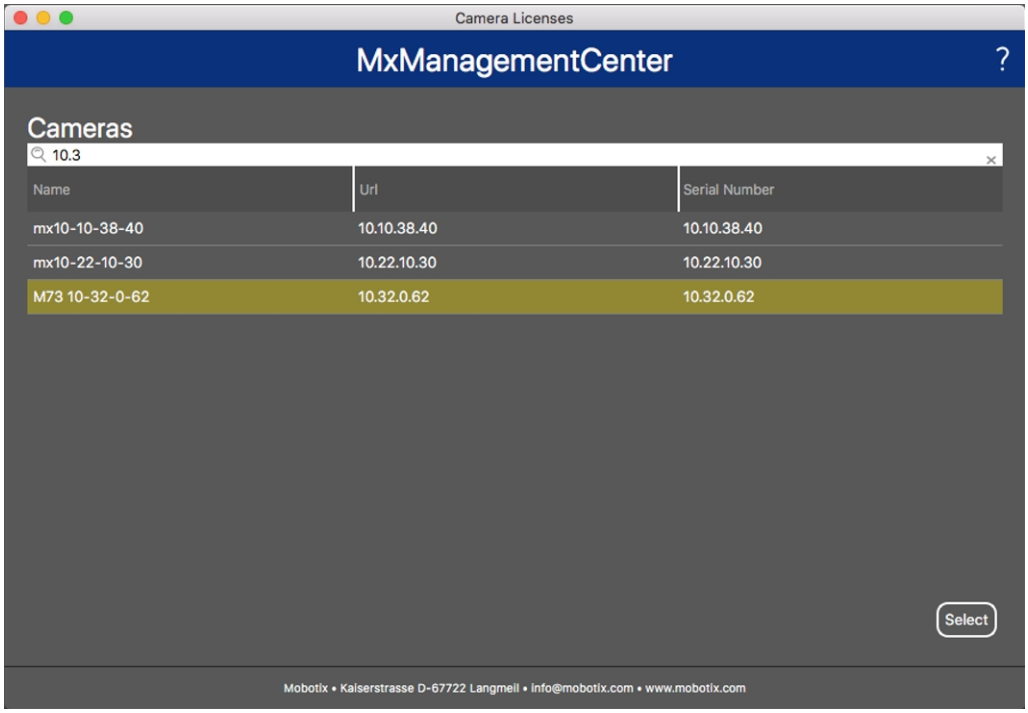


Fig. 8: Vue d'ensemble des licences d'applications de caméra dans MxManagementCenter

Une vue d'ensemble des licences installées sur la caméra peut s'afficher.

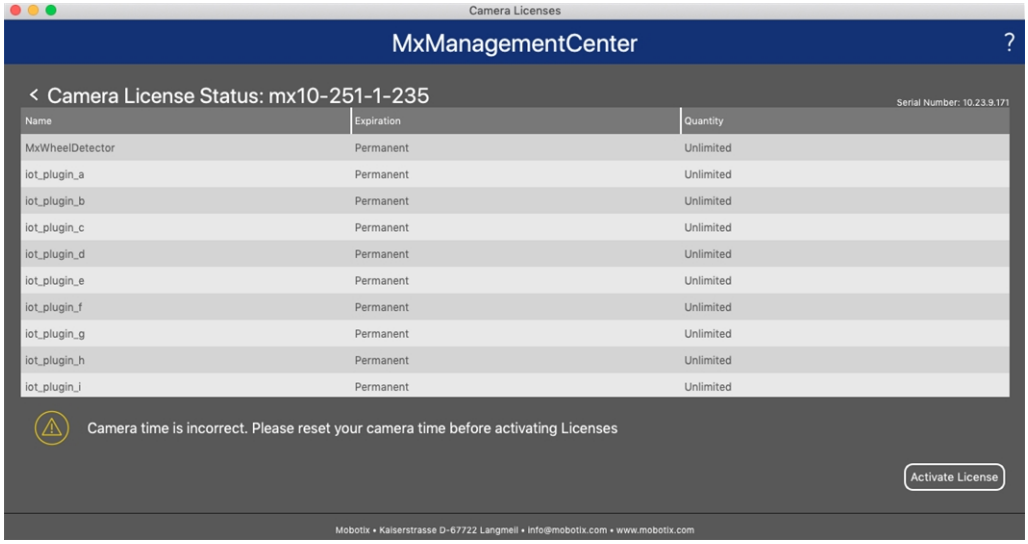


Fig. 9: Vue d'ensemble des licences installées sur la caméra

AVIS! Si nécessaire, modifiez l'heure définie sur la caméra.

Colonne	Explication
Nom	Nom de l'application sous licence
Expiration	Échéance de la licence
Quantité	Nombre de licences achetées pour un produit.
Numéro de série	Identification unique déterminée par MxMC pour l'appareil utilisé. Si des problèmes surviennent lorsque la licence est active, vous aurez besoin de l'ID de l'appareil.

Synchroniser les licences avec le serveur

Lorsque le programme démarre, il n'y a pas de comparaison automatique des licences entre l'ordinateur et le serveur de licences. Par conséquent, cliquez sur **Update (Mettre à jour)** pour recharger les licences à partir du serveur.

Mettre à jour les licences

Pour mettre à jour les licences temporaires, cliquez sur **Activate Licenses (Activer les licences)**. La boîte de dialogue de mise à jour/d'activation des licences s'ouvre.

AVIS! Vous devez disposer des droits d'administrateur pour synchroniser et mettre à jour les licences.

Exigences relatives à la caméra, à l'image et à la scène

La caméra doit être configurée de telle sorte que la combinaison de la distance, de la distance focale de l'objectif et de la résolution de la caméra fournisse une image qui peut être analysée avec précision. Par conséquent, la scène doit remplir les conditions préalables suivantes :

Positions de montage les plus élevées possibles pour des résultats optimaux

Lors de la planification de votre système de vidéosurveillance, préférez les positions de caméra les plus élevées possibles afin de couvrir autant de zones que possible avec chaque caméra. Prévoyez une hauteur d'installation d'au moins 5 mètres. Une hauteur d'installation de 10 à 25 mètres permet généralement d'obtenir de meilleurs résultats.

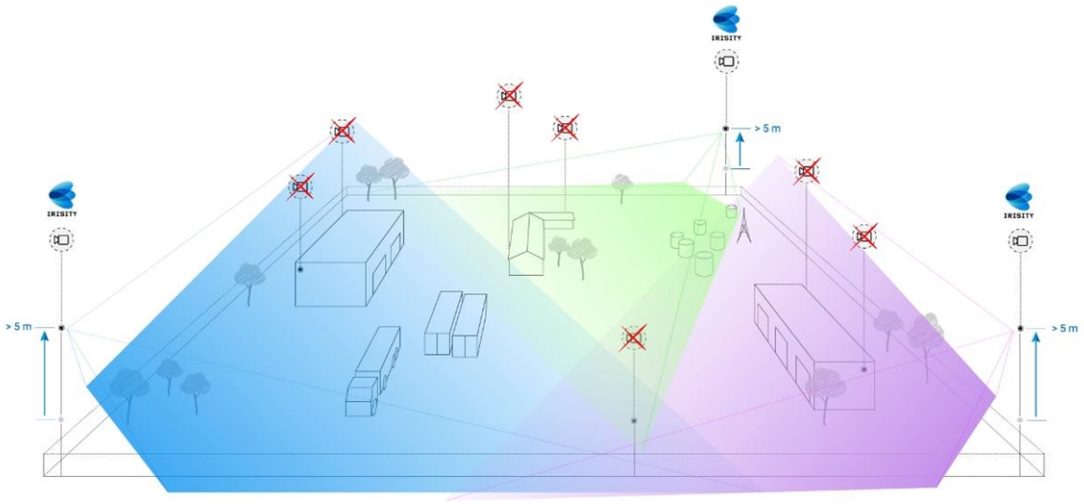


Fig. 10: L'utilisation de positions de montage élevées permet de réduire le nombre de caméras dans une installation CCTV classique.

Illumination de la scène

Des sources lumineuses optimales (nous en recommandons au moins deux) peuvent améliorer considérablement la qualité de l'analyse vidéo, et donc la sécurité de votre site.

- Éclairer suffisamment la zone surveillée.
- Assurer un bon contraste dans la zone de surveillance.
- Ne pas trop éclairer les objets à proximité des caméras afin d'éviter le mélange et le bruit.

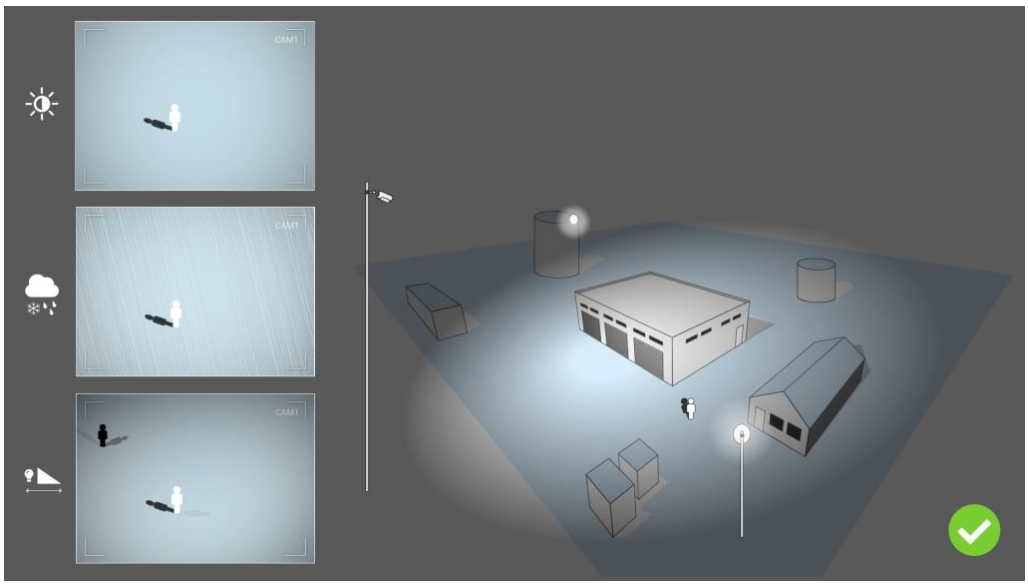


Fig. 11: L'éclairage indirect améliore considérablement la visibilité, le contraste et la détection d'objets. Il permet de réaliser des détections précises, même dans les conditions météorologiques les plus difficiles.

Dépannage

Problèmes de conception lumineuse

En plaçant la source lumineuse à proximité de la caméra et trop loin de l'objet protégé, la lumière émise peut compromettre la surveillance en créant des problèmes vidéo. Les problèmes possibles sont les suivants :

- Le contraste de l'image vidéo peut être trop faible (sans ombre)
- La source lumineuse peut créer du bruit dans l'image en accentuant l'effet gouttes de pluie et flocons de neige
- L'intensité lumineuse peut ne pas être suffisante pour éclairer l'objet protégé

Bien que l'éclairage intégré de la caméra ou tout autre éclairage axial soit souvent pratique, il réduit souvent l'efficacité du système de surveillance. Dans des conditions météorologiques difficiles, les intrus peuvent devenir presque invisibles, cachés derrière la pluie, la neige ou le brouillard

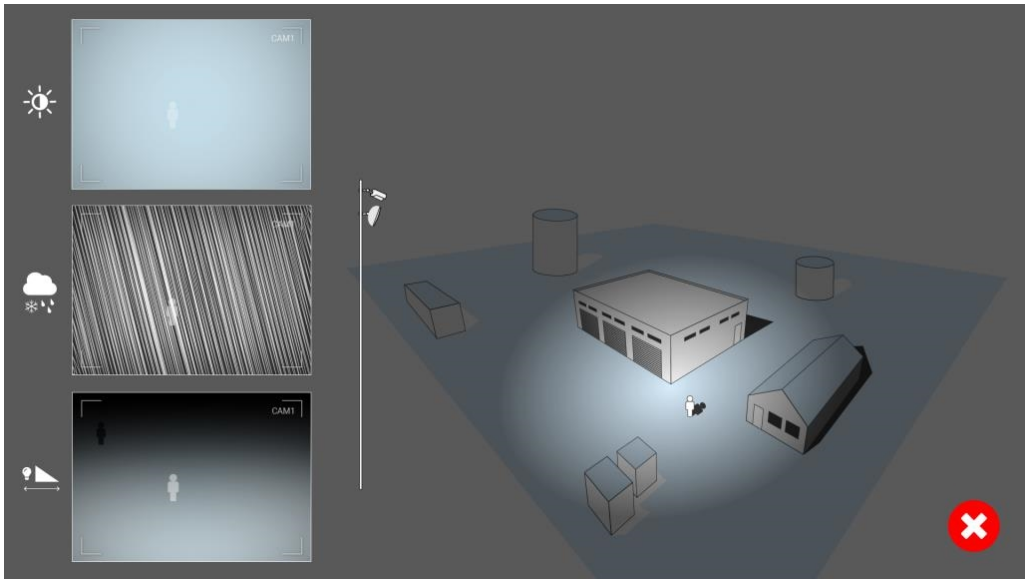


Fig. 12: Dans des conditions météorologiques difficiles, les intrus peuvent devenir presque invisibles, cachés derrière la pluie, la neige ou le brouillard

Activation de l'interface de l'App certifiée

ATTENTION! Irisity IRIS AI Analytics - Intrusion Detection ne prend pas en compte les zones sombres définies pour l'image en temps réel. Par conséquent, il n'y a pas de pixellisation dans les zones sombres lors de la configuration de l'application et pendant l'analyse d'image par l'application.

AVIS! L'utilisateur doit avoir accès au menu de configuration (http(s)://<adresse IP de la caméra>/control). Vérifiez donc les droits d'utilisateur de la caméra.

1. Dans l'interface Web de la caméra, ouvrez : **Menu Configuration / Paramètres des Apps certifiées** (http(s)://<adresse IP de la caméra>/control/app_config).

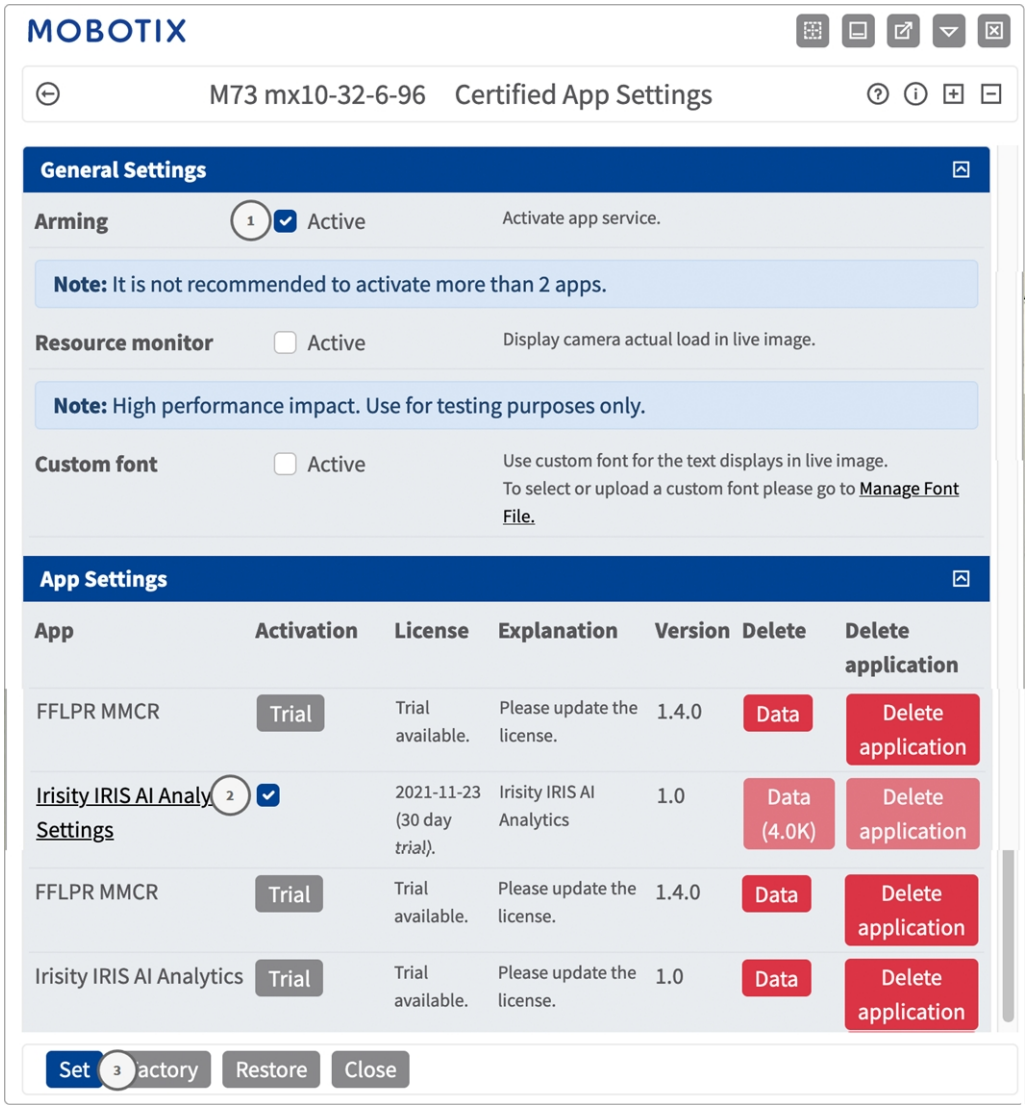


Fig. 13: App certifiée : Configuration

2. Sous **Paramètres généraux**, activez l'option **Armement** du service d'application MOBOTIX① .
3. Cliquez sur Définir ③ . Les applications installées figurent à présent dans la liste.
4. Sous **Paramètres de l'application**, cochez l'option **Actifs** de l'application concernée.
5. Cliquez sur le nom de l'application ② à configurer pour ouvrir son interface utilisateur.
6. Pour la configuration de l'application, voir Configuration de Irisity IRIS AI Analytics - Intrusion Detection, p. 23

Configuration de Irisity IRIS AI Analytics - Intrusion Detection

ATTENTION! L'utilisateur doit avoir accès au menu de configuration (http(s)://<adresse IP de la caméra>/control). Vérifiez donc les droits d'utilisateur de la caméra.

1. Dans l'interface Web de la caméra, ouvrez : **Menu Configuration / Paramètres des Apps certifiées** (http(s)://<adresse IP de la caméra>/control/app_config).
2. Cliquez sur le nom de **Irisity IRIS AI Analytics - Intrusion Detection**.

La fenêtre de configuration de l'application s'affiche avec les options suivantes :

Détection d'intrusion IRIS

Les configurations suivantes doivent être prises en compte :

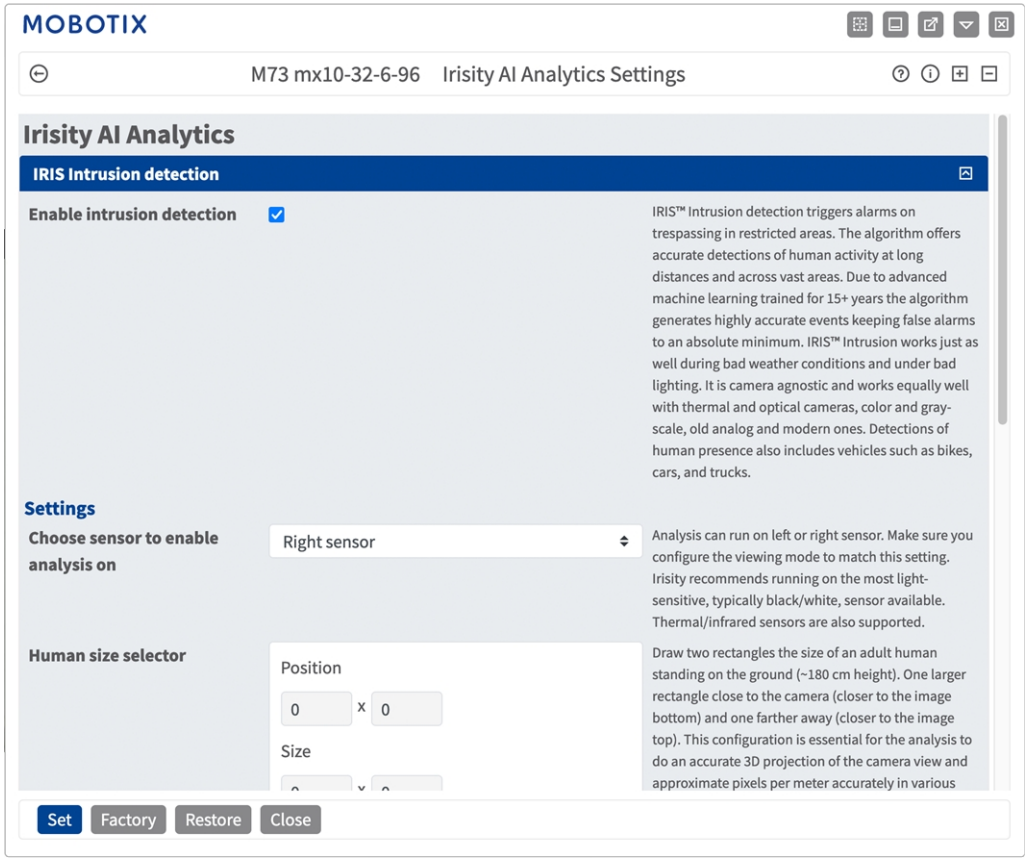


Fig. 14: Mode d'exploitation standard : Détection d'intrusion IRIS

Activer la détection d'intrusion : cochez cette case pour activer l'algorithme

Configuration

- **Choisir le capteur pour activer l'analyse :** sélectionnez le capteur à utiliser pour l'analyse d'image.
- **Sélecteur de taille humaine :** cette configuration est essentielle pour que l'analyse effectue une projection précise 3D de la vue de la caméra et donne une approximation du nombre de pixels par mètre avec précision dans différentes parties de l'image (voir Détection des effractions IRIS, p. 24).
- **Zones d'alarme :** au moins une zone d'alarme (zone de détection) doit être définie dans l'image en temps réel (voir Zones d'alarme, p. 25).
- **Détecter le type d'objet :** sélectionnez un filtre qui se déclenche uniquement en présence de personnes ou de véhicules. Les détections par défaut incluent tous les mouvements impliquant des personnes, tels que les piétons, les vélos, les voitures et les camions.

Paramètres avancés

- **Délai de récupération de zone d'alarme :** nombre de secondes pendant lesquelles une zone d'alarme est désactivée après le déclenchement d'une alarme.
- **Délai de récupération des événements d'alarme :** nombre de secondes pendant lesquelles une alarme désactive les autres détections du même objet d'alarme, y compris les objets à proximité.
- **Sensibilité :** niveau de sensibilité des objets à classer comme activité humaine. Un niveau moyen est recommandé dans la plupart des cas.

Détection des effractions IRIS

Permet de configurer les fonctions de détection des effractions.

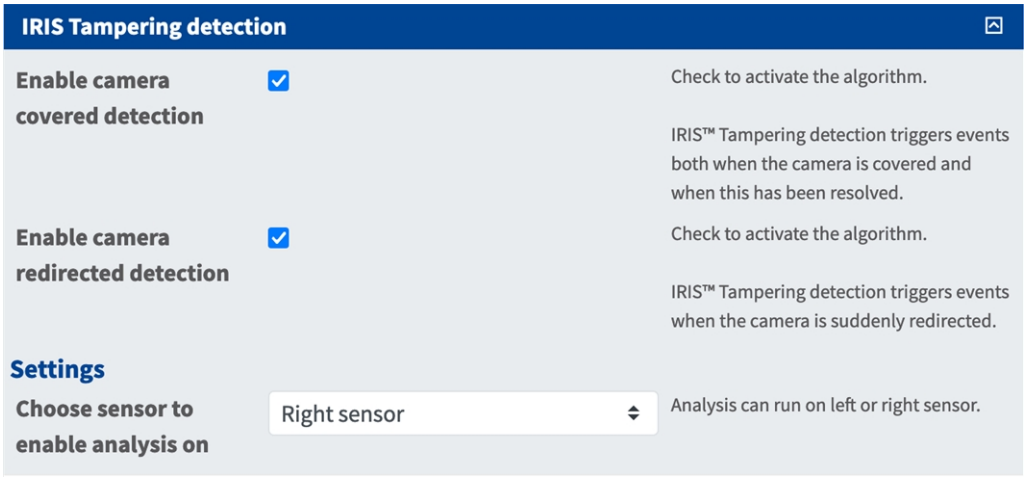


Fig. 15: Détection des effractions IRIS

Activer la détection de caméra couverte : cochez cette case pour activer l'algorithme.

AVIS! La détection des effractions IRIS™ déclenche des événements lorsque la caméra est couverte et lorsque ce problème a été résolu.

Activer la détection de redirection de caméra : activer la détection de redirection de caméra.

AVIS! La détection des effractions IRIS™ déclenche des événements lorsque la caméra est soudainement redirigée.

Choisir le capteur pour activer l'analyse : sélectionnez le capteur sur lequel l'analyse doit être réalisée.

Dessin d'un sélecteur de taille humaine

1. Dans la vue en direct, il suffit de cliquer et de faire glisser une zone de reconnaissance rectangulaire.
2. Faites glisser les points d'angle pour affiner la zone de reconnaissance.
3. Dans le coin supérieur droit de la vue en direct, cliquez sur **Submit (Soumettre)** pour appliquer les coordonnées du rectangle.

Zones d'alarme

Vous pouvez éventuellement définir une ou plusieurs zones d'alarme (zones de détection). Si elle est laissée vide, l'image entière sera utilisée pour les détections.

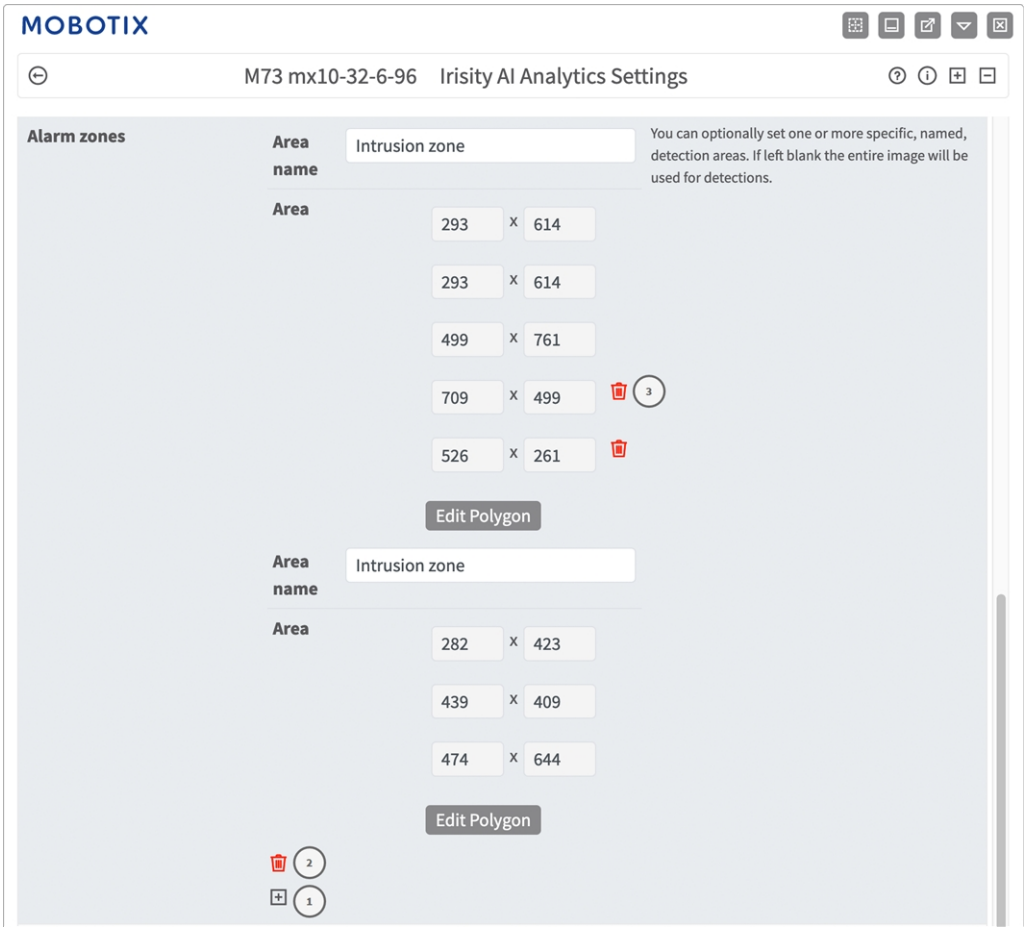


Fig. 16: Zones d'alarme

Nom de la zone Entrez un nom unique pour identifier la zone d'alarme

Zone : points d'angle définis de la zone d'alarme. Cliquez sur **Modifier le polygone** ① pour tracer la zone de détection dans la vue en direct (voir Traçage d'une zone de polygone dans la vue en direct, p. 27).

Ajouter une zone d'alarme : Cliquez sur l'icône **plus** ② pour définir une nouvelle zone d'alarme.

Supprimer une zone : Cliquez sur l'icône **Corbeille**② pour supprimer la zone de reconnaissance.

Superpositions visuelles

Vous pouvez sélectionner ici les objets et les données de la détection d'intrusion IRIS à afficher en temps réel dans l'image.

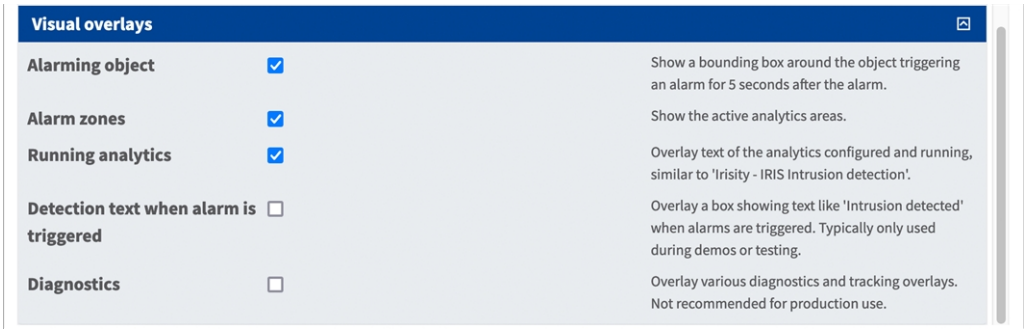


Fig. 17: Superpositions visuelles

Objet d'alarme : Cochez cette case pour afficher un cadre englobant autour de l'objet déclenchant une alarme pendant 5 secondes après l'alarme.

Zones d'alarme : Cochez cette case pour afficher les zones d'analyses actives.

Exécution des analyses : Cochez cette case pour superposer le texte des analyses configurées et en cours d'exécution, par exemple « Irisity - Détection d'intrusion IRIS ».

Texte de détection lorsque l'alarme est déclenchée : Superposez une zone contenant du texte tel que « Intrusion détectée » lorsque des alarmes sont déclenchées.

Diagnostics : Cochez cette case pour superposer différents diagnostics et superpositions de suivi (débogage, par exemple).

Traçage d'une zone de polygone dans la vue en direct

Dans la vue en direct, vous pouvez dessiner des zones basées sur des polygones en fonction de l'application. Il s'agit par exemple des zones de détection, des zones exclues, des zones de référence, etc.

1. Dans la vue en direct, il suffit de cliquer sur une zone rectangulaire et de la faire glisser.
2. Faites glisser les points d'angle vers la position souhaitée.
3. Pour ajouter un autre point d'angle, faites glisser un point plus petit entre deux points d'angle sur le contour de la zone.
4. Dans le coin supérieur droit de la vue en direct, cliquez sur **Soumettre** pour appliquer les coordonnées du polygone.
5. Vous pouvez également cliquer sur l'icône **Corbeille** pour supprimer la zone de reconnaissance.

Superpositions visuelles

Vous pouvez sélectionner ici les objets et les données de la détection d'intrusion IRIS à afficher en temps réel dans l'image.

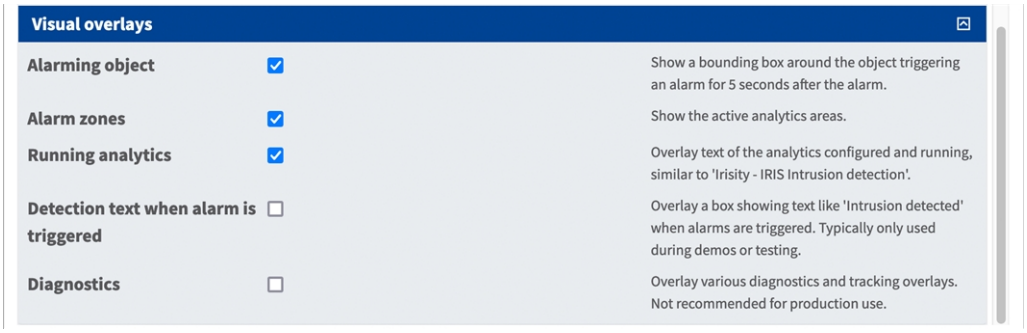


Fig. 18: Superpositions visuelles

Objet d'alarme : Cochez cette case pour afficher un cadre englobant autour de l'objet déclenchant une alarme pendant 5 secondes après l'alarme.

Zones d'alarme : Cochez cette case pour afficher les zones d'analyses actives.

Exécution des analyses : Cochez cette case pour superposer le texte des analyses configurées et en cours d'exécution, par exemple « Irisity - Détection d'intrusion IRIS ».

Texte de détection : Superposez une zone contenant du texte tel que « Intrusion détectée » lorsque des alarmes sont déclenchées.

Diagnostics : Cochez cette case pour superposer différents diagnostics et superpositions de suivi (débogage, par exemple).

Sauvegarde de la configuration

Vous disposez des options suivantes pour sauvegarder la configuration :

Fig. 19: Sauvegarde de la configuration

- Cliquez sur le bouton **Définir** pour activer les paramètres et les sauvegarder jusqu'au prochain démarrage de la caméra.
- Cliquez sur le bouton **Config. usine** pour charger les paramètres par défaut de cette boîte de dialogue (ce bouton peut ne pas apparaître dans toutes les boîtes de dialogue).
- Cliquez sur le bouton **Restaurer** pour annuler les modifications les plus récentes qui n'ont pas été sauvegardées de façon permanente dans la caméra.
- Cliquez sur le bouton **Fermer** pour fermer la boîte de dialogue. Lorsque la boîte de dialogue se ferme, le système vérifie si des modifications ont été apportées à l'ensemble de la configuration. Si des modifications sont détectées, un message vous demande si vous souhaitez sauvegarder l'ensemble de la configuration de manière permanente.

Une fois la configuration sauvegardée, l'événement et les métadonnées sont automatiquement envoyés à la caméra en cas d'événement.

MxMessageSystem

Qu'est-ce que MxMessageSystem ?

MxMessageSystem est un système de communication basé sur des messages orientés nom. Cela signifie que les messages doivent avoir des noms uniques d'une longueur maximale de 32 octets.

Chaque participant peut envoyer et recevoir des messages. Les caméras MOBOTIX peuvent également transférer des messages au sein du réseau local. Ainsi, les messages MxMessages peuvent être distribués sur l'ensemble du réseau local (voir Zone de messages : Globale).

Par exemple, une caméra de la série 7 MOBOTIX peut échanger un message MxMessage généré par une application de caméra avec une caméra Mx6 qui ne prend pas en charge les applications certifiées MOBOTIX.

Informations sur les messages MxMessages

- Le chiffrement de 128 bits garantit la confidentialité et la sécurité du contenu des messages.
- Les messages MxMessages peuvent être distribués à partir de n'importe quelle caméra des séries Mx6 et 7.
- La plage du message peut être définie de manière individuelle pour chaque message MxMessage.
  - **Locale :** la caméra attend un message MxMessage au sein de son propre système de caméra (par exemple, via une App certifiée).
  - **Globale :** la caméra attend un message MxMessage distribué sur le réseau local par un autre appareil MxMessage (par exemple, une autre caméra de la série 7 équipée d'une App certifiée MOBOTIX).
- Les actions que les destinataires doivent effectuer sont configurées individuellement pour chaque participant du MxMessageSystem.

MxMessageSystem : traitement des événements d'application générés automatiquement

Vérification des événements d'application générés automatiquement

AVIS! Une fois l'application activée (voir Activation de l'interface de l'App certifiée, p. 21), un événement de message générique est automatiquement généré dans la caméra pour cette application spécifique.

1. Accédez à **Menu Configuration/Paramètres événements/Vue d'ensemble des événements**. Dans la section **Événements de message**, le profil d'événement de message généré automatiquement porte le nom de l'application (par exemple : IRIS).

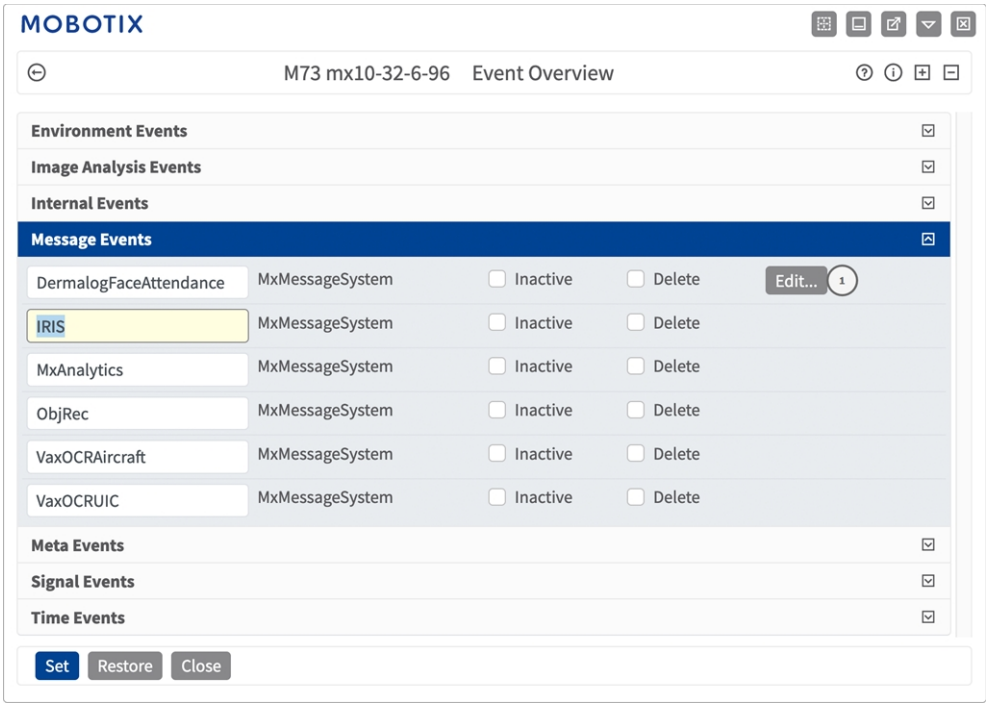


Fig. 20: Exemple : Événement de message générique de Irisity IRIS AI Analytics - Intrusion Detection

2. Cliquez sur **Modifier**① pour afficher une sélection de tous les événements de message configurés.

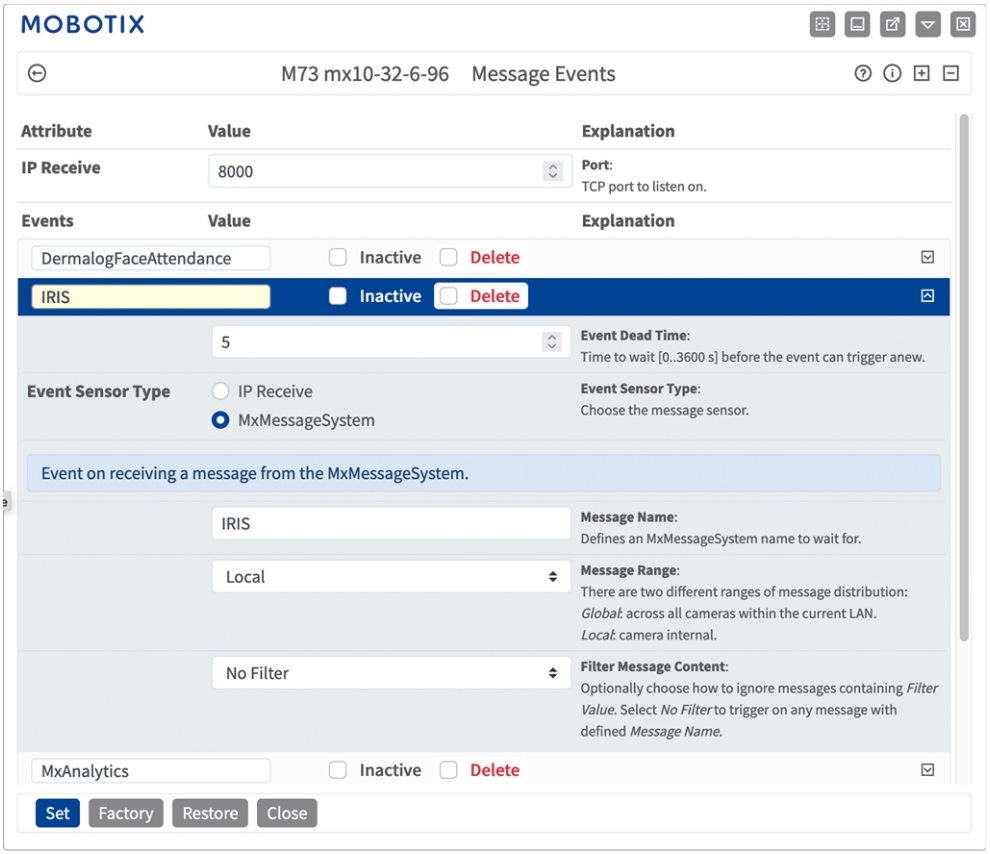


Fig. 21: Exemple : Détails d'événement de message générique - aucun filtre

Gestion des actions - Configuration d'un groupe d'actions

ATTENTION! Pour utiliser des événements, déclencher des groupes d'actions ou enregistrer des images, l'armement général de la caméra doit être activé (http(s)/<adresse IP de la caméra>/control/settings).

Les groupes d'actions définissent les actions qui sont déclenchées par les événements Irisity IRIS AI Analytics - Intrusion Detection.

1. Dans l'interface Web de la caméra, ouvrez : **Menu Configuration / Vue d'ensemble des groupes d'action** (http(s)://<adresse IP de la caméra>/control/app_config).

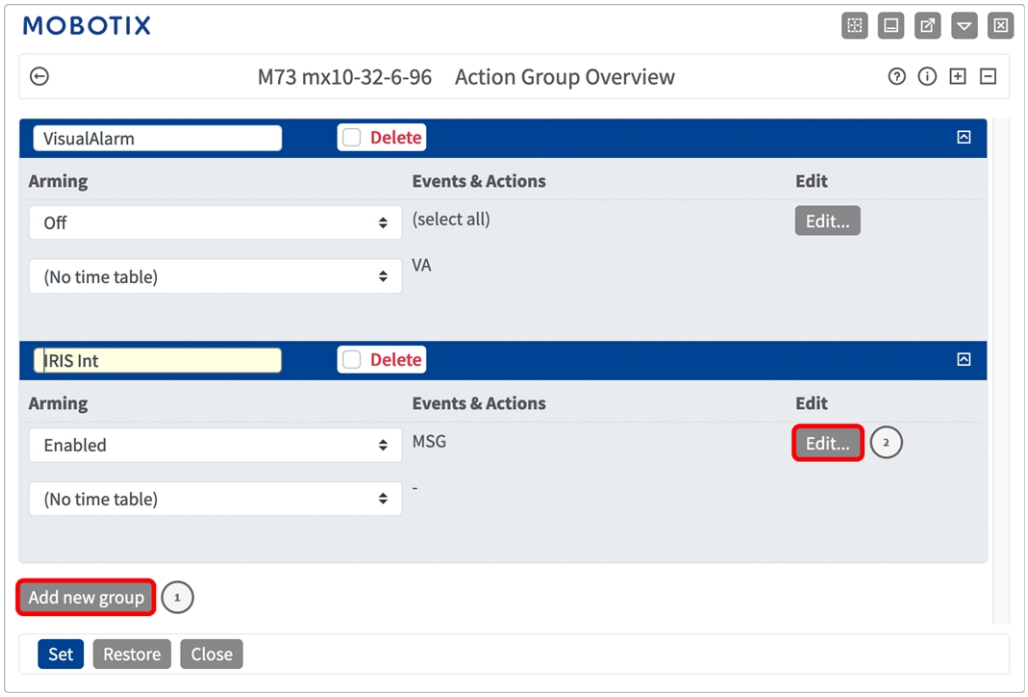


Fig. 22: Définir des groupes d'actions

2. Cliquez sur **Ajouter un nouveau groupe**① et donnez au groupe un nom pertinent.
3. Cliquez sur **Modifier**② pour configurer le groupe.

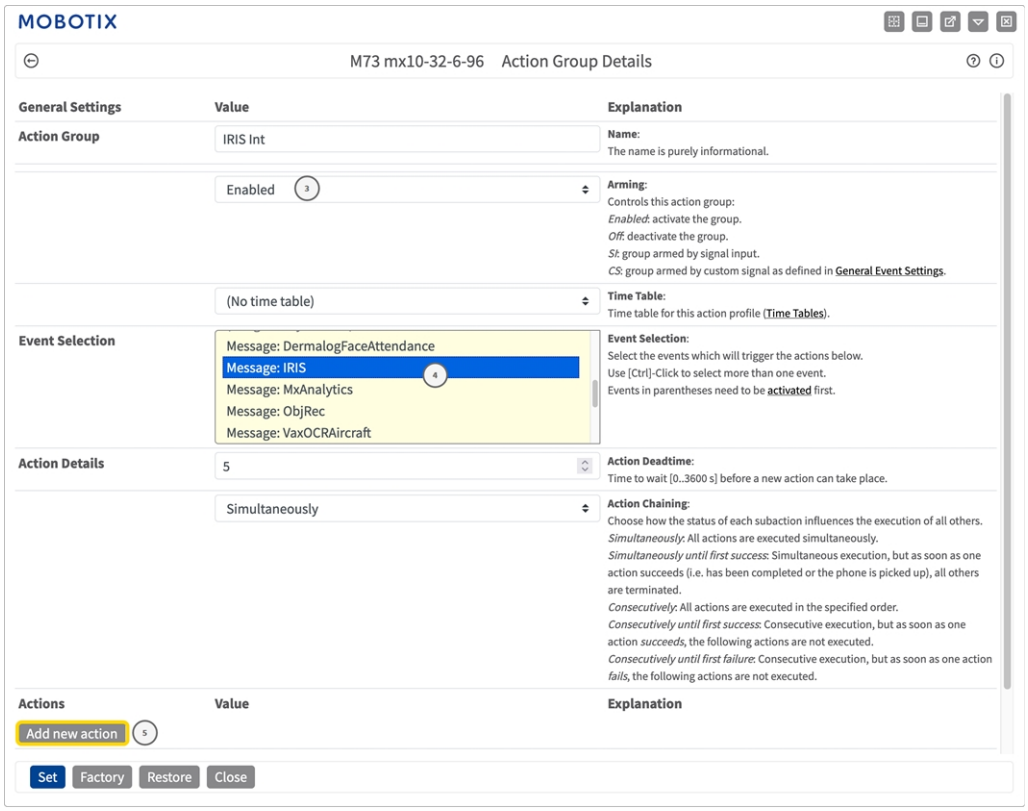


Fig. 23: Configurer un groupe d'actions

4. Activez l'option **Armement**③ pour le groupe d'actions.
5. Sélectionnez votre événement de message dans la liste **Sélection des événements**④ . Pour sélectionner plusieurs événements, maintenez la touche Maj enfoncée.
6. Cliquez sur **Ajouter une nouvelle action**⑤ .
7. Sélectionnez une action appropriée dans la liste **Type et profil d'action**⑥ .

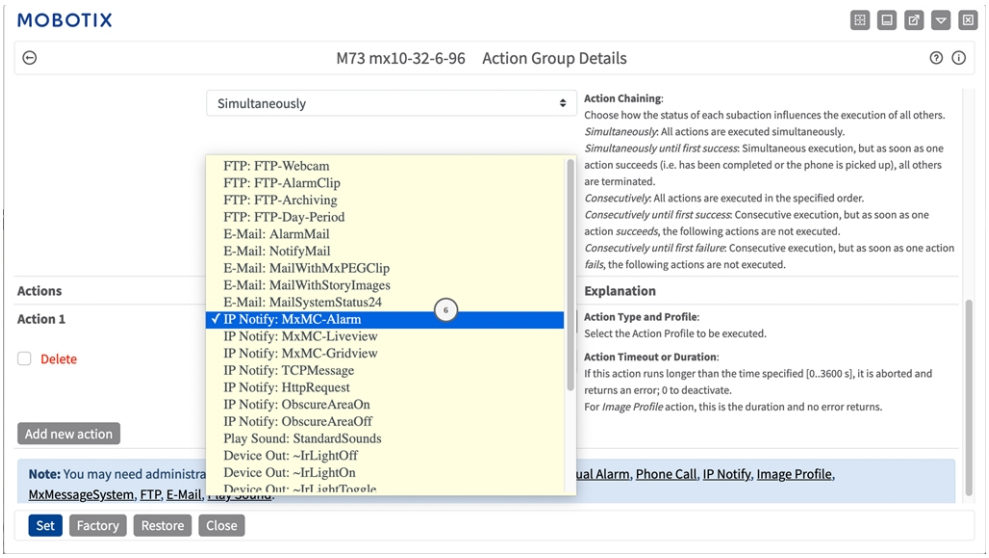


Fig. 24: Sélectionner le type et profil d'action.

AVIS! Si le profil d'action requis n'est pas encore disponible, vous pouvez créer un nouveau profil dans les sections « MxMessageSystem », « Profils de transfert » et « Audio et téléphone » du menu Admin.

Si nécessaire, vous pouvez ajouter d'autres actions en cliquant à nouveau sur le bouton. Dans ce cas, assurez-vous que l'« enchaînement des actions » est correctement configuré (par exemple, en même temps).

8. Cliquez sur le bouton **Set (Définir)** à la fin de la boîte de dialogue pour confirmer les paramètres.

Paramètres d'action - Configuration des enregistrements de la caméra

1. Dans l'interface Web de la caméra, ouvrez : **Menu Configuration / Paramètres événements / Recording (Enregistrement)** (http(s)/<adresse IP caméra>/control/recording).

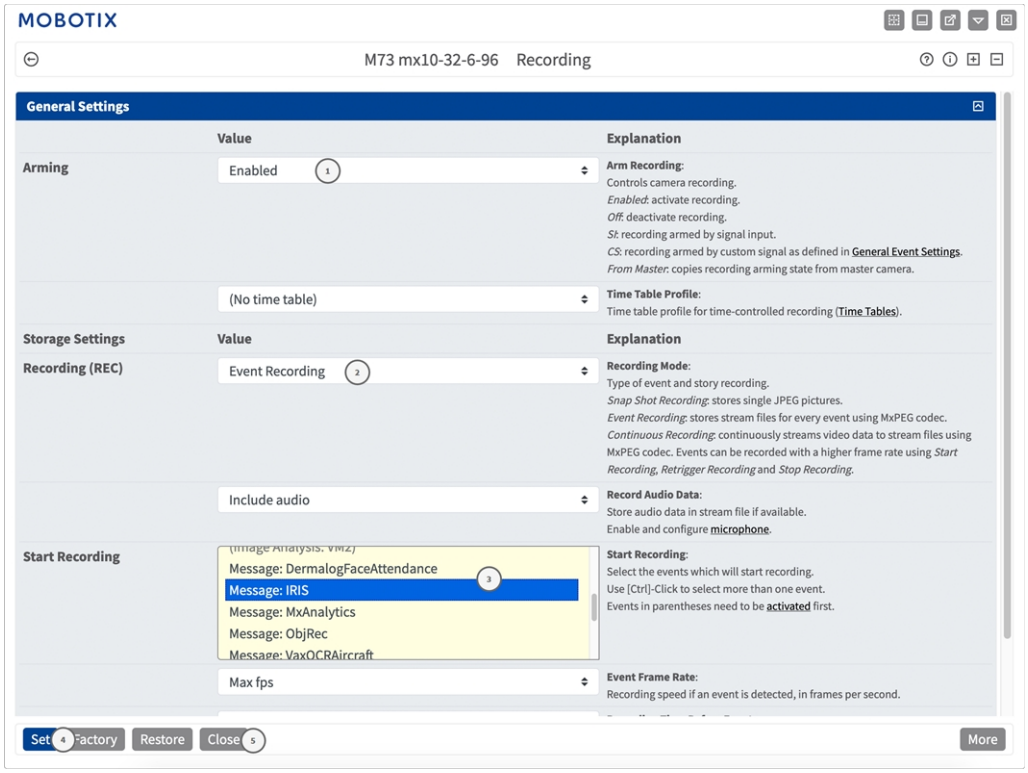


Fig. 25: Configuration des paramètres d'enregistrement de la caméra

2. Activez l'option **Activer l'enregistrement** ① .
3. Sous **Configuration d'enregistrement** / **Enregistrement (REC)**, sélectionnez un **Mode d'enregistrement** ② . Les modes suivants sont disponibles :
   - Enregistrement d'images uniques
   - Enregistrement d'événement
   - Enregistrement continu
4. Dans la liste **Lancer l'enregistrement** ③ , sélectionnez l'événement de message qui vient d'être créé.
5. Cliquez sur le bouton **Définir** ④ à la fin de la boîte de dialogue pour confirmer les paramètres.
6. Cliquez sur **Fermer** ⑤ pour enregistrer vos paramètres de manière permanente.

AVIS! Vous pouvez également enregistrer vos paramètres dans le menu Admin sous Configuration / Save current configuration to permanent memory (Enregistrer la configuration actuelle dans la mémoire permanente).

MxMessageSystem : traitement des métadonnées transmises par les applications

Métadonnées transférées dans le MxMessageSystem

Pour chaque événement, l'application transfère également des métadonnées vers la caméra. Ces données sont envoyées sous la forme d'un schéma JSON au sein d'un message MxMessage.

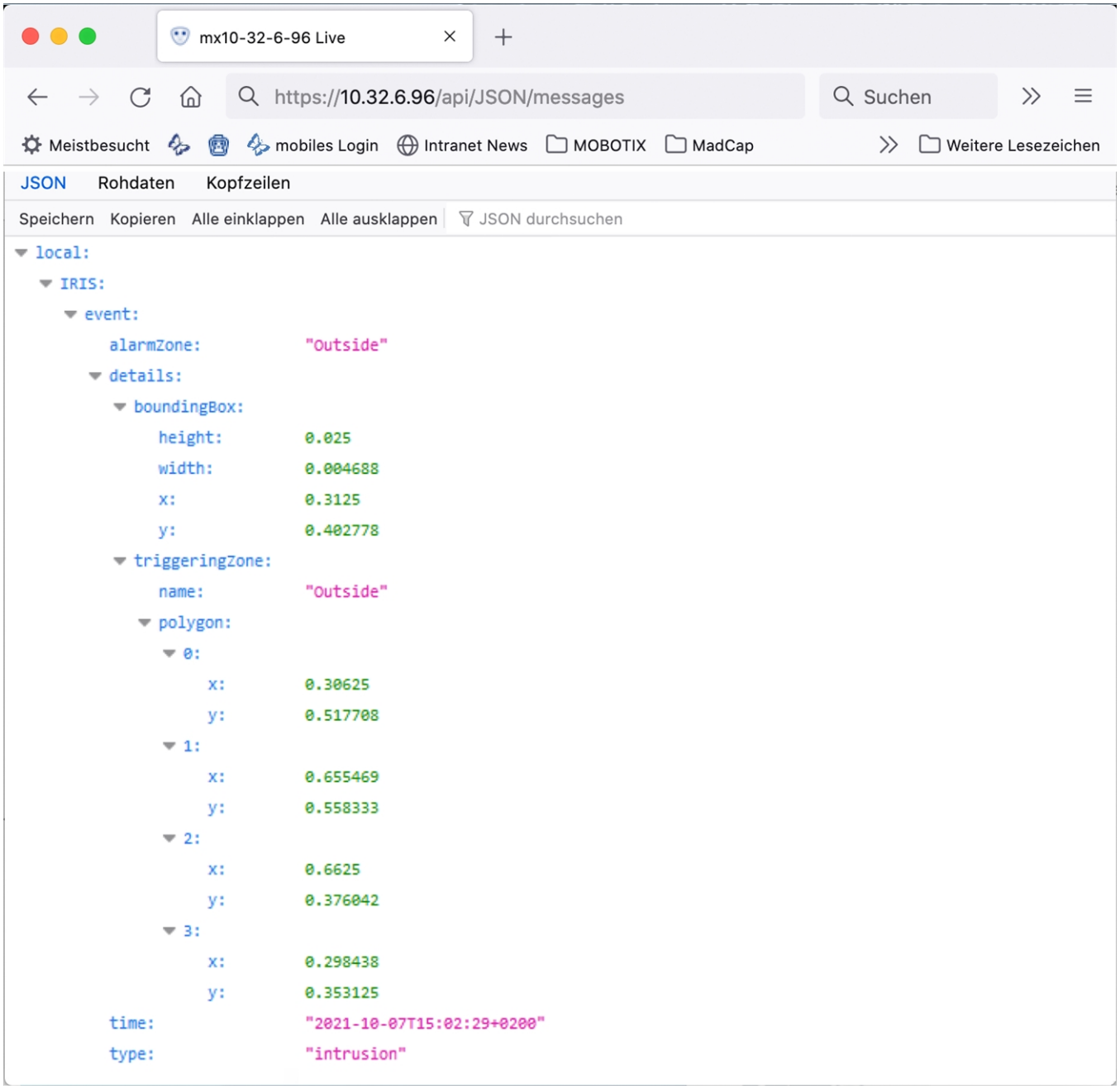


Fig. 26: Exemple : Métadonnées transmises dans un message MxMessage de Irisity IRIS AI Analytics - Intrusion Detection

AVIS! Pour afficher la structure des métadonnées du dernier événement de l'application, saisissez l'URL suivante dans la barre d'adresse de votre navigateur : http(s)/adresseIPdevotrecaméra/api/json/messages

Créer un événement de message personnalisé

1. Accédez à **Menu Configuration/Paramètres événements/Vue d'ensemble des événements**. Dans la section **Événements de message**, le profil d'événement de message généré automatiquement porte le nom de l'application (par exemple : IRIS).

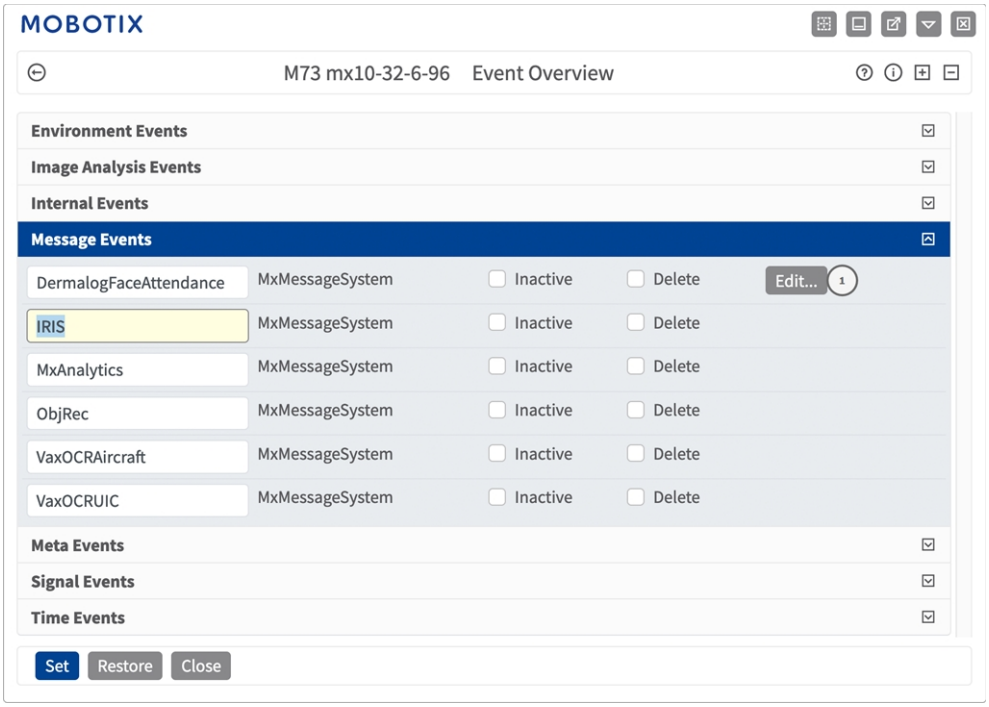


Fig. 27: Exemple : Événement de message générique de Irisity IRIS AI Analytics - Intrusion Detection

2. Cliquez sur **Modifier**① pour afficher une sélection de tous les événements de message configurés.

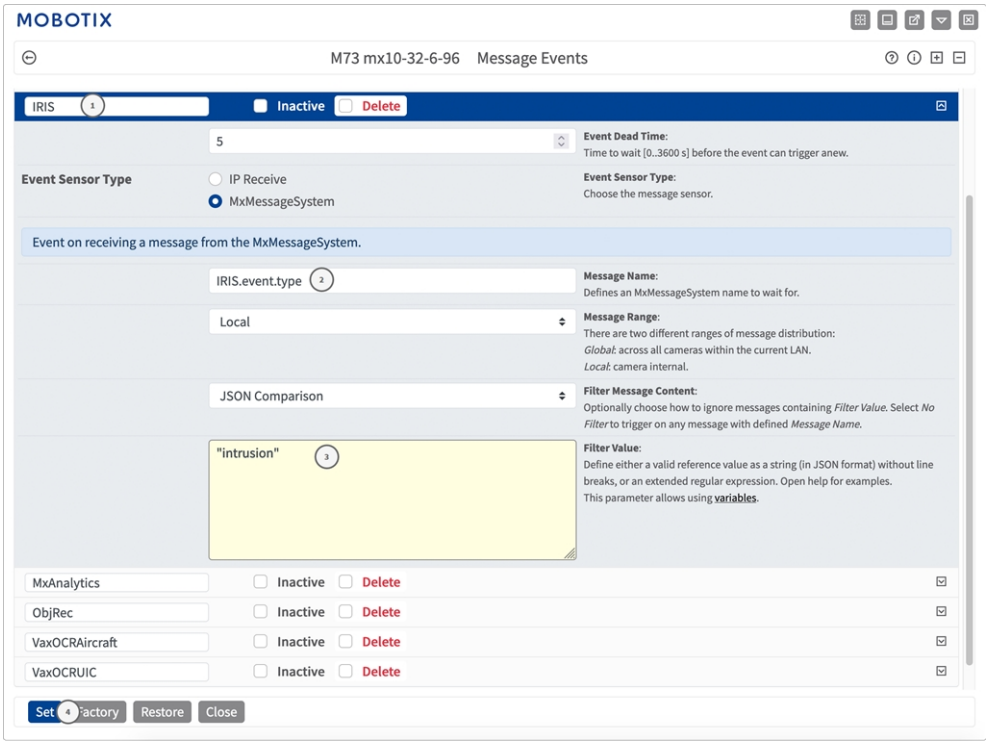


Fig. 28: Exemple : Événement de message d'intrusion

3. Cliquez sur l'événement (p. ex., IRIS) ① pour ouvrir les paramètres de l'événement.
4. Configurez les paramètres du profil d'événement comme suit :

   - **Nom du message :** saisissez le « nom du message » ② en tenant compte de la documentation des événements de l'application correspondante (voir Exemples de noms de message et de valeurs de filtre de Irisity IRIS AI Analytics - Intrusion Detection, p. 39)
   - **Plage de message :**
     - **Locale :** paramètres par défaut de Irisity IRIS AI Analytics - Intrusion Detection
     - **Globale :** le message MxMessage est transféré depuis une autre caméra MOBOTIX du réseau local.
   - **Filtre du contenu de message :**
     - **Événement Generic (Générique) :** « No Filter »
     - **Événement Filtered (Filtré) :** « Comparaison JSON »
   - **Filter Value (Valeur de filtre) :** ③ voir Exemples de noms de message et de valeurs de filtre de Irisity IRIS AI Analytics - Intrusion Detection, p. 39.

ATTENTION! La valeur du filtre sert à différencier les messages MxMessages d'une application/d'un package d'applications (bundle). Utilisez cette entrée pour bénéficier des différents types d'événements des applications (le cas échéant).

Choisissez « No Filter » si vous voulez utiliser tous les messages MxMessages entrants comme événements génériques de l'application associée.

2. Cliquez sur le bouton **Définir**④ à la fin de la boîte de dialogue pour confirmer les paramètres.

Exemples de noms de message et de valeurs de filtre de Irisity IRIS AI Analytics - Intrusion Detection

Détection d'intrusion IRIS	Nom MxMessage	Valeur de filtre
Événement Generic	IRIS	
Événement de zone d'alarme	IRIS.event.alarmZone	Nom de la zone d'alarme, par exemple : « Zone d'intrusion 2 »
Type d'événement	IRIS.event.type	« intrusion »

MOBOTIX

BeyondHumanVision

FR_03/23
MOBOTIX AG • Kaiserstrasse D-67722 Langmeil • Tél. : +49 6302 9816-103 • sales@mobotix.com • www.mobotix.com