PERCEPT

Caméra d'Intervention IONODES PERCEPT / Milestone XProtect®

Guide de déploiement

Date: 19 juillet, 2023

CONTENU

1 Introduction

L'une des caractéristiques uniques de la caméra d'intervention PERCEPT est qu'il s'agit d'un appareil à plate-forme ouverte, permettant une intégration avec des solutions VMS de pointe telles que Milestone XProtect®. Il implémente les fonctionnalités étendues des profils ONVIF G, S et T, ainsi que des configurations réseau flexibles (LAN, Wi-Fi, 4G/LTE) pour la vidéo en direct et la récupération des enregistrements sauvegardés sur mémoire interne.

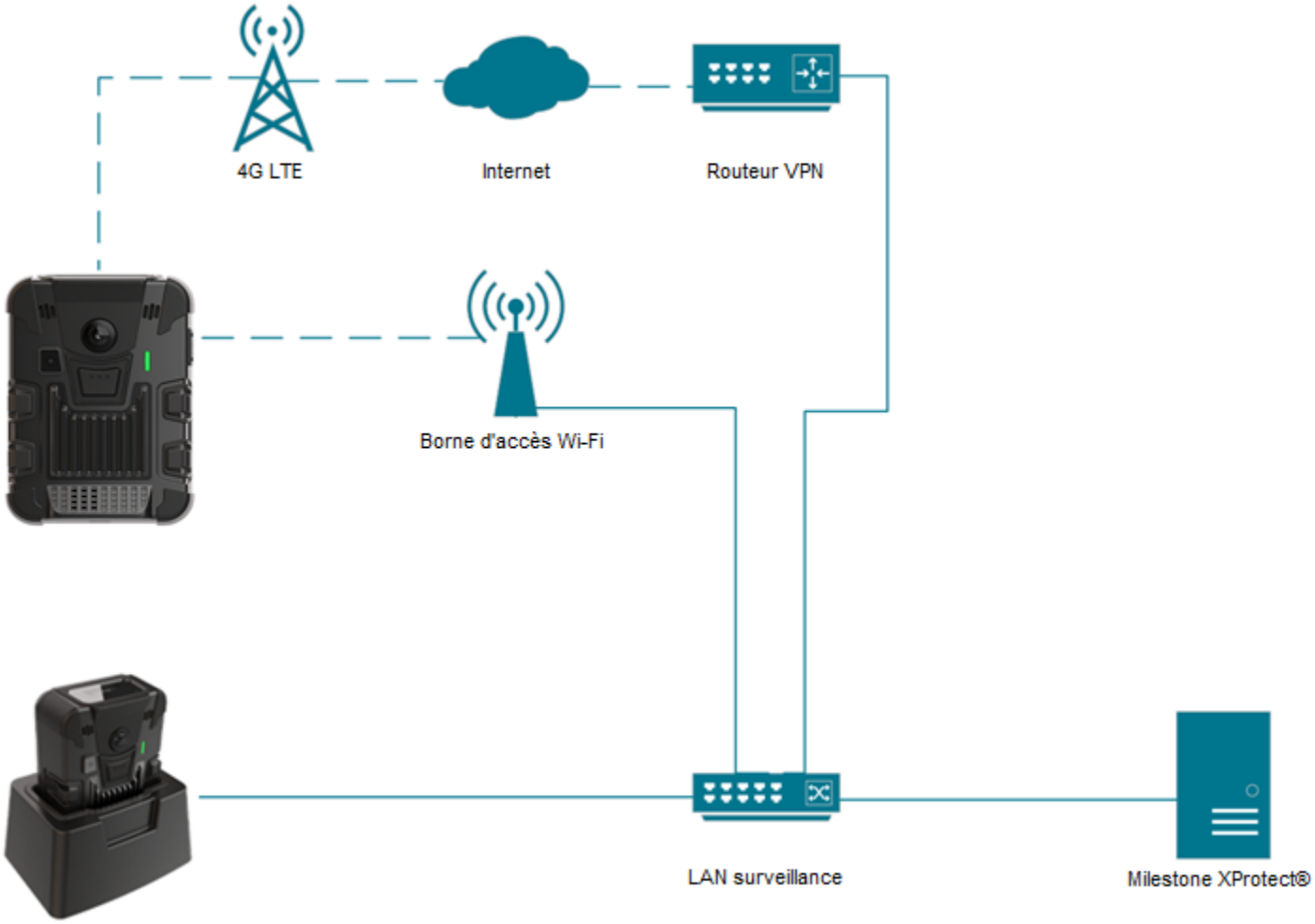
Cette intégration est prise en charge à partir du microgiciel 10.7.2.5 de la caméra d'intervention PERCEPT et a été validée avec XProtect® Expert 2022R3. Il nécessite l'édition Professional+ ou supérieure de XProtect®. Les éditions Essential+ et Express+ ne prennent pas en charge le transfert de vidéo de la mémoire interne. Ce document décrit le déploiement recommandé tel que validé par IONODES et Milestone et un exemple de scénario est présenté pour illustrer les différentes étapes de déploiement. Les intégrateurs système et les utilisateurs finaux doivent l'adapter à leurs besoins spécifiques et à leur environnement système.

2 Déploiement recommandé

2.1 Disposition des composants

Un scénario de déploiement typique, illustré dans le diagramme ci-dessous, comprend les éléments suivants:

- Caméra d'intervention PERCEPT,
- Station d'accueil PERCEPT,
- Borne d'accès Wi-Fi,
- Serveur de réseau privé virtuel (VPN),
- Infrastructure de réseau local (LAN), et
- Logiciel de gestion vidéo locale (VMS), Milestone XProtect®



La caméra d'intervention PERCEPT peut techniquement enregistrer directement sur XProtect® via la diffusion 4G LTE ou Wi-Fi, mais cela n'est pas recommandé en raison des contraintes de bande passante. La configuration recommandée consiste à configurer deux (2) profils de flux vidéo ; un flux en direct à faible débit, activé sur demande via 4G LTE et Wi-Fi, et un flux d'enregistrement à haut débit enregistré sur la mémoire interne de la caméra, puis transféré vers le serveur d'enregistrement XProtect® via l'Ethernet câblé de la station d'accueil.

Note: Bien que le schéma ci-dessus montre le point d'accès Wi-Fi et la station d'accueil connectés à l'infrastructure LAN, ceux-ci peuvent également se connecter à Internet. Dans une telle configuration, ils accèdent à l'infrastructure LAN via le VPN, permettant le transfert de vidéos à partir d'un emplacement distant avec accès Internet.

2.2 Fonctionnalités disponibles

Le tableau ci-dessous récapitule les fonctionnalités disponibles avec le déploiement détaillé dans ce guide.

Fonctionnalité	Remarque
Audio et vidéo en direct à faible débit déclenchés depuis XProtect® Smart Client et XProtect® Web Client	Diffusion en direct sur demande pour minimiser l'utilisation des données Wi-Fi/LTE
Communication audio bidirectionnelle avec XProtect® Smart Client et XProtect® Web Client	
Enregistrement audio et vidéo à haut débit sur mémoire interne de l'appareil (carte microSD)	
Transfert automatique de l'audio et de la vidéo de la mémoire locale vers le serveur d'enregistrement XProtect®	Avec des règles qui déclenchent une tâche de transfert récurrente
Événements et alarmes configurables déclenchés par le porteur. Visible en temps réel dans XProtect® Smart Client et XProtect® Web Client	
Synchronisation Date / Heure	Avec serveur NTP commun à XProtect® et PERCEPT
Mises à jour du micrologiciel depuis XProtect® Management Client	
Commutation automatique entre la Station d'accueil PERCEPT (LAN), le Wi-Fi et le LTE	Avec serveur/routeur VPN
Cryptage de bout en bout	Avec serveur/routeur VPN

3 Configuration de la Caméra d'intervention PERCEPT

Commencez par initialiser la connectivité réseau de la caméra d'intervention PERCEPT avec XProtect® via Wi-Fi. Reportez-vous au Guide de démarrage rapide PERCEPT pour les instructions d'initialisation du réseau.

Note: Les instructions de ce guide supposent que l'état initial de la caméra d'intervention PERCEPT est réglé sur les paramètres d'usine par défaut. Si la caméra d'intervention a déjà été utilisée, il est fortement conseillé de la réinitialiser avant de l'intégrer à XProtect®.

3.1 Déploiement de plusieurs Caméras d'intervention PERCEPT

La caméra d'intervention PERCEPT a plusieurs paramètres de configuration. Pour éviter le risque d'erreur humaine lors du déploiement de plusieurs caméras, il est recommandé de commencer par configurer et valider une seule caméra.

Une fois la configuration entièrement validée, l'utilitaire IONConfigTool (lien IONConfigTool - IONODES) permet d'exporter sa configuration puis de l'importer vers d'autres caméras. Tous les paramètres de configuration sont exportés/importés, à l'exception des utilisateurs et des informations d'identification, des paramètres réseau et de la clé de chiffrement des fichiers locaux. Ceux-ci doivent manuellement être saisis à nouveau après l'importation.

3.2 Configurer le réseau local

Pour s'intégrer à XProtect®, la caméra d'intervention PERCEPT et l'infrastructure LAN doivent être configurées pour que chaque caméra obtienne toujours la même adresse IP sur toutes les interfaces réseau ; Wi-Fi, station d'accueil et VPN. Si le Wi-Fi et la station d'accueil se connectent toujours au réseau local vidéo, il peut être approprié de définir des adresses IP statiques pour ces interfaces.

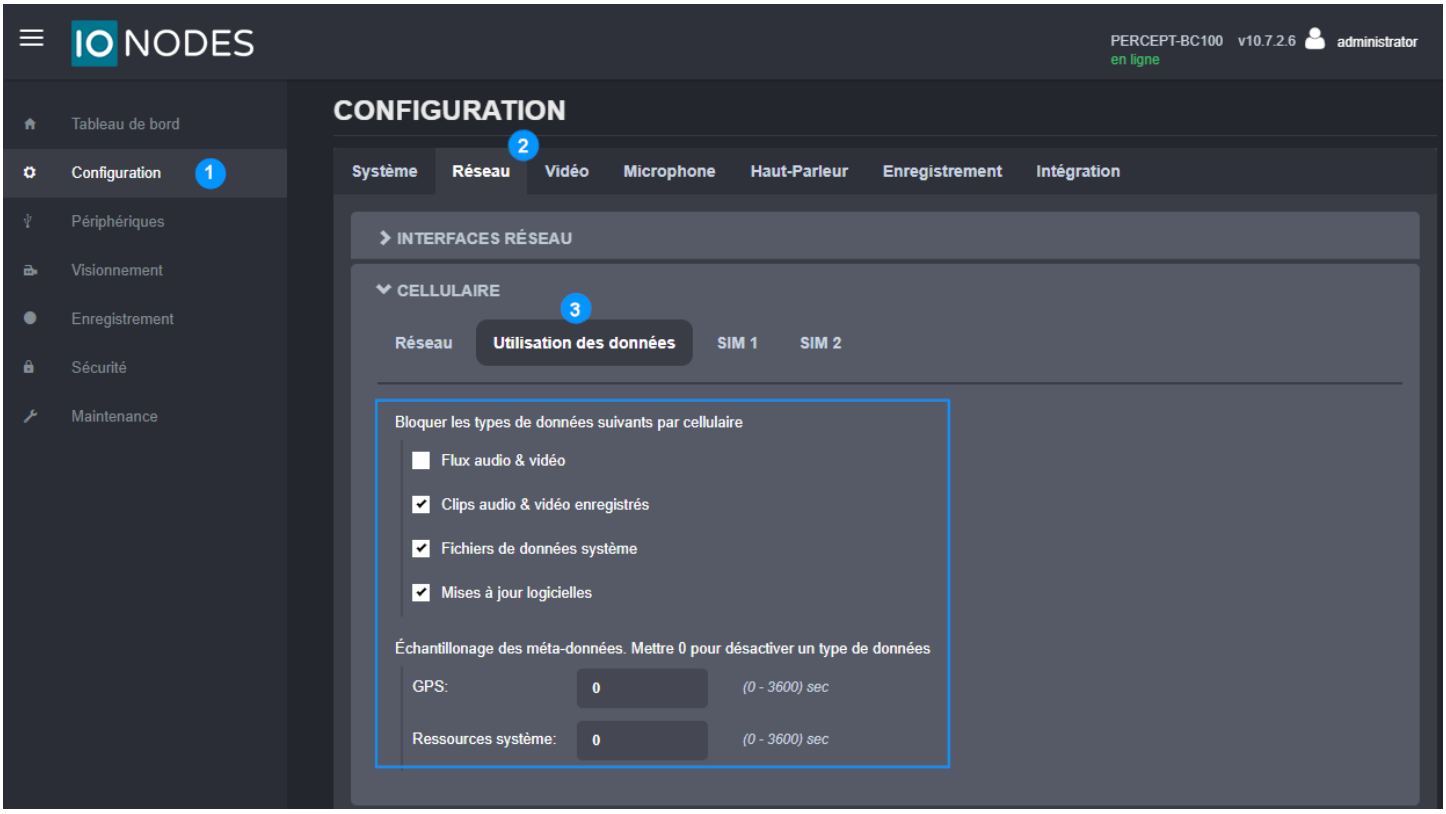
Cependant, les adresses IP statiques peuvent empêcher la connexion à d'autres réseaux pour accéder au LAN vidéo via l'internet et le VPN. Pour cette raison, il est recommandé de conserver les interfaces réseau de la caméra en mode DHCP et de configurer le routeur VPN et/ou le serveur DHCP du LAN vidéo pour distribuer des adresses IP réservées à chaque caméra. Ceci est détaillé dans la section **Error! Reference source not found.** ci-dessous.

3.2.1 Configurer le réseau cellulaire

Toutes les caméras d'intervention PERCEPT incluent une carte SIM qui peut être activée à tout moment. Contactez-nous pour activer un forfait de données.

3.2.2 Configurer l'utilisation des données cellulaires

Pour mieux contrôler l'utilisation des données, la caméra d'intervention PERCEPT peut être configurée pour bloquer différents types de données sur les liaisons cellulaires.



1. À partir de la page **Configuration**
2. Sélectionnez l'onglet **Réseau**
3. Développez la section **CELLULAIRE** et configurez les paramètres dans l'onglet **Utilisation des données**
    a. Décochez **Flux audio & vidéo** pour autoriser la diffusion en direct sur cellulaire
    b. Cochez **Clips audio & vidéo enregistrés** pour bloquer leur transfert sur cellulaire

c. Cochez **Fichiers de données système** pour bloquer le téléchargement du journal de dépannage sur le réseau cellulaire
d. Cochez **Mises à jour logicielles** pour bloquer le téléchargement du micrologiciel sur le réseau cellulaire
e. Définissez le taux d'échantillonnage à **0** pour le **GPS** et les **Ressources système** afin de bloquer la diffusion de métadonnées sur le réseau cellulaire.

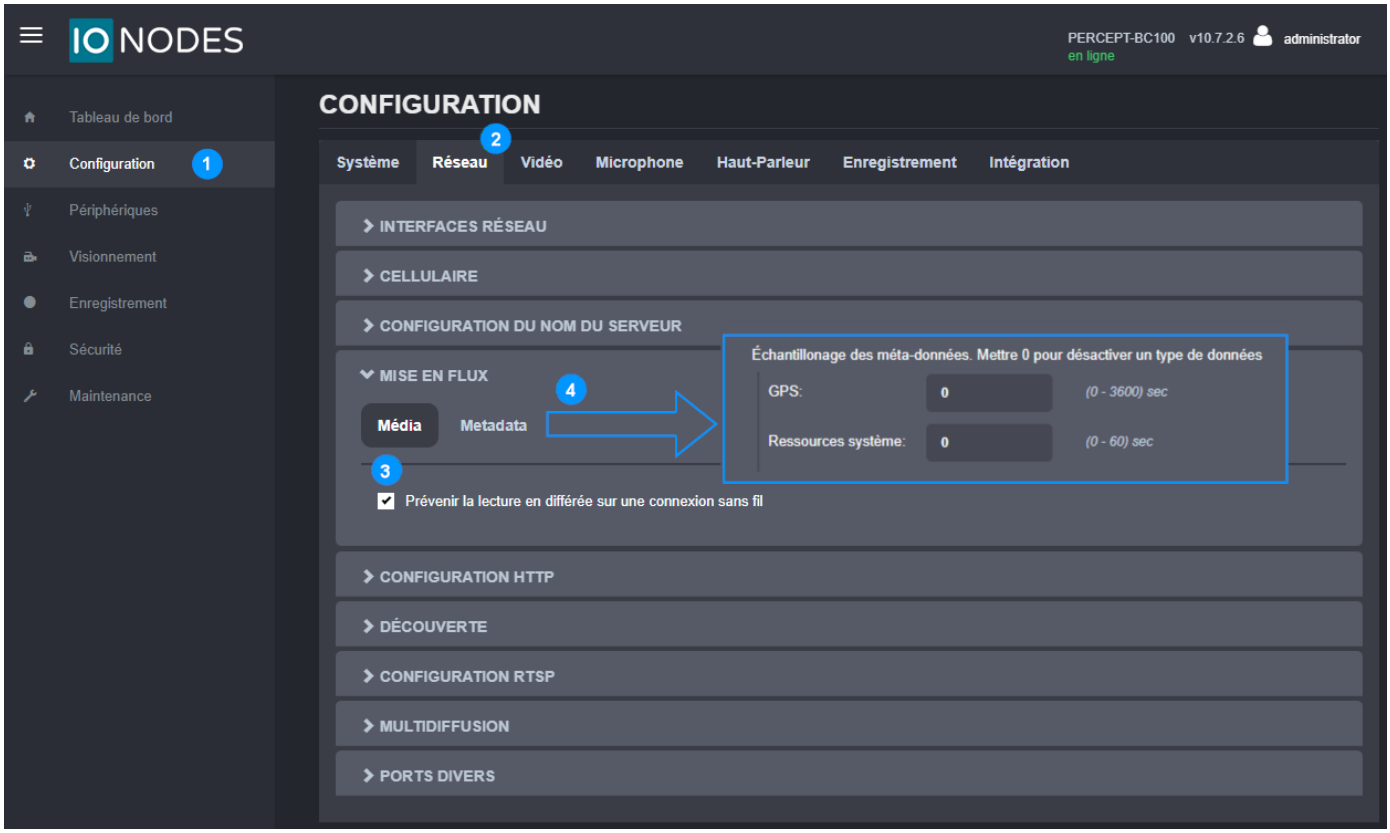
Note: Les paramètres ci-dessus sont destinés à maintenir les données cellulaires au strict minimum pour obtenir les fonctionnalités de ce scénario de déploiement. D'autres types de données peuvent être autorisés en fonction du cas d'utilisation individuel.

Note: Il est recommandé de désactiver les métadonnées car l'intégration de la caméra d'intervention PERCEPT avec Milestone XProtect® ne les utilise pas actuellement. Des révisions futures sont prévues pour inclure des cas d'utilisation des métadonnées.

3.2.3 Configurer l'utilisation des données Wi-Fi

Les caméras d'intervention PERCEPT peuvent être configurées pour bloquer le flux de métadonnées et le transfert d'enregistrements multimédia via Wi-Fi. Ce transfert peut consommer toute la bande passante disponible d'un réseau Wi-Fi, par exemple lorsque plusieurs utilisateurs de caméras reviennent à un emplacement central à la fin d'un quart de travail.

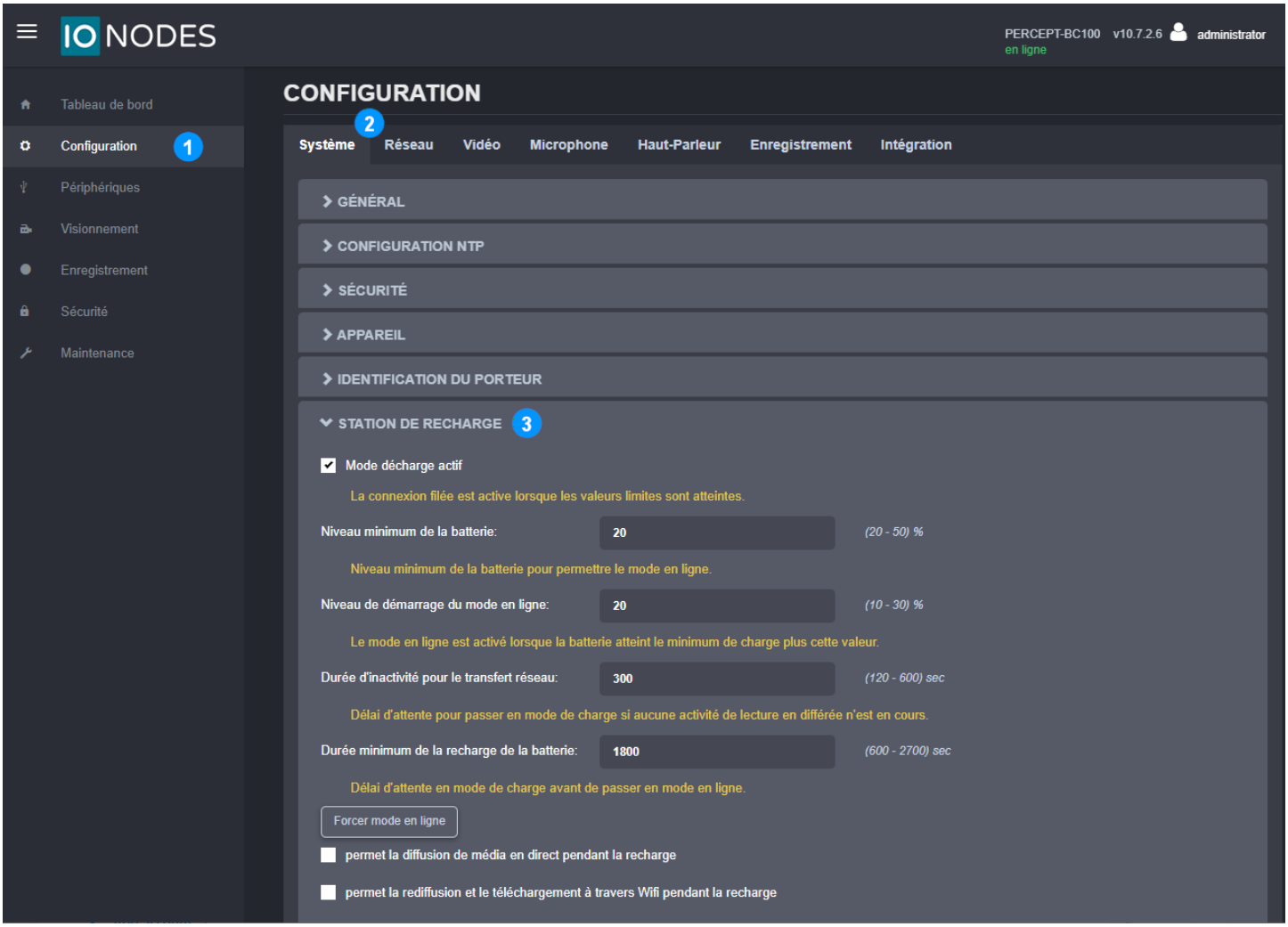
Le serveur d'enregistrement XProtect® peut être configuré pour limiter les tâches simultanées de transfert et leur bande passante. Ou encore, la lecture peut être complètement désactivée via Wi-Fi à partir de l'interface utilisateur Web de la caméra d'intervention PERCEPT. Ce dernier est recommandé lors du déploiement avec les stations d'accueil PERCEPT. Les transferts seront alors effectués exclusivement sur le port Ethernet filaire des stations d'accueil.



1. À partir de la page **Configuration**
2. Sélectionnez l'onglet **Réseau**
3. Développez la section **MISE EN FLUX** et cochez **Prévenir la lecture en différée sur une connexion sans fil** dans l'onglet **Média**
4. Sélectionnez l'onglet **Metadata** et réglez l'échantillonnage **GPS** et **Ressources système** à **0** pour désactiver le flux de métadonnées

3.2.4 Configurer l’usage de stations d'accueil

Lors du déploiement avec station(s) d'accueil PERCEPT. Il est recommandé de désactiver la diffusion en direct et la lecture via Wi-Fi lorsqu'ancré.



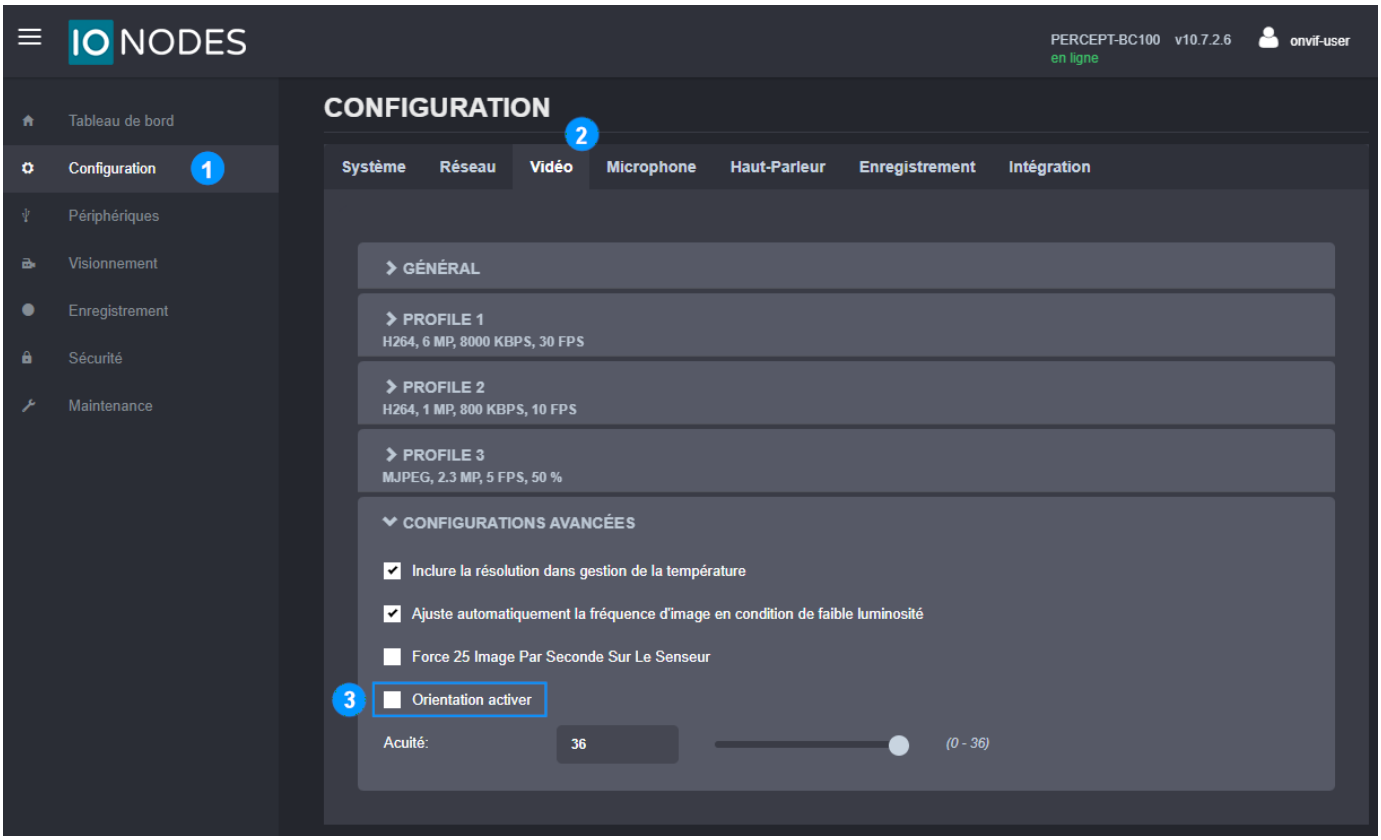
1. À partir de la page **Configuration**
2. Sélectionnez l'onglet **Système**
3. Développez la section **STATION DE RECHARGE** et configurez les paramètres comme suit
    a. Cochez **Mode décharge actif**
    b. Décochez **permet la diffusion de média en direct pendant la recharge**
    c. Décochez **permet la rediffusion et le téléchargement à travers WiFi pendant la recharge**

Note: Le téléversement de données peut créer une augmentation de la bande passante de plus de 200 Mbps vers le VMS. Assurez-vous que le réseau peut gérer le débit attendu selon le nombre de caméras installées. La configuration avancée de XProtect® Recording Server (RecorderConfig.xml) peut être ajustée pour limiter les tâches de transfert en fonction de l'échelle et de la capacité du système.

3.3 Configurer la vidéo

3.3.1 Désactiver les métadonnées d'orientation

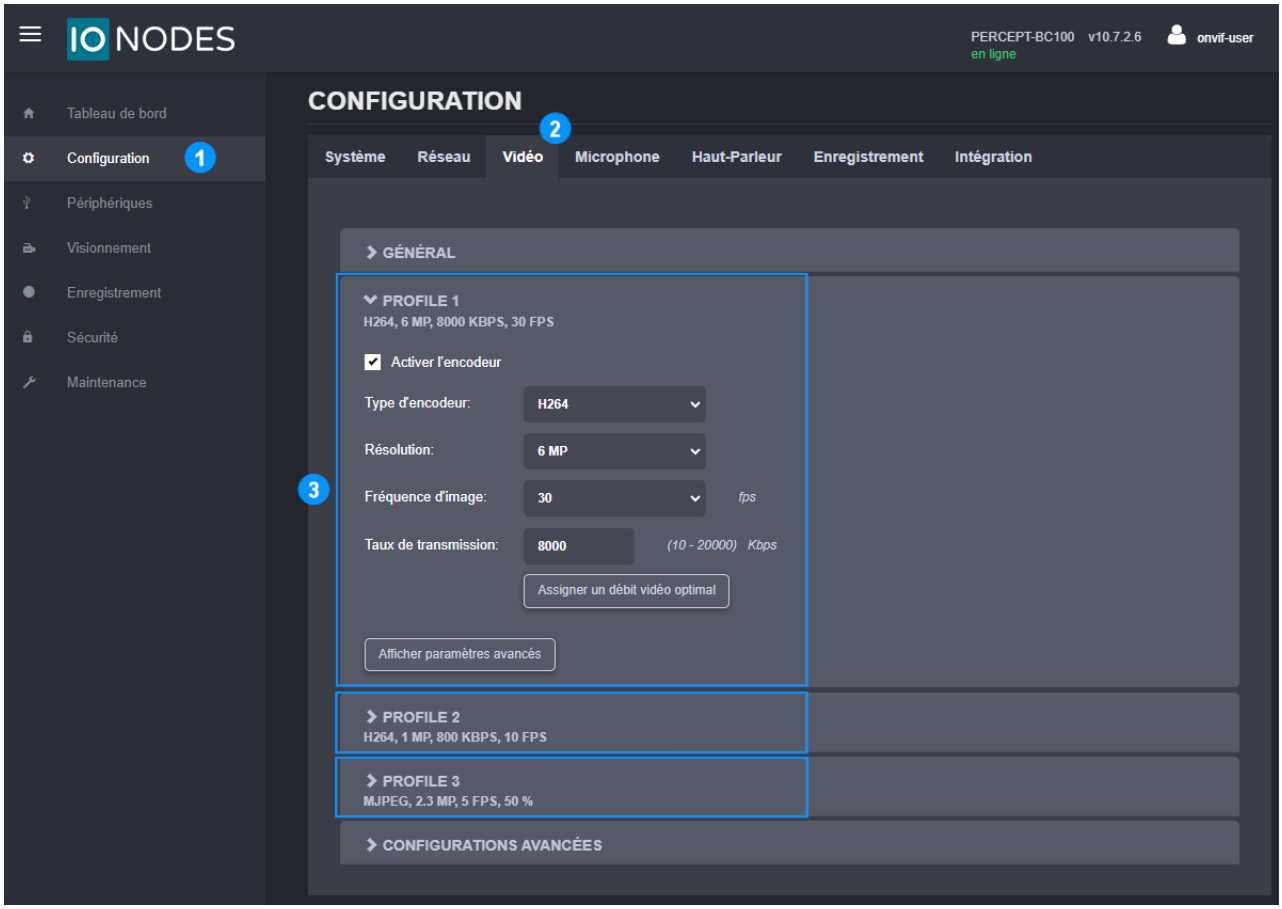
La caméra d'intervention PERCEPT inclut des métadonnées d'orientation utilisées par certains logiciels de rendu vidéo pour la stabilisation de l'image corrigée. Cette fonction n'est pas prise en charge par Milestone XProtect® et doit être désactivée dans la caméra d'intervention.



1. À partir de la page **Configuration**
2. Sélectionnez l'onglet **Vidéo**
3. Décochez la case **Orientation activer**

3.3.2 Configurer les profils vidéo

La caméra d'intervention PERCEPT prend en charge deux (2) profils d'encodage vidéo H.264/265 et un (1) profil MJPEG. Chaque profil activé dans la caméra d'intervention PERCEPT sera accessible à XProtect®.



1. À partir de la page **Configuration**
2. Sélectionnez l'onglet **Vidéo**
3. Activez et configurez chaque profil vidéo. Les paramètres recommandés sont:
    a. PROFILE 1 (enregistrement sur mémoire locale):
        i. **Type d'encodeur: H264**
        ii. **Résolution: 6 MP**
        iii. **Fréquence d'image: 30 fps**
        iv. **Taux de transmission: 8000 kbps**
        v. **Intervalle Intra: 240 frames**

vi. **Rate Control: Débit variable**
vii. **Profil: Main**
viii. **Contrôle VBR: Modéré**

b. PROFILE 2 (direct):
i. **Type d'encodeur: H264**
ii. **Résolution: 1 MP**
iii. **Fréquence d'image: 10 fps**
iv. **Taux de transmission: 800 kbps**
v. **Intervalle Intra: 30 frames**
vi. **Rate Control: Débit variable**
vii. **Profil: Main**
viii. **Contrôle VBR: Modéré**

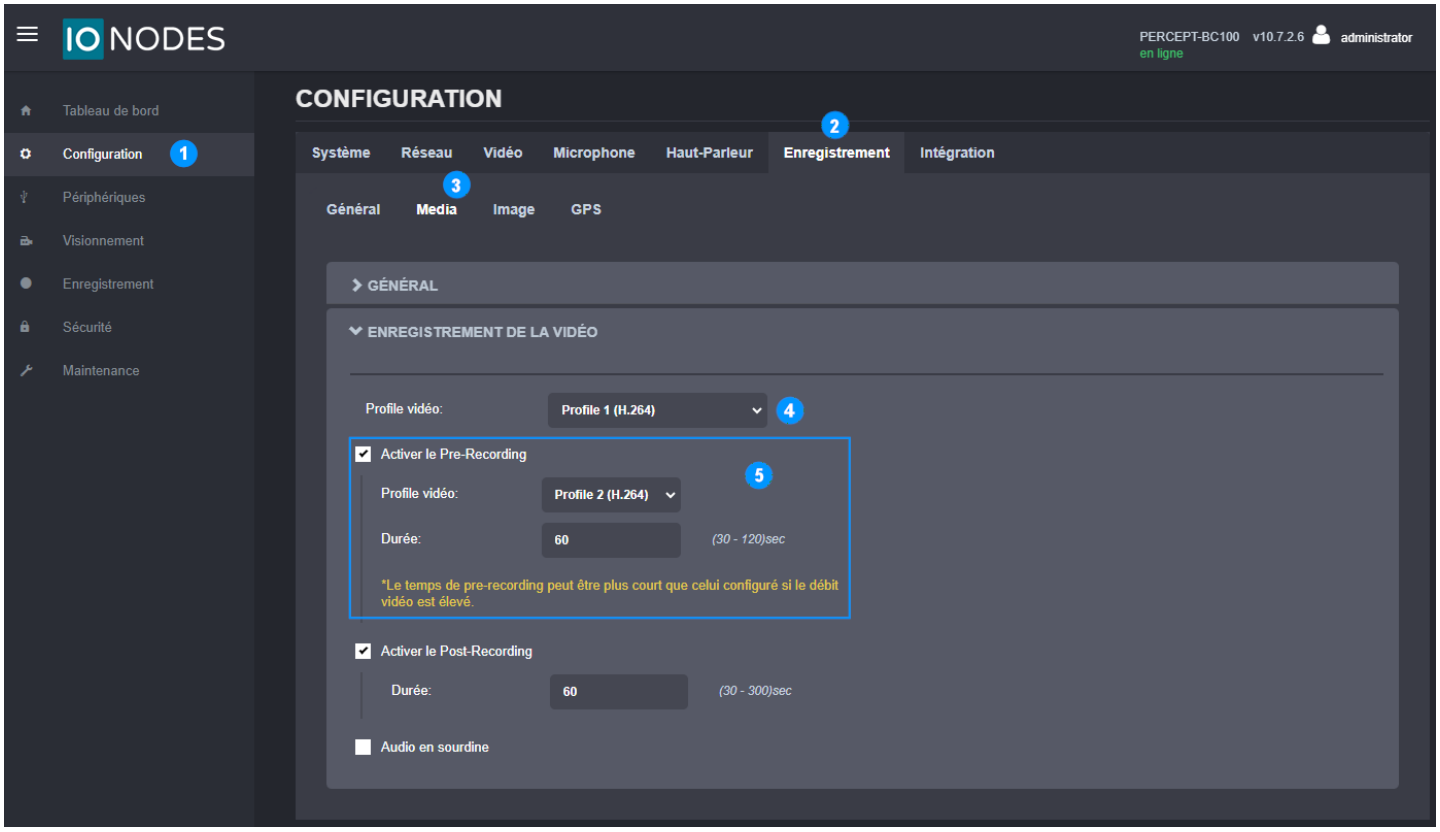
c. PROFILE 3 (utilisé par l'interface web PERCEPT): **Type d'encodeur: MJPEG**

Note: Le type d'encodeur (codec) et l'état activé du profil sont détectés par XProtect® lors de l'ajout de la caméra d'intervention. Ces paramètres doivent donc être configurés dans la caméra d'intervention PERCEPT avant de l'ajouter à XProtect®. La modification du type d'encodeur nécessite le redémarrage de l'appareil.

Note: Une fois ajoutés à XProtect®, les paramètres de profil vidéo tels que la résolution, la fréquence d'images, etc. doivent être configurés à partir de XProtect® Management Client.

Note: H.264 est recommandé pour les utilisateurs qui ont l'intention de visualiser des flux à partir de XProtect® Web Client sans que XProtect® Mobile Server dépense des ressources pour le transcodage. Les profils vidéo peuvent être configurés avec le codec H.265 si les limitations du client Web ou de ressources de transcodage ne sont pas préoccupantes.

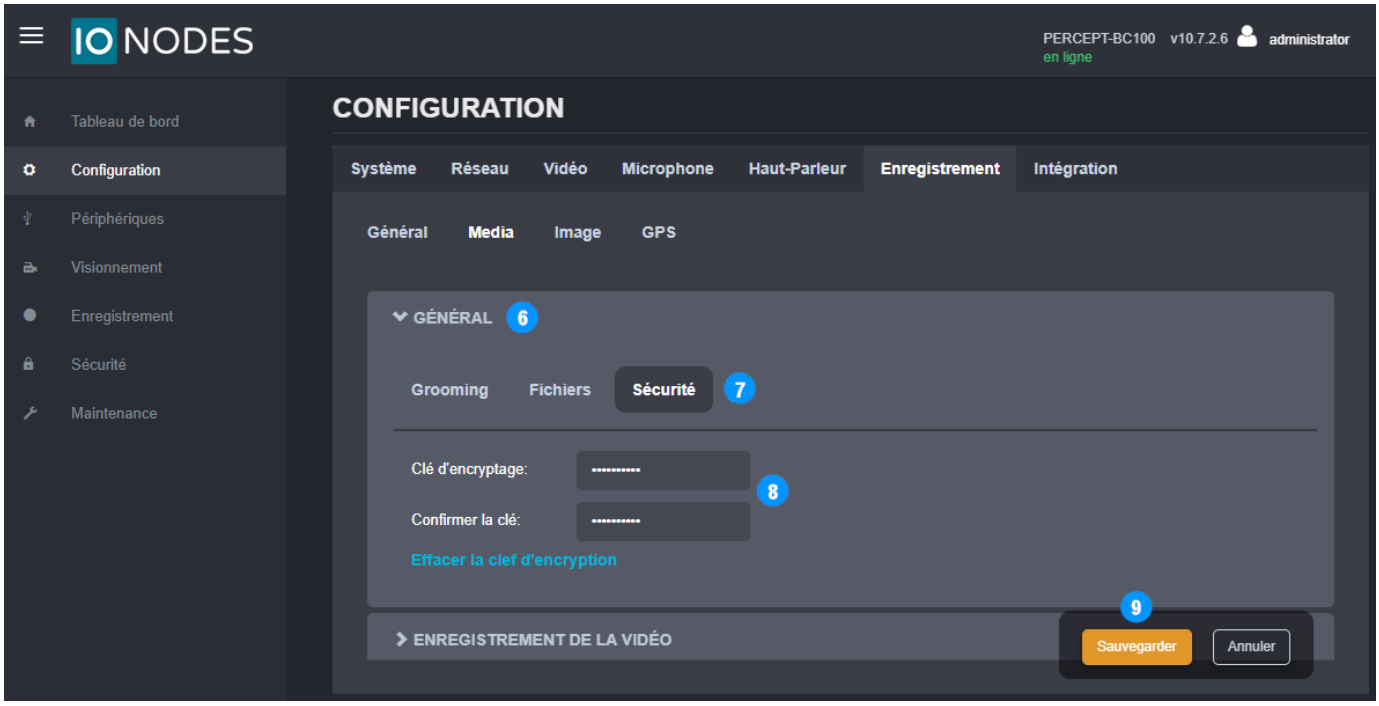
3.4 Configurer l'enregistrement local sur la caméra d'intervention



1. À partir de la page **Configuration**
2. Sélectionnez l'onglet **Enregistrement**
3. Sélectionnez le sous-onglet **Media**
4. Sélectionnez le profil vidéo pour l'enregistrement local (**Profil 1** pour l'enregistrement tout au long de ce guide)
5. Activez le pré/post-enregistrement selon les besoins et définissez leur durée. Le profil vidéo de préenregistrement doit être celui à faible débit (**Profil 2** dans ce guide)

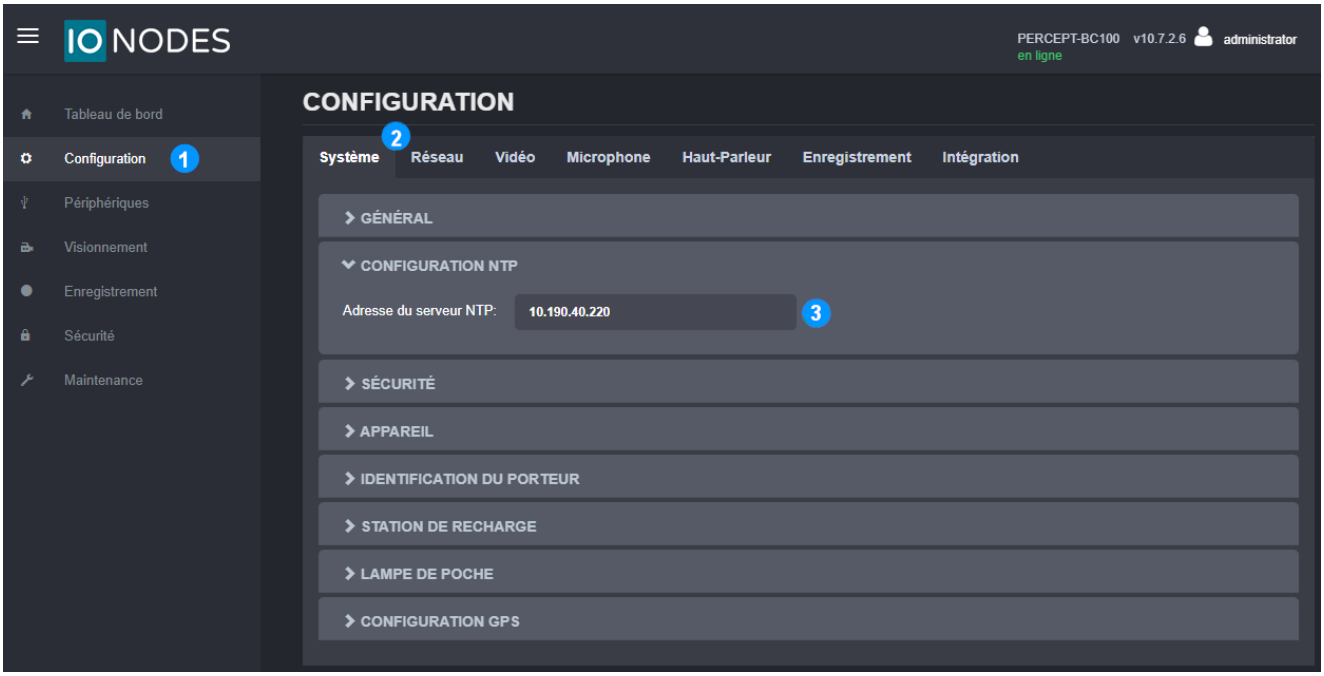
Note: Lorsque le préenregistrement est activé, la caméra encode et met en mémoire tampon la vidéo en permanence. Si le préenregistrement n'est pas nécessaire, sa désactivation augmente considérablement la durée de vie de la batterie. Si le préenregistrement est réglé sur un profil à débit élevé, la caméra pourrait surchauffer sous certaines conditions environnementales.

Note: Pour empêcher l'accès non autorisée aux fichiers enregistrés localement en cas de perte ou de vol, la caméra dispose d'un cryptage AES-256 pour les fichiers au repos.



6. Sous **Configuration**, **Enregistrement**, onglet **Media**, développez le sous-onglet **Général**
7. Sélectionnez la section **Sécurité**
8. Saisissez un mot de passe pour le cryptage AES-256 de l'enregistrement multimédia local au repos (saisissez et confirmez la clé de cryptage). Il n'y a pas de politique de mot de passe ou d'exigence de complexité.
9. **Sauvegarder**

3.5 Configurer la synchronisation de l'heure sur la caméra d'intervention



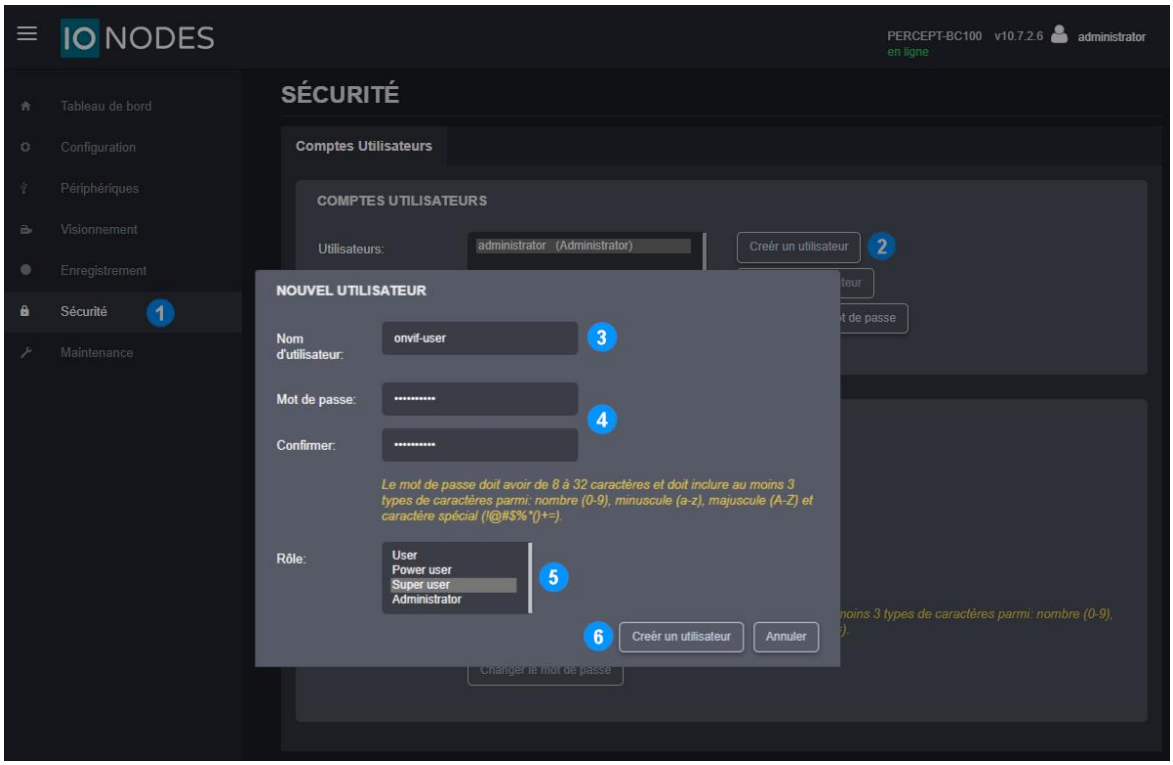
1. À partir de la page **Configuration**
2. Sélectionnez l'onglet **Système**
3. Dans la section **Configuration NTP**, entrez l'adresse IP du même serveur de temps réseau utilisé par Milestone XProtect® pour synchroniser l'heure

Note: La synchronisation de l'heure garantit que les clips enregistrés sur la carte SD des caméras d'intervention PERCEPT et transférés ultérieurement vers XProtect® sont horodatés avec précision.

Note: En configurant ses services, tout ordinateur exécutant Windows® peut agir comme serveur NTP pour les appareils connectés au réseau local de surveillance. Les caméras d'intervention PERCEPT qui se connectent au LAN directement ou via VPN peuvent garder leurs horloges synchronisées avec XProtect® en utilisant cette approche.

3.6 Créer un nouvel utilisateur ONVIF dédié (recommandé)

Le compte administrateur par défaut peut être utilisé pour intégrer la caméra d'intervention à XProtect®. Cependant, il est recommandé de créer un compte utilisateur ONVIF dédié à cet effet. Le rôle « *Super user*» donne au compte toutes les autorisations pour les fonctionnalités prises en charge par XProtect®.



1. À partir de la page **Sécurité**
2. Cliquez sur le bouton **Créer un utilisateur**
3. Dans la fenêtre contextuelle **Nouvel utilisateur**, entrez le N**om d'utilisateur**
4. Entrez le **Mot de passe** et répétez-le pour confirmer
5. Sélectionnez le role **Super user**
6. Cliquez sur **Créer un utilisateur**

Note: La configuration détaillée dans ce guide doit être effectuée à l'aide d'un compte au rôle « *Administrator* », l'utilisateur ONVIF dédié est utilisé par XProtect® lors de l'intégration de la caméra d'intervention PERCEPT.

4 Configuration VPN

Cette section détaille les exigences VPN, y compris un exemple pratique.

4.1 Exigences VPN

- Protocole: La caméra d'intervention PERCEPT prend en charge le protocole VPN L2TP/IPSec avec clé pré-partagée (PSK). La fonction VPN est toujours active ; il se connecte lorsqu'il peut atteindre le serveur VPN.
- Nb de tunnels et Bande passante: Ce protocole crypte les tunnels VPN. Lors de l'évaluation d'un serveur VPN (matériel ou logiciel), le nombre maximal de tunnels VPN et la bande passante cryptée pris en charge doivent couvrir le nombre de caméras d'intervention PERCEPT déployées.
- Adresse IP statique publique: Le serveur ou routeur VPN doit se connecter à Internet avec une adresse IP statique publique. La redirection de port pour le protocole L2TP/IPSec doit être configurée lorsque le serveur VPN est connecté derrière un autre routeur Internet.
- Réservation d'adresse: La solution VPN doit fournir un moyen d'attribuer des adresses IP spécifiques à chaque appareil. Cela peut être mis en œuvre en ayant un utilisateur VPN distinct pour chaque appareil et en attribuant une adresse IP spécifique à chaque utilisateur.

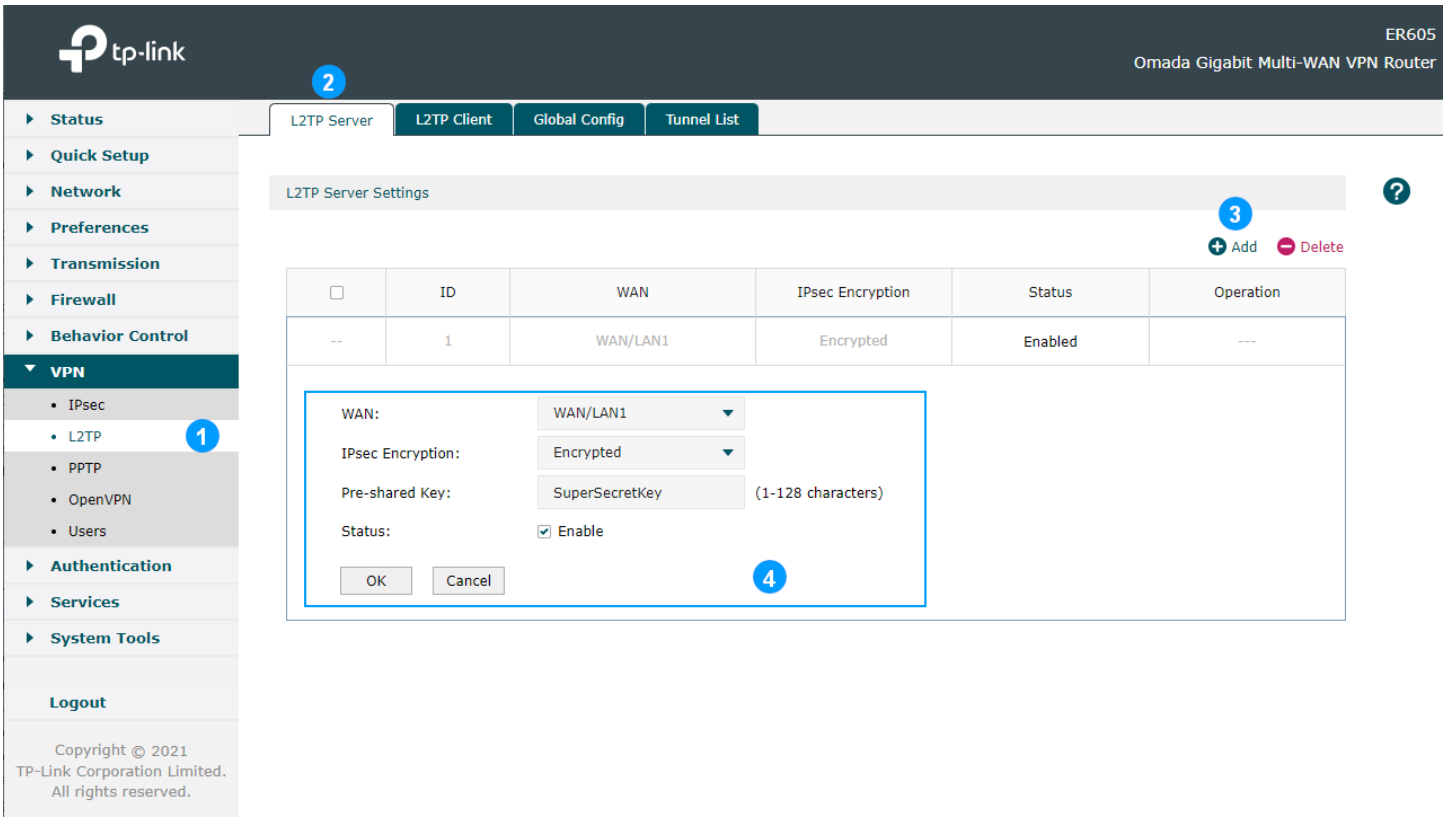
4.2 Exemple de VPN

La sélection et la configuration de VPN spécifiques sortent du cadre de ce guide. Cet exemple est inclus pour mieux illustrer les exigences VPN.

Cet exemple utilise un routeur VPN Omada de TP-Link ; plus précisément, le modèle d'entrée de gamme ER605 v2. Il prend en charge jusqu'à seize (16) tunnels VPN L2TP avec un débit de 47,11 Mbps cryptés. Les paramètres recommandés dans ce guide de déploiement donnent ~ 1,0 à 1,2 Mbps par caméra lors de la diffusion audio et vidéo en direct. En supposant que le transfert de de clips enregistrés sur mémoire interne ne soit pas effectué à distance via VPN, ce routeur d'entrée de gamme peut prendre en charge un déploiement PERCEPT à petite échelle.

4.2.1 Configurer le serveur L2TP

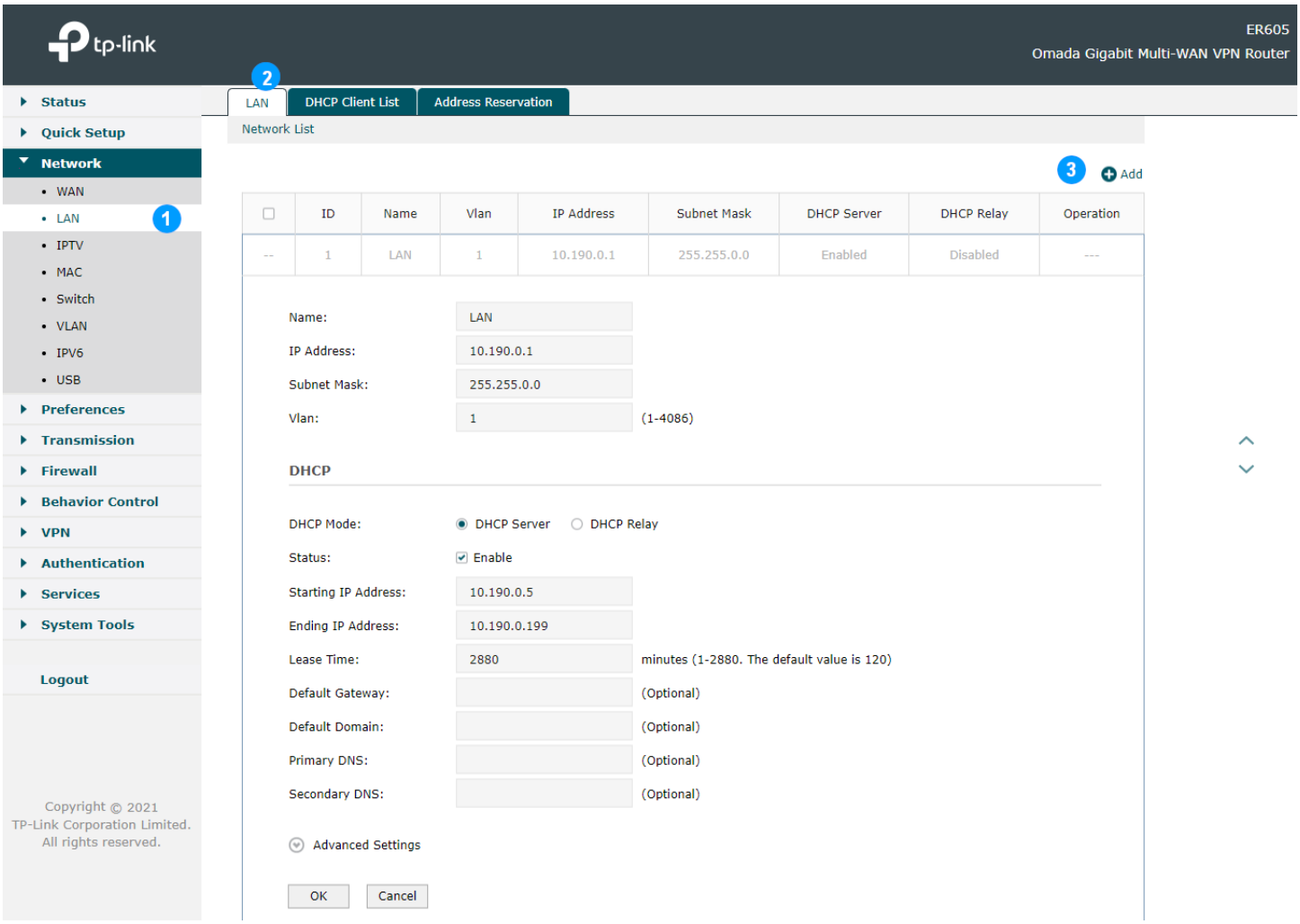
Les ports WAN/LAN de ce routeur sont configurables. Une fois les paramètres IP de base du routeur et les ports WAN/LAN connectés et configurés, ajoutez un serveur L2TP.



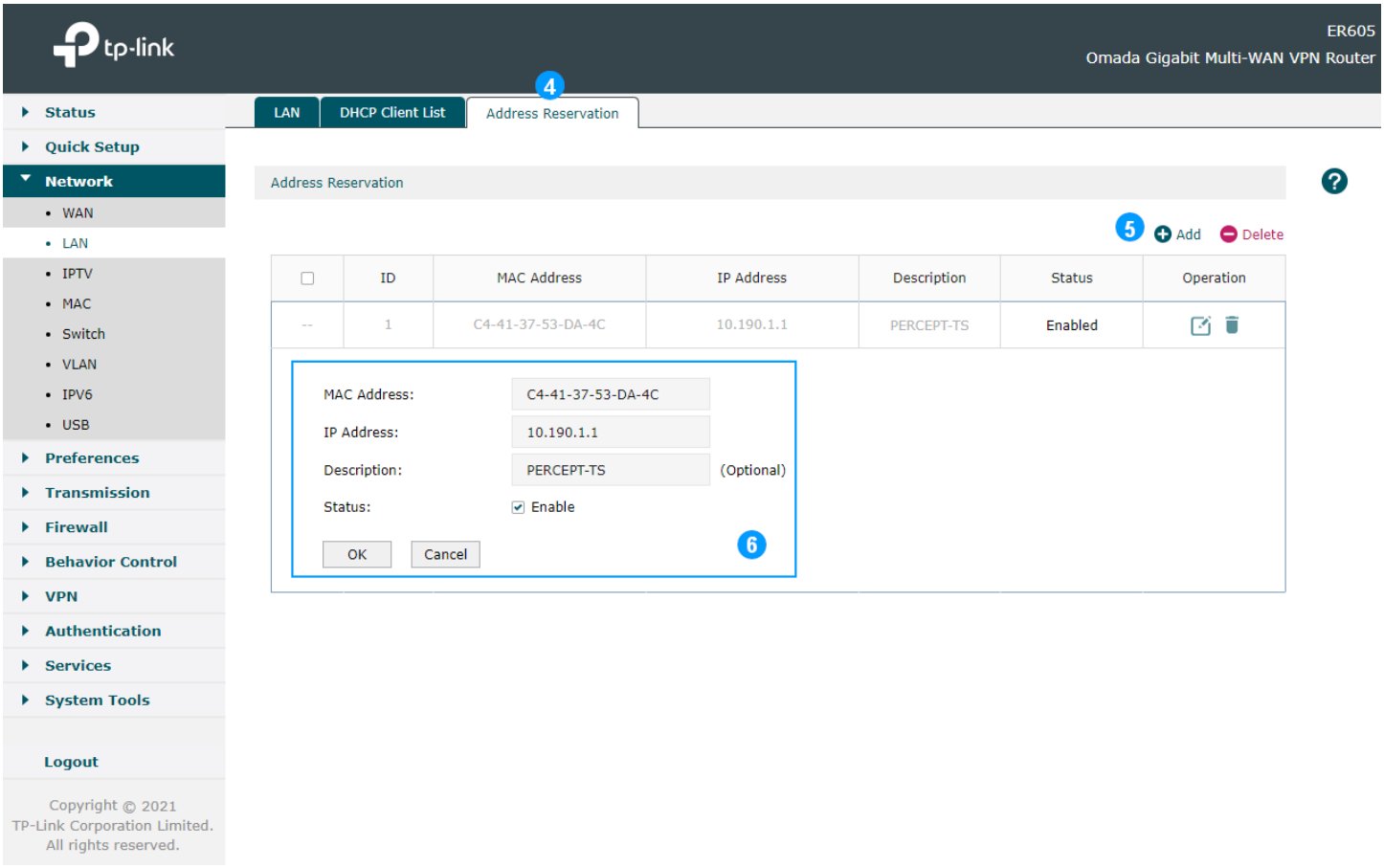
1. Développez le menu **VPN** et sélectionnez **L2TP**
2. Sélectionnez l'onglet **L2TP Server**
3. Ajouter (**Add**) un nouveau serveur L2TP
4. Configurez le serveur L2TP puis cliquez sur **OK**
    a. Sélectionnez le port **WAN** qui recevra les connexions entrantes via l'internet
    b. Sélectionnez **Encrypted**
    c. Choisissez une clé secrète pré-partagée (**Pre-shared Key)**
    d. Activer (**Enable**) le serveur L2TP

4.2.2 Réservation d'adresse IP LAN

Ce routeur peut faire office de serveur ou de relai DHCP. Pour configurer les adresses IP LAN et VPN à partir de ce routeur, la fonction de serveur DHCP est activée dans notre exemple.



1. Développez le menu **Network** et sélectionnez **LAN**
2. Sélectionnez l'onglet **LAN**
3. Cliquez sur **Add**
    a. Entrez les paramètres du réseau LAN
    b. Activer le **DHCP Server** et configurer ses paramètres



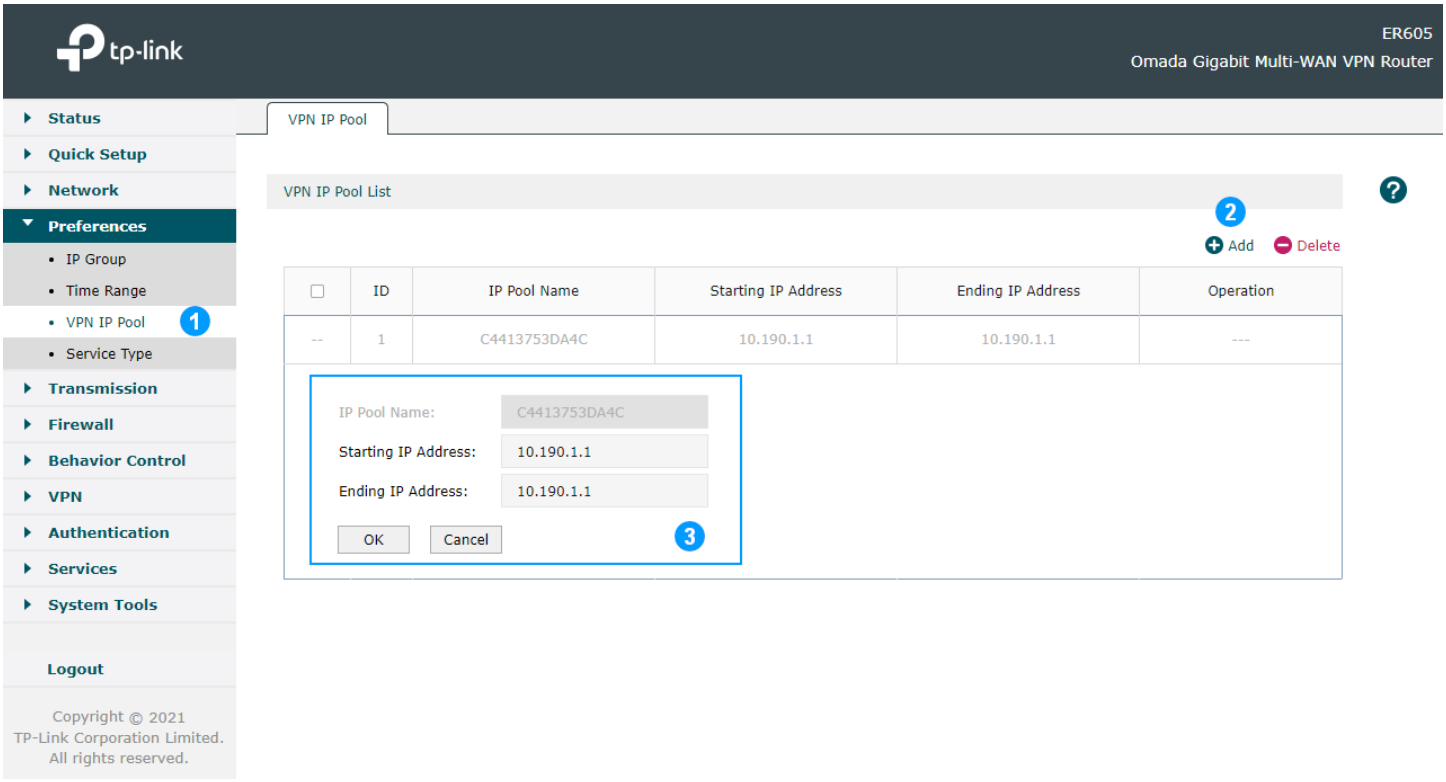
4. Sélectionnez l'onglet **Address Reservation**
5. Cliquez sur **Add**
6. Saisissez la **MAC Address** de la caméra d'intervention PERCEPT et l'adresse IP souhaitée, puis activez

Note: L'adresse MAC peut être trouvée sur le tableau de bord de l'interface utilisateur Web de la caméra d'intervention PERCEPT ou sur son écran OLED en appuyant brièvement sur le bouton d'alimentation pour faire défiler les informations d'état.

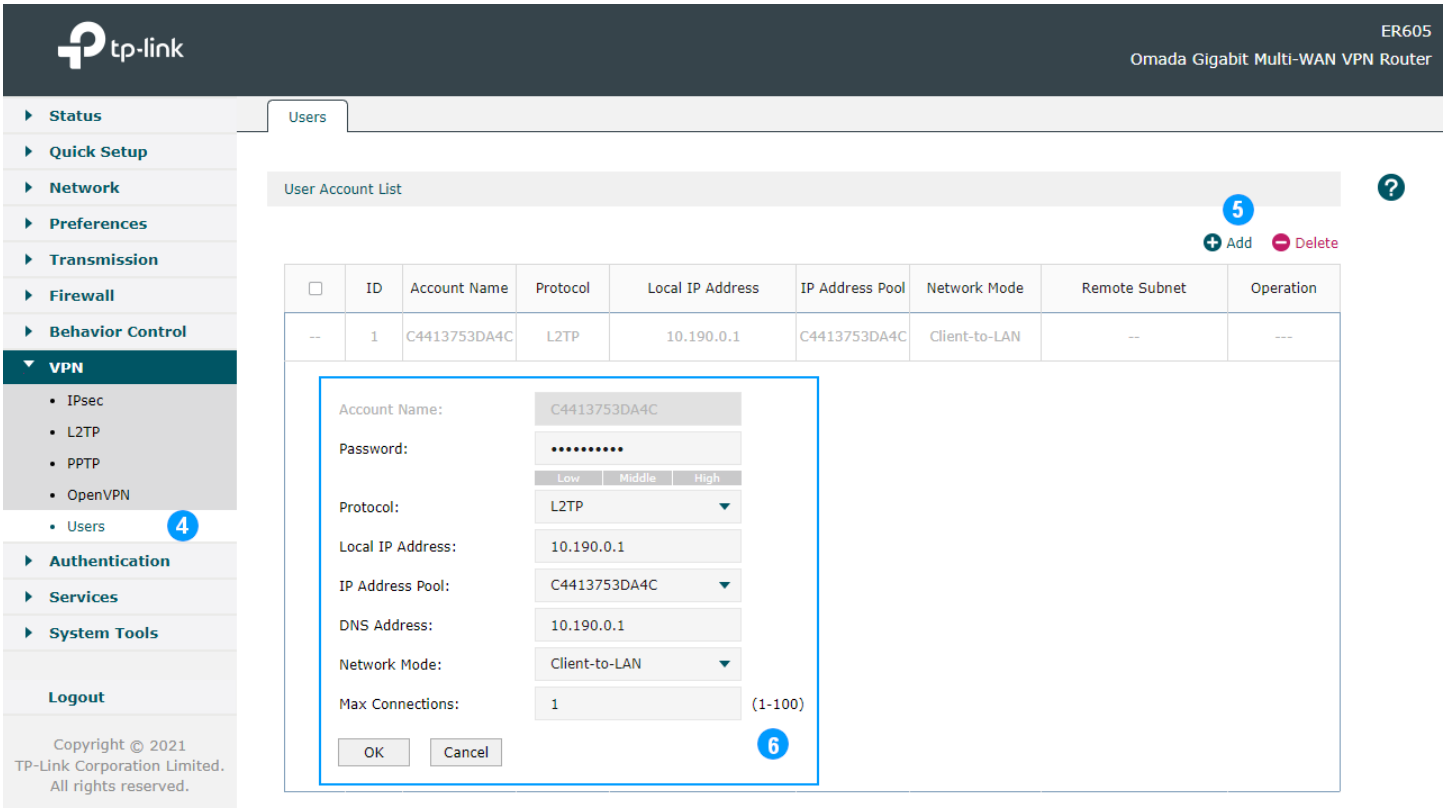
4.2.3 Réservation d'adresse IP VPN

Ce routeur attribue des adresses IP aux clients VPN. Chaque utilisateur VPN peut être affecté à un pool IP VPN spécifique. En créant des pools IP VPN à adresse unique et un utilisateur VPN pour

chaque caméra d'intervention PERCEPT, une connexion d'un utilisateur VPN spécifique se verra toujours attribuer la même adresse IP.



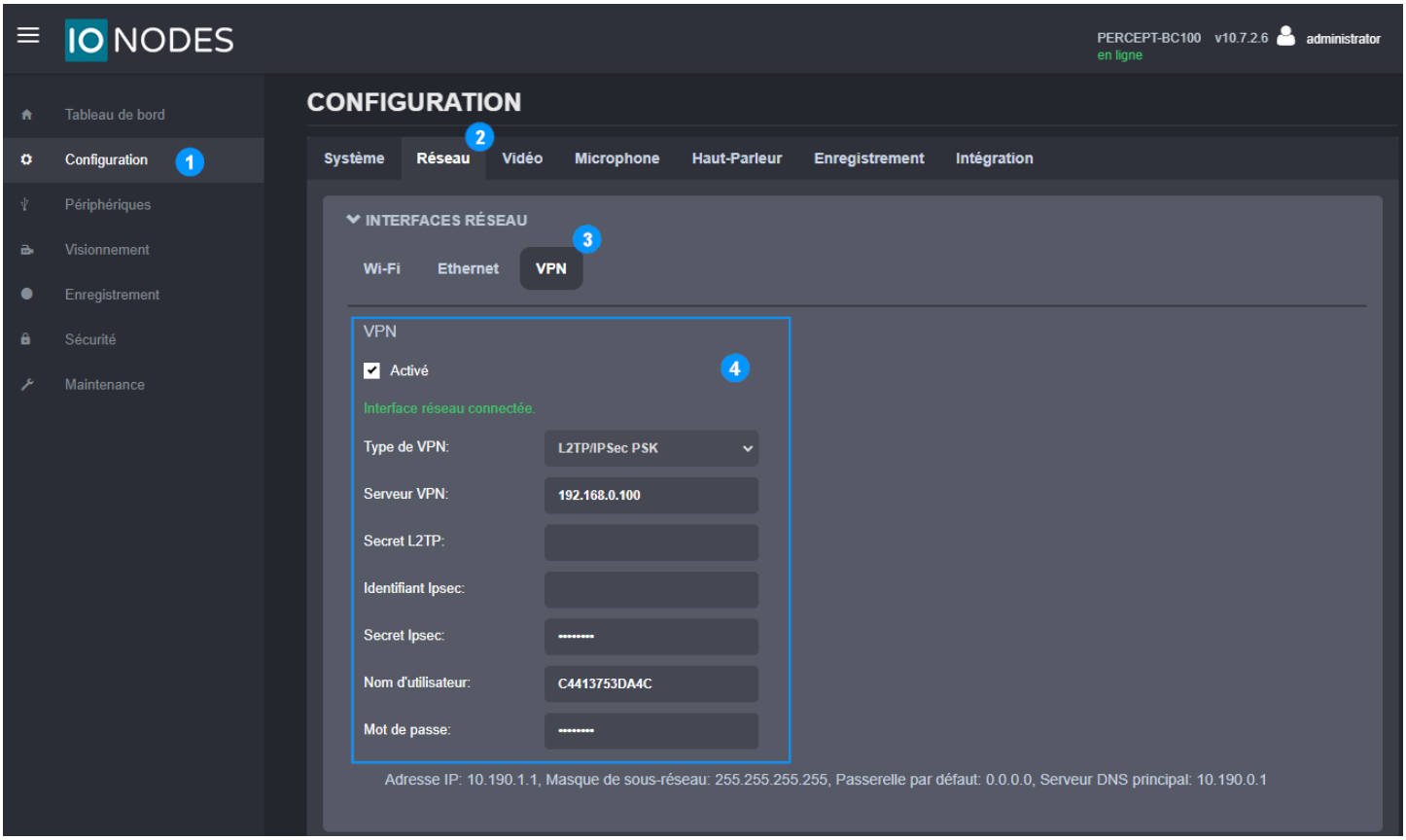
1. Développez le menu **Preferences** et sélectionnez **VPN IP Pool**
2. Cliquez sur **Add**
3. Choisissez un **IP Pool Name** et définissez les **Starting IP Address** et **Ending IP Address** sur la même adresse réservée sur le serveur DHCP LAN pour cette caméra d'intervention PERCEPT. Pour faciliter la configuration dans cet exemple, le nom du pool IP est défini comme étant l'adresse MAC de la caméra.



4. Développez le menu **VPN** et sélectionnez **Users**
5. Cliquez sur **Add**
6. Créez et configurez l'utilisateur VPN :
    a. **Account Name**: choisissez un nom d'utilisateur VPN unique pour chaque caméra d'intervention PERCEPT. Dans cet exemple, il est réglé sur l'adresse MAC de la caméra
    b. **Password**: Un mot de passe pour cet utilisateur VPN (peut être le même pour plus d'un utilisateur)
    c. **Protocol**: **L2TP**
    d. **Local IP address**: adresse IP LAN du routeur VPN
    e. **IP address Pool**: Pool d'adresses IP créé à l'étape précédente pour cette caméra d'intervention PERCEPT. Dans cet exemple, il s'agit de l'adresse MAC de la caméra
    f. **DNS address**: adresse IP LAN du routeur VPN
    g. **Network Mode**: **Client-to-LAN**
    h. **Max Connections**: **1**

4.2.4 Configurer les paramètres VPN de la caméra d'intervention

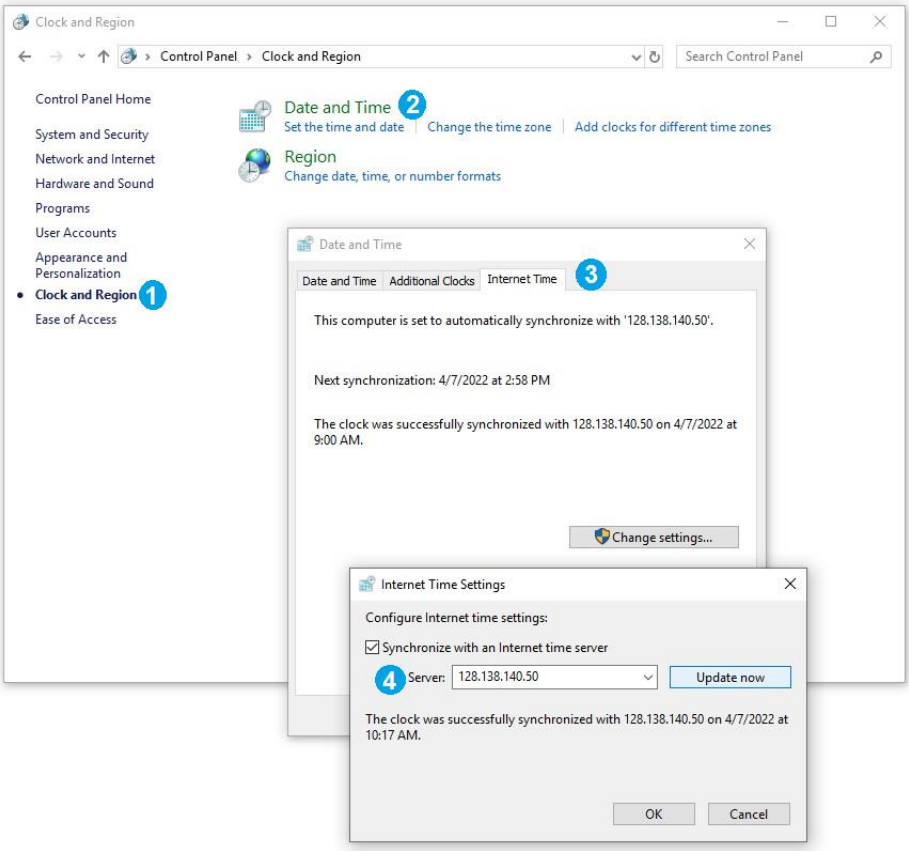
Les paramètres VPN affichés sont basés sur l'exemple de réservation d'adresse IP VPN ci-dessus.



1. À partir de la page **Configuration**
2. Sélectionnez l'onglet **Réseau**
3. Développez la section **INTERFACES RÉSEAU** et sélectionnez le sous-onglet **VPN**
4. Activer et configurer les paramètres **VPN**
    a. **Serveur VPN** : adresse IP statique publique du port WAN du routeur VPN
    b. **Ipsec Secret** : clé pré-partagée du serveur L2TP (définie à la section 4.2.1)
    c. **Nom d'utilisateur** : nom d'utilisateur VPN (défini dans la section 4.2.3, adresse MAC de la PERCEPT Body Camera dans cet exemple)
    d. **Mot de passe** : mot de passe utilisateur VPN (défini dans la section 4.2.3)

5 Configuration de Milestone XProtect® avant l'intégration

5.1 Configurer la synchronisation de l'heure



Par défaut, XProtect® Recording Server utilise l'heure de l'ordinateur sur lequel il est hébergé. Pour modifier les paramètres d'heure sur le PC hôte:

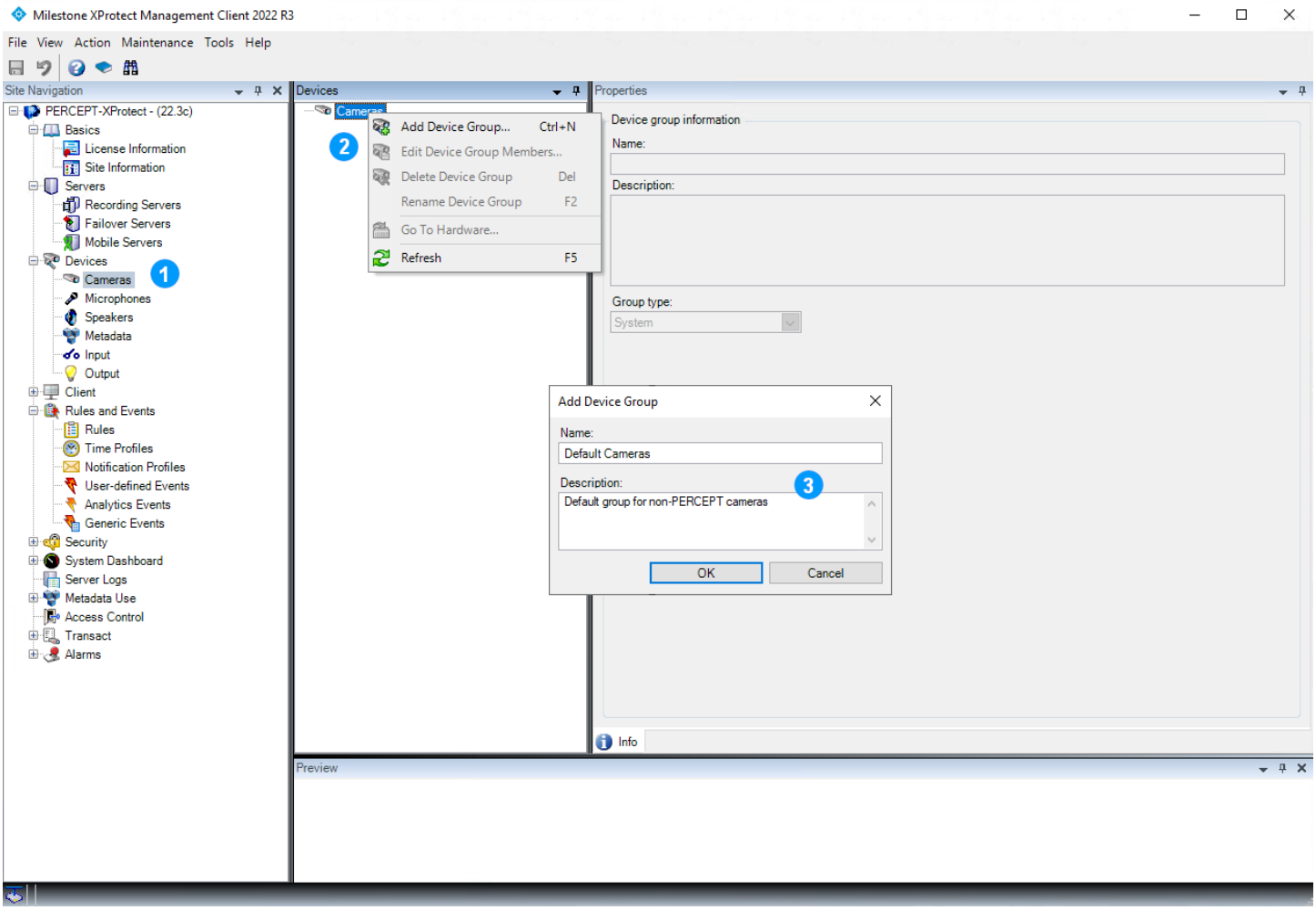
1. Depuis le **Panneau de configuration** > **Horloge et région**
2. Sélectionnez l'onglet **Régler l'heure et la date**
3. Sélectionnez **Heure Internet**, puis accédez à **Modifier les paramètres...**
4. Sélectionnez **Synchroniser avec un serveur de temps Internet** et sélectionnez un serveur de temps valide

Note: Les caméras d'intervention PERCEPT doivent utiliser le même serveur NTP (Network Time Protocol) s'il est accessible sur le LAN. Si le serveur XProtect® se connecte à ce serveur NTP via Internet, les services du serveur XProtect® peuvent être configurés pour agir comme un serveur NTP pour les appareils locaux.

5.2 Configurer les groupes de périphériques

Lorsque des appareils sont ajoutés à XProtect®, ils doivent être ajoutés à des groupes d'appareils spécifiques pour les caméras, les microphones, les haut-parleurs, les métadonnées, et les entrées/sorties. Pour faciliter la configuration et la gestion, les règles peuvent ensuite être appliquées à des groupes d'appareils plutôt qu'à des appareils individuels.

L'intégration de caméras d'intervention PERCEPT diffère de l'intégration typique d'une caméra fixe, en utilisant des règles personnalisées pour obtenir le comportement souhaité. Au minimum, le déploiement recommandé nécessite la création de groupes d'appareils spécifiques pour les caméras et les microphones PERCEPT.

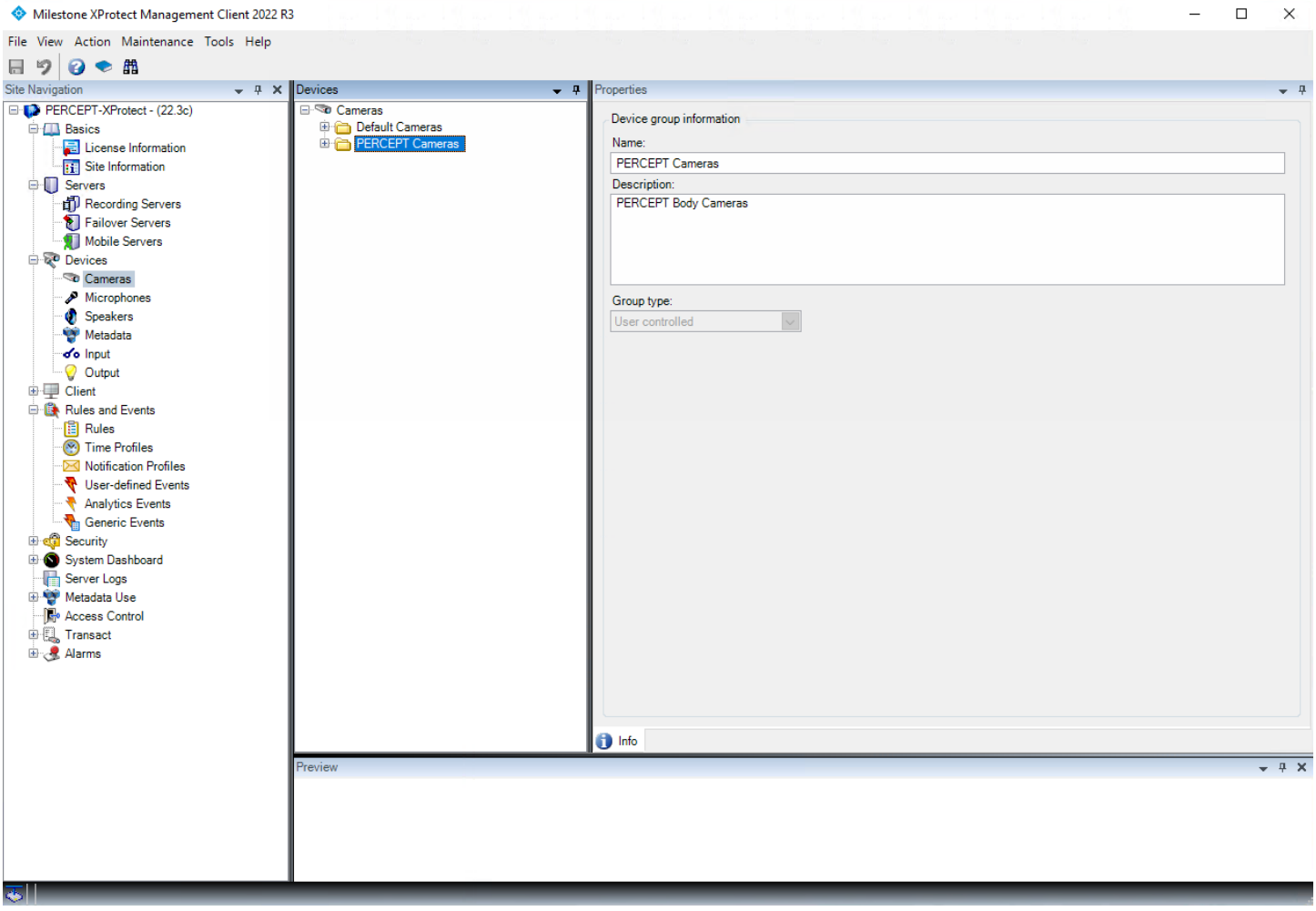


1. Dans le volet gauche de **XProtect® Management Client**, sélectionnez **Devices** > **Cameras**

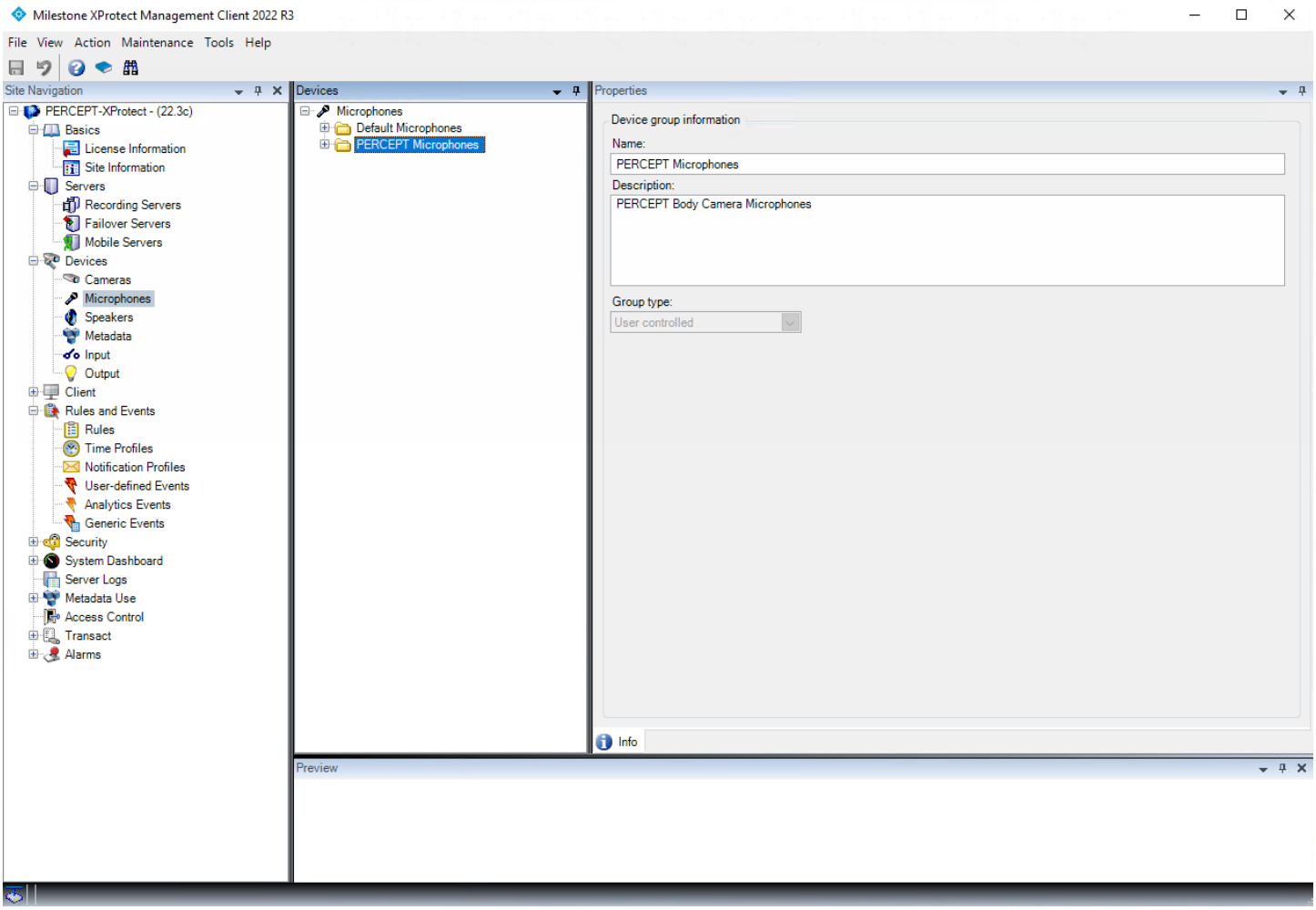
2. Dans le volet central **Devices**, cliquez avec le bouton droit sur **Cameras** et sélectionnez **Add Device Group** dans le menu contextuel.
3. Ajoutez un groupe par défaut pour les caméras autres que PERCEPT et une description facultative, puis cliquez sur **OK**.

Note: L'ajout d'un groupe de caméras par défaut n'est requis que lors du démarrage d'une nouvelle installation de XProtect®. Si des caméras sont déjà intégrées au système, un groupe de caméras par défaut a déjà été créé lors de l'ajout de la première caméra.

4. Répétez les étapes ci-dessus, cette fois en créant un groupe de caméras pour les caméras PERCEPT. Les groupes résultants ressembleraient à l'image ci-dessous.

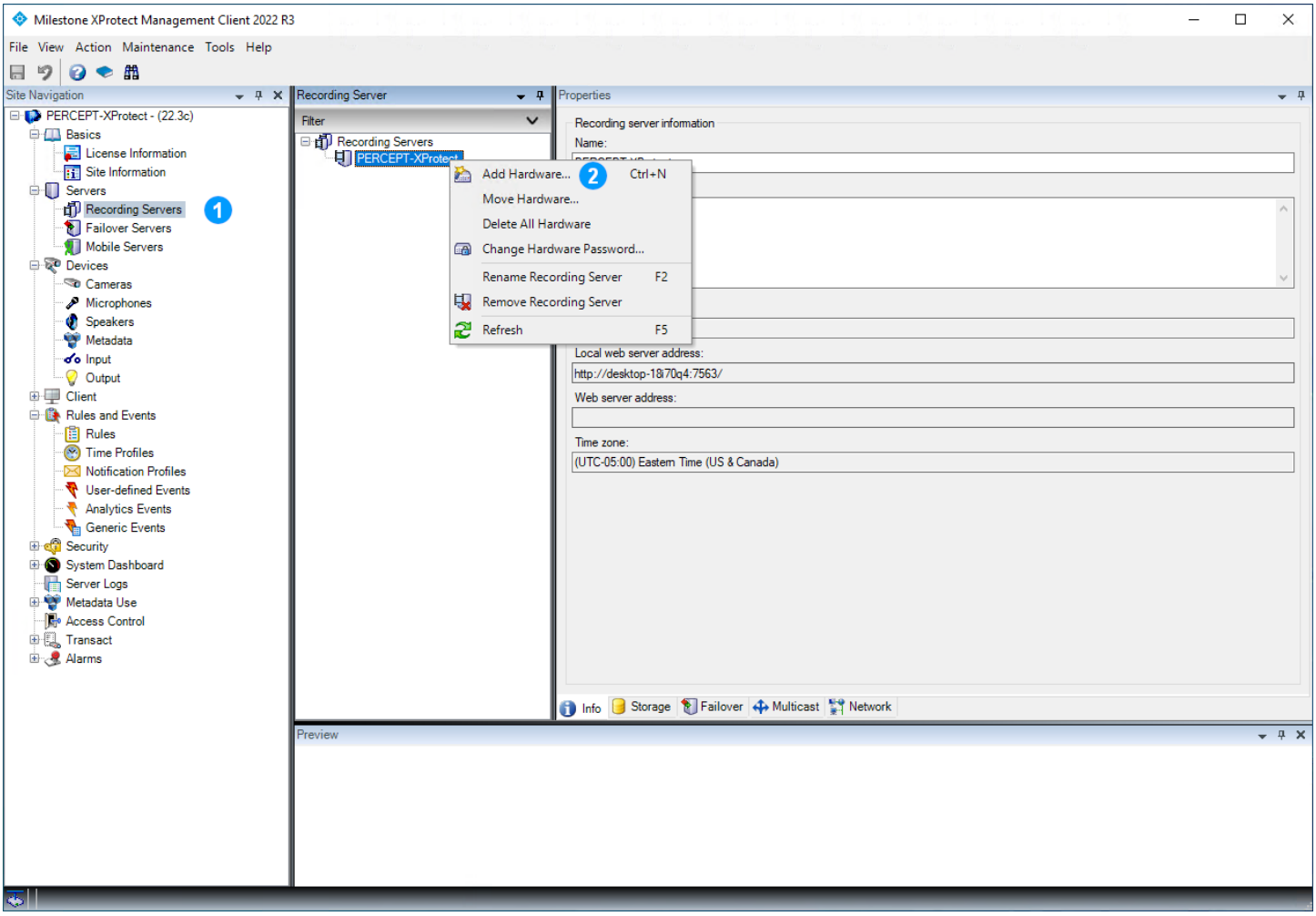


5. Répétez les étapes ci-dessus, cette fois en créant les groupes Microphones par défaut et PERCEPT. Les groupes résultants ressembleraient à l'image ci-dessous.

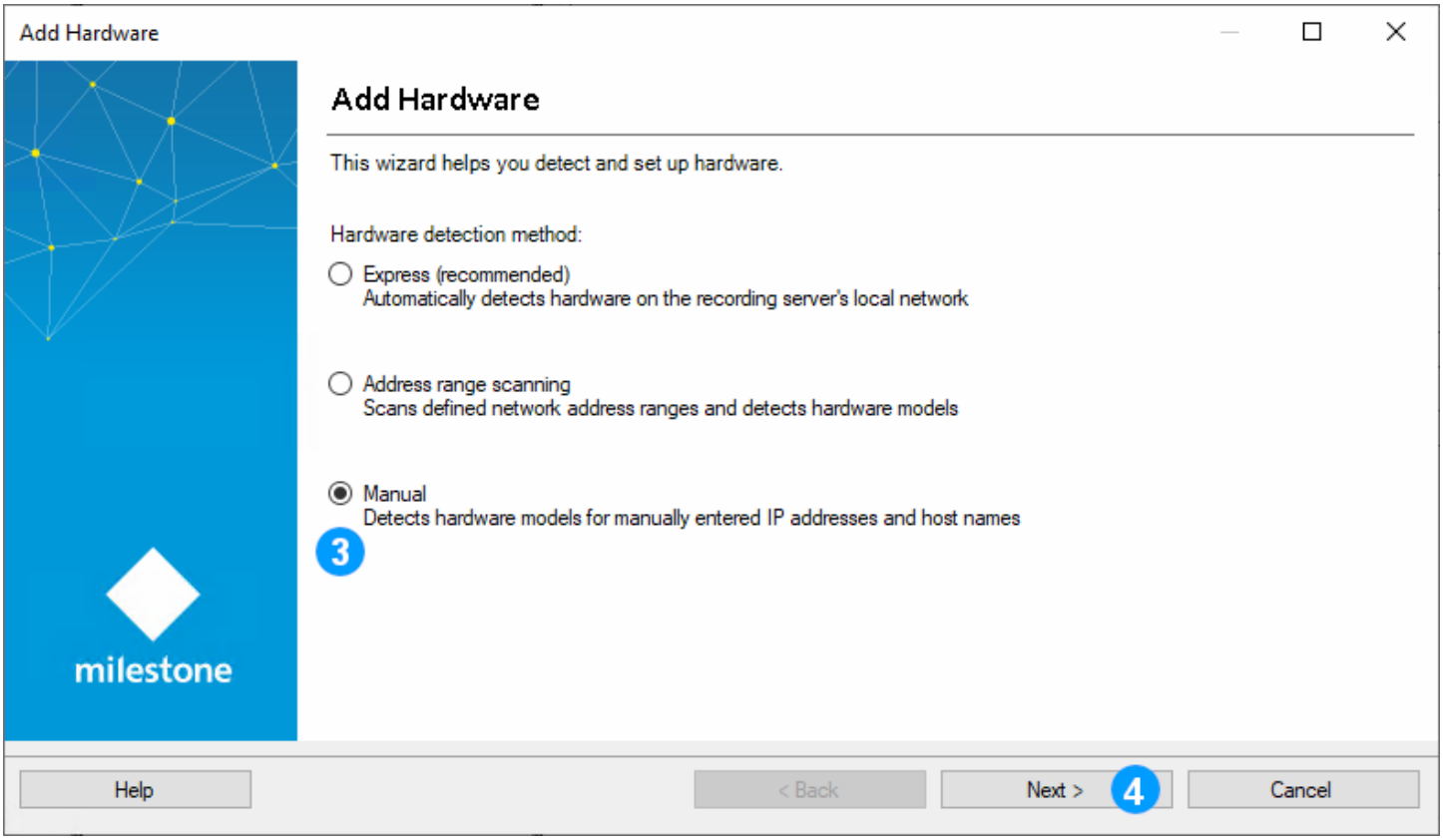


6. Les haut-parleurs des caméras d'intervention PERCEPT ne nécessitent pas de règles spécifiques, ils peuvent donc être ajoutés au groupe de haut-parleurs par défaut. Si aucun dispositif avec haut-parleur n'a déjà été ajouté dans XProtect®, un groupe de haut-parleurs par défaut peut être ajouté à ce moment. Sinon, il sera créé lors de l'ajout de la première caméra d'intervention PERCEPT.

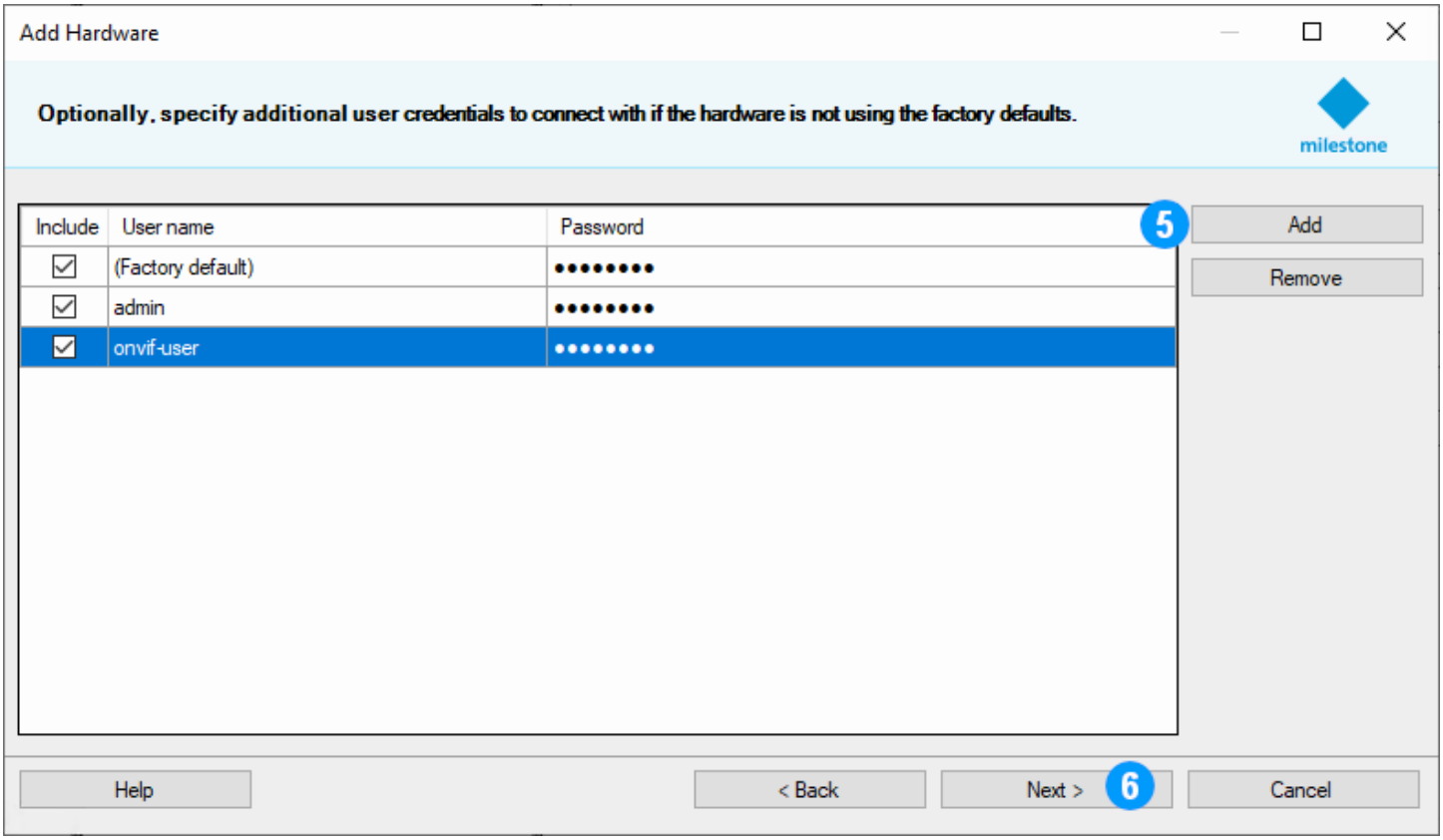
6 Ajout de la caméra d'intervention PERCEPT dans XProtect®



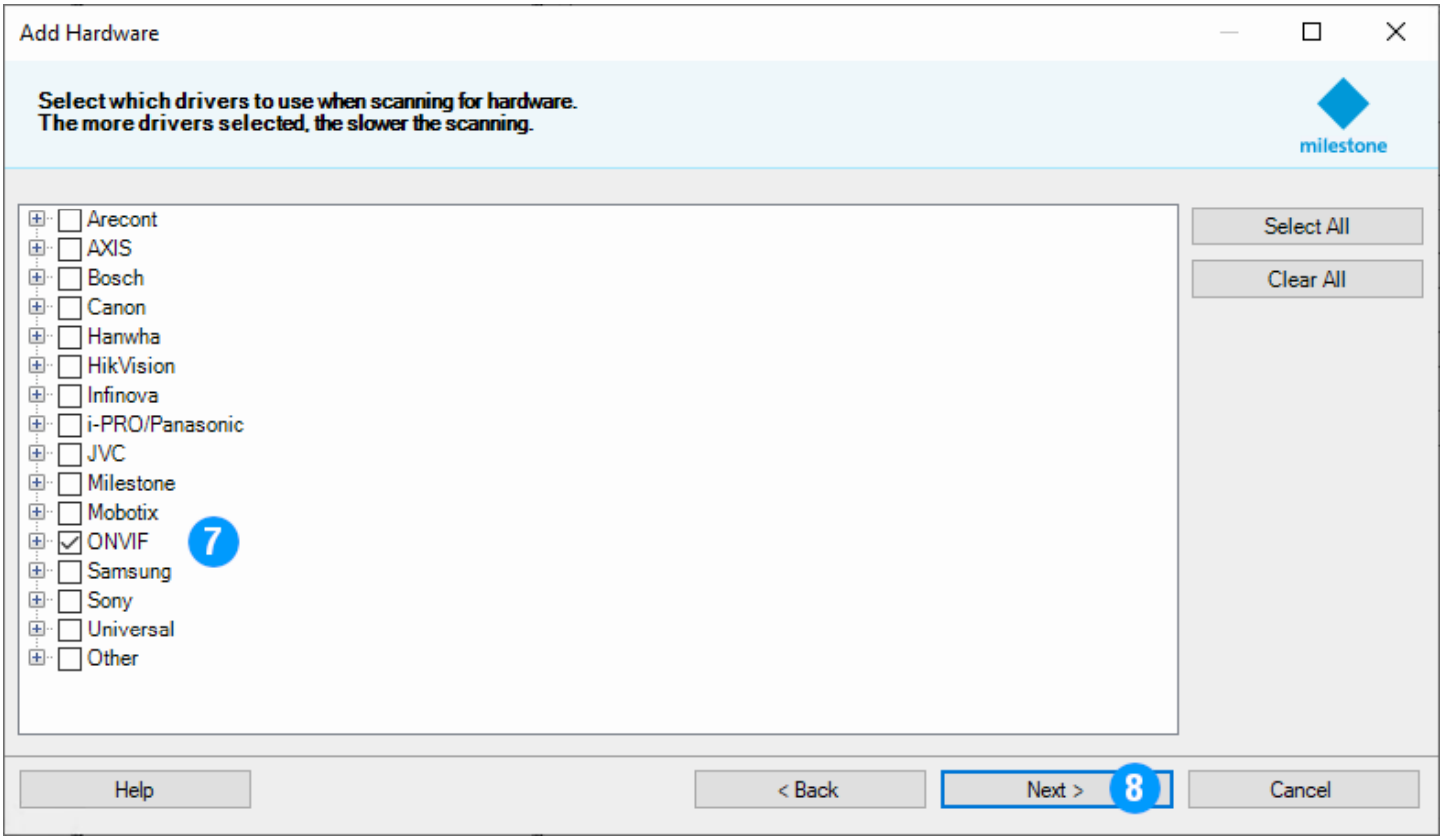
1. Dans **XProtect® Management Client**, cliquez sur **Recording Servers**
2. Faites un clic droit sur le serveur d'enregistrement où vous souhaitez ajouter la caméra d'intervention PERCEPT et choisissez **Add Hardware** dans le menu contextuel



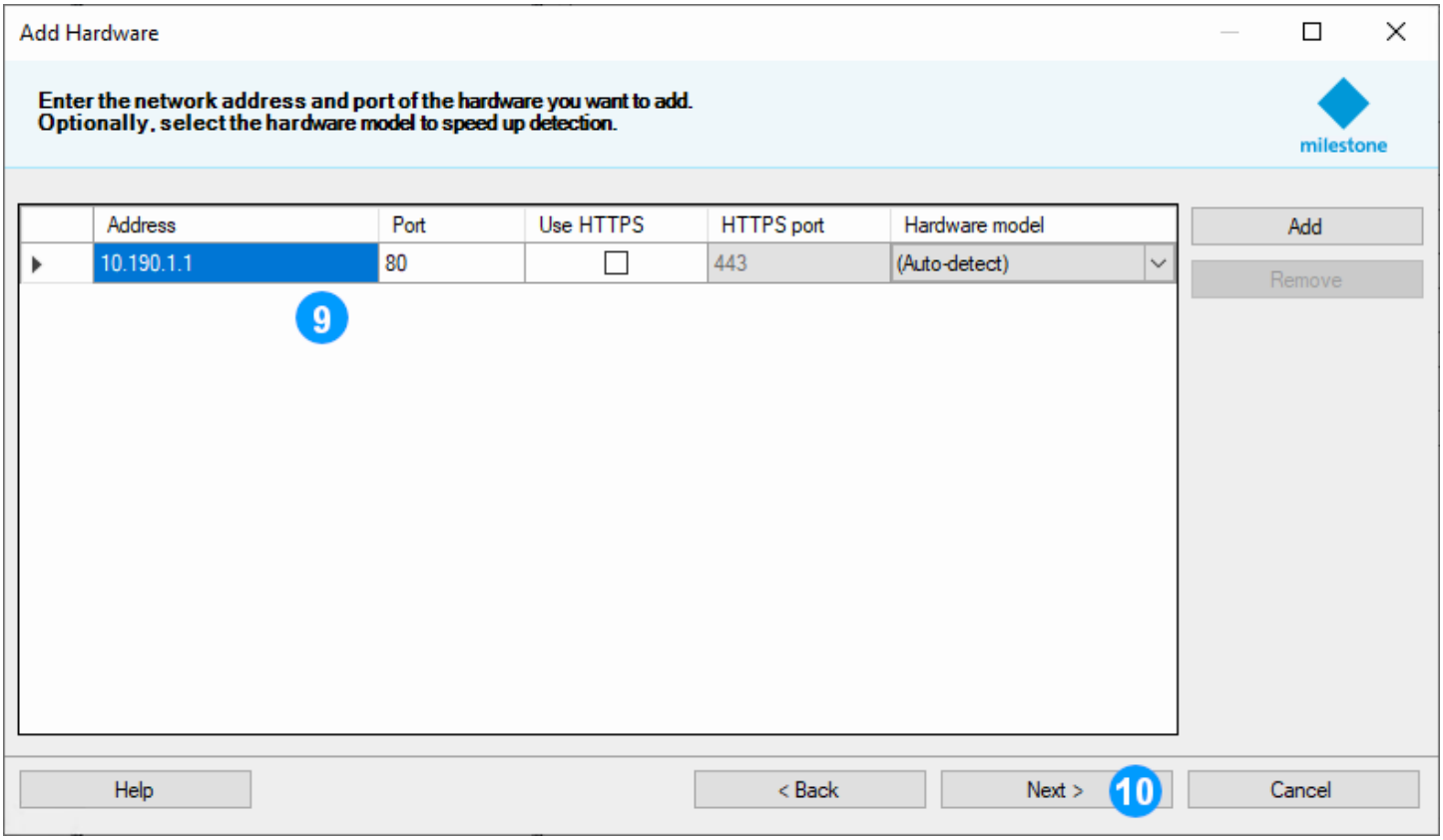
3. Sélectionnez **Manual**
4. Cliquez sur **Next**



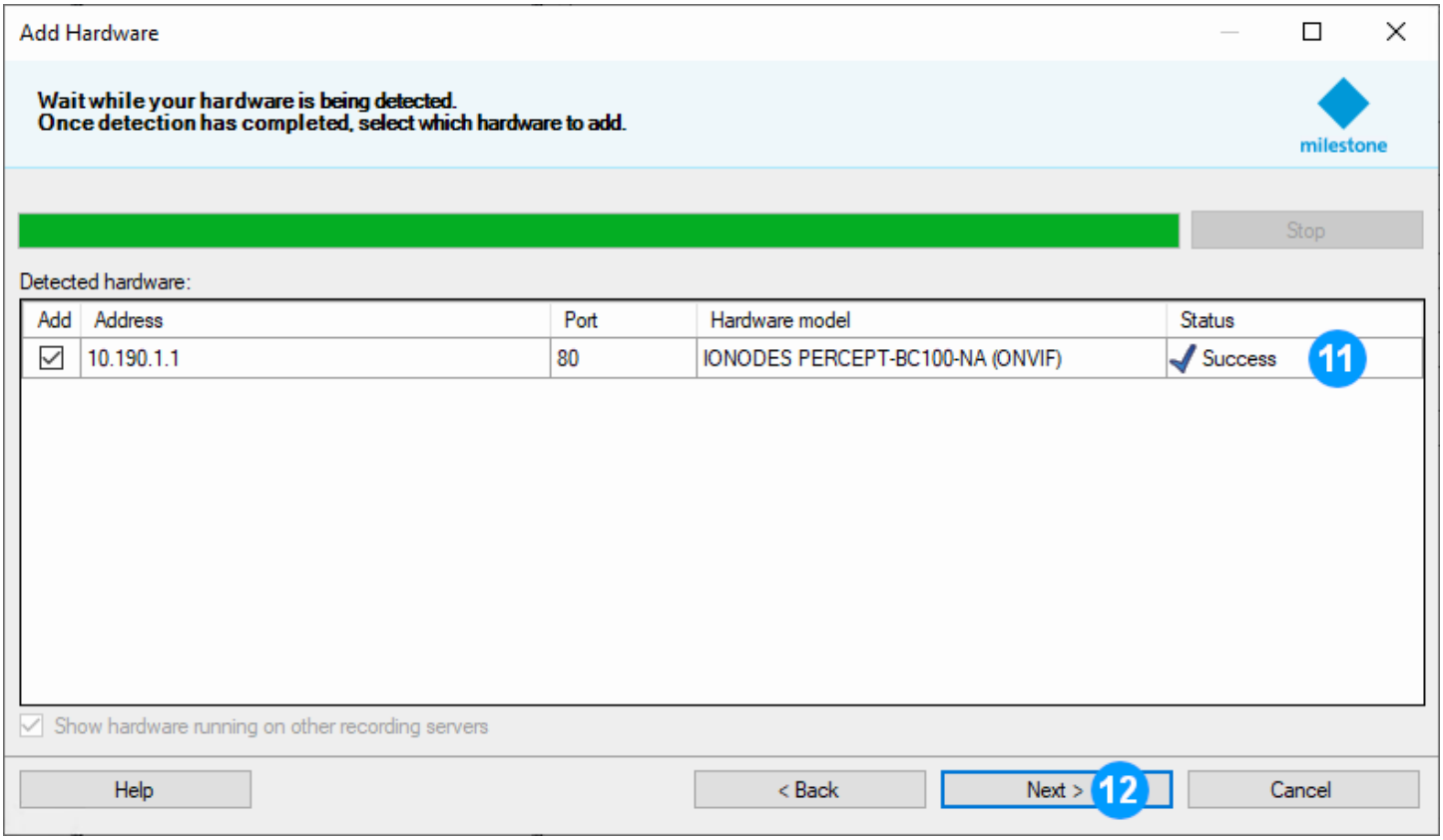
5. Si les informations d'identification de la caméra d'intervention PERCEPT n'existent pas déjà, sélectionnez **Add** pour créer un nouvel utilisateur pour se connecter à la caméra d'intervention, sinon sélectionnez les informations d'identification existantes (voir section 3.6)
6. Cliquez sur **Next**



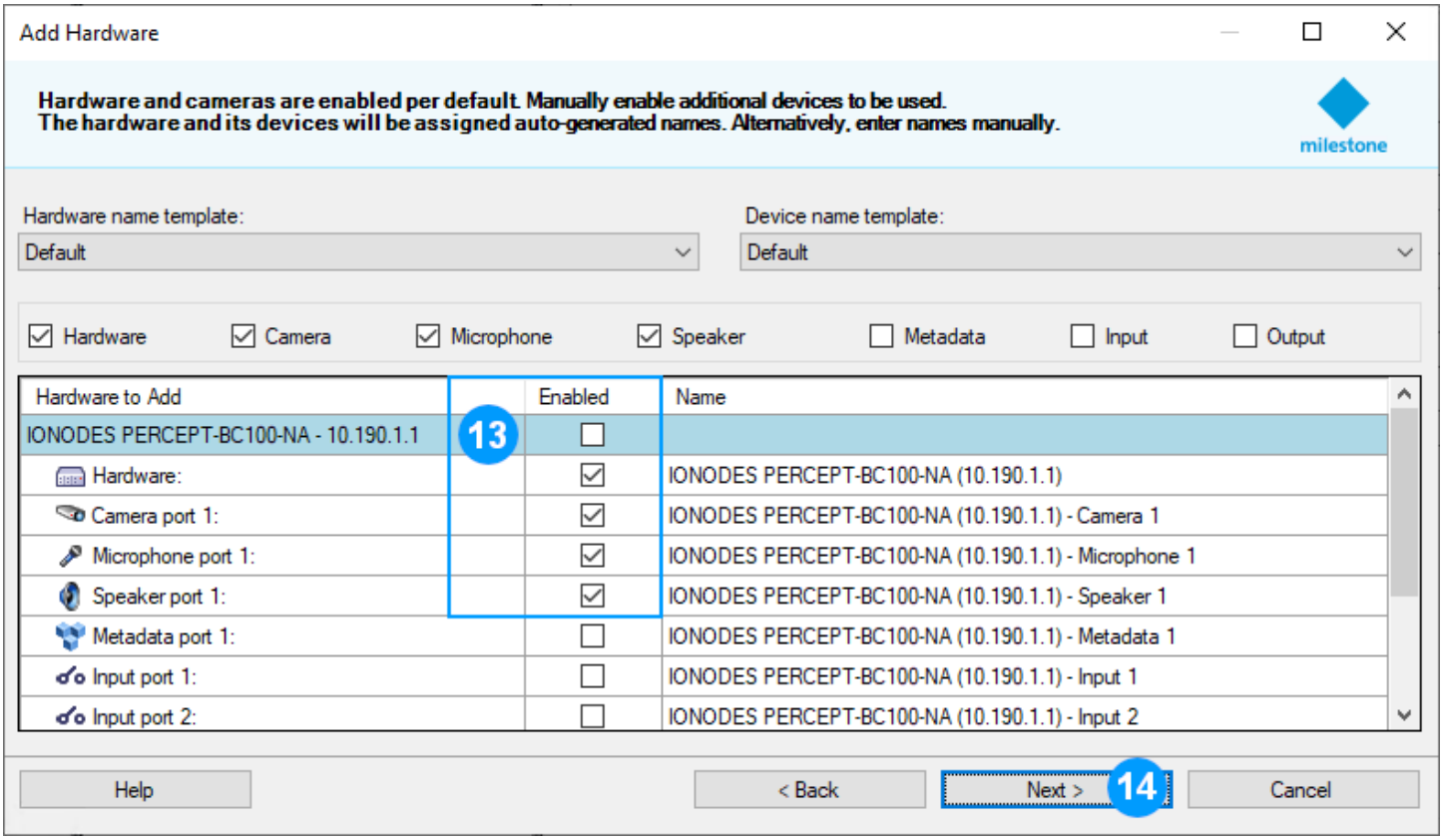
7. Sélectionnez **ONVIF** afin d'utiliser le pilote générique ONVIF pour ajouter la caméra d'intervention
8. Cliquez sur **Next**



9. Entrez l'adresse IP de la caméra d'intervention
10. Cliquez sur **Next**

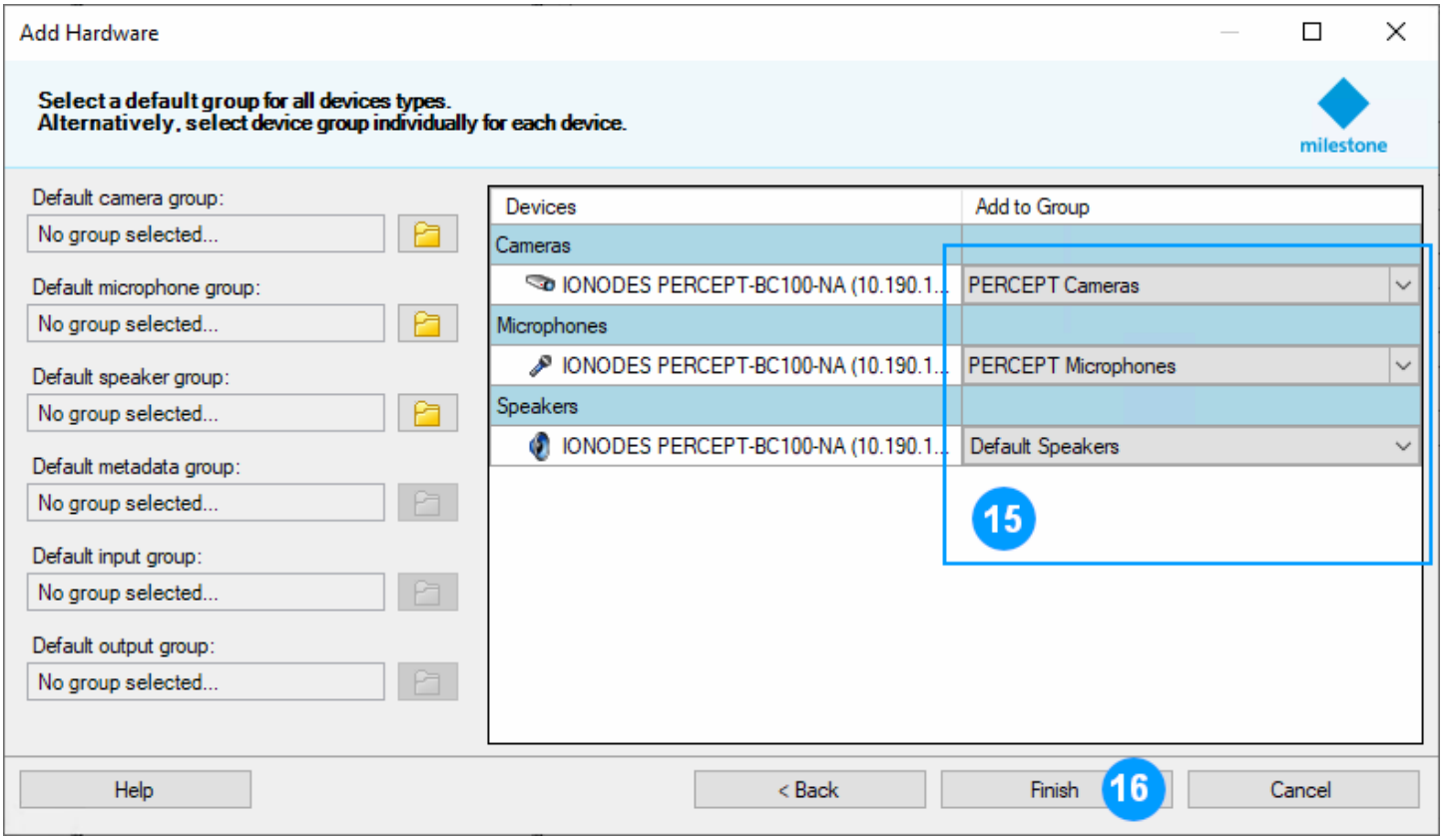


11. XProtect® affichera un message **Success** si l'adresse IP et les informations d'identification sont valides
12. Cliquez sur **Next**, XProtect® affichera un autre message de succès si la caméra d'intervention PERCEPT est ajoutée. Cliquez également sur **Next** dans cette boîte de dialogue.



13. Sélectionnez les sous-composants de l'appareil à activer dans XProtect®. Pour ce déploiement, activez les éléments suivants:
    a. Hardware
    b. Camera port 1
    c. Microphone port 1
    d. Speaker port 1
14. Cliquez sur **Next**

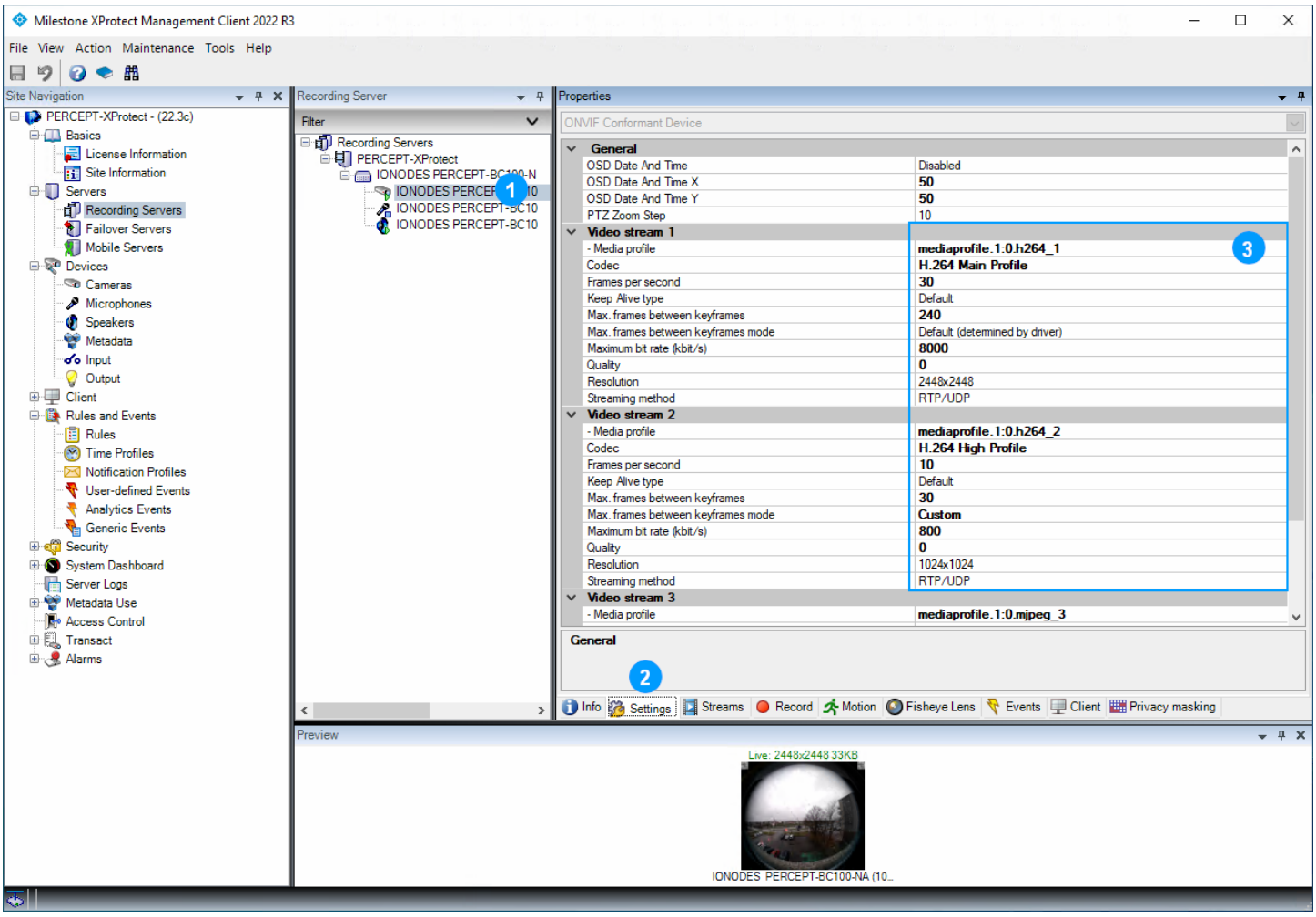
Note: Il est possible d'activer les ports d'entrée pour que XProtect® reçoive des événements lorsque le porteur appuie sur les boutons de la caméra d'intervention. Étant donné que la caméra d'intervention PERCEPT utilise une logique interne, telle qu'un même bouton avec une durée d'appui différente pour démarrer/arrêter l'enregistrement, il n'y a pas de corrélation univoque entre un bouton enfoncé et un comportement spécifique. Il est recommandé d'utiliser les événements ONVIF à la place.



15. Attribuez chaque sous-composant de la caméra d'intervention à un groupe d'appareils (un groupe peut être créé à ce stade s'il ne l'était pas déjà, conformément à la section 5.2). Les caméras d'intervention PERCEPT et leurs microphones doivent être affectés à des groupes spécifiques à PERCEPT. Les haut-parleurs peuvent être affectés au groupe par défaut car aucune règle spécifique n'est requise pour ceux-ci.
16. Cliquez sur **Finish**

6.1 Configurer la caméra

6.1.1 Paramètres

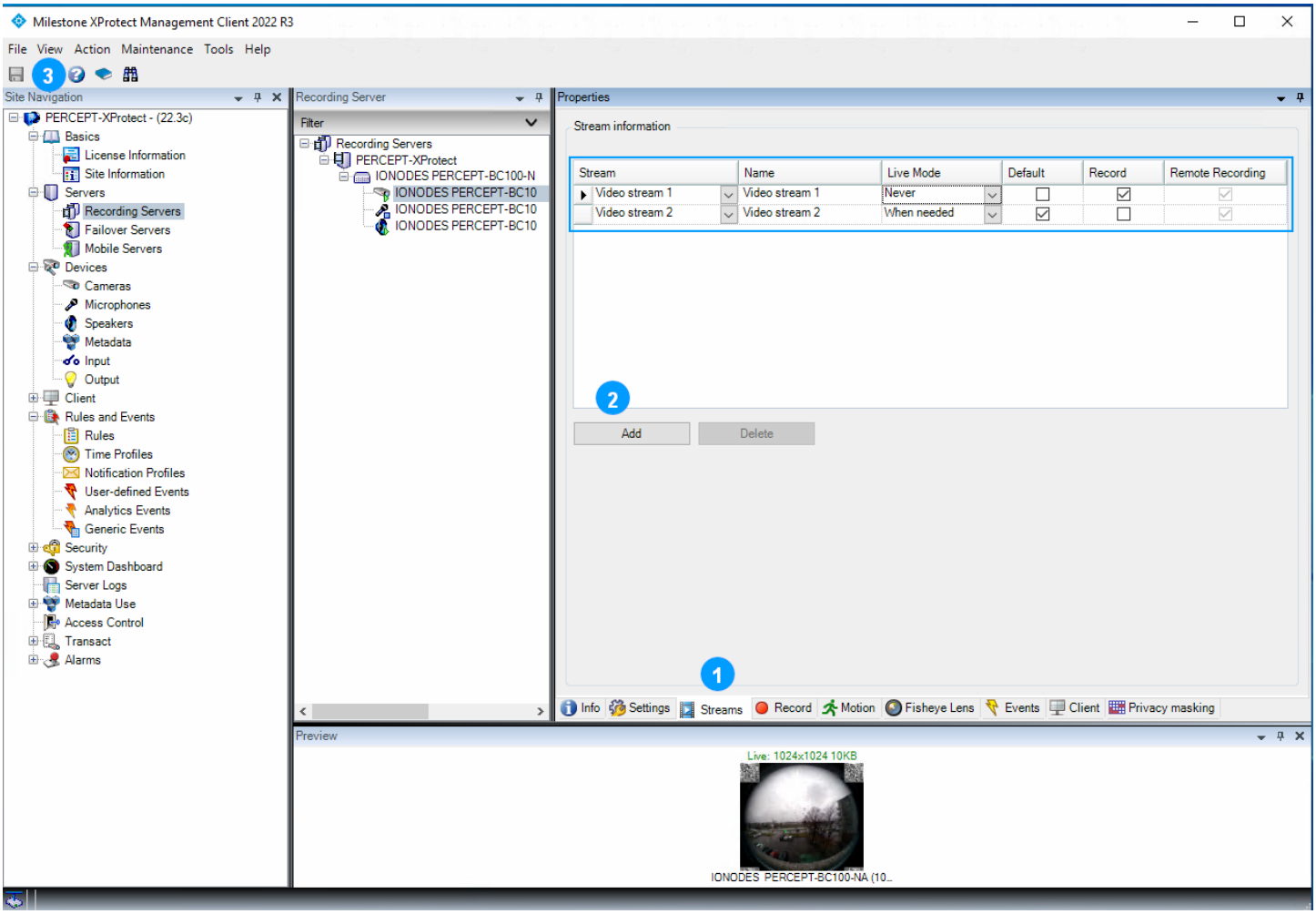


1. Développez la caméra PERCEPT nouvellement ajouté et sélectionnez sa **Camera 1**
2. Sélectionnez l'onglet **Settings**
3. Vérifiez que les paramètres **Video stream 1** et **2** correspondent à la configuration de la section 3.3.2. Une fois ajoutée dans XProtect®, toute modification doit être effectuée depuis XProtect® Management Client; pas à partir de l'interface utilisateur Web de la caméra d'intervention PERCEPT.

Note: La méthode de diffusion (**Streaming method**) aura un impact sur la vidéo en direct lorsque la caméra d'intervention est connectée via des réseaux LTE ou Wi-Fi à faible puissance. Les pertes de paquets entraînent des artefacts vidéo sur RTP/UDP, tandis qu'avec les protocoles basés sur

TCP (RTP/RTSP/TCP ou RTP/RTSP/http/TCP), elles entraînent une fréquence d'images irrégulière (jitter). Il est recommandé d'utiliser RTP/UDP.

6.1.2 Flux



1. Sélectionnez l'onglet **Streams**
2. Seul le flux 1 est activé par défaut. Ajoutez (**Add**) un flux vidéo puis configurez comme suit :
    a. **Video stream 1:**
        i. **Live Mode: Never**
        ii. **Default: Unchecked**
        iii. **Record: Checked**

b. Video stream 2:

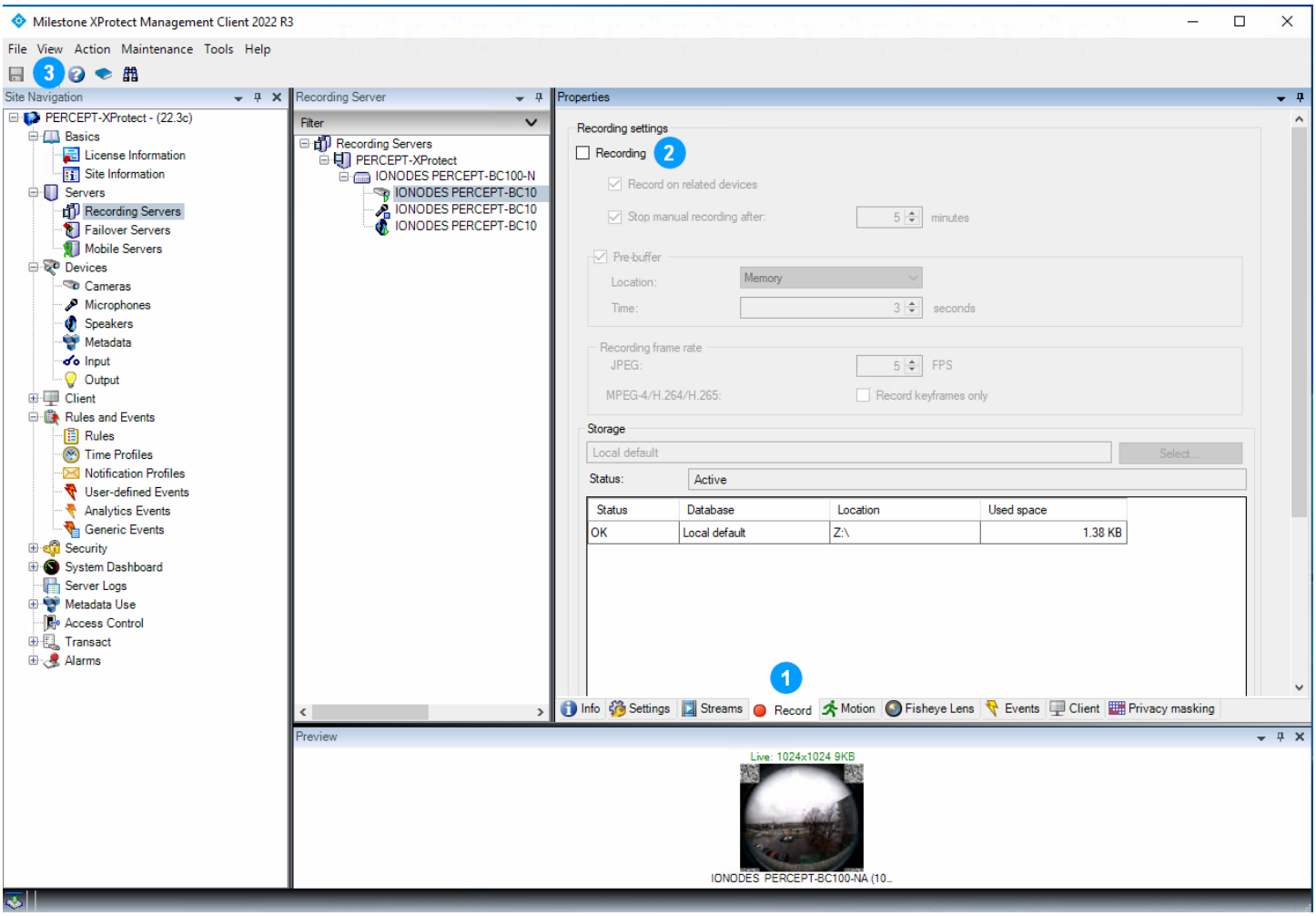
i. **Live Mode: When needed**

ii. **Default: Checked**

iii. **Record: Unchecked**

3. Cliquez sur **Save**

6.1.3 Enregistrement

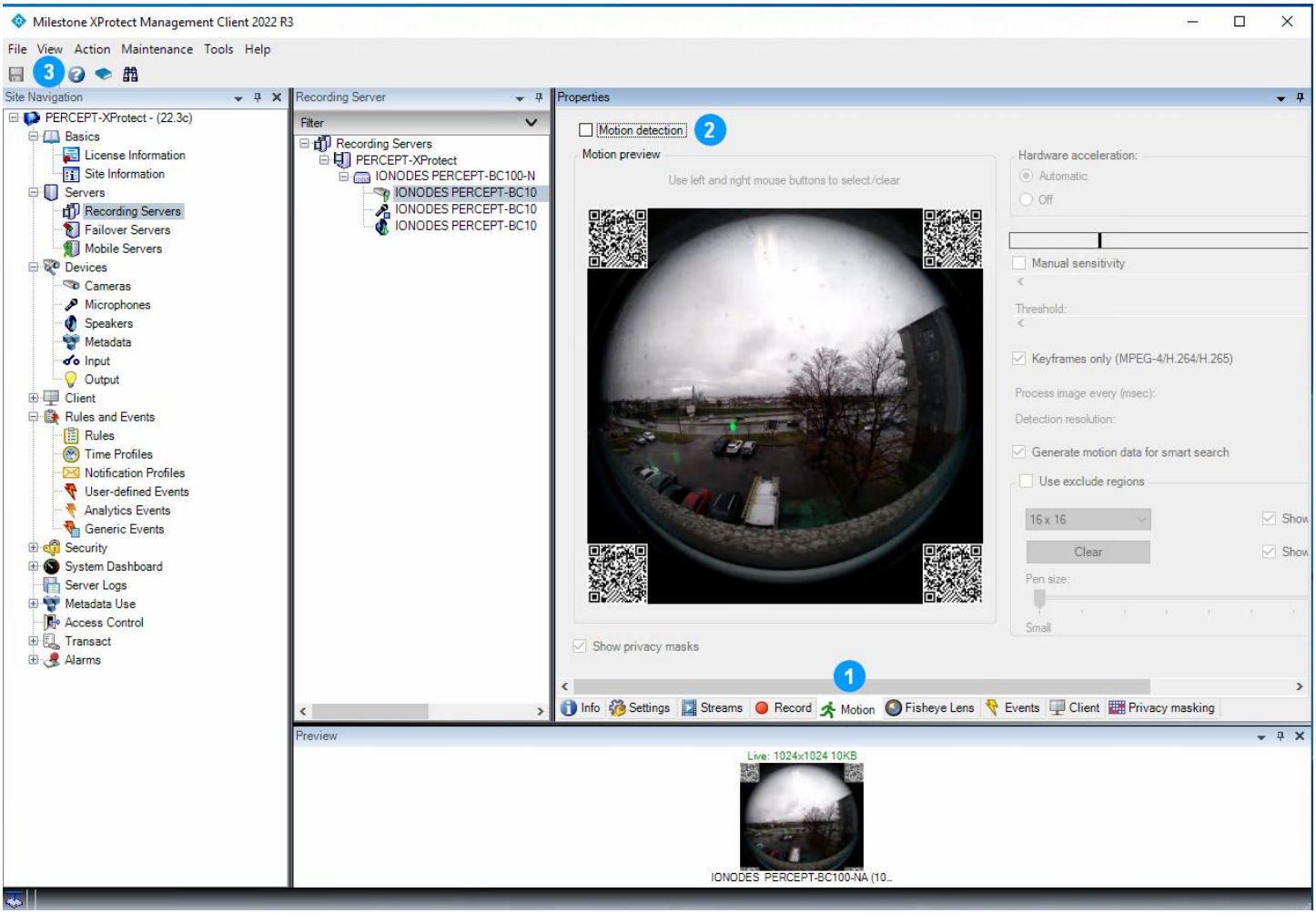


1. Sélectionnez l'onglet **Record**
2. Décochez **Recording**
3. Cliquez sur **Save**

Note: Si l'enregistrement est activé, XProtect® se connecte en permanence au flux vidéo configuré pour l'enregistrement (flux à haut débit), ce qui entraîne une utilisation élevée de la bande

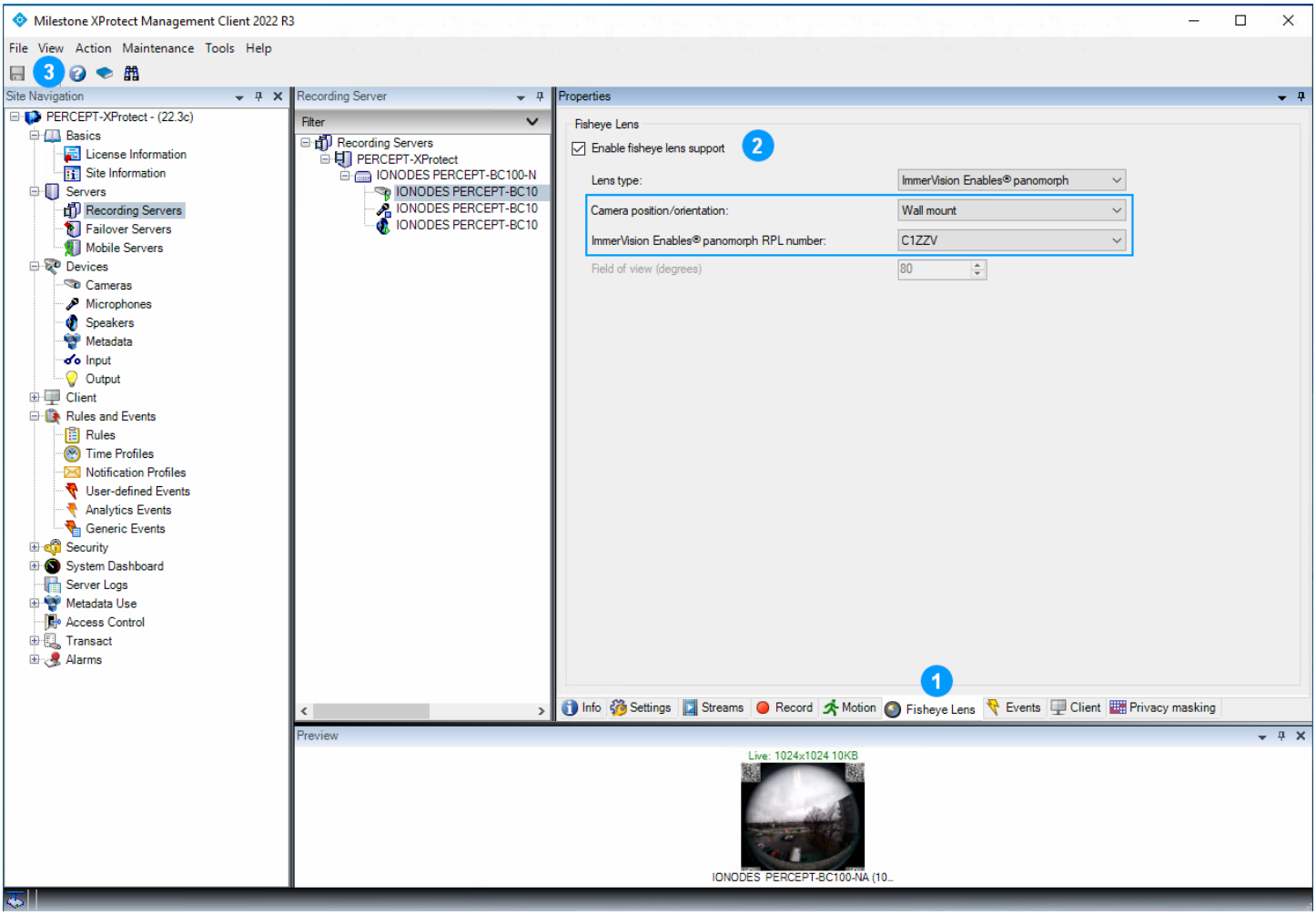
passante et des données. Le déploiement recommandé consiste à désactiver les fonctions d'enregistrement intégrées et à créer des règles pour le transfert automatique des clips enregistrés sur mémoire interne des caméras d'intervention PERCEPT.

6.1.4 Mouvement



1. Sélectionnez l'onglet **Motion**
2. Décochez **Motion detection**
3. Cliquez sur **Save**

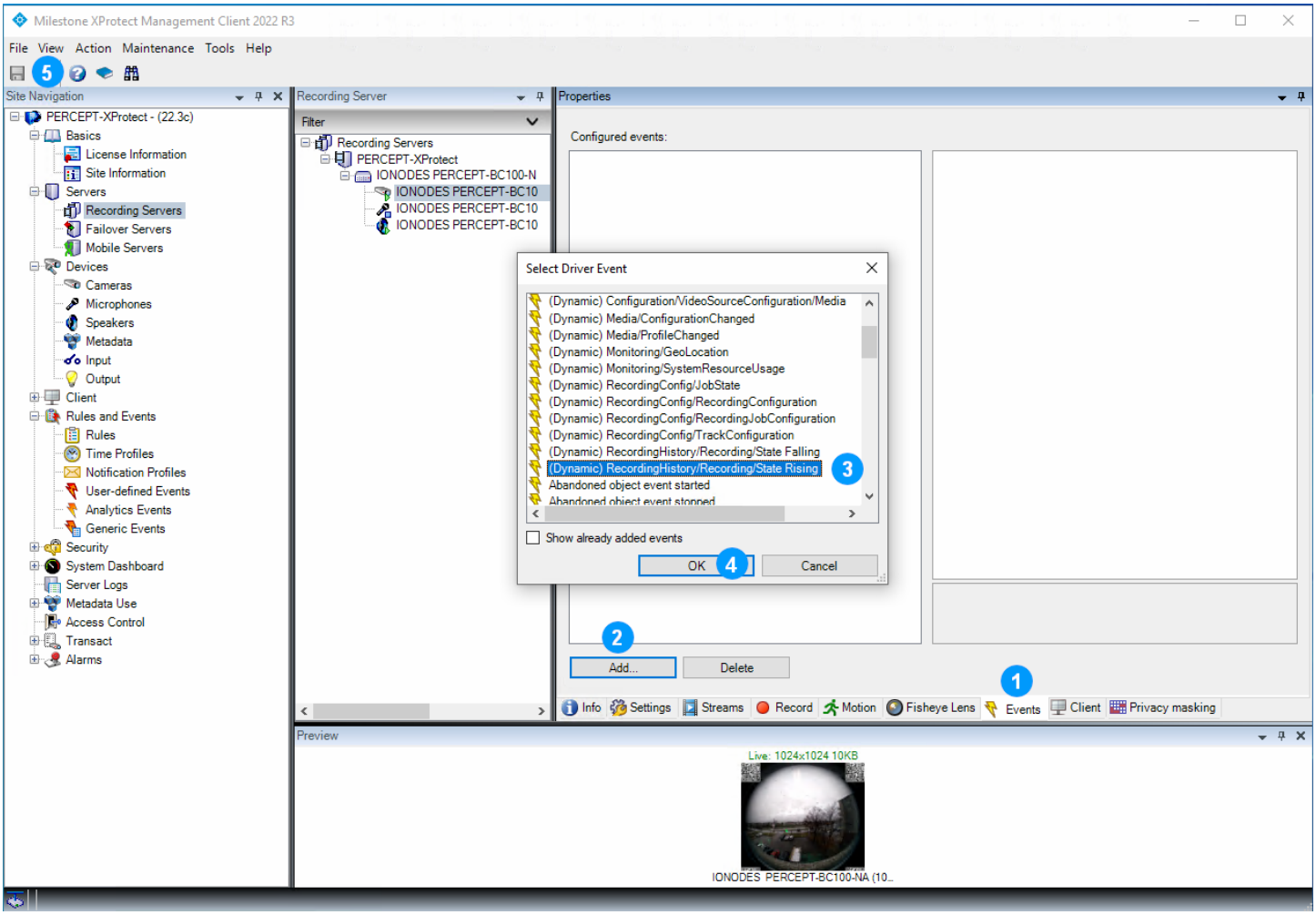
6.1.5 Lentille Panomorphe



1. Sélectionnez l'onglet **Fisheye Lens**
2. Cochez **Enable fisheye lens support** et configurez comme suit:
    a. **Camera position/orientation: Wall mount**
    b. **Immervision Enables® Panomorph RPL number: C1ZZV**
3. Cliquez sur **Save**

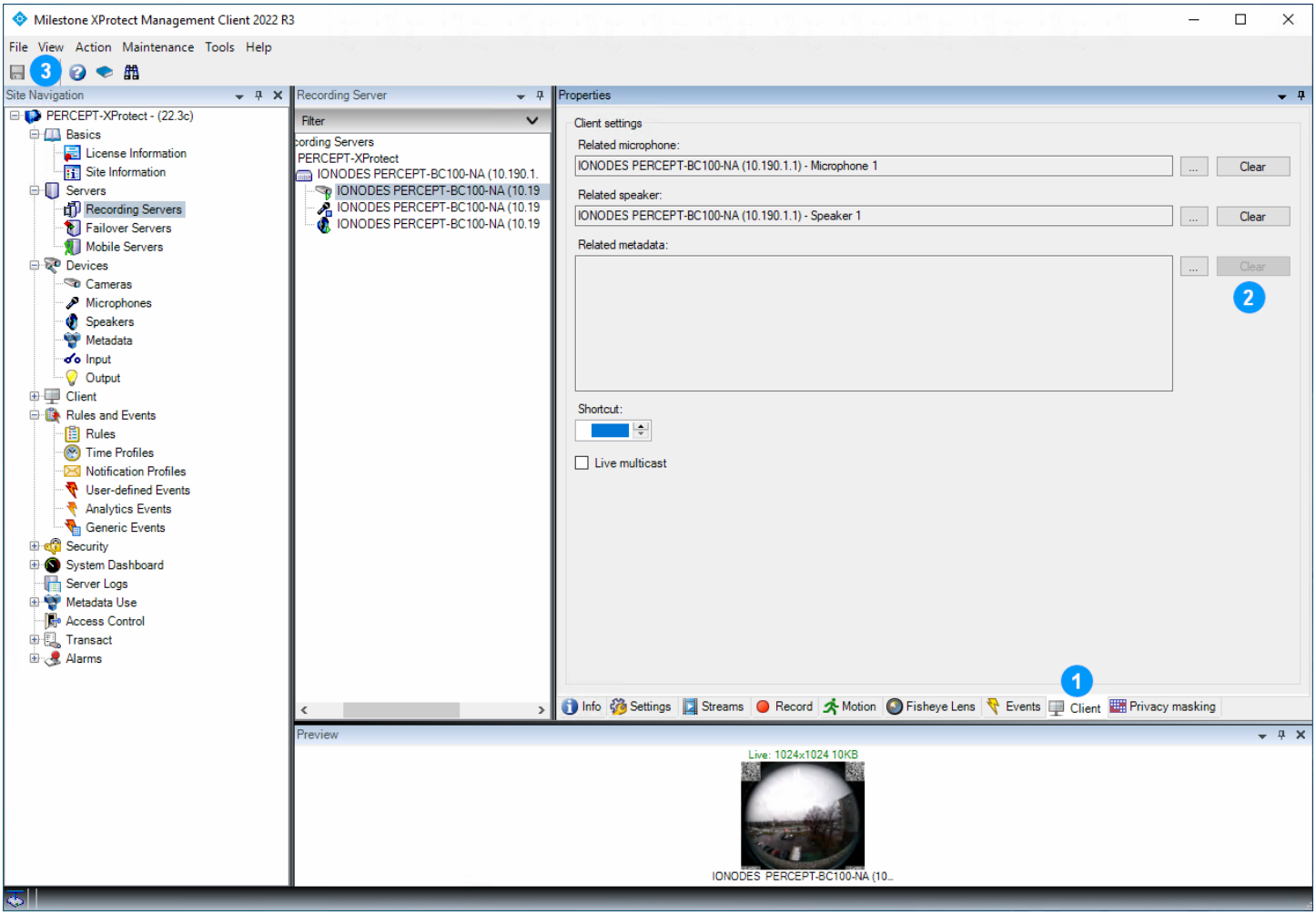
Avis: Certaines versions et Service Packs de XProtect® Smart Client peuvent rencontrer des plantages en basculant entre Live et Playback, ou lorsque les flux vidéo pré/post-enregistrement sont à des résolutions différentes avec des caméras à lentille panomorphe. Installez les derniers service packs et/ou désactivez panomorphe si vous rencontrez ce problème et qu'aucun service pack n'est disponible pour la version et l'édition spécifiques utilisées.

6.1.6 Événements



1. Sélectionnez l'onglet **Events**
2. Cliquez sur **Add**
3. Dans le menu contextuel, faites défiler pour sélectionner **(Dynamic) RecordingHistory/Recording/State Rising**
4. Cliquez sur **OK**
5. Cliquez sur **Save**

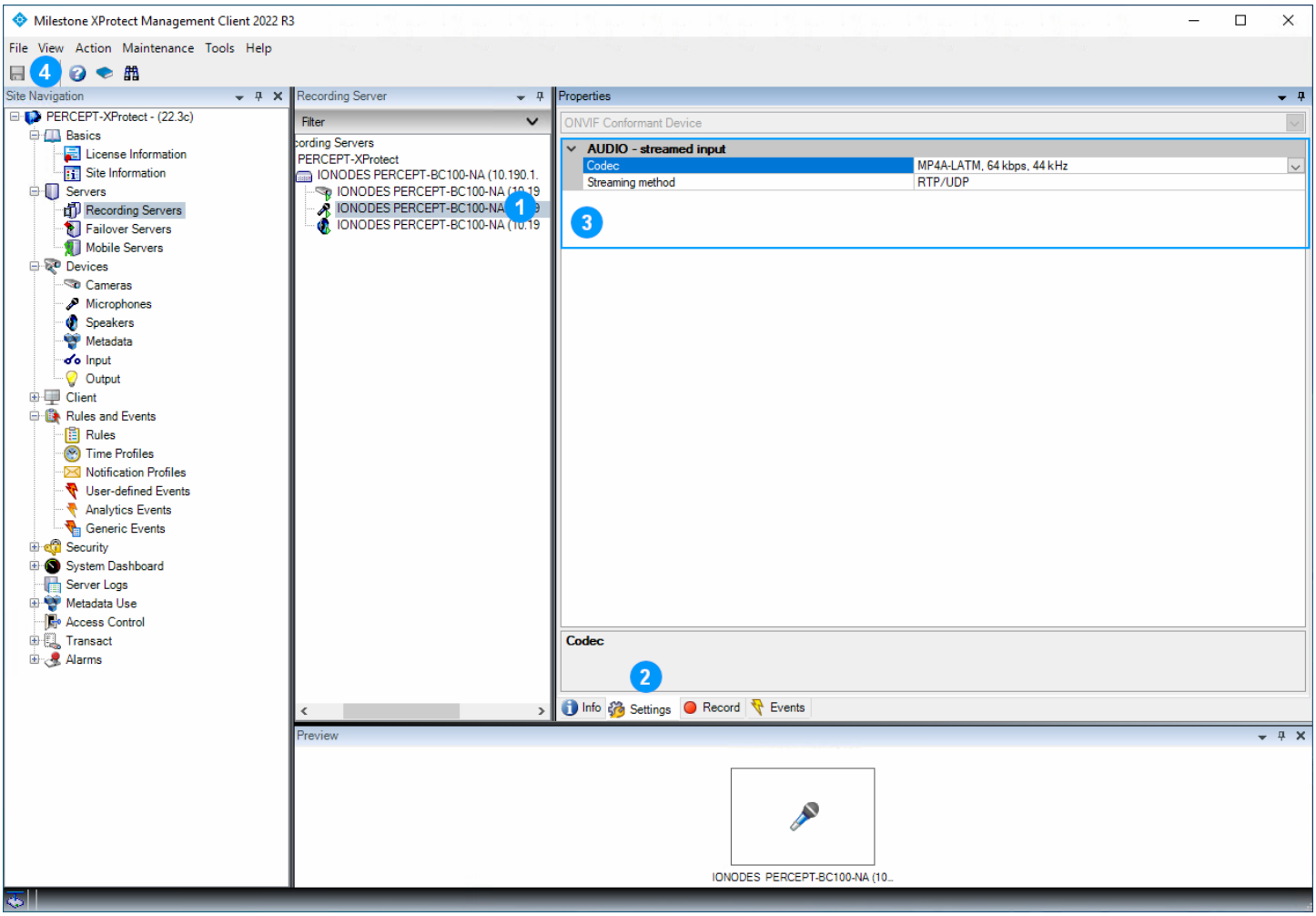
6.1.7 Client



1. Sélectionnez l'onglet **Client**
2. Dans la section **Related metadata**, cliquez sur **Clear** (indiqué déjà effacé ci-dessus)
3. Cliquez sur **Save**

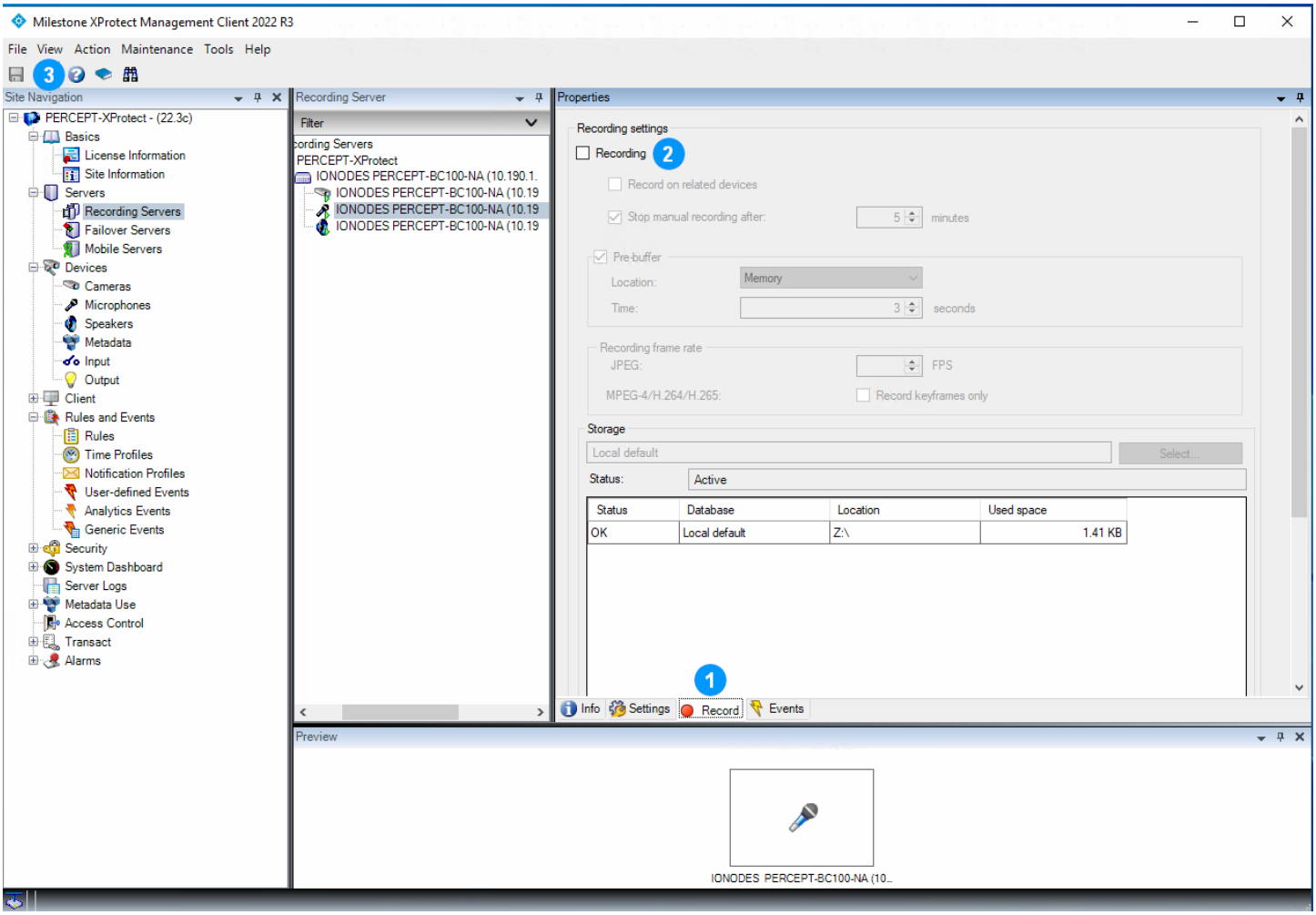
6.2 Configurer le microphone

6.2.1 Paramètres



1. Sélectionnez le **Microphone 1** de la caméra d'intervention PERCEPT
2. Sélectionnez l'onglet **Settings**
3. Vérifiez les paramètres audio. Les paramètres par défaut de XProtect® sont convenables; AAC (MP4A-LATM) avec débit relativement faible à 32 kHz ou 44 kHz est recommandé (64 kpbs, 44 kHz illustré ci-dessus). La méthode de streaming (**Streaming method)** recommandée est **RTP/UDP**
4. Cliquez sur **Save** si les paramètres ont été modifiés

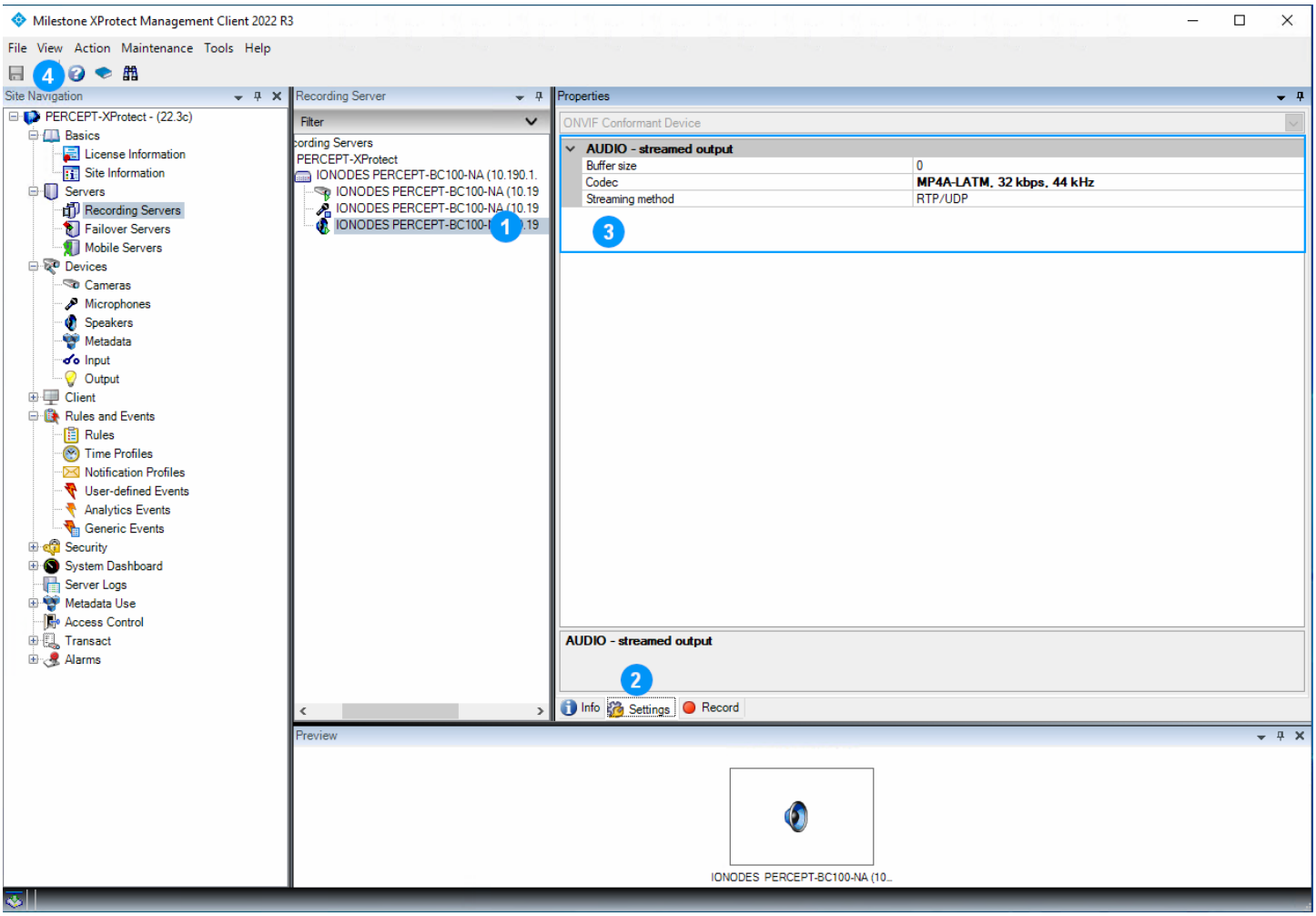
6.2.2 Enregistrement



1. Sélectionnez l'onglet **Record**
2. Décochez **Recording**
3. Cliquez sur **Save**

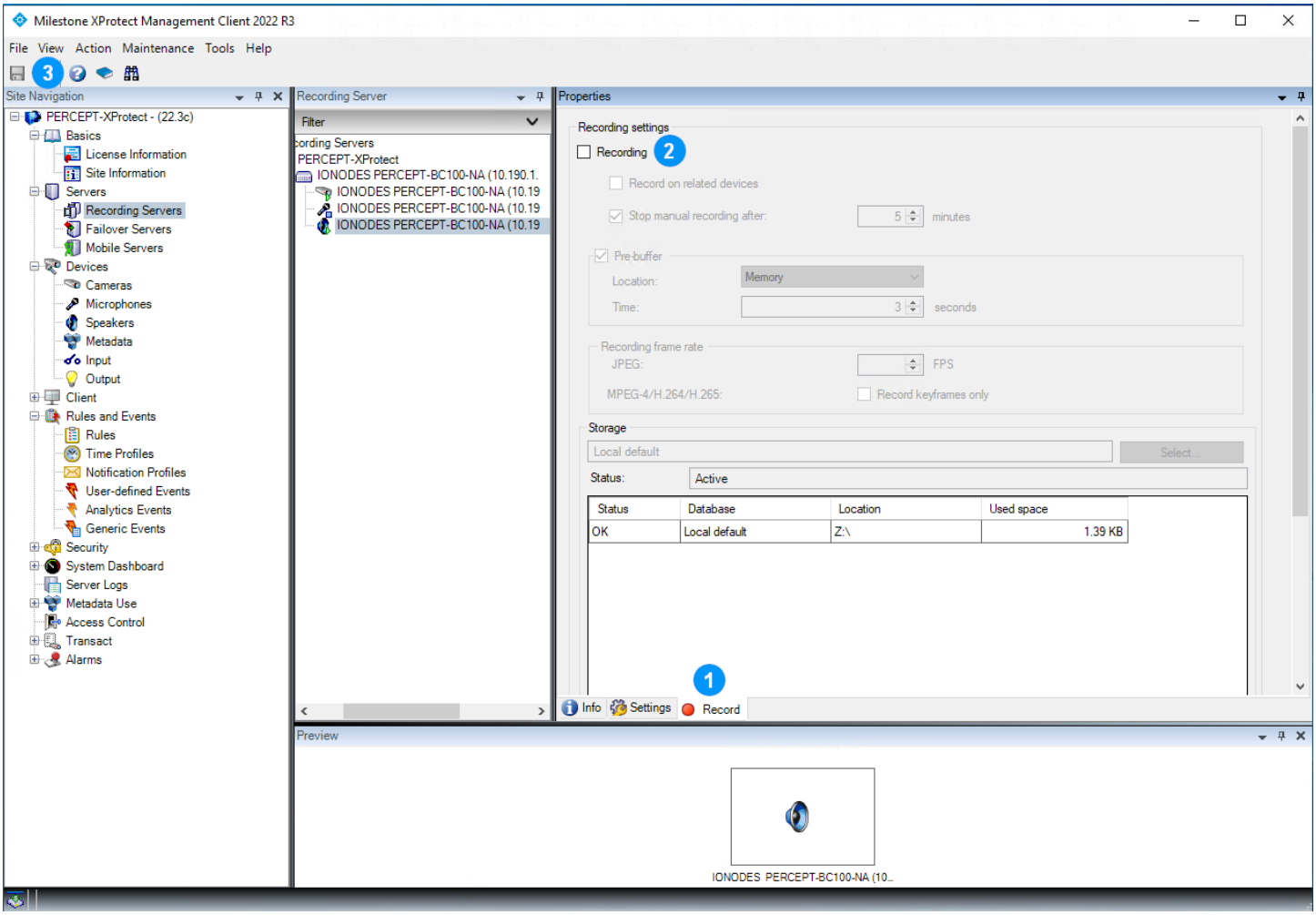
6.3 Configurer le haut-parleur

6.3.1 Paramètres



1. Sélectionnez le **Speaker 1** de la caméra d'intervention PERCEPT
2. Sélectionnez l'onglet **Settings**
3. Configurez les paramètres audio. AAC (MP4A-LATM) avec débit relativement faible à 32 kHz ou 44 kHz est recommandé (32 kpbs, 44 kHz illustré ci-dessus). La méthode de streaming (**Streaming method)** recommandée est **RTP/UDP**
4. Cliquez sur **Save**

6.3.2 Enregistrement



1. Sélectionnez l'onglet **Record**
2. Décochez **Recording**
3. Cliquez sur **Save**

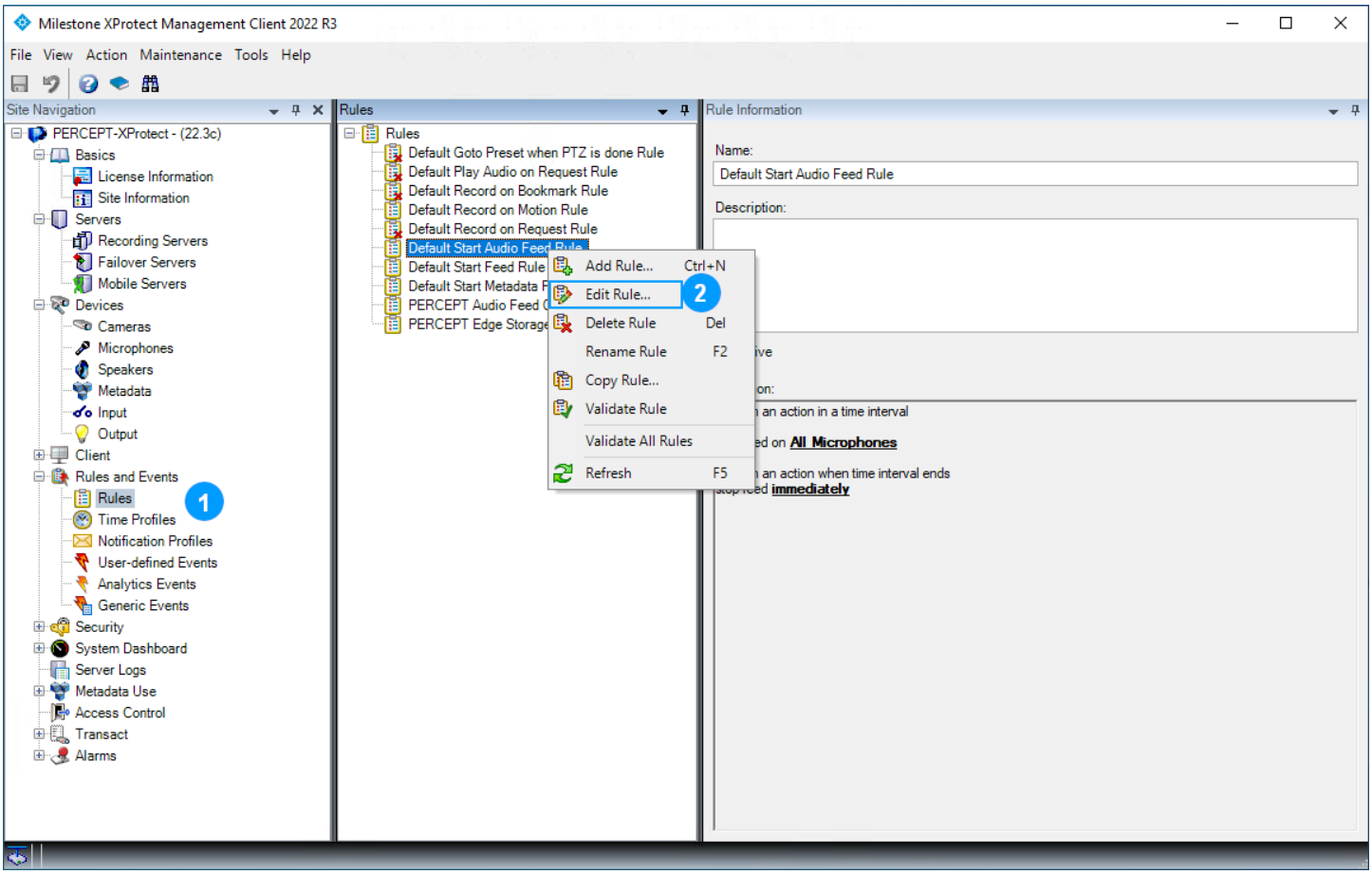
7 Configuration des règles XProtect®

La configuration effectuée dans la section précédente garantit que XProtect® ne se connectera qu'au flux vidéo en direct à faible débit sur demande; jamais au flux d'enregistrement à haut débit. Le flux du haut-parleur n'est activé que lorsqu'un utilisateur de XProtect® Smart ou Web Client appuie sur le bouton *push-to-talk*.

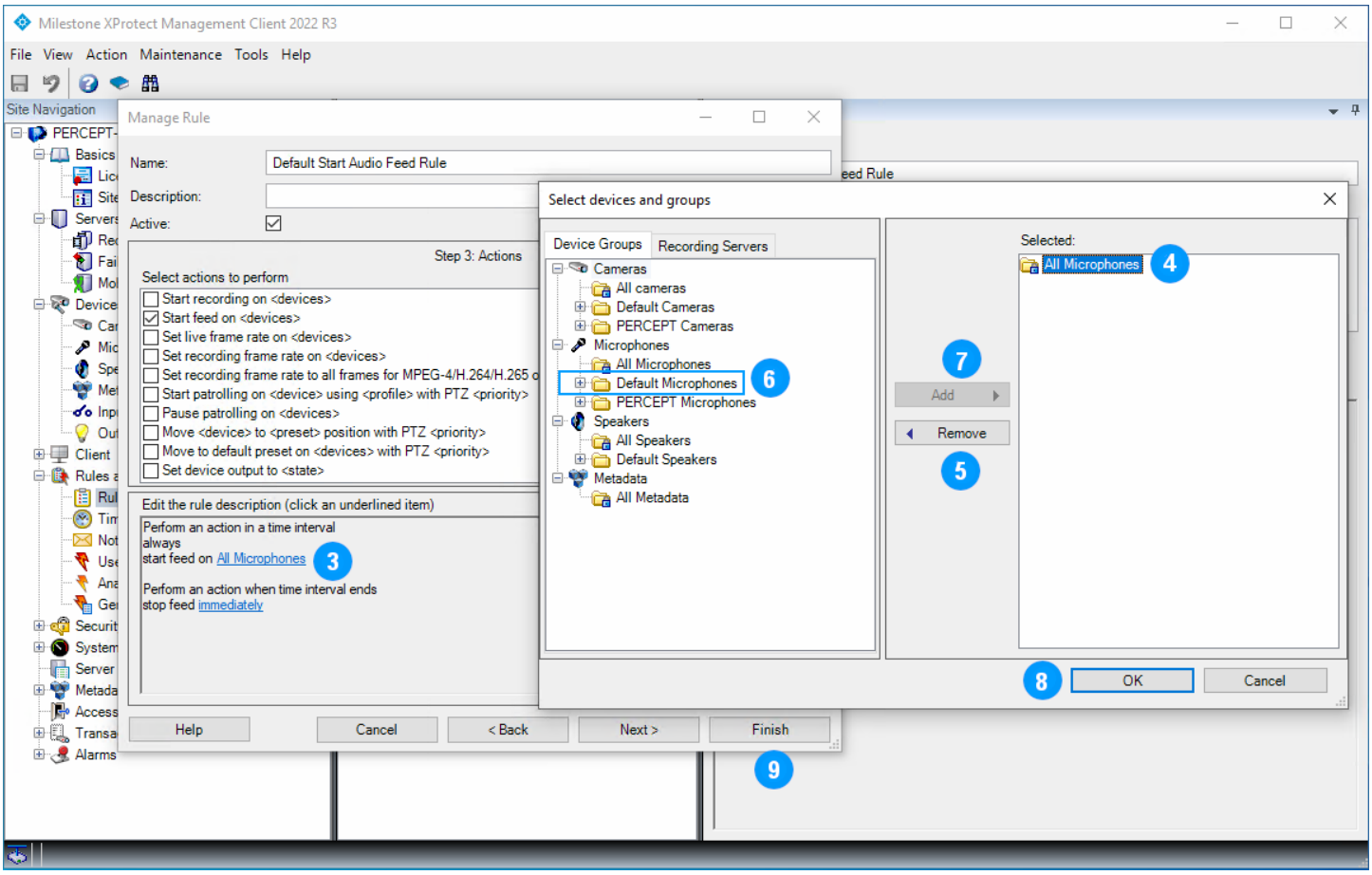
Les règles XProtect® par défaut connectent toujours le flux du microphone. Ces règles doivent être modifiées pour démarrer le microphone des caméras d'intervention PERCEPT uniquement sur demande, ainsi que pour adapter les transferts de clips sauvegardés sur mémoire interne.

7.1.1 Règle de démarrage par défaut des flux audio

Modifiez cette règle pour exclure le microphone des caméras d'intervention PERCEPT.



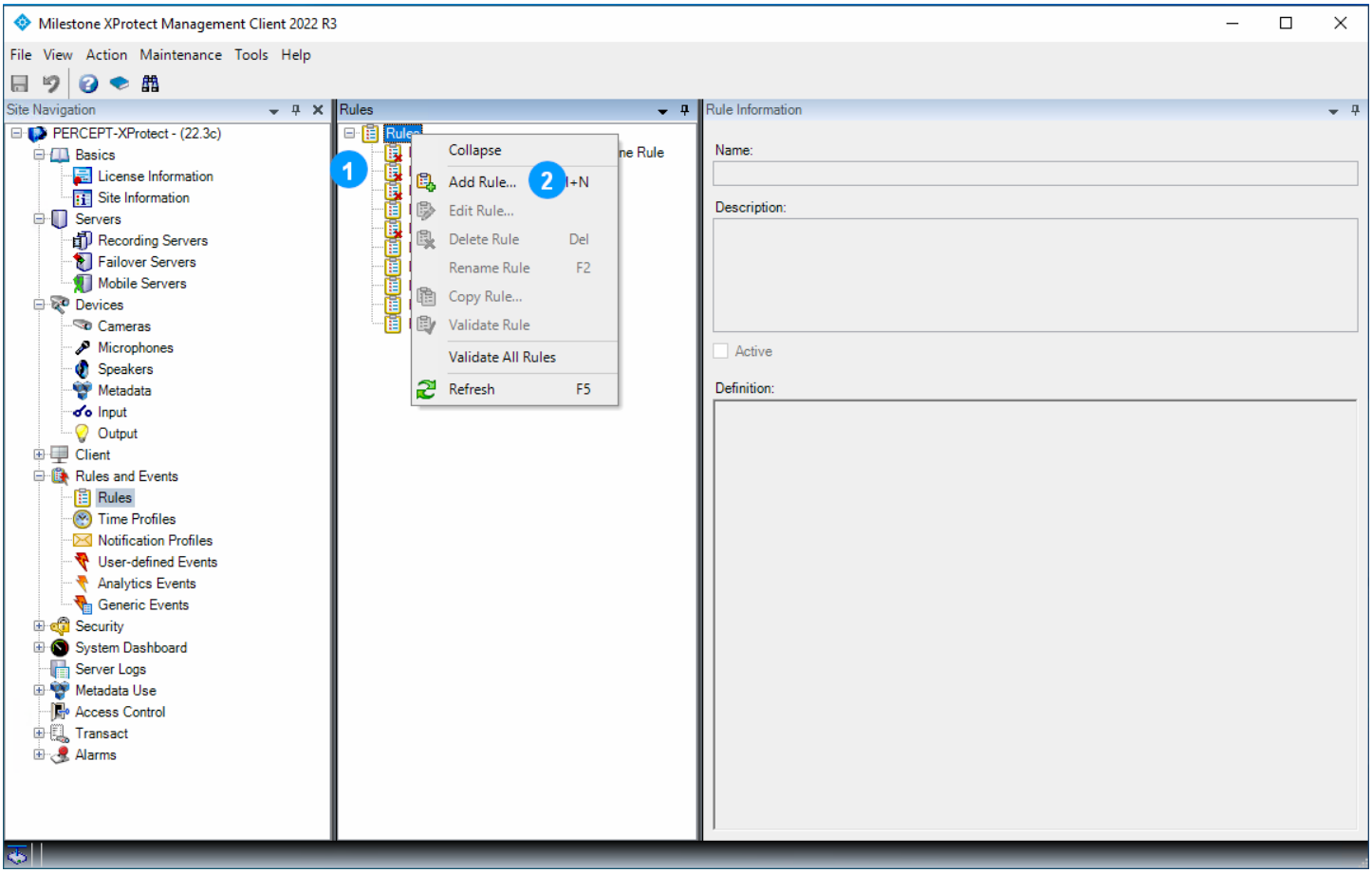
1. Dans le volet gauche de **XProtect® Management Client**, sélectionnez **Rules and Events** > **Rules**
2. Dans le volet central **Rules**, cliquez avec le bouton droit sur **Default Start Audio Feed Rule** et sélectionnez **Edit Rule...**



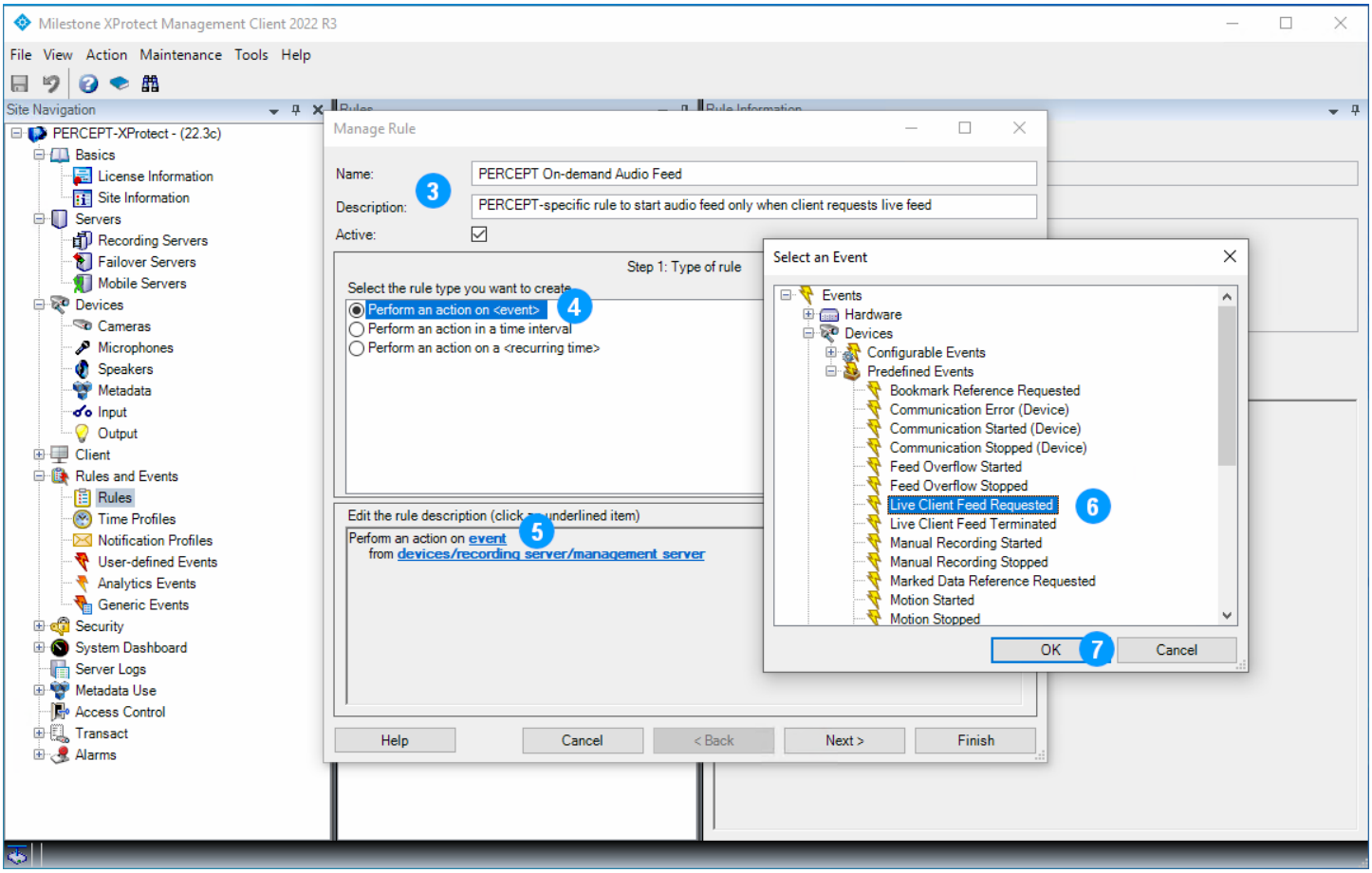
3. À l'étape **Step 3: Actions** (la boîte de dialogue **Manage Rule** s'ouvre à cette étape), dans le volet inférieur '**Edit the rule description**', cliquez sur **All Microphones**
4. Dans le volet **Selected** de la boîte de dialogue **Select devices and groups**, sélectionnez **All Microphones**
5. Cliquez sur **Remove**
6. Dans le volet de gauche, sous l'onglet **Device Groups**, sélectionnez **Default Microphones**
7. Cliquez sur **Add**
8. Cliquez sur **OK**
9. Cliquez sur **Finish**

Note: Sur un déploiement existant où différents groupes de microphones existent déjà, la règle modifiée peut différer. L'intention est de conserver les règles existantes pour tous les microphones autre que caméra d'intervention PERCEPT et d'en créer une distincte pour lesdites caméras d'intervention (dans la sous-section suivante).

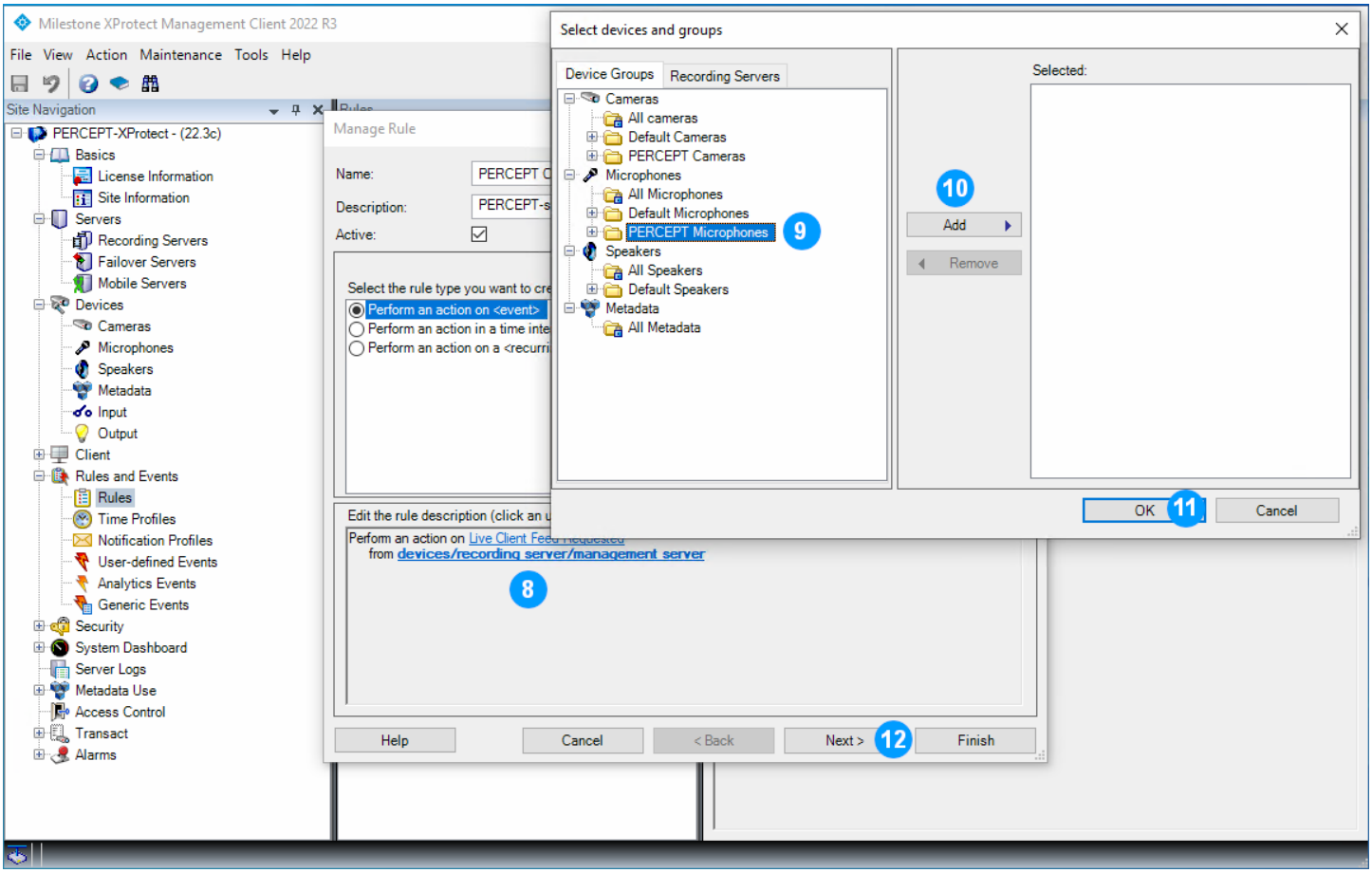
7.1.2 Flux audio sur demande PERCEPT



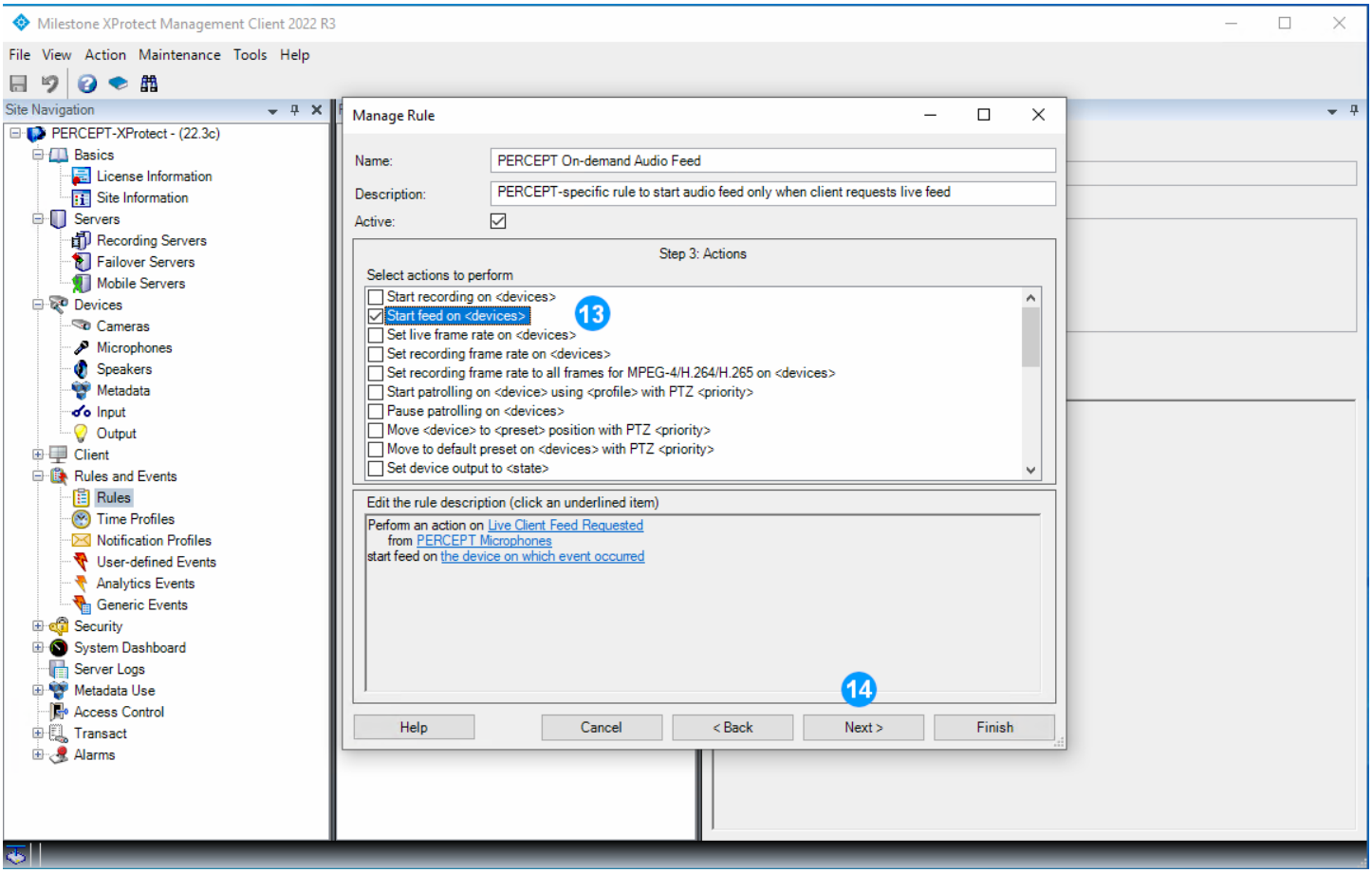
1. Dans le volet central **Rules**, cliquez avec le bouton droit sur **Rules**
2. Sélectionnez **Add Rule...** dans le menu contextuel



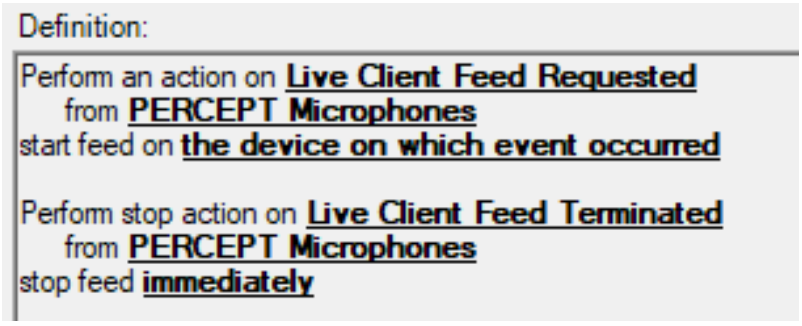
3. Dans la boîte de dialogue **Manage Rule**, entrez un nom (**Name)** pour cette règle et une description facultative
4. À l'étape **Step 1: Type of rule** (volet central), sélectionnez **Perform an action on <event>**
5. Dans **Edit the rule description** (volet inférieur), cliquez sur **event**
6. Dans la boîte de dialogue contextuelle **Select an Event**, sélectionnez **Devices > Predefined Events > Live Client Feed Requested**
7. Cliquez sur **OK**



8. Dans **Edit the rule description** (volet inférieur), cliquez sur **devices/recording server/management server**
9. Dans le volet gauche de la boîte de dialogue **Select devices and groups**, sous l'onglet **Device Groups**, sélectionnez **PERCEPT Microphones**
10. Cliquez sur **Add**
11. Cliquez sur **OK**
12. Cliquez sur **Next**, puis à l'étape **Step 2: Conditions** cliquez à nouveau sur **Next** pour passer à l'étape **Step 3: Actions**

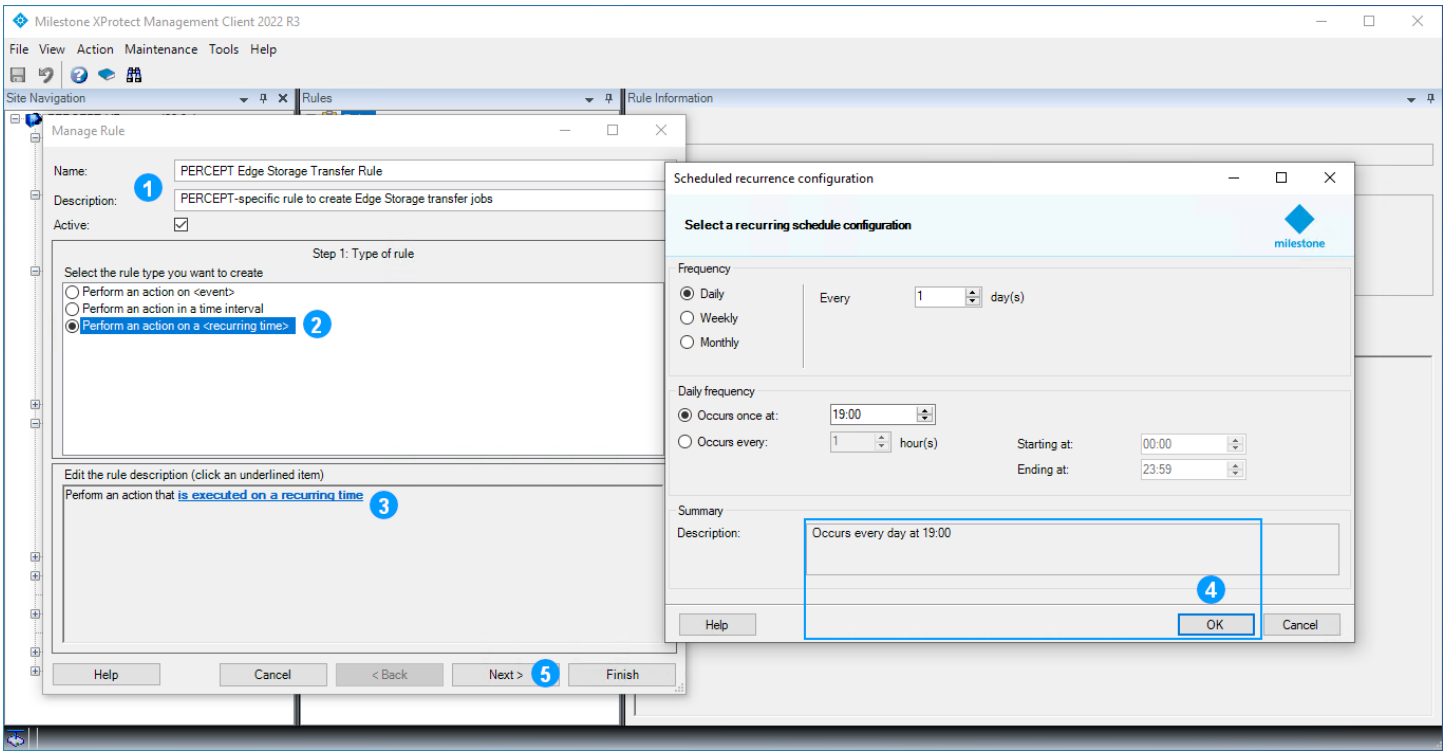


13. À partir de l'étape **Step 3: Actions** (volet central), cochez **Start feed on <devices>**. Le '**start feed on the device on which event occurred**' par défaut qui sera créé est correct, pas besoin de le modifier
14. Cliquez sur **Next**, puis à l'étape **Step 4: Stop criteria**, cliquez à nouveau sur **Next**. Enfin, à l'étape **Step 5: Stop actions**, cliquez sur **Finish**. Les valeurs par défaut créées par XProtect® pour ces étapes sont correctes, aucune modification n'est nécessaire.
15. La définition de règle résultante devrait ressembler à :

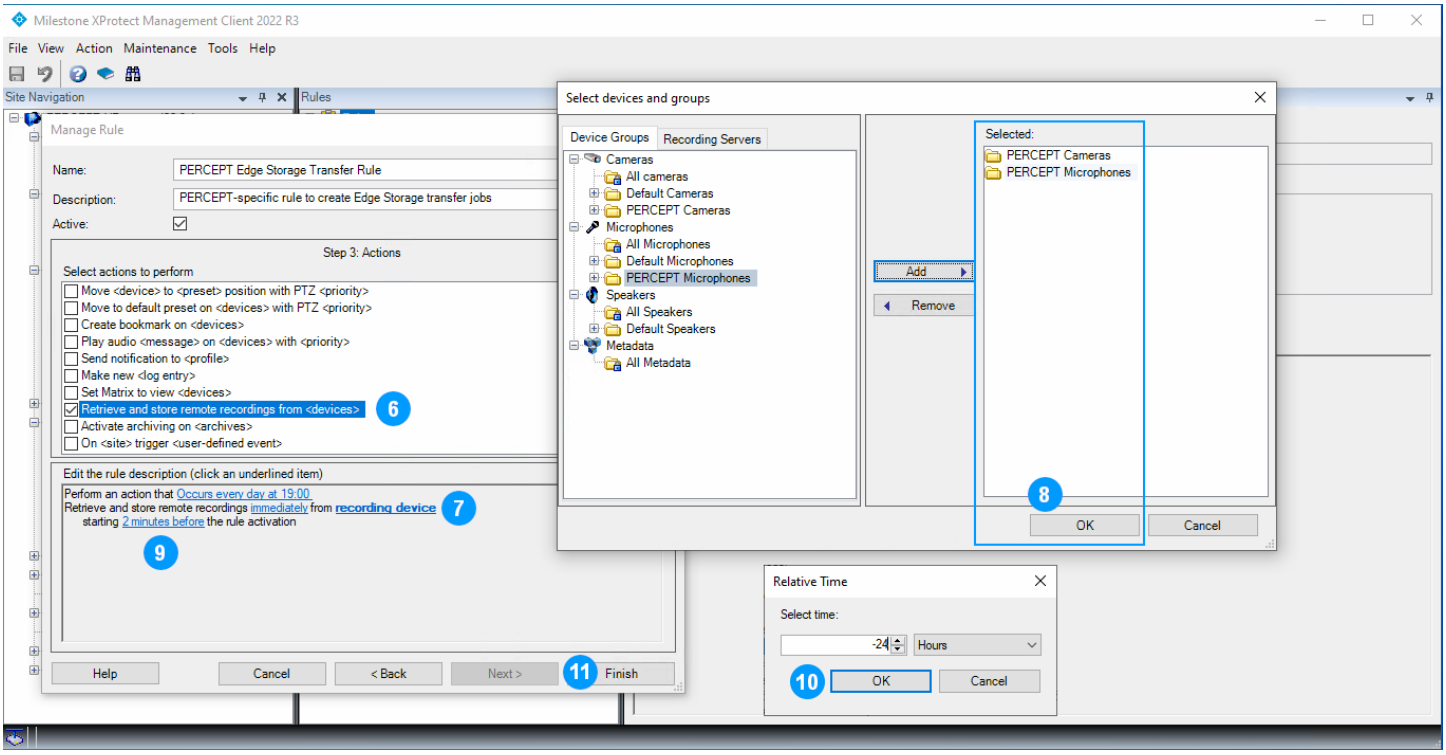


7.1.3 Règle de transfert de clips de la mémoire interne

Ajoutez une nouvelle règle (reportez-vous aux 2 premières étapes de la sous-section précédente).

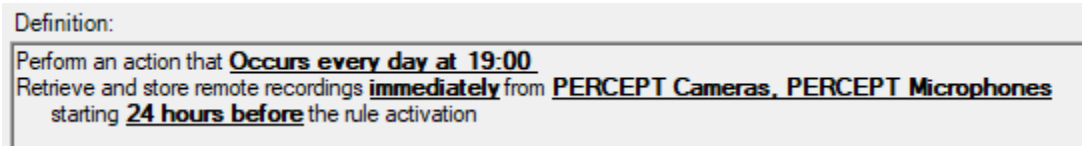


1. Dans la boîte de dialogue **Manage Rule**, entrez un nom (**Name**) pour cette règle et une description facultative
2. À l'étape **Step 1: Type of rule** (volet central), sélectionnez **Perform an action on a <recurring time>**
3. Dans **Edit the rule description** (volet du bas), cliquez sur **is executed on a recurring time**
4. Dans la fenêtre **Scheduled recurrence configuration**, définissez la récurrence et cliquez sur **OK**
5. Cliquez sur **Next**, puis à l'étape **Step 2: Conditions** cliquez à nouveau sur **Next** pour passer à l'étape **Step 3: Actions**



6. À l'étape **Step 3: Actions** (volet central), sélectionnez **Retrieve and store remote recordings from <devices>**
7. Dans **Edit the rule description** (volet inférieur), cliquez sur **recording devices**
8. Dans la boîte de dialogue **Select devices and groups**, ajoutez **PERCEPT Cameras** et **PERCEPT Microphones** (groupes d'appareils) à la liste **Selected**, puis cliquez sur **OK**
9. Dans **Edit the rule description** (volet inférieur), cliquez sur **2 minutes before**
10. Dans la fenêtre **Relative Time**, sélectionnez **-24 hours** et cliquez sur **OK**
11. Cliquez sur **Finish**

La définition de règle résultante devrait ressembler à:



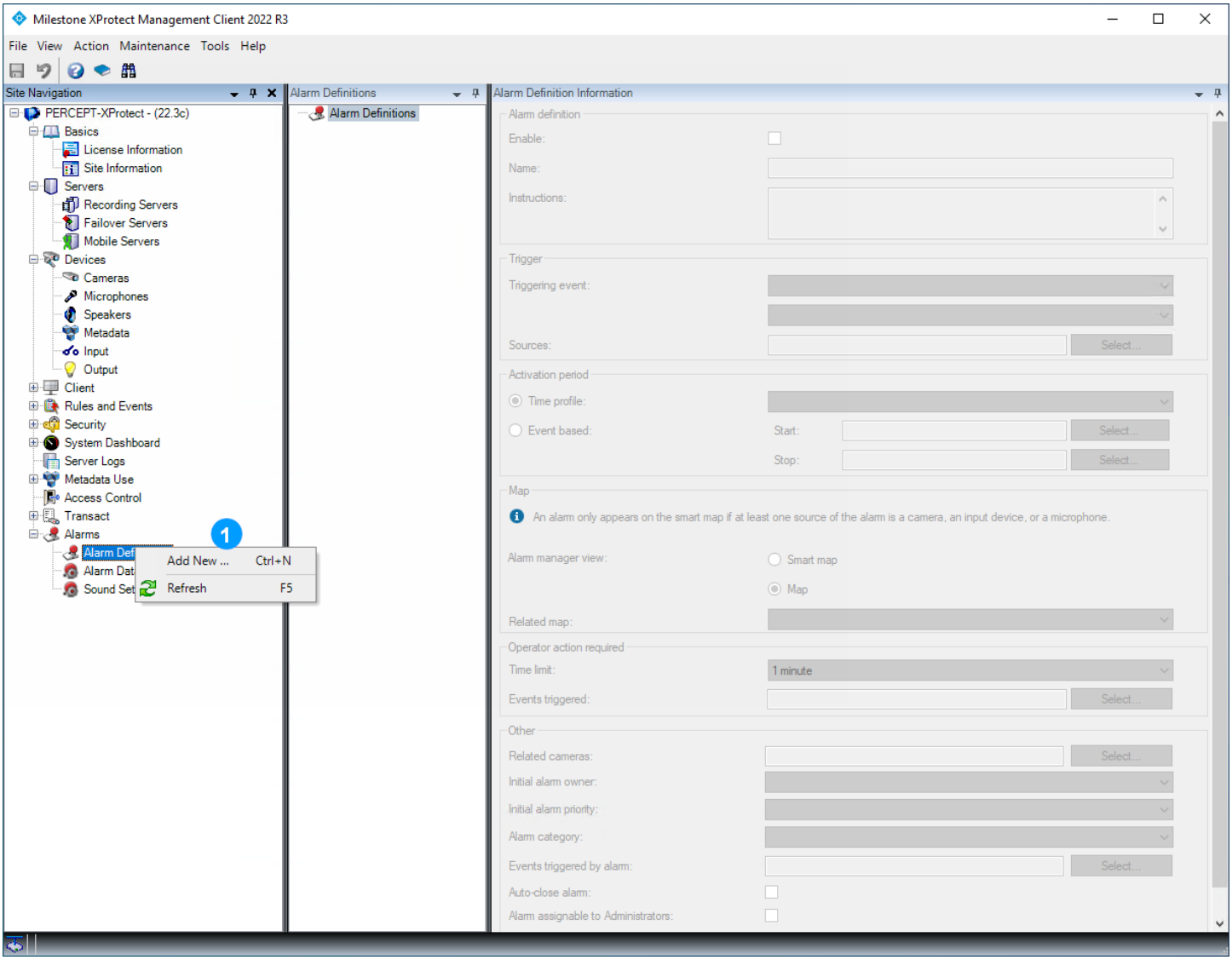
Pour optimiser l'utilisation des données, la récurrence doit être adaptée au calendrier prévu d'utilisation des caméras d'intervention PERCEPT. La règle indiquée ci-dessus créera une tâche de transfert tous les soirs à 19h00, demandant que les 24 heures précédentes d'enregistrements audio-vidéo soient téléchargées à partir de toutes les caméras d'intervention PERCEPT pour être stockées sur le serveur d'enregistrement XProtect®.

Lorsqu'une tâche de transfert est créée, *XProtect® Edge Storage Manager* tentera de l'exécuter toutes les 15 secondes jusqu'à ce qu'il réussisse. Une caméra éteinte, déconnectée ou connectée à une interface réseau configurée pour bloquer le transfert lecture entraînera l'échec et une nouvelle tentative 15 secondes plus tard.

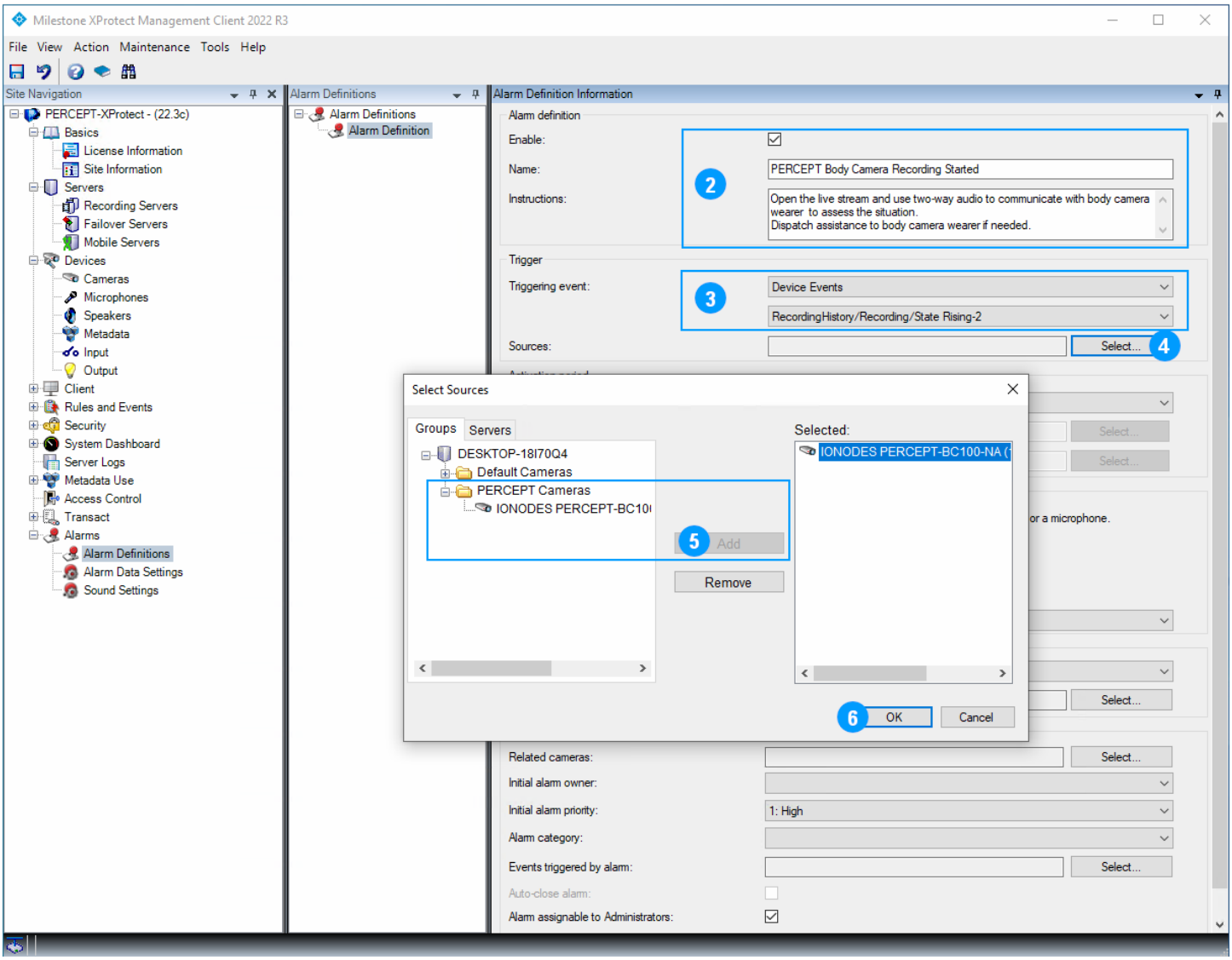
La configuration d'utilisation des données LTE définie dans la section 3.2.2 bloque les tentatives de récupération d'enregistrements lorsque connecté au réseau cellulaire. La configuration recommandée dans la section 3.2.3 pour le déploiement à l'aide de la ou des stations d'accueil PERCEPT bloque également ces transferts via Wi-Fi. Ces tentatives bloquées consommeront tout de même quelques kilo-octets de données chacune. Il est recommandé de programmer la récurrence à un moment où on s’attend que les caméras d’intervention PERCEPT soient ancrées.

8 Événement à alarme

Cette section décrit un cas d'utilisation simple pour les événements générés par la caméra d'intervention PERCEPT. En suivant la configuration de la section 6.1.6, XProtect® s'abonne à un événement déclenché chaque fois que le porteur de la caméra d'intervention démarre un enregistrement. Cet événement peut être utilisé pour déclencher des alarmes dans XProtect® Smart et Web Clients.



1. Dans le volet gauche de **XProtect® Management Client**, cliquez avec le bouton droit sur **Alarms** > **Alarm Definitions** et sélectionnez **Add New...** dans le menu contextuel

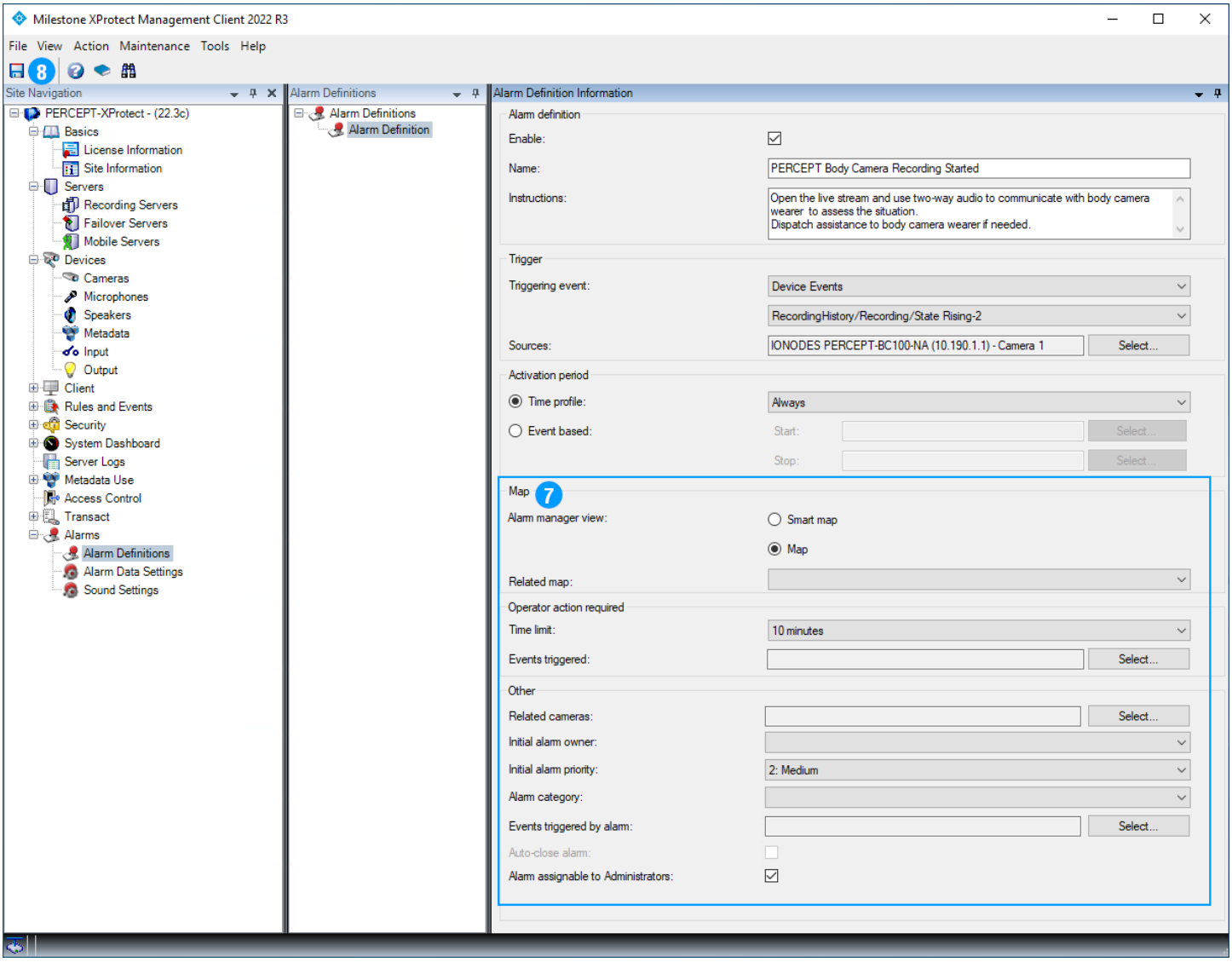


2. Activez (**Enable)** la nouvelle définition d'alarme, définissez un nom et fournissez des instructions (facultatives)
3. Utilisez les menus déroulants pour définir **Triggering event**. L'événement défini dans la section 6.1.6 est un **Device Event** nommé **RecordingHistory/Recording/State Rising**

Note: Dans la capture d'écran ci-dessus, XProtect® a ajouté un suffixe de numérotation automatique (-2) au nom de l'événement.

4. Cliquez sur **Select...**
5. Dans la boîte de dialogue **Select Sources**, sélectionnez toutes les caméras d'intervention PERCEPT pour lesquelles cet événement doit générer l'alarme et cliquez sur **Add**

6. Cliquez sur **OK**



7. Entrez les paramètres restants selon les besoins
8. Cliquez sur **Save**

Note: D'autres paramètres peuvent être configurés dans **Alarms > Alarm Data Settings**, tels que la création d'une priorité d'alarme et/ou d'une catégorie d'alarme distinctes spécifiquement pour les caméras d'intervention PERCEPT afin de personnaliser leurs états et comportements.

9 Validation de l'intégration

Cette section décrit les fonctionnalités clés à valider avant le déploiement sur le terrain via LTE/VPN, ou à grande échelle.

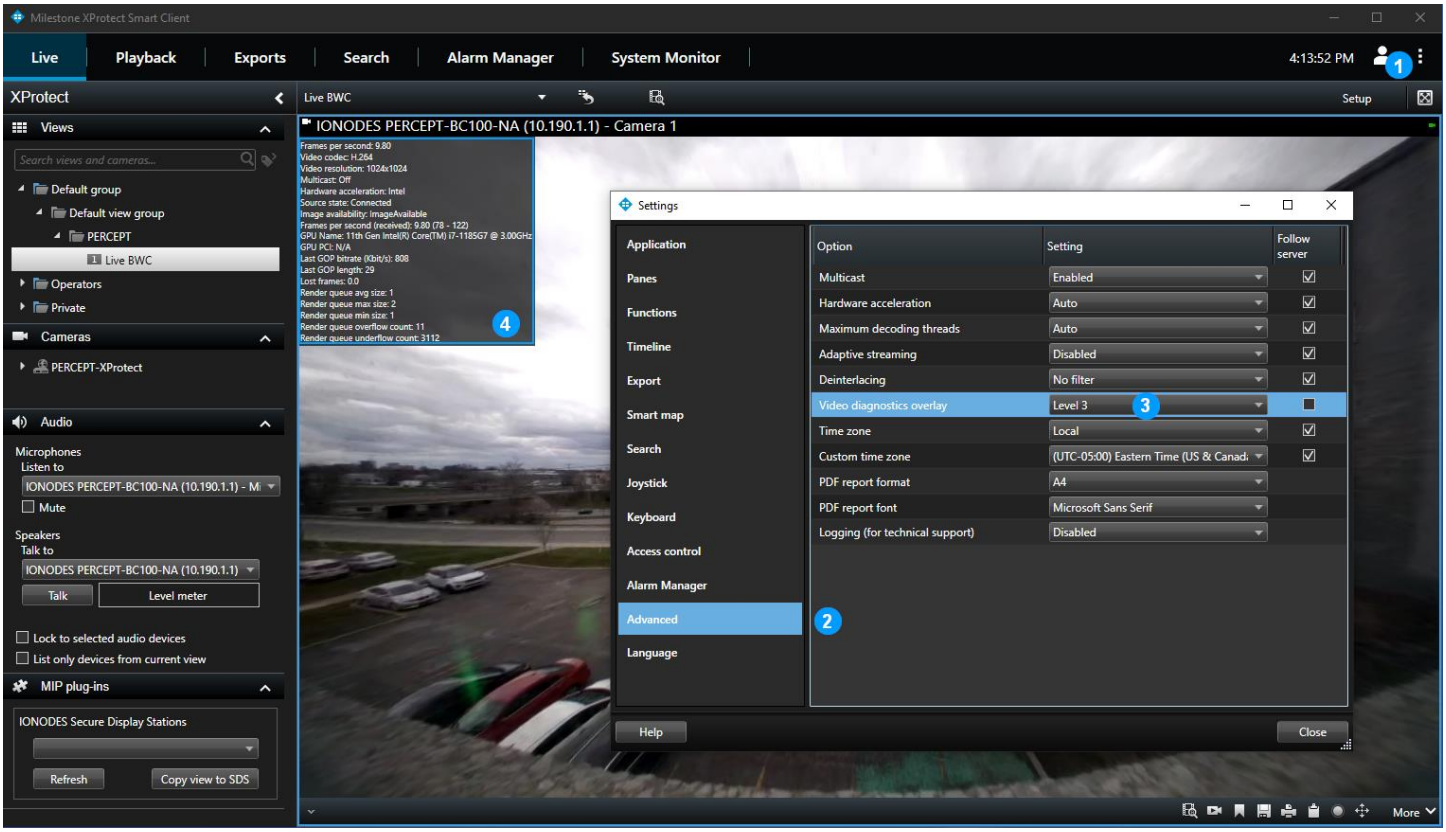
9.1 Diffusion sur demande

Lorsqu'aucun XProtect® Smart Client, Web Client ou Management Client n'affiche d'audio/vidéo en direct, les caméras d'intervention PERCEPT ne doivent pas diffuser. Cela peut être vérifié par le voyant d'état de la caméra d'intervention qui est bleu fixe. Dans cet état, la communication réseau est limitée à l'interrogation d'événements ONVIF et validation de connectivité.

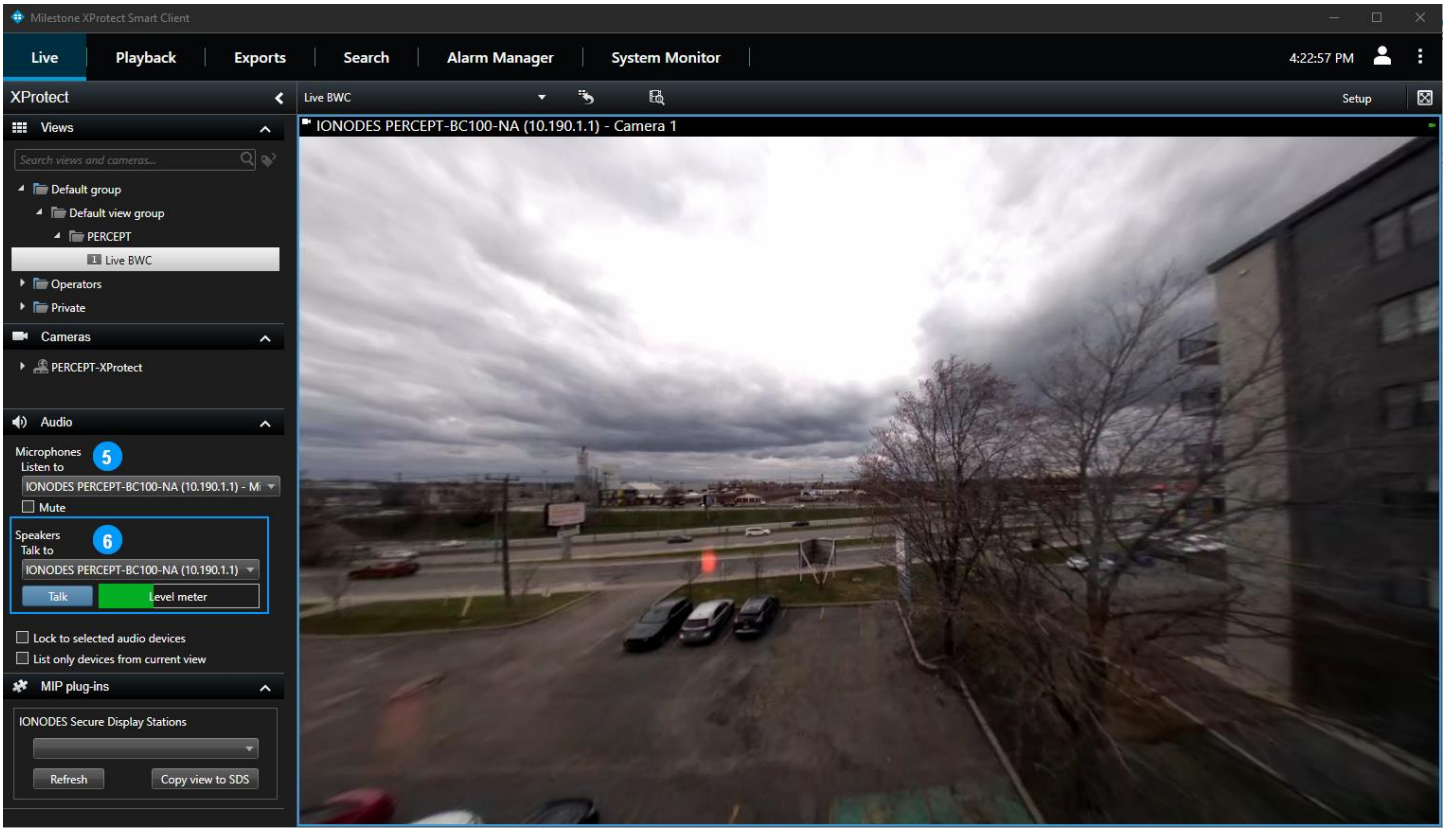
Le voyant clignotant en alternance rouge/vert indique qu'une caméra d'intervention envoie un flux. Si cela n'est pas prévu, vérifiez qu'aucune application cliente n'est connectée et passez en revue les configurations détaillées dans les sections 6.1.2, 6.1.3, 6.1.4, 6.2.2, 6.3.2, 7.1.1 et 7.1.2.

9.2 Diffusion en direct

Ouvrez XProtect® Smart Client et créez une vue avec une caméra d'intervention PERCEPT. Vérifiez que le flux vidéo en direct démarre. Si la lentille panormorphe a été configurée dans la section 6.1.5, vérifiez que vous pouvez corriger la vidéo et naviguer la scène. Si la lentille panormorphe n'est pas configurée, la navigation et le zoom dans l'image hémisphérique sont activés, sans correction d'image.



1. Cliquez sur l'icône **...** et ouvrez la boîte de dialogue **Settings**
2. Sélectionnez l'onglet **Advanced**
3. Réglez **Video diagnostics overlay** sur **Level 3**
4. Vérifiez que les paramètres vidéo (résolution, fréquence d'images, débit, etc.) correspondent au flux à faible débit configuré dans les sections 6.1.1 et 6.1.2



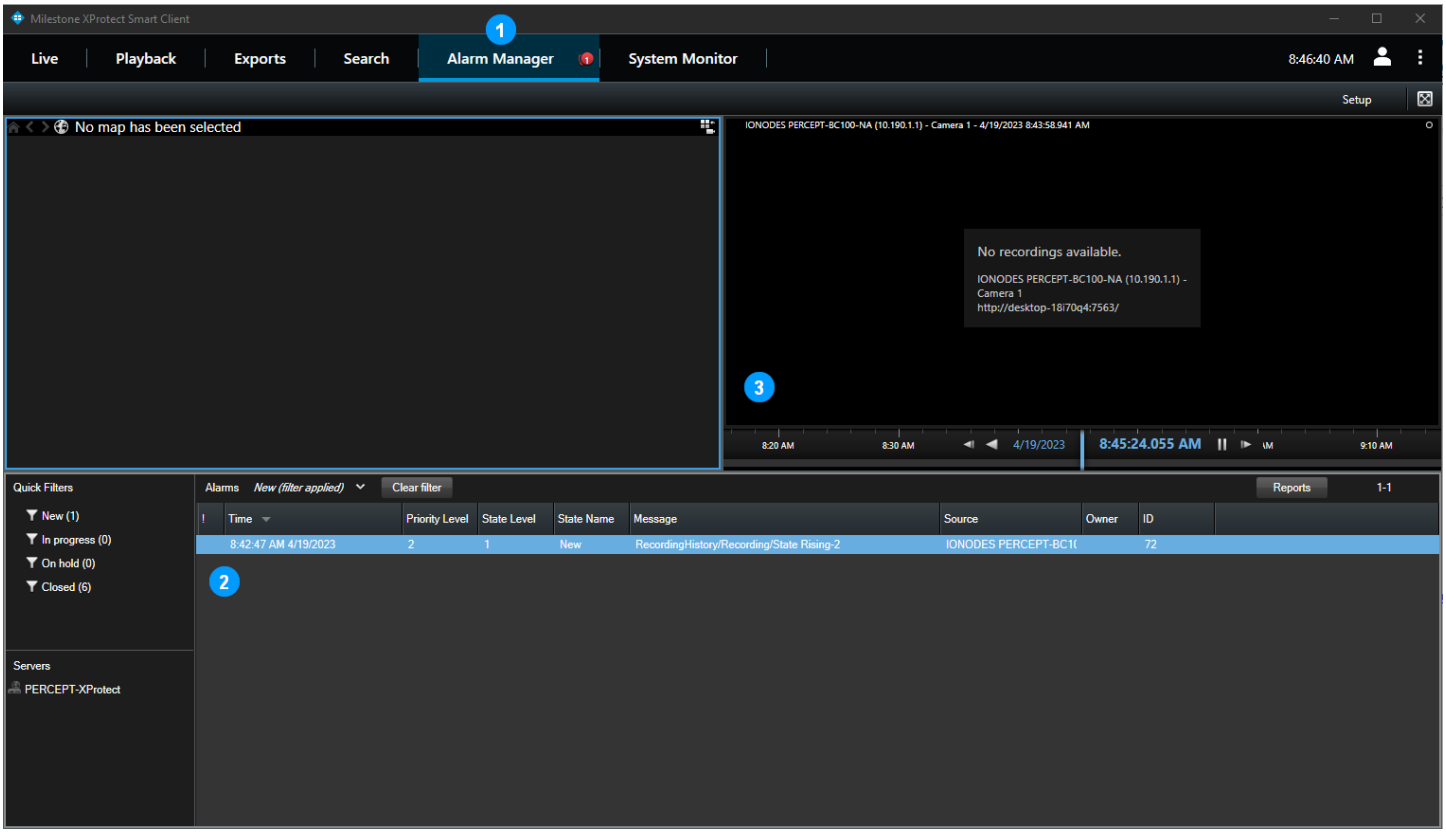
5. Si l'ordinateur est équipé de haut-parleurs, d'un casque ou d'un autre périphérique de sortie audio, sélectionnez le microphone de la caméra d'intervention PERCEPT et vérifiez que le son de la caméra est audible.
6. Si l'ordinateur est équipé d'un microphone, d'un casque ou d'un autre périphérique d'entrée audio, sélectionnez le haut-parleur de la caméra d'intervention PERCEPT, appuyez sur le bouton **Talk** et vérifiez que:
    a. L'indicateur de niveau augmente lorsque vous parlez dans le microphone de l'ordinateur
    b. Le son est audible sur le haut-parleur de la caméra d'intervention

Après avoir fermé tous les flux d'affichage en direct, vérifiez que l'état de la DEL de la caméra d'intervention PERCEPT redevient bleu fixe, indiquant qu'aucun flux n'est transmis sur le réseau.

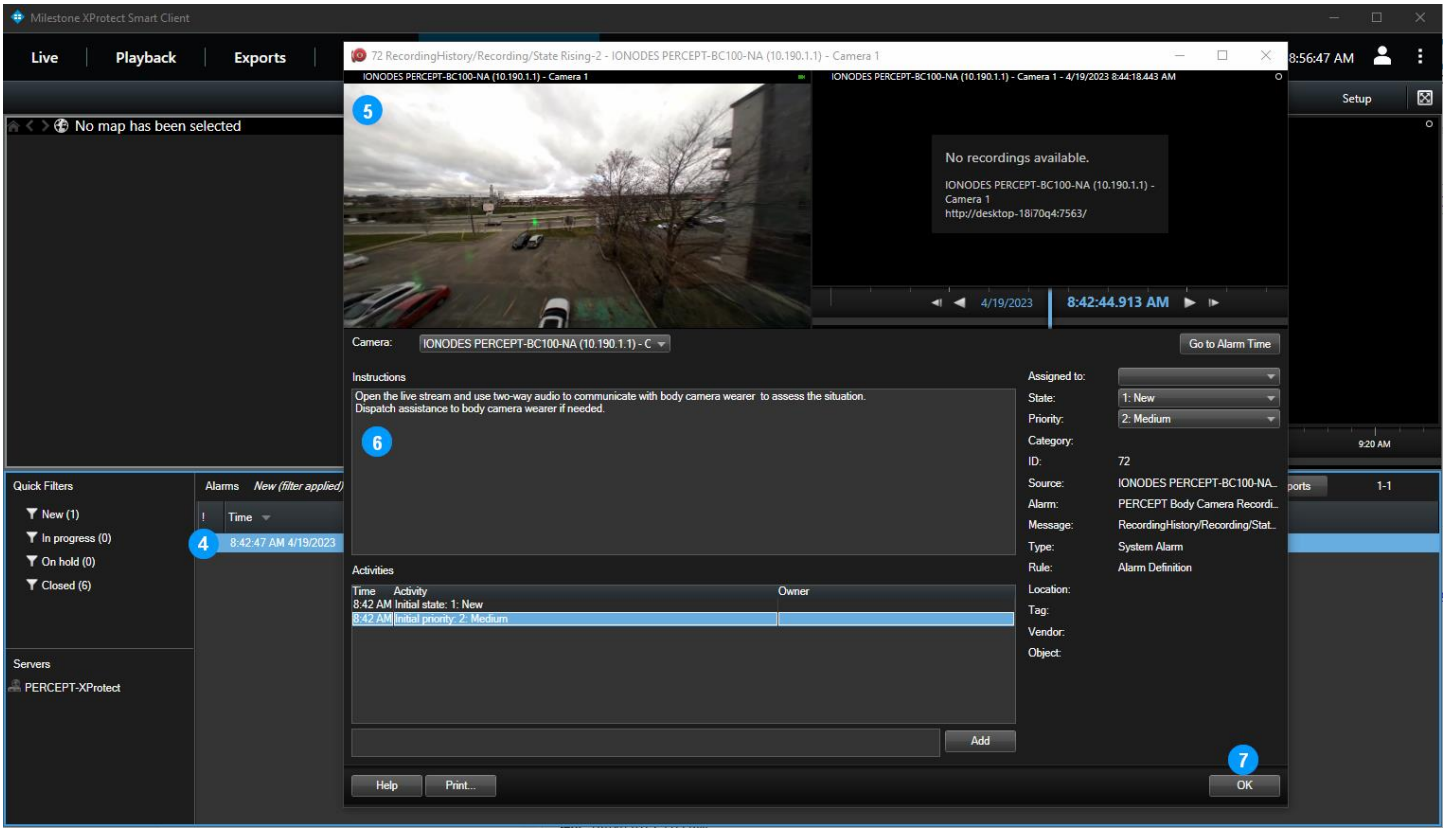
Note: Il y a une demi-seconde à une seconde de délai de mise en mémoire tampon intégrée dans le flux audio XProtect® pour les haut-parleurs et les microphones. Les opérateurs doivent être conscients que la première seconde après avoir appuyé sur le bouton **Talk** peut ne pas être transmise au porteur, et que la réponse du porteur sera légèrement retardée.

9.3 Enregistrement

Avec **XProtect® Smart Client** ouvert, appuyez sur le bouton **F5** de la caméra d'intervention PERCEPT pour démarrer un enregistrement. Vérifiez qu'une nouvelle alarme apparaît dans la section **Alarm Manager** de la barre d'outils.



1. Cliquez sur l'onglet **Alarm Manager**
2. Sélectionnez la nouvelle alarme et vérifiez que ses paramètres correspondent à la source, à l'événement déclencheur (message), au niveau de priorité, etc. configurés dans la section 8. Vérifiez que l'heure de l'alarme est correcte.
3. Notez que l'enregistrement n'est pas encore disponible. Il le deviendra après l'exécution réussie de la tâche de transfert, configurée dans la section 7.1.3.

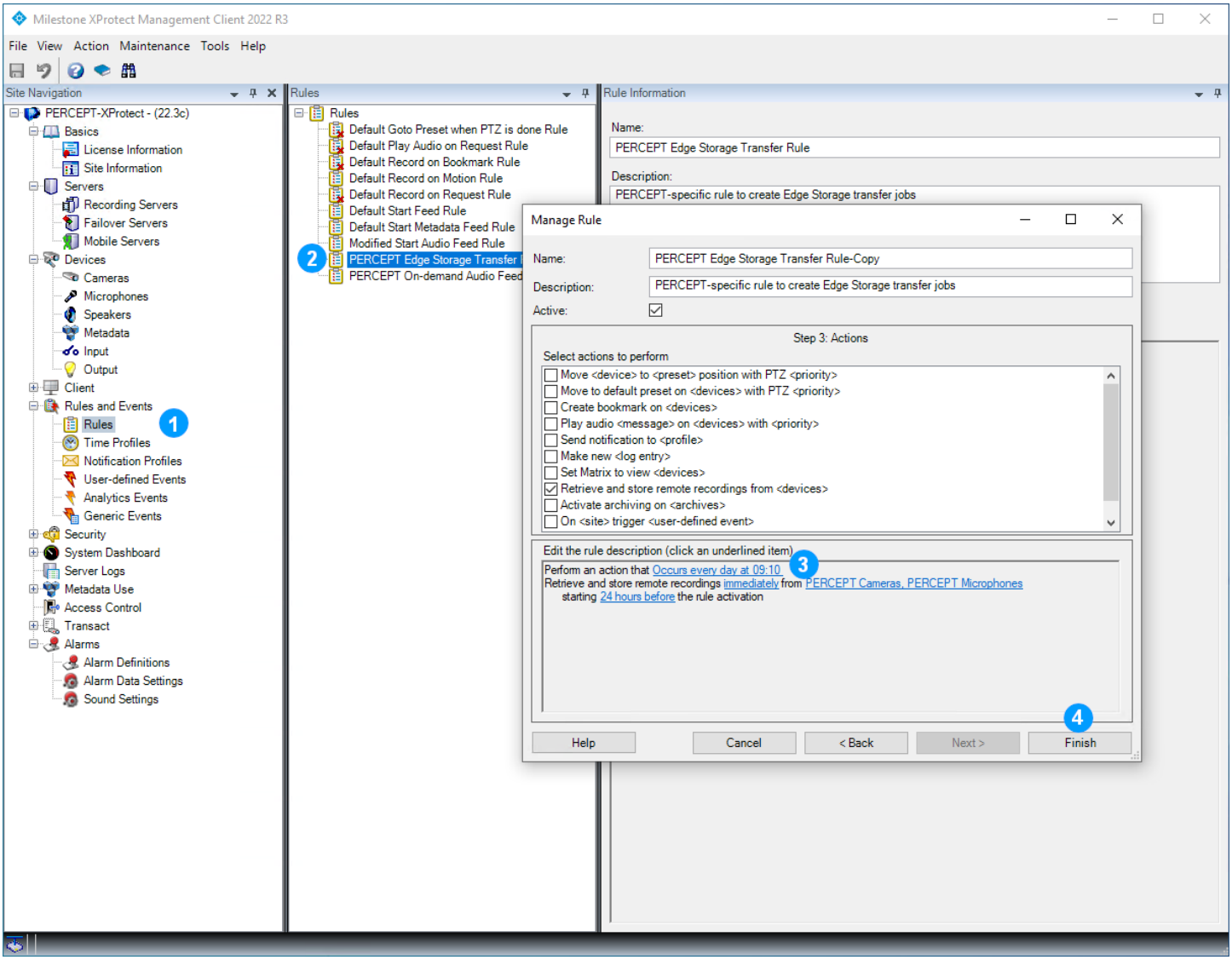


4. Double-cliquez sur l'alarme pour ouvrir la fenêtre de détail de l'alarme
5. Vérifiez qu'un aperçu en direct est disponible. Notez que l'audio bidirectionnel n'est pas disponible à partir de cette fenêtre. Si la communication avec le porteur est justifiée, l'opérateur doit afficher cette caméra à partir de l'onglet **Live**
6. Vérifiez que les instructions configurées dans la section 8 sont affichées
7. Cliquez sur **OK** pour fermer

9.3.1 Transfert de la mémoire interne

Si le transfert de la mémoire interne a été désactivé via Wi-Fi dans la section 3.2.3, insérez la caméra d'intervention PERCEPT dans une station d'accueil. Sinon, la caméra d'intervention bloquera la lecture et XProtect® Edge Storage Manager réessayera jusqu'à ce qu'elle réussisse.

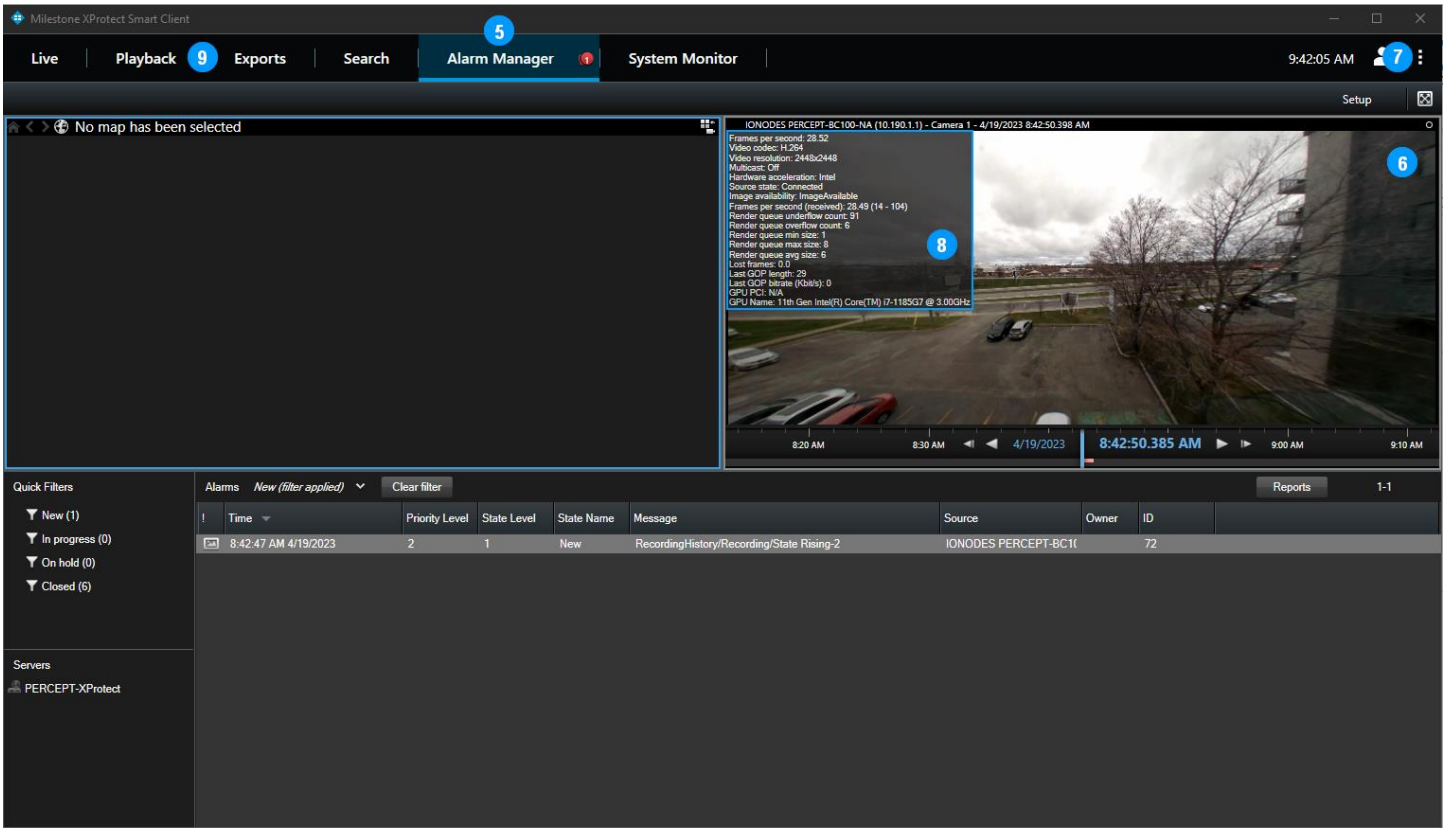
Pour valider l'exécution du transfert, attendez que la règle récurrente s'exécute ou testez-la immédiatement en faisant une copie temporaire de la règle avec une heure récurrente modifiée.



1. Dans le volet gauche de **XProtect® Management Client**, sélectionnez **Rules and Events** > **Rules**
2. Dans le volet central **Rules**, cliquez avec le bouton droit sur la règle de transfert créée à la section 7.1.3 et sélectionnez **Copy Rule...** dans le menu contextuel
3. Dans la boîte de dialogue **Manage Rule**, cliquez sur l'heure de récurrence et modifiez-la à la minute à venir la plus proche
4. Assurez-vous que la règle est activée (case **Active** cochée en haut de la fenêtre) avant de cliquer sur **Finish**

Attendez quelques minutes que la règle se déclenche et que la tâche de transfert exécute. Les journaux sont accessibles à partir du dossier des journaux XProtect® Recording Server pour

surveiller l'état des tâches. Emplacement par défaut: ProgramData\Milestone\XProtect Recording Server\Logs\EdgeStorage.log.



5. Ouvrez l'onglet **Alarm Manager** de **XProtect® Smart Client** avec l'alarme sélectionnée
6. Vérifiez que l'enregistrement est maintenant disponible et démarre automatiquement à partir du moment où l'alarme (enregistrement) a été déclenchée
7. Ouvrez la boîte de dialogue **Settings**, sélectionnez l'onglet **Advanced** et définissez **Video diagnostics overlay** sur **Level 3**
8. Vérifiez que les paramètres vidéo (résolution, fréquence d'images, débit, etc.) correspondent au flux à haut débit configuré dans les sections 6.1.1 et 6.1.2. Si vous recherchez une heure avant l'alarme, les paramètres vidéo de préenregistrement doivent correspondre au profil de préenregistrement configuré dans la section 3.4.
9. Notez que l'audio n'est pas disponible à partir du **Alarm Manager**, ouvrez l'onglet **Playback** pour vérifier que l'audio est disponible et synchronisé avec la vidéo.

Note: Si une règle temporaire a été créée pour tester le transfert, n'oubliez pas de la désactiver ou de la supprimer une fois le test terminé. Il en va de même pour les **Video diagnostics overlay**.

Note: Si vous utilisez XProtect® Web Client, effectuez les mêmes tests que pour XProtect® Smart Client, en gardant à l'esprit que Web Client ne prend pas en charge la correction panomorphe et nécessite le transcodage XProtect® Mobile Server si les flux vidéo sont configurés avec le codec H.265.

9.4 Commutation d'interface réseau

Si vous utilisez uniquement le Wi-Fi et la station d'accueil, la commutation de l'interface réseau entre les deux a déjà été testée lors des étapes précédentes. Cette section valide la commutation entre LAN et VPN sur Wi-Fi et/ou LTE.

Si un réseau Wi-Fi avec accès Internet est disponible, reportez-vous au Guide de démarrage rapide de la caméra d'intervention PERCEPT pour générer un code QR et connecter la caméra d'intervention à ce réseau. À partir de l'écran OLED de la caméra, vérifiez l'état de la connexion Wi-Fi, la force du signal et que son adresse IP est celle attendue pour ce réseau. Après quelques secondes, le VPN se connecte automatiquement et affiche son adresse IP. L'adresse IP VPN doit être la même que l'adresse IP LAN:

Note: La plupart des routeurs Wi-Fi n'achemineront pas le trafic VPN de son réseau Wi-Fi principal vers l'adresse IP statique publique du routeur Internet principal auquel il est connecté. Cela peut généralement être résolu en connectant la caméra d'intervention PERCEPT au réseau Wi-Fi invité du routeur.

La commutation d'interface réseau est automatique, basée sur la priorité suivante:

1. LAN sur station d'accueil
2. Wi-Fi
3. LTE / Cellulaire

Si LTE et VPN sont correctement configurés et activés, le passage au VPN sur LTE est automatique lorsque la connexion LAN et Wi-Fi est perdue.

Vérifiez que la diffusion en direct, l'audio bidirectionnel et les alarmes fonctionnent sur VPN comme sur Wi-Fi. Si un flux en direct est connecté lorsque l'interface réseau change, cela peut prendre environ 20 secondes pour que le flux reprenne sur XProtect® Smart Client ou Web Client.