The open platform company

Milestone Systems

XProtect® Advanced VMS 2016 R3

Manuel de l'administrateur

Table des matières

Droits d'auteur, marques et exclusions

Marques

XProtect est une marque déposée de Milestone Systems A/S.

Microsoft et Windows sont des marques déposées de Microsoft Corporation. App Store est une marque de service d'Apple Inc. Android est une marque déposée de Google Inc.

Toutes les autres marques citées dans ce document sont des marques déposées de leurs propriétaires respectifs.

Exonération de responsabilité

Ce manuel est un document d'information générale et il a été réalisé avec le plus grand soin.

L'utilisateur assume tous les risques découlant de l'utilisation de ces informations. Aucun élément de ce manuel ne peut constituer une garantie d'aucune sorte, implicite ou explicite.

Milestone Systems A/S se réserve le droit d'effectuer des modifications sans préavis.

Les noms de personnes et d'organisations utilisés dans les exemples de ce document sont fictifs. Toute ressemblance avec des organisations ou des personnes réelles, existantes ou ayant existé, est purement fortuite et involontaire.

Ce produit peut utiliser des logiciels tiers pour lesquels des dispositions spécifiques peuvent s'appliquer. Dans ce cas, vous pouvez trouver plus d'informations dans le fichier **3rd_party_software_terms_and_conditions.txt** situé dans le dossier d'installation Milestone de votre système de surveillance.

Avant de commencer

Introduction à l'aide

L'aide est divisée en sections qui ont chacune un objectif ciblé. Les sections sont organisées selon un ordre logique :

Vue d'ensemble du système (voir "**Présentation du système**" á la page 15)
Présente une introduction de votre système de surveillance vidéo, des composants du système, et des concepts. Ce qui est utile si vous êtes nouveau sur le système. La vue d'ensemble du système fournit également un tableau comparatif qui répertorie les différences les plus importantes entre les produits.

Installation (á la page 28)
Fournit des conditions préalables d'installation et des procédures étape par étape pour vous aider à installer et à mettre à jour votre système.

Première installation (voir "**Première utilisation**" á la page 58)
Offre une vue d'ensemble de Management Client et des informations sur les meilleures pratiques à suivre pour le bon fonctionnement de votre système. Cet aperçu est utile si vous êtes nouveau sur le système.

Éléments Management Client (á la page 67)
Offre une présentation approfondie grâce à chacun des nœuds du volet **Navigation du site** de Management Client. Cette section contient des informations conceptuelles et procédurales sur les éléments de base de votre système.

Configuration des fonctions (á la page 280)
Offre des informations autonomes et détaillées sur les fonctionnalités supplémentaires et les produits complémentaires pris en charge par votre système.

Maintenance du système (á la page 414)
Offre une vue d'ensemble des ports utilisés dans le système et décrit les procédures étape par étape, par exemple, pour la sauvegarde de votre système et la surveillance des performances du système. Cette section est utile après l'installation et la configuration afin de maintenir, d'accroître et d'optimiser les performances de votre système.

Naviguer dans le système d'aide intégré

Appuyez sur F1 pour accéder à une rubrique d'aide ou sélectionnez **Aide Sommaire** dans la barre d'outils Management Client pour lancer l'aide complète.

Vous pouvez naviguer entre les trois onglets de la fenêtre d'aide : **Contenu**, **Index**, et **Rechercher** ou utiliser les liens internes du texte de l'aide.

Onglet	Description
Table des matières	parcourez l'arborescence du système d'aide.
Index	Sélectionnez la première lettre du mot qui vous intéresse et faites défiler la lise jusqu'à ce que vous le trouviez. Cliquez sur le titre de l'une de ces rubriques dans la liste des résultats de la recherche pour ouvrir la rubrique concernée.

Onglet	Description
Rechercher	Effectuez une recherche dans toutes les rubriques de l'aide, sur un terme en particulier. Par exemple, recherchez le terme **zoom** et obtenez une liste dans les résultats de recherche de toutes les rubriques d'aide qui contiennent le terme **zoom**. Cliquez sur le titre de l'une de ces rubriques dans la liste des résultats de la recherche pour ouvrir la rubrique concernée.

Pour imprimer une rubrique de l'aide, allez dans la rubrique concernée et cliquez sur le bouton **Imprimer** du navigateur.

Présentation du système

Présentation générale du produit

Ce système XProtect est une solution intégralement distribuée, conçue pour une installation de grande envergure sur plusieurs sites et plusieurs serveurs nécessitant une surveillance 24h/24, 7j/7 supportée par des périphériques de marques différentes. La solution supporte une administration centralisée de tous les périphériques, serveurs et utilisateurs et permet d'utiliser un système basé sur des règles extrêmement flexibles et contrôlé par des programmes et des événements.

Votre système comprend les principaux éléments suivants :

- Le **serveur de gestion** : au cœur de votre installation, il se compose de plusieurs serveurs
- Un ou plusieurs **serveurs d'enregistrement**
- Un ou plusieurs **XProtect Management Clients**
- Le **XProtect Download Manager**
- Un ou plusieurs **XProtect® Smart Clients**.
- Un ou plusieurs **XProtect Web Clients** et/ou **Milestone Mobile clients** le cas échéant

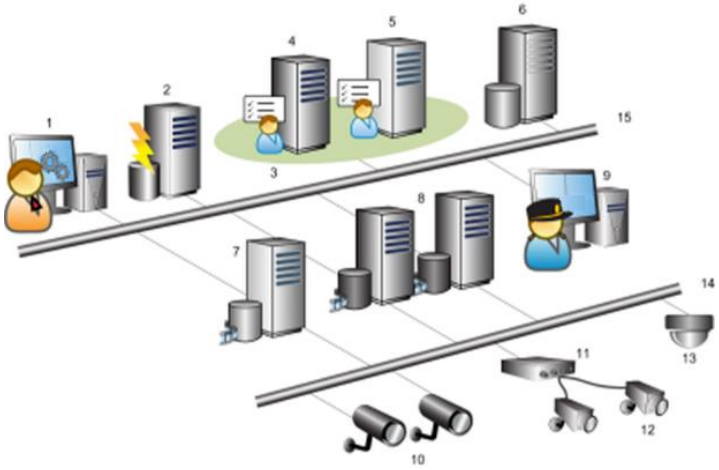
Votre système comprend également une fonction Matrix entièrement intégrée pour la visualisation distribuée des vidéos de n'importe quelle caméra de votre système de surveillance sur n'importe quel ordinateur doté d'un XProtect Smart Client.

Vous pouvez installer votre système XProtect sur les serveurs virtualisés ou sur plusieurs serveurs physiques dans une configuration distribuée.

Le système offre également la possibilité d'inclure un XProtect® Smart Client – Player indépendant lorsque vous exportez des vidéos à partir du XProtect Smart Client. Le XProtect Smart Client – Player permet aux destinataires des preuves vidéo (comme les officiers de police, les inspecteurs internes ou externes, etc.) de parcourir et de lire les enregistrements exportés sans avoir à installer de logiciel sur leur ordinateur.

Votre système peut supporter un nombre illimité de caméras, serveurs et utilisateurs et des sites multiples le cas échéant. Votre système peut supporter IPv4 ainsi que IPv6.

Une configuration distribuée du système



Exemple d'une configuration du système. Le nombre de caméras, de serveurs d'enregistrement et le nombre de clients connectés peut être aussi élevé que nécessaire.

Légende :

1. Management Client(s)
2. Serveur d’événements
3. Grappe Microsoft
4. Serveur de gestion
5. Serveur de gestion de redondance
6. Serveur SQL
7. Serveur d'enregistrement de redondance
8. Serveur(s) d’enregistrement
9. XProtect Smart Client(s)
10. Caméras vidéo IP
11. Encodeur vidéo
12. Caméras analogiques
13. Caméra IP PTZ
14. Réseau de caméras
15. Réseau de serveurs

Composants du système

Serveur de gestion

Le serveur de gestion conserve la configuration du système de surveillance dans une base de données relationnelle, sur l'ordinateur du serveur de gestion ou sur un serveur SQL séparé sur le réseau. Il gère également l'authentification de l'utilisateur, les droits de l'utilisateur, le système de

règles, entre autres. Pour améliorer les performances du système, vous pouvez exécuter plusieurs serveurs de gestion comme une architecture fédérée Milestone Federated Architecture™. Le serveur de gestion fonctionne en tant que service, et est généralement installé sur un serveur dédié.

Les utilisateurs se connectent au serveur de gestion pour une authentification initiale, puis, de façon transparente aux serveurs d'enregistrement pour accéder aux enregistrements vidéo, etc.

Serveur de gestion de redondance

La prise en charge du basculement sur le serveur de gestion est réalisée par l'installation du serveur de gestion dans un cluster Microsoft Windows. Le groupe veillera ensuite à ce qu'un autre serveur prenne le relais du serveur de gestion si le premier serveur venait à tomber en panne.

Serveur d'enregistrement

Le serveur d'enregistrement est chargé de communiquer avec les caméras réseau et les encodeurs vidéo, d'enregistrer l'audio et la vidéo récupérés ainsi que de garantir l'accès du client à la fois à l'audio et à la vidéo enregistrés et en direct.

En outre, le serveur d'enregistrement est chargé de communiquer avec d'autres produits Milestone connectés via la technologie Milestone Interconnect.

Pilotes de périphérique

- La communication avec les caméras réseau et les encodeurs vidéo s'effectue par un pilote de périphérique développé spécifiquement pour les périphériques individuels ou une série de périphériques semblables de la même fabrication.
- Les pilotes de périphériques sont installés par défaut lorsque le serveur d'enregistrement est installé, mais ils peuvent être mis à jour par la suite par le téléchargement et l'installation d'une nouvelle version du pack de pilotes de périphérique.

Base de données multimédia

- Les données audio et vidéo récupérées sont stockées dans la base de données multimédia haute performance sur mesure optimisée pour l'enregistrement et le stockage de données audio et vidéo.
- La base de données multimédia prend en charge diverses fonctionnalités uniques comme, l'archivage en plusieurs étapes, le groupage de vidéo, cryptage et l'ajout d'une signature numérique aux enregistrements.

Serveur d'enregistrement de redondance

Le serveur d'enregistrement de basculement prend en charge la tâche d'enregistrement si un serveur d'enregistrement tombe en panne.

Le serveur d'enregistrement de basculement dispose de deux modes de fonctionnement :

- Basculement standard - pour la surveillance de serveurs d'enregistrement multiples
- Serveur de secours - pour la surveillance d'un serveur d'enregistrement unique

La différence entre le mode de basculement standard et le mode serveur de secours est que pour le mode de basculement standard, le serveur d'enregistrement de basculement ne sait pas quel serveur prendre en charge, il ne peut donc pas commencer avant qu'un serveur d'enregistrement

ne tombe en panne. En mode serveur de secours, le temps de basculement est beaucoup plus court, comme le serveur d'enregistrement de basculement sait déjà quel serveur d'enregistrement il doit prendre en charge et peut pré-charger la configuration et le démarrage complètement - sauf pour la dernière étape de connexion aux caméras.

Serveur d'événements

Le serveur d'événements gère différentes tâches liées à des événements, des alarmes, des cartes et des intégrations tierces via le kit de développement logiciel MIP (SDK).

Événements :

- Tous les événements du système sont regroupés dans le serveur d'événements afin d'avoir un seul endroit et une seule interface pour que les partenaires effectuent des intégrations qui utilisent les événements du système.
- En outre, le serveur d'événements offre un accès tiers à l'envoi d'événements au système via les événements génériques ou l'interface d'analyse d'événements.

Alarmes :

- Le serveur d'événements héberge la fonction d'alarme, la logique d'alarme, l'état d'alarme ainsi que la manipulation de la base de données de l'alarme. La base de données de l'alarme est stockée dans le même serveur SQL que le serveur de gestion utilise.

Plans :

- Le serveur d'événements héberge également les cartes qui sont configurées et utilisées dans XProtect Smart Client.

MIP SDK :

- Enfin, les plug-ins développés par des tiers peuvent être installés sur le serveur d'événements et utiliser l'accès à des événements du système.

Serveur de journaux

Le serveur de journaux est chargé de stocker tous les messages du journal pour l'ensemble du système. Le serveur de journaux utilise le même serveur SQL que le serveur de gestion et est généralement installé sur le même serveur que ce dernier. Cependant, afin d'augmenter les performances des serveurs de gestion et de journalisation il peut être installé sur un serveur distinct si nécessaire.

Serveur SQL

Le serveur de gestion, le serveur d'événements et le serveur de journaux utilisent un serveur SQL pour stocker, par exemple, la configuration, les alarmes, les événements et les messages du journal.

Le programme d'installation du système inclut Microsoft SQL Server Express qui peut être utilisé gratuitement pour des systèmes jusqu'à 300 caméras.

Pour les systèmes ayant plus de 300 caméras, il est recommandé d'utiliser le SQL Server 2008 R2 édition Standard ou Enterprise sur un serveur dédié car ces éditions peuvent gérer des bases de données plus grandes et offrir des fonctionnalités de sauvegarde.

Active Directory

Active Directory est un service d'annuaire distribué mis en œuvre par Microsoft pour les réseaux avec domaine Windows. Il est inclus dans la plupart des systèmes d'exploitation Windows Server. Il identifie les ressources sur un réseau afin que les utilisateurs ou applications puissent y accéder.

Lorsqu'Active Directory est installé, vous pouvez ajouter des utilisateurs Windows à partir d'Active Directory, mais vous pouvez également ajouter des utilisateurs sans Active Directory. Veuillez noter que le système est soumis à certaines limites au niveau des utilisateurs de base.

Serveurs virtuels

Vous pouvez exécuter tous les composants du système sur des serveurs Windows® virtualisés, comme VMware® et Microsoft® Hyper-V®.

La virtualisation est bien souvent favorisée pour une meilleure utilisation des ressources matérielles. Normalement, les serveurs virtuels fonctionnant sur le serveur hôte matériel ne chargent pas beaucoup le serveur virtuel, et rarement en même temps. Cependant, les serveurs d'enregistrement enregistrent toutes les caméras et flux vidéo. Le processeur, la mémoire, le réseau et le système de stockage sont ainsi soumis à une charge élevée. Ainsi, lorsqu'il est exécuté sur le serveur virtuel, le gain de virtualisation normal disparaît majoritairement, puisque, dans la plupart des cas, il utilise toutes les ressources disponibles.

S'il est exécuté dans un environnement virtuel, il est important que l'hôte matériel dispose de la même quantité de mémoire physique que celle affectée aux serveurs virtuels et que le serveur virtuel exécutant le serveur d'enregistrement bénéficie de suffisamment de puissance de traitement et de mémoire, c'est-à-dire plus que ce que n'octroient les paramètres par défaut. Généralement le serveur d'enregistrement a besoin de 2 à 4 Go selon les configurations. Un autre goulet d'étranglement se situe au niveau de l'affectation de l'adaptateur réseau et de la performance du disque dur. Pensez à affecter un adaptateur réseau physique au serveur hôtel du serveur virtuel exécutant le serveur d'enregistrement. Il est alors plus facile de s'assurer que l'adaptateur réseau n'est pas surchargé par le trafic en direction d'autres serveurs virtuels. Si l'adaptateur réseau est utilisé pour plusieurs serveurs virtuels, le trafic du réseau peut empêcher le serveur d'enregistrement de récupérer et d'enregistrer la quantité d'images configurée.

Clients

À propos du Management Client

Un client d'administration riche en fonctionnalités pour la configuration et la gestion quotidienne du système. Disponible en plusieurs langues.

Généralement installé sur le poste de travail de l'administrateur du système de surveillance ou équivalent.

Pour un aperçu détaillé de Management Client, voir vue d'ensemble Management Client (á la page 60).

À propos de XProtect Smart Client

Conçu pour le logiciel de gestion vidéo IP Milestone XProtect® , le XProtect Smart Client est une application client facile à utiliser qui offre un contrôle intuitif des installations de sécurité. La gestion des installations de sécurité avec XProtect Smart Client permet aux utilisateurs d'avoir un accès continu aux vidéos en direct et enregistrées, un contrôle instantané des caméras et périphériques de sécurité connectés et une vue d'ensemble des enregistrements. Disponible en 26 langues, XProtect Smart Client est une interface utilisateur flexible pouvant être optimisée pour les

tâches de chaque opérateur et réglée en fonction de ses compétences et niveaux d'autorité spécifiques.

L'interface vous permet de personnaliser votre expérience de visionnement pour les environnements de travail spécifiques en sélectionnant un thème clair ou foncé, en fonction de l'éclairage ambiant ou de la luminosité de la vidéo. Elle dispose également d'onglets travail optimisés et d'une chronologie de la vidéo intégrée pour une opération de surveillance aisée. En utilisant MIP SDK, les utilisateurs peuvent intégrer différents types de systèmes de sécurité, de gestion et d'applications d'analyse vidéo, que vous gérez à travers XProtect Smart Client.

XProtect Smart Client doit être installé sur tous les ordinateurs des utilisateurs. Les administrateurs du système de surveillance gèrent l'accès des clients à ce dernier via Management Client. Les enregistrements consultés par les clients sont fournis par le service Image Server de votre système XProtect. Le service fonctionne en arrière-plan sur le serveur du système de surveillance. Aucun matériel supplémentaire n'est nécessaire.

Pour télécharger XProtect Smart Client, vous devez vous connecter au serveur de système de surveillance qui affiche une page d'accueil répertoriant les clients disponibles et les versions linguistiques. Les administrateurs du système utilisent le XProtect Download Manager pour contrôler les clients et langues qui doivent être disponibles sur la page d'accueil XProtect Download Manager pour les utilisateurs.

À propos du client Milestone Mobile

Le client Milestone Mobile est une solution de surveillance mobile étroitement intégrée au reste de votre configuration de surveillance XProtect. Elle s'exécute sur votre tablette Android, votre smartphone, votre dispositif Apple® (tablette, smartphone ou lecteur de musique portable) ou votre tablette ou smartphone Windows Phone 8 et vous donne accès aux caméras, aux vues et aux autres configurations de fonctionnalité dans les clients de gestion.

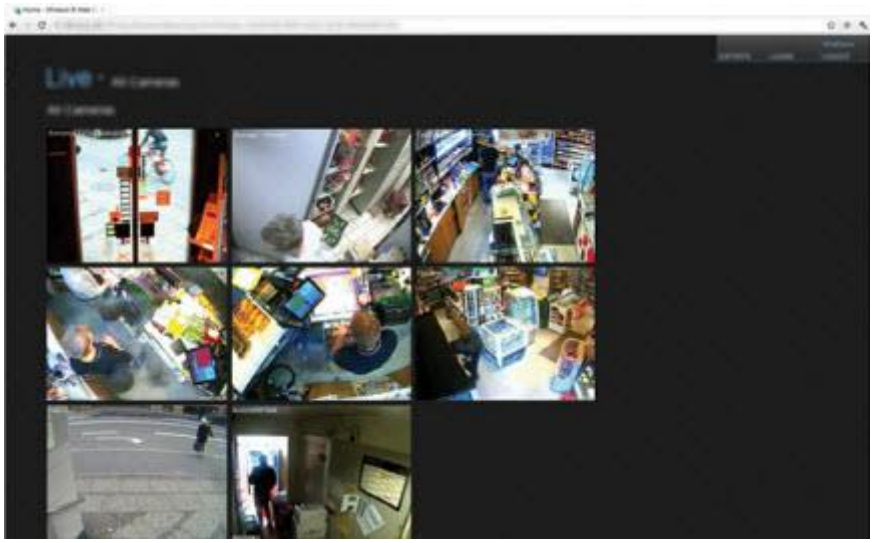
Utilisez le client Milestone Mobile pour voir et lire la vidéo en direct et enregistrée à partir d'une ou de plusieurs caméras, des caméras de contrôle PTZ (pan-tilt-zoom), de la sortie de déclenchement et des événements. Utilisez la fonctionnalité vidéo push pour envoyer de la vidéo à partir de votre périphérique sur votre système XProtect.

Si vous souhaitez utiliser le client Milestone Mobile avec votre système, vous devez ajouter un serveur mobile afin d'établir la connexion entre le client Milestone Mobile et votre système. Une fois que le serveur mobile est configuré, téléchargez le client Milestone Mobile gratuitement sur Google Play, l'App Store ou le Windows Phone Store pour commencer à utiliser Milestone Mobile.

Vous n'avez besoin que d'une licence de périphérique matériel par périphérique capable de pousser la vidéo vers votre système XProtect.

À propos de XProtect Web Client

XProtect Web Client est une application en ligne permettant de visualiser, lire et partager des vidéos. Il fournit un accès instantané aux fonctions les plus couramment utilisées de surveillance, telles que l'affichage vidéo en direct, la lecture de la vidéo enregistrée, l'impression et l'exportation des preuves. L'accès aux fonctionnalités dépend des droits d'utilisateurs individuels qui sont configurés dans le client d'administration.



Pour pouvoir utiliser le XProtect Web Client, vous devez ajouter un serveur mobile afin d'établir la connexion entre le XProtect Web Client et votre système. Le XProtect Web Client ne nécessite lui-même aucune installation et fonctionne avec la plupart des navigateurs Internet. Une fois le serveur mobile est mis en place, vous pouvez contrôler votre système XProtect n'importe où à partir de n'importe quel ordinateur ou tablette avec un accès Internet (si vous connaissez l'adresse externe/Internet correcte, le nom d'utilisateur et le mot de passe).

À propos des licences

Lors de l'achat de votre logiciel et des licences, vous recevez :

- Une confirmation de commande.
- Un fichier de licence logicielle (SLC) doté de l'extension .lic et nommé en fonction de votre SLC (code de licence du logiciel).

Votre SLC est également imprimé sur votre confirmation de commande et contient des chiffres et des lettres reliés par des tirets.

- Version 2014 du produit ou antérieure : xxx-xxxx-xxxx
- Version 2016 du produit ou ultérieure : xxx-xxx-xxx-x-xxxxxx

Le fichier de la licence du logiciel contient toutes les informations relatives à vos licences et produits VMS.

Milestone vous recommande de conserver les informations relatives à votre SLC et une copie du fichier de la licence de votre logiciel dans un endroit sûr et accessible. Dans l'arborescence, vous pouvez également voir votre SLC si vous sélectionnez **Bases** > **Renseignements sur la licence.** Vous aurez besoin du fichier de la licence de votre logiciel ou de votre SLC pour créer un compte utilisateur My Milestone, contacter votre revendeur ou pour apporter des modifications à votre système.

Commencez par télécharger le logiciel sur notre site Internet http://www.milestonesys.com/downloads. Lors de l'installation (á la page 28) du logiciel, il vous sera demandé de fournir un fichier de licence logicielle.

Au terme de l'installation et une fois vos licences activées, vous pourrez afficher un aperçu de vos licences (voir "Renseignements sur la licence" á la page 67) pour toutes les installations sous le même SLC sur la page **Bases** > **Renseignements sur la licence.**

Vous avez acheté au moins deux types de licences :

Licence de base : Vous disposez au moins d'une licence de base pour l'un des produits XProtect. Il se peut que vous ayez une ou plusieurs licences pour les produits complémentaires XProtect.

Licences de périphérique : Chaque périphérique ajouté à votre système XProtect nécessite une licence de périphérique. Vous n'avez pas besoin de licences de périphérique pour les haut-parleurs, microphones ni pour les périphériques d'entrée et de sortie connectés à votre caméra. Vous n'avez besoin que d'une seule licence de périphérique par adresse IP d'encodeur vidéo si vous connectez plusieurs caméras à l'encodeur vidéo. Un encodeur vidéo peut avoir une ou plusieurs adresses IP.

Pour plus d'informations, consulter la liste des périphériques pris en charge sur le site web de Milestone https://www.milestonesys.com/supported-hardware. Si vous souhaitez utiliser la fonction vidéo push dans Milestone Mobile, vous aurez besoin d'une licence de périphérique pour chaque portable ou tablette pouvant utiliser cette fonction dans votre système. Si vous êtes à court de licences, vous pouvez désactiver (voir "Désactiver/activer le matériel" á la page 105) les périphériques moins importants pour permettre à de nouveaux périphériques de fonctionner.

Si votre système de surveillance est le site central d'une plus grande hiérarchie utilisant Milestone Interconnect, vous aurez besoin de licences de caméra Milestone Interconnect pour voir les vidéos des périphériques sur un site distant. N'oubliez pas que seul XProtect Corporate peut servir de site central.

La plupart des produits complémentaires XProtect nécessitent des types de licences supplémentaires. Le fichier de licence du logiciel comprend également des informations relatives aux licences pour les produits complémentaires. Certains produits complémentaires possèdent leurs propres fichiers de licence du logiciel. Vous pouvez obtenir plus d'informations au sujet des licences des produits complémentaires sur :

- XProtect Access (voir "Licences XProtect Access" á la page 313)
- XProtect LPR (voir "Licences LPR" á la page 322)
- XProtect Transact (voir "Démarrage" á la page 362)
- XProtect Smart Wall (voir "Licences XProtect Smart Wall" á la page 305) (compris dans XProtect Corporate)
- Pour les licences de produits complémentaires pour XProtect Retail et XProtect Screen Recorder, consulter la documentation des produits en question.

Graphique de comparaison des produits

XProtect Advanced VMS est disponible en deux versions :

- XProtect Expert
- XProtect Corporate

La liste complète des fonctionnalités est disponible sur la page de présentation du produit surle site Internet de Milestone http://www.milestonesys.com/our-products/xprotect-software-suite.

Vous trouverez ci-après une liste des différences entre les deux produits :

Nom	XProtect Expert	XProtect Corporate
Milestone Interconnect™	Site distant	Site central/distant
Milestone Federated Architecture™	Site distant	Site central/distant
Services de connexion à distance	-	✓
Stockage de vidéo multiniveau	Base de données XProtect Corporate Bases de données actives + 1 archive	Base de données XProtect Corporate Bases de données actives + nombre illimité d'archives
Réduire la fluidité d'image (affinage)	-	✓
Cryptage des données vidéo (serveur d'enregistrement)	-	✓
Signature de base de données (serveur d'enregistrement)	-	✓
Droits d'accès utilisateur contrôlés dans le temps	-	✓
Fonction de signet	Manuelle uniquement	Manuelle et à partir de règles
Sécurité globale	Droits de l'utilisateur client	Droits de l'utilisateur client/ Droits d'utilisation administrateur
Profils XProtect Management Client	-	✓
Profils XProtect Smart Client	3	Illimité
XProtect Smart Wall	facultatif	✓
Protection de preuves	-	✓
Réserver une session PTZ	-	✓
Débuter et terminer une patrouille manuelle	-	✓
Gérer les positions prédéfinies PTZ et les profils de patrouille	Management Client seulement	✓

À propos de IPv6 et IPv4

Votre système supporte IPv6 ainsi que IPv4. Tout comme XProtect Smart Client.

IPv6 est la dernière version du Protocole Internet (IP). Le protocole internet détermine le format et l'utilisation des adresses IP. IPv6 coexiste avec la version IP IPv4, encore la plus largement répandue. IPv6 a été développée afin de résoudre l'épuisement d'adresse de l'IPv4. Les adresses IPv6 font 128 bits, alors que les adresses IPv4 ne font que 32 bits.

Cela signifie que l'annuaire d'Internet est passé de 4,3 milliards d'adresses uniques à 340 undécillion (340 trillions de trillions de trillions) d'adresses. Un facteur de croissance de 79 octillions (milliards de milliards de milliards).

De plus en plus d'organisations mettent en place IPv6 sur leurs réseaux. Par exemple, toutes les infrastructures de l'agence fédérale américaine doivent être conformes IPv6. Les exemples et illustrations contenues dans ce manuel reflètent l'utilisation de l'IPv4 puisqu'il s'agit toujours de la version IP la plus largement utilisée. IPv6 fonctionne également avec le système.

À propos de l'utilisation du système avec IPv6

Les conditions suivantes s'appliquent lorsque vous utilisez le système avec IPv6 :

Serveurs

Les serveurs peuvent souvent supporter IPv4 et IPv6. Cependant, si un seul serveur de votre système (par exemple, un serveur de gestion ou un serveur d'enregistrement) requiert une version IP particulière, tous les autres serveurs de votre système doivent communiquer en utilisant la même version.

> **Exemple** : Tous les serveurs de votre système, sauf un, peuvent utiliser IPv4 et IPv6. L'exception est un serveur qui ne supporte qu'IPv6. Cela signifie que tous les serveurs doivent communiquer entre eux avec IPv6.

Périphériques

Vous pouvez utiliser des périphériques (caméras, entrées, sorties, microphones, haut-parleurs) ayant une version IP différente que celle utilisée pour la communication des serveurs pourvu que votre équipement réseau et les serveurs d'enregistrement supportent également la version IP des périphériques. Voir également l'illustration ci-dessous.

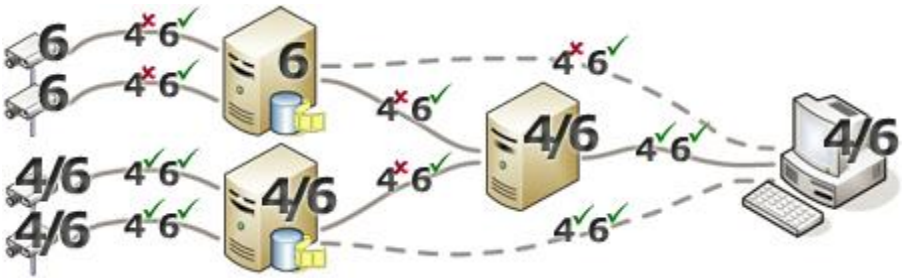
Clients

Si votre système utilise IPv6, les utilisateurs doivent se connecter avec le XProtect Smart Client. Le XProtect Smart Client supporte IPv6 ainsi que IPv4.

Si un ou plusieurs serveurs de votre système ne peuvent utiliser **que** IPv6, les utilisateurs XProtect Smart Client **doivent** utiliser IPv6 pour leur communication avec ces serveurs. Dans ce contexte, il est important de ne pas oublier que XProtect Smart Clients techniquement se connectent à un serveur de gestion pour une première authentification, puis aux serveurs d'enregistrement requis pour accéder aux enregistrements.

Cependant, les utilisateurs XProtect Smart Client n'ont pas à être eux-mêmes sur le réseau IPv6, pourvu que votre équipement réseau supporte la communication entre les différentes versions IP, et qu'ils ont installé le protocole IPv6 sur leurs ordinateurs. Voir également l'illustration. Pour installer IPv6 sur un ordinateur client, ouvrez une invite de commande, saisissez *installer IPv6*, et appuyez sur **ENTRÉE**.

Illustration en exemple



Exemple : Puisqu'un serveur du système n'utilise que IPv6, toutes les communications avec ce serveur doivent utiliser IPv6. Cependant, ce serveur indique également la version IP de communication entre tous les autres serveurs du système.

Aucune compatibilité Matrix Monitor

Si vous utilisez IPv6, vous ne pouvez pas utiliser l'application Matrix Monitor avec votre système. la fonction Matrix de XProtect Smart Client s n'est pas affectée.

À propos de l'écriture des adresses IPv6

Une adresse IPv6 est généralement écrite en huit blocs de quatre chiffres hexadécimaux, et chaque bloc est séparé par deux points.

Exemple : *2001:0B80:0000:0000:0000:0F80:3FA8:18AB*

Vous pouvez raccourcir les adresses en supprimant les zéros non significatifs d'un bloc. Notez également que certains des blocs à quatre chiffres peuvent se composer de zéros uniquement. Si quelques-uns de ces blocs 0000 sont consécutifs, vous pouvez raccourcir les adresses en remplaçant les blocs 0000 par deux doubles points tant qu'il n'y a pas d'autres deux doubles points dans l'adresse.

Exemple :
2001:0B80:0000:0000:0000:0F80:3FA8:18AB peut être ramené à

2001:B80:0000:0000:0000:F80:3FA8:18AB si vous supprimez les zéros non significatifs, ou à

2001:0B80::0F80:3FA8:18AB si vous supprimez les blocs 0000, ou encore à

2001:B80::F80:3FA8:18AB si vous supprimez les zéros non significatifs et les blocs 0000.

Utiliser les adresses IPv6 dans les URL

Les adresses IPv6 contiennent deux points. Les deux points, cependant, sont également utilisés dans d'autres types de syntaxe d'adresse réseau. Par exemple, IPv4 utilise deux points pour séparer l'adresse IP du numéro de port lorsque les deux sont utilisés dans une URL. IPv6 a hérité de ce principe. Par conséquent, pour éviter toute confusion, des crochets sont placés autour des adresses IPv6 lorsqu'elles sont utilisées dans les URL.

Exemple d'une URL avec une adresse IPv6 :
http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB*]*, qui peut être évidemment abrégé, par exemple, http://[2001:B80::F80:3FA8:18AB*]*

Exemple d'une URL avec une adresse IPv6 et un numéro de port : http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB*]*, qui peut être évidemment abrégé, par exemple, http://[2001:B80::F80:3FA8:18AB*]*

Pour plus d'informations sur IPv6, voir, par exemple, le site web de l'IANA http://www.iana.org/numbers/. IANA, Internet Assigned Numbers Authority, est l'organisation responsable de la coordination mondiale des adresses IP.

Configuration système

Important : Votre système ne prend plus en charge Microsoft® Windows® 2003 (cependant, vous pouvez encore exécuter/accéder aux clients à partir d'ordinateurs équipés de Windows 2003).

Important : Votre système ne prend plus en charge le système d'exploitation Microsoft® Windows® 32 bits (cependant, vous pouvez encore exécuter/accéder à XProtect Web Client et XProtect Smart Client à partir d'ordinateurs équipés du système d'exploitation Windows 32 bits).

Pour obtenir de plus amples informations sur la configuration système **minimale** des divers éléments de votre système, allez sur le site web http://www.milestonesys.com/SystemRequirements de Milestone.

Installation

Si vous procédez à une mise à niveau à partir d'une version XProtect antérieure, consultez la rubrique À propos de la mise à niveau (á la page 54).

Avant de commencer l'installation

Vous êtes tenu de passer en revue toutes ces conditions préalables importantes avant de commencer l'installation.

Préparer Active Directory

Si vous souhaitez ajouter des utilisateurs à votre système par le biais du service Active Directory, vous devez disposer d'un serveur équipé d'Active Directory et agissant comme contrôleur de domaine disponible sur votre réseau.

À des fins de gestion aisée des utilisateurs et des groupes, Milestone vous recommande d'avoir Microsoft Active Directory® en place et configuré, avant de procéder à l'installation de votre système XProtect. Si vous ajoutez le serveur de gestion à Active Directory après l'installation, vous devrez réinstaller le serveur de gestion et remplacer des utilisateurs par de nouveaux utilisateurs Windows définis dans Active Directory.

Les utilisateurs basiques ne sont pas pris en charge dans les systèmes Milestone Federated Architecture, ainsi, si vous prévoyez d'utiliser des utilisateurs basiques dans votre système, vous devrez ajouter des utilisateurs via le service Active Directory. Si vous n'installez pas Active Directory, suivez les étapes Installation pour les groupes de travail (á la page 43) lors de l'installation.

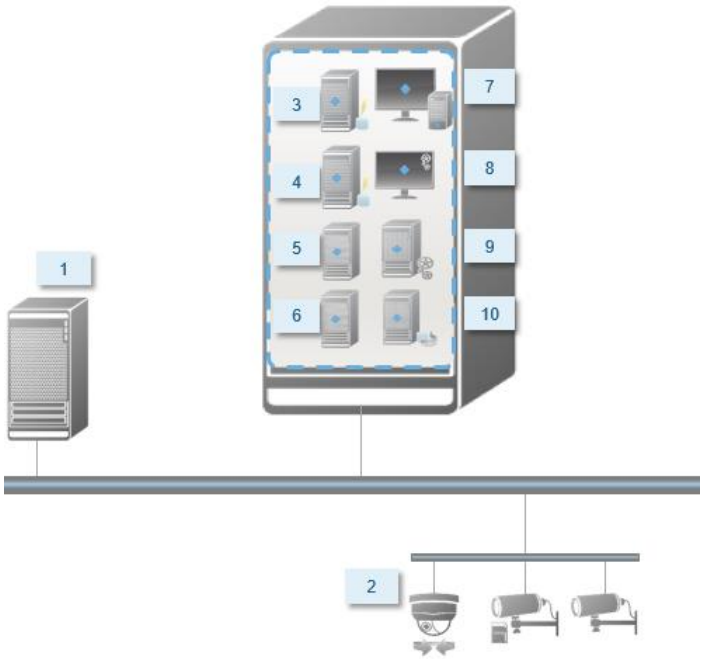
Méthode d'installation

Dans le cadre de l'assistant d'installation, vous devez décider quelle méthode d'installation utiliser. Vous devriez baser votre sélection sur les besoins de votre organisation, mais il est très probable que vous ayez déjà décidé de la méthode à adopter au moment de l'achat du système.

Options	Description
Serveur unique	Installe tous les composants du serveur de gestion, le serveur d'enregistrement et XProtect Smart Client sur l'ordinateur actuel. Il vous suffit de faire quelques choix et tous les composants sont présélectionnés dans la liste de composants non modifiables. Selon le matériel et la configuration, des systèmes de plus faible envergure ne contenant que 50 à 100 caméras peuvent fonctionner sur un serveur unique. Le serveur SQL ne figure pas dans la liste, mais est également installé sur l'ordinateur actuel.
Distribué	Installe uniquement les composants du serveur de gestion sur l'ordinateur actuel. Cela signifie que le serveur d'enregistrement et XProtect Smart Client ne sont pas visibles dans la liste de composants. Vous ne pouvez modifier aucun élément de la liste de composants. Vous devez installer le serveur d'enregistrement, XProtect Smart Client et le serveur SQL sur d'autres ordinateurs par la suite.

Options	Description
Personnaliser	Le serveur de gestion est toujours sélectionné dans la liste des composants du système et il est toujours installé, mais vous pouvez choisir les éléments à installer sur l'ordinateur actuel, et notamment d'autres composants du serveur de gestion, le serveur d'enregistrement et XProtect Smart Client. Par défaut, la case du serveur d'enregistrement est décochée dans la liste de composants, mais vous pouvez modifier cette configuration. Selon vos choix, vous devez ensuite installer les composants non sélectionnés et le serveur SQL sur d'autres ordinateurs.

Serveur unique

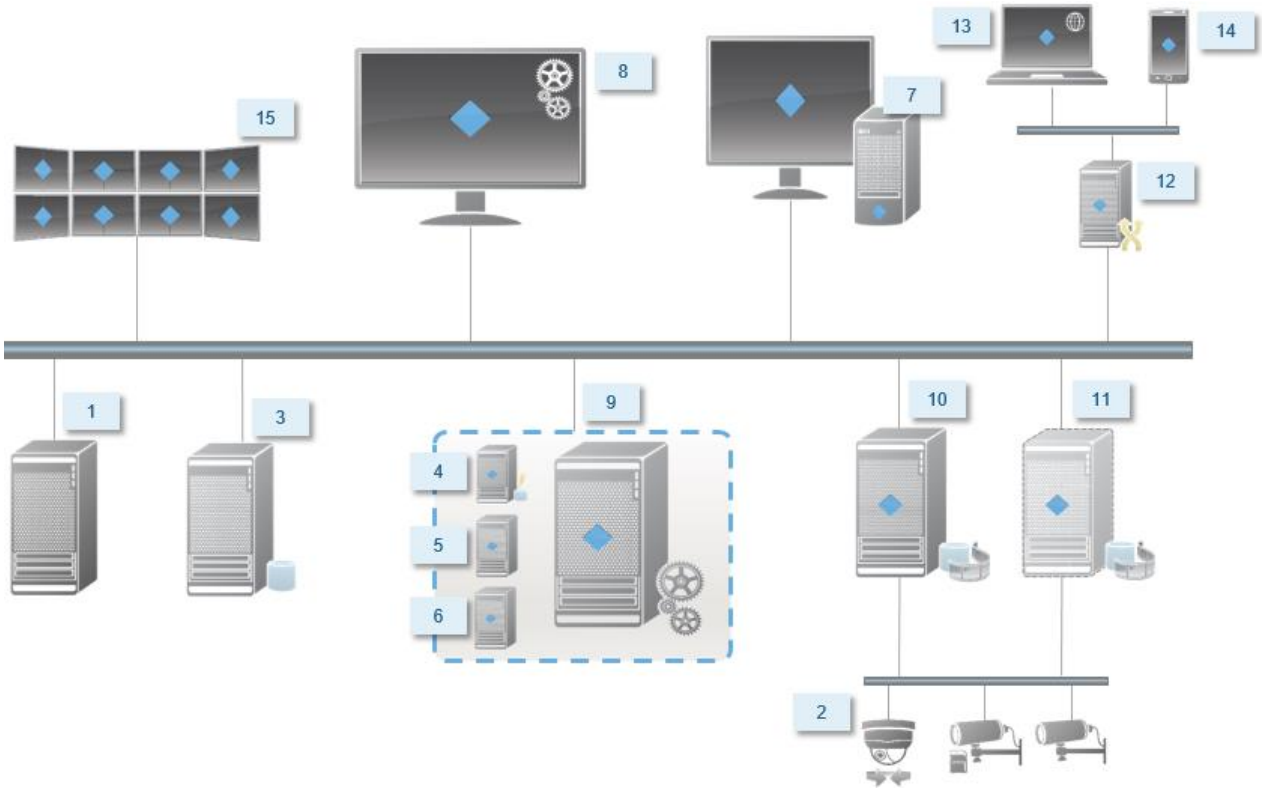


Composants typiques d'un système :

1. **Active Directory**
2. **Périphériques**
3. **Serveur SQL**
4. **Serveur d'événements**
5. **Serveur de journaux**
6. **Canal de service**
7. **XProtect Smart Client**
8. **Management Client**
9. **Serveur de gestion**
10. **Serveur d'enregistrement**
11. **Serveur d'enregistrement de redondance**

12. **Serveur Milestone Mobile**
13. **XProtect Web Client**
14. **Client Milestone Mobile**
15. **XProtect Smart Client avec XProtect Smart Wall**

Distribué



Déterminer le type de serveur SQL

Microsoft SQL Server Express Edition est une version « légère » d'un serveur SQL complet. Il est facile à installer et prêt à l'utilisation, et il représente souvent un choix idéal pour les systèmes comprenant moins de 300 caméras. Cette version du serveur SQL est comprise dans l'installation à un serveur.

Pour les installations de grande envergure de 300 caméras ou plus, Milestone recommande l'utilisation d'un serveur SQL dédié existant sur un ordinateur dédié du réseau. Vous devez disposer de droits d'administrateur sur le serveur SQL.

Milestone vous recommande d'installer la base de données sur un disque dur dédié dont l'utilisation exclut toute autre fin. L'installation de la base de données sur son propre disque améliore la performance du système entier.

Lorsque vous sélectionnez **Distribué** ou **Personnaliser** dans le cadre de l'assistant d'installation, vous devez décider quoi faire concernant le serveur SQL.

Si vous n'avez pas de serveur SQL installé, les options sont les suivantes :

- **Installer SQL Server Express sur cet ordinateur**.

- **Utiliser un serveur SQL existant sur le réseau :** Lorsque vous utilisez un ordinateur dédié pour la base de données SQL sur le réseau, la liste des serveurs SQL auxquels votre compte peut accéder s'affiche.

Si vous avez un serveur SQL installé, les options sont les suivantes :

- **Utiliser la base de données Microsoft SQL Server Express installée sur cet ordinateur**.
- **Utiliser un serveur SQL existant sur le réseau :** Lorsque vous utilisez un ordinateur dédié pour la base de données SQL sur le réseau, la liste des serveurs SQL auxquels votre compte peut accéder s'affiche.

  Il vous sera également demandé si vous souhaitez créer une nouvelle base de données, utiliser une base de données existante ou remplacer une base de données existante.

  - **Créer une nouvelle base de données** : Pour une nouvelle installation.
  - **Utiliser une base de données existante** : Si vous installez la base de données dans le cadre d'une mise à niveau du système, et que vous souhaitez utiliser votre base de données existante.

Sélectionner un compte de service

Dans le cadre de l'installation, il vous est demandé préciser un compte pour exécuter les services de Milestone sur cet ordinateur. Le service fonctionne toujours sur ce compte, quel que soit l'utilisateur connecté. Assurez-vous que le compte dispose de tous les droits d'utilisateur nécessaires, les droits permettant d'exécuter les taches, le bon réseau et accès aux fichiers et l'accès aux répertoires partagés sur le réseau.

Vous pouvez sélectionner un compte prédéfini ou un compte d'utilisateur. Votre décision doit se baser sur l'environnement sur lequel vous souhaitez installer votre système :

Environnement de domaine

Dans un domaine de domaine :

- Milestone recommande l'utilisation du compte Network Service (service réseau) intégré. Il est plus facile à utiliser même si vous devez élargir le système sur plusieurs ordinateurs.
- Vous pouvez aussi utiliser des comptes d'utilisateur de domaine, bien qu'ils puissent être plus difficiles à configurer.

Environnement de groupe de travail

Dans un environnement de groupe de travail, Milestone recommande l'utilisation d'un compte d'utilisateur local disposant de tous les droits nécessaires. Ceci est souvent le compte administrateur.

Important : Si votre installation couvre plusieurs ordinateurs, le compte d'utilisateur sélectionné doit exister sur tous les ordinateurs de votre installation avec les mêmes nom d'utilisateur, mot de passe et droits d'accès.

À propos de l’authentification Kerberos

Kerberos est un protocole d’authentification réseau basé sur tickets. Il est conçu pour fournir une forte authentification pour les applications client/serveur ou serveur/serveur.

Utilisez l’authentification Kerberos comme alternative protocole d’authentification Microsoft NT LAN (NTLM) plus ancien.

L’authentification Kerberos exige une authentification mutuelle, en d’autres termes le client s’authentifie auprès du service et le service s’authentifie auprès du client. Vous pouvez ainsi vous authentifier de manière plus sécurisée entre les XProtect clients et XProtect les serveurs sans exposer votre mot de passe.

Pour rendre possible l’authentification dans votre XProtect video management software vous devez inscrire les Service Principal Names (SPN) dans le répertoire actif. Un SPN est un alias qui identifie de manière unique une entité telle qu’un service de serveur XProtect. Chaque service utilisant l’authentification mutuelle doit avoir un SPN inscrit pour que les clients puissent identifier le service sur le réseau. Sans SPN correctement enregistrés, l’authentification mutuelle est impossible.

Le tableau ci-dessous présente les différents servicesMilestone ainsi que les numéros de port correspondants que vous devez inscrire :

Service	Numéro de port
Serveur de gestion - IIS	80 - Configurable
Serveur de gestion - Interne	8080
Serveur d’enregistrement - Data Collector	7609
Serveur de redondance	8990
Serveur d'événements	22331
Serveur LPR	22334

Le nombre de services que vous devez inscrire dans le répertoire actif dépend de votre installation actuelle. Data Collector est installé automatiquement quand vous installez le serveur de gestion, le serveur d’enregistrement, le serveur d’événements, le serveur LPR ou le serveur de redondance.

Vous devez inscrire deux SPN pour l'utilisateur exploitant le service : le premier avec le nom de l’hôte et le second avec le nom de domaine entièrement qualifié.

Si vous exploitez le service sous un compte de service d’utilisateur réseau, vous devez inscrire les deux SPN pour chaque ordinateur exploitant ce service.

Voici laMilestone convention de nomination SPN :
VideoOS/[Nom d’hôte DNS] :[Port]
VideoOS/[Nom de domaine entièrement qualifié]:[Port]

Voici un exemple de SPN pour le service de serveur d’enregistrement fonctionnant sur un ordinateur avec les détails ci-dessous :
Nom de l’hôte : Record-Server1
Domaine : Surveillance.com

SPN à inscrire :
VideoOS/Record-Server1:7609
VideoOS/Record-Server1.Surveillance.com:7609

À propos de la détection de virus

Comme avec tout autre logiciel de base de données, si un programme antivirus est installé sur un ordinateur exécutant le logiciel XProtect, il est important d'exclure certains types de fichiers et emplacements, ainsi qu'un trafic du réseau. Sans appliquer ces exceptions, la détection de virus utilise une quantité considérable de ressources système. En plus de cela, le processus de numérisation peut verrouiller temporairement les fichiers qui peut se traduire par une interruption du processus d'enregistrement ou encore la corruption de la base de données.

Lorsque vous avez besoin d'effectuer une analyse antivirus, n'analysez pas les répertoires Recording Server contenant les bases de données d'enregistrement (par défaut C:\mediadatabase\, ainsi que tous les dossiers sous cet emplacement). Évitez également d'effectuer une analyse antivirus sur les répertoires de stockage d'archives.

Créer les exclusions supplémentaires suivantes :

- Types de fichiers : .blk, .idx, .pic
- Répertoires et sous-répertoires :
  - C:\Program Files\Milestone ou C:\Program Files (x86)\Milestone
  - C:\ProgramData\Milestone\MIPSDK
  - C:\ProgramData\Milestone\Milestone Mobile Server\Logs
  - C:\ProgramData\Milestone\XProtect Data Collector Server\Logs
  - C:\ProgramData\Milestone\XProtect Event Server\logs
  - C:\ProgramData\Milestone\XProtect Log Server
  - C:\ProgramData\Milestone\XProtect Management Server\Logs
  - C:\ProgramData\Milestone\XProtect Recording Server\Logs
  - C:\ProgramData\Milestone\XProtect Report Web Server\Logs
  - C:\ProgramData\Milestone\XProtect Service Channel\Logs
- Exclure l'analyse en réseau sur les ports TCP suivants :

Produit	Ports TCP
XProtect Advanced VMS	80, 8080, 7563, 25, 21, 9993
Milestone Mobile	8081

ou

- Exclure l'analyse en réseau des processus suivants :

Produit	Processus
XProtect Advanced VMS	VideoOS.Recording.Service.exe, VideoOS.Server.Service.exe, VideoOS.Administration.exe

Produit	Processus
Milestone Mobile	VideoOS.MobileServer.Service.exe

Les entreprises peuvent avoir des directives strictes concernant les analyses antivirus, mais il est important que les emplacements et les fichiers mentionnés soient exclus de l'analyse antivirus.

Enregistrer le code de licence du logiciel

Avant de procéder à l'installation, vous devez disposer du nom et de l'emplacement du fichier de licence que vous avez reçu de la part de Milestone.

Le code de licence du logiciel (SLC) est imprimé sur la confirmation de commande et le nom du fichier de licence du logiciel contient votre SCL. Milestone vous recommande d'enregistrer votre SLC sur notre site internet http://www.milestonesys.comavant l'installation.

Prérequis pour une installation hors ligne

Si vous installez le système sur un serveur hors ligne, vous aurez besoin des éléments suivants :

- Le fichier `Milestone XProtect Advanced VMS Products 2016 R3 System Installer.exe`.
- Le fichier de licence logicielle pour votre système Milestone XProtect Advanced VMS.
- Média d'installation du système d'exploitation incluant la version .NET requise http://www.milestonesys.com/SystemRequirements.

Installer le système

Sélectionnez l'une des options d'installation :

- Installer votre système - option Serveur unique (á la page 34)
- Installer votre système - option Distribué (á la page 35)
- Installer votre système - option Personnaliser (á la page 36)

Installer votre système - option Serveur unique

L'option **Serveur unique** installe tous les composants du serveur de gestion, le serveur d'enregistrement et XProtect Smart Client sur l'ordinateur actuel. Selon le matériel et la configuration, des systèmes de plus faible envergure ne contenant que 50 à 100 caméras peuvent fonctionner sur un serveur unique. Il vous suffit de faire quelques choix et tous les composants sont présélectionnés dans la liste de composants non modifiables. Le serveur SQL ne figure pas dans la liste, mais est également installé sur l'ordinateur actuel.

1. Si vous installez une version téléchargée sur Internet, exécutez le fichier `Milestone XProtect Advanced VMS Products 2016 R3 System Installer.exe` à partir de l'emplacement où il a été sauvegardé.

Autrement, insérez le DVD du logiciel. Si la boîte de dialogue ne s'ouvre pas automatiquement, exécutez le fichier `Milestone XProtect Advanced VMS Products 2016 R3 System Installer.exe` à partir du DVD.

2. La décompression des fichiers d'installation débute. Selon vos paramètres de sécurité, un ou plusieurs avertissements de sécurité Windows® apparaissent. Acceptez-les afin de poursuivre la décompression.

3. Une fois cette opération terminée, la boîte de dialogue **Milestone XProtect Advanced VMS** s'affiche.

   a) Sélectionnez la **Langue** à utiliser au cours de l'installation (il ne s'agit **pas** de la langue que votre système utilise une fois qu'il est installé, celle-ci est sélectionnée par la suite). Cliquez sur **Continuer**.

   b) Dans **Saisir l'emplacement du fichier de licence**, saisissez le fichier de licence envoyé par votre prestataire XProtect. Autrement, utilisez la fonction Parcourir pour le trouver. Le système vérifie votre fichier de licence avant que vous puissiez poursuivre. Cliquez sur **Continuer**.

   c) Lisez le *Contrat de licence utilisateur final Milestone*. Cochez la case **J'accepte les termes du contrat de licence**.

4. Sélectionnez **Serveur unique**. Une liste de composants à installer apparaît (vous ne pouvez pas modifier cette liste). Cliquez sur **Continuer**.

5. Sélectionnez l'**Emplacement des fichiers** pour le fichier du programme. Dans **Langue du produit**, sélectionnez la langue dans laquelle votre produit XProtect doit être installé. Cliquez sur **Installer**.

6. Le logiciel procède maintenant à l'installation. Une fois l'installation terminée, une liste des composants installés correctement s'affiche. Cliquez sur **Fermer.**

   Microsoft® IIS est installé automatiquement au cours du processus. Vous serez ensuite invité à redémarrer votre ordinateur. Faites-le puis, après le redémarrage et selon vos paramètres de sécurité, un ou plusieurs avertissements de sécurité Windows peuvent apparaître. Acceptez-les afin de terminer l'installation.

7. Une fois cette opération terminée, votre installation se termine et vous pouvez poursuivre la configuration, voir Processus de configuration (voir "Configurer le système dans le Management Client" á la page 44).

Installer votre système - option Distribué

L'option **Distribué** installe uniquement les composants du serveur de gestion sur l'ordinateur actuel. Cela signifie que le serveur d'enregistrement et XProtect Smart Client ne sont pas visibles dans la liste de composants non modifiable. Vous devez installer le serveur d'enregistrement, XProtect Smart Client et le serveur SQL sur d'autres ordinateurs.

1. Si vous installez une version téléchargée sur Internet, exécutez le fichier `Milestone XProtect Advanced VMS Products 2016 R3 System Installer.exe` à partir de l'emplacement où il a été sauvegardé.

   Autrement, insérez le DVD du logiciel. Si la boîte de dialogue ne s'ouvre pas automatiquement, exécutez le fichier `Milestone XProtect Advanced VMS Products 2016 R3 System Installer.exe` à partir du DVD.

2. La décompression des fichiers d'installation débute. Selon vos paramètres de sécurité, un ou plusieurs avertissements de sécurité Windows® apparaissent. Acceptez-les afin de poursuivre la décompression.

3. Une fois cette opération terminée, la boîte de dialogue **Milestone XProtect Advanced VMS** s'affiche.

   a) Sélectionnez la **Langue** à utiliser au cours de l'installation (il ne s'agit **pas** de la langue que votre système utilise une fois qu'il est installé, celle-ci est sélectionnée par la suite). Cliquez sur **Continuer**.

   b) Dans **Saisir l'emplacement du fichier de licence**, saisissez le fichier de licence envoyé par votre prestataire XProtect. Autrement, utilisez la fonction Parcourir pour le trouver. Le système vérifie votre fichier de licence avant que vous puissiez poursuivre. Cliquez sur **Continuer**.

   c) Lisez le *Contrat de licence utilisateur final Milestone*. Cochez la case **J'accepte les termes du contrat de licence**.

4. Sélectionnez **Distribué.** Une liste non modifiable de composants à installer apparaît. Cliquez sur **Continuer**.

5. Sélectionnez le type de base de données de serveur SQL souhaité. Spécifiez également le nom du serveur SQL. Cliquez sur **Continuer**.

6. Sélectionnez **Créer une nouvelle base de données** ou **Utiliser une base de données existante** et nommez la base de données. Si vous choisissez cette dernière option, choisissez de **Conserver** ou **Écraser** les données existantes. Cliquez sur **Continuer**.

7. Sélectionnez l'**Emplacement des fichiers** pour le fichier du programme. Dans **Langue du produit**, sélectionnez la langue dans laquelle votre produit XProtect doit être installé. Cliquez sur **Installer**.

8. Le logiciel procède maintenant à l'installation. Une fois l'installation terminée, une liste des composants installés correctement s'affiche. Cliquez sur **Fermer.**

   Microsoft® IIS est installé automatiquement au cours du processus. Vous serez ensuite invité à redémarrer votre ordinateur. Faites-le puis, après le redémarrage et selon vos paramètres de sécurité, un ou plusieurs avertissements de sécurité Windows peuvent apparaître. Acceptez-les afin de terminer l'installation.

9. Installez au moins un serveur d'enregistrement et XProtect Smart Client sur un autre ordinateur.

Voir également

Installer le serveur d’enregistrement (á la page 38)

Installer les clients (á la page 47)

Installer votre système - option Personnaliser

L'option **Personnaliser** installe toujours le serveur de gestion, mais vous pouvez faire votre choix librement parmi les autres composants du serveur de gestion, le serveur d'enregistrement et XProtect Smart Client pour une installation sur l'ordinateur actuel. Par défaut, la case du serveur d'enregistrement est décochée dans la liste de composants, mais vous pouvez modifier cette configuration. En fonction de vos choix, vous devez installer les composants non sélectionnés par la suite sur d'autres ordinateurs et le serveur SQL.

1. Si vous installez une version téléchargée sur Internet, exécutez le fichier `Milestone XProtect Advanced VMS Products 2016 R3 System Installer.exe` à partir de l'emplacement où il a été sauvegardé.

   Autrement, insérez le DVD du logiciel. Si la boîte de dialogue ne s'ouvre pas automatiquement, exécutez le fichier `Milestone XProtect Advanced VMS Products 2016 R3 System Installer.exe` à partir du DVD.

2. La décompression des fichiers d'installation débute. Selon vos paramètres de sécurité, un ou plusieurs avertissements de sécurité Windows® apparaissent. Acceptez-les afin de poursuivre la décompression.

3. Une fois cette opération terminée, la boîte de dialogue **Milestone XProtect Advanced VMS** s'affiche.

   a) Sélectionnez la **Langue** à utiliser au cours de l'installation (il ne s'agit **pas** de la langue que votre système utilise une fois qu'il est installé, celle-ci est sélectionnée par la suite). Cliquez sur **Continuer**.

   b) Dans **Saisir l'emplacement du fichier de licence**, saisissez le fichier de licence envoyé par votre prestataire XProtect. Autrement, utilisez la fonction Parcourir pour le trouver. Le système vérifie votre fichier de licence avant que vous puissiez poursuivre. Cliquez sur **Continuer**.

   c) Lisez le *Contrat de licence utilisateur final Milestone*. Cochez la case **J'accepte les termes du contrat de licence**.

4. Sélectionnez **Personnaliser**. Une liste de composants à installer apparaît. Hormis le serveur de gestion, tous les éléments de la liste sont facultatifs. Le serveur d'enregistrement est décoché par défaut, mais vous pouvez modifier ce paramètre si nécessaire. Cliquez sur **Continuer**.

5. Sélectionnez le type de base de données de serveur SQL souhaité. Le cas échéant, spécifiez également le nom du serveur SQL. Cliquez sur **Continuer**.

6. Sélectionnez **Créer une nouvelle base de données** ou **Utiliser une base de données existante** et nommez la base de données. Si vous choisissez cette dernière option, choisissez de **Conserver** ou **Écraser** les données existantes. Cliquez sur **Continuer**.

7. Sélectionnez **Ce compte prédéfini** ou **Ce compte** pour sélectionner le compte de service. Si nécessaire, saisissez un mot de passe et confirmez-le. Cliquez sur **Continuer**.

8. Si vous avez plus d'un site web IIS disponible, vous pouvez sélectionner n'importe lequel. Cependant, si l'un de vos sites est doté d'une liaison HTTPS, sélectionnez l'un de ceux-ci. Cliquez sur **Continuer**.

9. Sélectionnez l'**Emplacement des fichiers** pour le fichier du programme. Dans **Langue du produit**, sélectionnez la langue dans laquelle votre produit XProtect doit être installé. Cliquez sur **Installer**.

10. Le logiciel procède maintenant à l'installation. Une fois l'installation terminée, une liste des composants installés correctement s'affiche. Cliquez sur **Fermer.**

    Microsoft® IIS est installé automatiquement au cours du processus. Vous serez ensuite invité à redémarrer votre ordinateur. Faites-le puis, après le redémarrage et selon vos paramètres de sécurité, un ou plusieurs avertissements de sécurité Windows peuvent apparaître. Acceptez-les afin de terminer l'installation.

11. En fonction de vos sélections, installez les serveurs restants sur d'autres ordinateurs :

a) Allez sur la page web de téléchargement du serveur de gestion à partir du menu **Démarrer**.

b) Sélectionnez **Programmes** > **Milestone** > **Page d'installation administrative** et copiez l'adresse Internet.

c) Connectez-vous sur chacun des ordinateurs pour installer :

- Serveur de journaux.
- Serveur d'événements.
- Management Client.

d) Ouvrez un navigateur Internet, collez l'adresse de la page web de téléchargement du serveur de gestion dans le champ d'adresse et téléchargez l'installateur concerné.

e) Lancez l'installateur.

12. Installez le serveur d'enregistrement sur un ordinateur séparé, voir Installer le serveur d'enregistrement (voir "Installer le serveur d'enregistrement" á la page 38).

Installer le serveur d'enregistrement

Une fois que vous avez installé le serveur de gestion, téléchargez l'installateur du serveur d'enregistrement séparé à partir de la page web du serveur de gestion.

Reportez-vous à la rubrique Installer un serveur d'enregistrement de basculement (voir "Installer un serveur d'enregistrement de redondance" á la page 99) si vous souhaitez installer un serveur de basculement.

1. Sur le serveur de gestion, allez sur la page web de téléchargement du serveur de gestion à partir du menu Démarrer.
2. Sélectionnez **Programmes**, **Milestone**, **Page d'installation administrative** et copiez l'adresse Internet.
3. Connectez-vous sur l'ordinateur où vous souhaitez installer le serveur d'enregistrement.
4. Ouvrez un navigateur Internet, collez l'adresse de la page web de téléchargement du serveur de gestion dans le champ d'adresse et sélectionnez l'installateur du serveur d'enregistrement. Sauvegardez l'installateur dans un emplacement approprié et exécutez-le à partir de là ou directement sur la page web.
5. Sélectionnez la **Langue** que vous souhaitez utiliser pendant l'installation. Cliquez sur **Continuer**.
6. Sélectionnez :

   Typique : pour installer un serveur d'enregistrement avec des valeurs par défaut, ou

   Personnaliser : pour installer un serveur d'enregistrement avec des valeurs personnalisées.
7. Spécifiez les paramètres du serveur d'enregistrement :

   - Nom.
   - Adresse du serveur de gestion.

- Chemin pour sauvegarder les enregistrements, et cliquez sur **Continuer**.

8. Si vous avez sélectionné **Personnaliser** :

   a) Précisez le nombre de serveurs d'enregistrement que vous souhaitez installer sur cet ordinateur. Cliquez sur **Continuer**.

   b) Précisez le compte de service. Si nécessaire, saisissez un mot de passe et confirmez-le. Cliquez sur **Continuer**.

9. Sélectionnez l'**Emplacement des fichiers** pour le fichier du programme. Dans **Langue du produit**, sélectionnez la langue dans laquelle votre système doit être installé. Cliquez sur **Installer**.

10. Le logiciel procède maintenant à l'installation. Une fois l'installation terminée, une liste des composants installés correctement s'affiche. Cliquez sur **Fermer.**

    Une fois que vous avez installé le serveur d'enregistrement, vous pouvez vérifier son état à partir de l'icône **Service Recording Server**.

11. Une fois cette opération terminée, votre installation se termine et vous pouvez poursuivre la configuration, voir Processus de configuration (voir "Configurer le système dans le Management Client" á la page 44).

Installation silencieuse d'un serveur d'enregistrement

L'avantage d'une installation silencieuse est qu'elle peut être effectuée à distance. Suivre les étapes ci-dessous :

1. Localisez le fichier d'installation du serveur d'enregistrement : *MilestoneXProtectRecordingServerInstaller_x64.exe*.

   1. Connectez-vous au serveur de gestion.

   2. Ouvrez une fenêtre de navigation Internet et saisissez l'adresse : http://localhost/Installation/Admin/

   3. Enregistrez le fichier d'installation sur le serveur sur lequel vous souhaitez installer le nouveau serveur d'enregistrement.

   Vous pouvez aussi naviguer vers le fichier. En règle générale, le chemin d'accès est le suivant :
   C:\Program Files\Milestone\XProtect Management Server\IIS\httpdocs\Admin\Recording Server Installer\[version number] [bit-version]\All Languages\en-US

2. Exécutez une installation silencieuse grâce à ces options :

   - Exécuter avec les paramètres par défaut :

     Pour exécuter une installation silencieuse à l'aide des valeurs par défaut pour tous les paramètres, lancez une invite de commande (cmd.exe) dans le répertoire dans lequel se trouve le programme d'installation et exécutez la commande suivante :

     >MilestoneXProtectRecordingServerInstaller_x64.exe --quiet

- Pour effectuer une installation personnalisée, vous devez préciser la liste des paramètres que vous voulez écraser :

  Par exemple, pour modifier le chemin d'accès vers le serveur de gestion de l'installation, exécutez :

  ><MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --parameters=SERVERHOSTNAME:DKWS-OKR-02

  Vous pouvez utiliser les paramètres suivants via les paramètres de ligne de commande :

  - Pour modifier le nom du serveur d'enregistrement :

  RECORDERNAME – nom de l'enregistreur qui apparaitra dans le client d'administration.

  --quiet --parameters=RECORDERNAME:NewRecorderName

  - Pour installer un serveur d'enregistrement de redondance :

  ISFAILOVER – sélectionnez Vrai pour cet indicateur

  --quiet --parameters=ISFAILOVER:True

  - Pour modifier le serveur de gestion :

  SERVERHOSTNAME – nom d'hôte du serveur de gestion sur lequel le serveur d'enregistrement sera connecté

  SERVERPORT – port du serveur de gestion (80 par défaut)

  --quiet --parameters=SERVERHOSTNAME:DKWS-OKR-02

  - Pour installer le serveur d'enregistrement en tant qu'utilisateur différent que NT AUTHORITY\NETWORK SERVICE :

  RECUSERACCOUNT – indicateur qui détermine si le compte d'utilisateur est utilisé ou l'un des comptes prédéfinis

  RECSERVICEACCOUNT – nom de l'utilisateur utilisé ou compte d'utilisateur prédéfini

  RECPASSWORD – mot de passe crypté ! pour l'utilisateur. À laisser vide pour les comptes prédéfinis.

  Pour trouver la version cryptée du mot de passe, vous pouvez exécuter l'installation en mode habituel. Ouvrez c:\ProgramData\Milestone\Installer\Milestone XProtect Recording Server (64_bit)I.log (il se peut qu'il y ait des chiffres supplémentaires à la fin du nom si plus d'une installation ont été effectuées sur l'ordinateur)

  Trouvez la chaîne "Ligne de commande". Il s'agit de la liste complète des paramètres utilisée au cours de l'installation. Celle marquée ENCRYPTEDPASSWORD possède un mot de passe crypté.

  --quiet --parameters=RECUSERACCOUNT:true:RECSERVICEACCOUNT:Milestone\okr:RECPASSWORD:encryptedpasswork

- Afin de modifier l'emplacement de l'installation par défaut, vous devez d'abord exécuter :

  ><MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=C:\temp

Dans l'emplacement spécifié, vous trouverez un fichier .xml contenant les paramètres. Vous devez modifier les paramètres contenus dans ce fichier et exécuter votre installation avec le nouveau fichier.

- Pour modifier l'emplacement de l'installation :

INSTALLDIR - chemin d'accès où le serveur d'enregistrement doit être installé

TARGETDIR – devrait être identique à INSTALLDIR

INSTALLLOCATION – devrait être identique à INSTALLDIR

- Pour modifier l'emplacement de l'enregistrement :

MEDIADBPATH – chemin d'accès vers la base de données multimédia avec tous les enregistrements

P. ex. modifications dans my Agreements_.xml Le nouvel emplacement de l'installation sera %ProgramFiles(x86)%\Milestone\ et le nouvel emplacement pour les enregistrements est C:\MD

<KeyValueParametersOfStringString>

*<Value>***%ProgramFiles(x86)%\Milestone\bla***</Value>*

<Key>INSTALLDIR</Key>

</KeyValueParametersOfStringString>

<KeyValueParametersOfStringString>

*<Value>***%ProgramFiles(x86)%\Milestone\bla***</Value>*

<Key>TARGETDIR</Key>

</KeyValueParametersOfStringString>

<KeyValueParametersOfStringString>

*<Value>***%ProgramFiles(x86)%\Milestone\bla***</Value>*

<Key>INSTALLLOCATION</Key>

</KeyValueParametersOfStringString>

<KeyValueParametersOfStringString>

*<Value>***C:\MD***</Value>*

*<Key>***MEDIADBPATH***</Key>*

</KeyValueParametersOfStringString>

Exécutez :

><MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --arguments=C:\temp\Arguments_.xml

Dépannage

Où puis-je trouver les fichiers journaux de l'installation ?

Les fichiers journaux de l'installation se trouvent sous **C:\ProgramData\Milestone\Installer**

Comment puis-je voir la liste des paramètres par défaut qui seront utilisés au cours de l'installation d'un seul serveur ?

Pour voir la liste des paramètres avec toutes les valeurs par défaut, vous pouvez exécuter **MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=C:\temp**

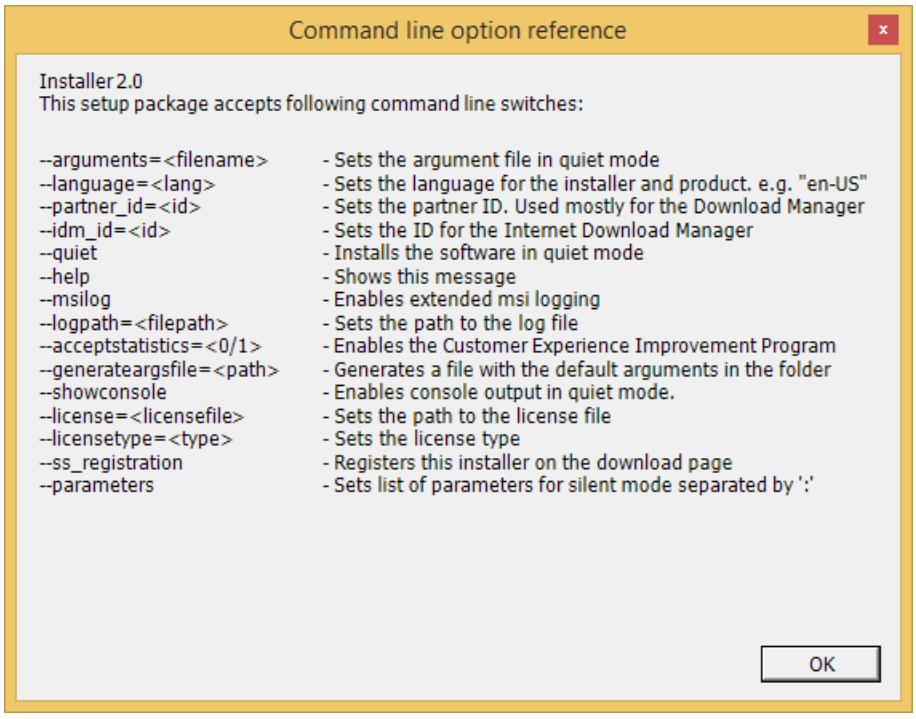
Cela génèrera un fichier appelé Arguments.xml dans le répertoire spécifié.

Comment puis-je voir les paramètres utilisés au cours de mon installation personnalisée ?

La liste complète des paramètres utilisés pour exécuter l'installation se trouve dans **C:\ProgramData\Milestone\Installer\Milestone XProtect Recording Server (64_bit)I.log** + recherchez "Ligne de commande"

Comment afficher une liste complète des paramètres possibles ?

Exécutez **MilestoneXProtectRecordingServerInstaller_x64.exe --help**



Configurer l’authentification Kerberos

Utilisez l’authentification Kerberos comme alternative protocole d’authentification Microsoft NT LAN (NTLM) plus ancien.

Voir À propos de l’authentification Kerberos (á la page 31) pour plus d'informations.

Installation pour les groupes de travail

Si vous avez recours non pas à une configuration de domaine mais à un serveur Active Directory, procédez comme suit lors de l'installation :

1. Connectez-vous à Windows en utilisant un compte administrateur commun.

   Assurez-vous d'utiliser le même compte sur tous les ordinateurs du système.

2. Selon vos besoins, démarrez l'installation du serveur de gestion ou d'enregistrement et cliquez sur **Personnaliser**.

3. Selon votre sélection lors de la 2ème étape, choisissez d'installer le service Management Server ou Recording Server à l'aide d'un compte d'administrateur commun.

4. Terminez l'installation.

5. Répétez les étapes 1 à 4 pour installer tous les autres systèmes que vous souhaitez connecter. Ils doivent tous être installés en utilisant un compte administrateur commun.

Vous ne pouvez pas utiliser cette méthode lorsque vous **mettez à jour** les installations de groupe de travail. Consultez la rubrique Mise à niveau alternative pour les groupes de travail (á la page 56).

Dépannage à l'installation

Les problèmes suivants peuvent survenir après ou au cours de l'installation du serveur de gestion ou des serveurs d'enregistrement. Pour chaque problème, une ou plusieurs solutions sont disponibles.

Problème : Le démarrage du serveur d'enregistrement échoue en raison d'un conflit de port.

Ce problème peut apparaître uniquement si le service Simple Mail Transfer Protocol **(**SMTP) est en cours de fonctionnement car il utilise le port 25. Si le port 25 est déjà en cours d'utilisation, il n'est alors pas possible de démarrer le service Recording Server. Il est important que le port numéro 25 soit disponible pour le service SMTP du serveur d'enregistrement.

Service SMTP : Vérification et solutions

Pour vérifier si le service SMTP est installé :

1. Dans le menu **Démarrer** de Windows, sélectionnez **Panneau de configuration.**

2. Dans le **Panneau de configuration**, double-cliquez sur **Ajouter/supprimer des programmes**.

3. Dans la partie gauche de la boîte de dialogue **Ajouter/supprimer des programmes**, cliquez sur **Ajouter/supprimer des composants Windows**.

4. Dans l'assistant **Composants Windows**, sélectionnez **Internet Information Services (IIS)**, et cliquez sur le bouton **Détails**.

5. Dans la fenêtre **Internet Information Services (IIS)**, vérifiez si la case **SMTP Service** est cochée ou non. Si c'est le cas, SMTP Service est installé.

Si SMTP Service est installé, sélectionnez l'une des solutions suivantes :

Solution 1 : Désactivez SMTP Service, ou réglez-le sur manual startup (démarrage manuel)

Cette solution vous permet de démarrer le serveur d'enregistrement sans avoir à interrompre SMTP Service à chaque fois :

1. Dans le menu **Démarrer** de Windows, sélectionnez **Panneau de configuration.**
2. Dans le **Panneau de configuration**, double-cliquez sur **Outils d'administration**.
3. Dans la fenêtre **Outils d'administration**, double-cliquez sur **Services**.
4. Dans la fenêtre **Services**, double-cliquez sur **Simple Mail Transfer Protocol (SMTP)**.
5. Dans la fenêtre **Propriétés SMTP**, cliquez sur **Arrêt**, puis réglez **Type de démarrage** sur **Manuel** ou **Désactivé**.

   Lorsqu'il est réglé sur **Manuel**, SMTP Service peut être démarré manuellement à partir de la fenêtre **Services**, ou à partir d'une invite de commande, en utilisant la commande *net start SMTPSVC*.
6. Cliquez sur **OK**.

Solution 2 : Supprimer SMTP Service

La suppression de SMTP Service peut affecter d'autres applications utilisant le service SMTP.

1. Dans le menu **Démarrer** de Windows, sélectionnez **Panneau de configuration.**
2. Dans la fenêtre **Panneau de configuration**, double-cliquez sur **Ajouter/supprimer des programmes**.
3. Dans la partie gauche de la boîte de dialogue **Ajouter/supprimer des programmes**, cliquez sur **Ajouter/supprimer des composants Windows**.
4. Dans l'assistant **Composants Windows**, sélectionnez l'élément **Internet Information Services (IIS)**, et cliquez sur le bouton **Détails**.
5. Dans la fenêtre **Internet Information Services (IIS)**, décochez la case **SMTP Service**.
6. Cliquez sur **OK**, **Suivant**, puis sur **Terminer**.

Problème : Des modifications au niveau de l'emplacement du serveur SQL empêchent tout accès à la base de données

Ceci représente un problème en cas de modification de l'emplacement du serveur SQL, par exemple lors de la modification du nom d'hôte de l'ordinateur exécutant le serveur SQL. En conséquence, l'accès à la base de données est perdu.

Solution : Utiliser l'outil de mise à jour d'adresse SQL, qui se trouve sur l'icône de notification.

Configurer le système dans le Management Client

Dans le paragraphe suivant, vous trouverez une liste de tâches généralement impliquées dans la configuration du système.

Bien que les tâches soient présentées sous la forme d'une liste de contrôle, effectuer tous ces contrôles ne garantit pas en soi que le système soit parfaitement adapté aux besoins de votre organisation. Pour que le système soit adapté aux besoins de votre organisation, Milestone vous recommande de contrôler et d'ajuster le système de façon continue.

Par exemple, il est judicieux de tester et de régler les paramètres de sensibilité aux mouvements des caméras individuelles dans des conditions physiques différentes (et notamment jour/nuit, vent fort/absence de vent) une fois que le système est en fonctionnement.

La création de règles qui déterminent la plupart des actions exécutées par votre système (y compris quand enregistrer des vidéos), est un autre exemple de configuration que vous pouvez modifie en fonction des besoins de votre entreprise.

☑	Vous avez terminé l'installation initiale de votre système. Voir Installer le système (á la page 34).
☑	Changer le SLC d'essai au profit d'un SLC permanent (si nécessaire). Voir Changer le code de licence du logiciel (voir "Modifier le code de licence du logiciel" á la page 46).
☑	Connectez-vous au Management Client.
☐	Autoriser l'utilisation des serveurs d'enregistrement de votre système. Voir Autoriser un serveur d'enregistrement (á la page 75).
☐	Vérifier que les paramètres de stockage de chaque serveur d'enregistrement répondent à vos besoins. Voir À propos du stockage et de l'archivage (á la page 79).
☐	Vérifier que les paramètres d'archivage de chaque serveur d'enregistrement répondent à vos besoins. Voir Propriétés des paramètres d'archive (á la page 87).
☐	Détecter les périphériques, caméras et encodeurs vidéo, qui peuvent être ajoutés à chaque serveur d'enregistrement. Voir Ajout de matériels (voir "Ajouter matériel" á la page 104).
☐	Configurer les caméras individuelles de chaque serveur d'enregistrement. Voir À propos des périphériques de caméras (voir "À propos des périphériques de la caméra" á la page 119).
☐	Activer le stockage et l'archivage pour des caméras individuelles ou pour un groupe de caméras. Cette opération peut être effectuée à partir des caméras individuelles ou à partir du groupe de périphériques. Voir Relier un périphérique ou un groupe de périphériques à un emplacement de stockage (á la page 82).
☐	Activer et configurer des périphériques. Voir Travailler avec des périphériques (á la page 119).
☐	Les règles déterminent largement le comportement du système. Les règles incluent quand les caméras doivent enregistrer, quand les caméras PTZ (pan-tilt-zoom) doivent patrouiller et quand les notifications doivent être envoyées. Créer des règles. Voir À propos des règles et événements (á la page 174).

☐	Ajouter des rôles au système. Voir À propos des rôles (á la page 214).
☐	Ajouter des utilisateurs et/ou des groupes d'utilisateurs à chacun des rôles. Voir Assigner et supprimer des utilisateurs et groupes aux/des rôles (á la page 218).
☐	Activer des licences. Voir Activer des licences en ligne (voir "Activation des licences en ligne" á la page 72) ou Activer des licences hors ligne (voir "Activation des licences hors ligne" á la page 72).

Modifier le code de licence du logiciel

Si votre installation fonctionne avec un code de licence du logiciel (SLC) d'essai pendant la première période, vous pouvez le changer au profit d'un SLC permanent sans avoir besoin de désinstaller ni de réinstaller quoi que ce soit lorsque vous recevez un nouveau fichier de licence logicielle.

Important : Cette opération doit être effectuée localement sur le serveur de gestion. Vous **ne pouvez pas** le faire à partir du Management Client.

1. Sur le serveur de gestion, allez dans la zone de notification de la barre des tâches.

2. Cliquez avec le bouton droit sur l'icône **Serveur de gestion** et sélectionnez **Changer de licence**.
3. Cliquez sur **Importer une licence**.
4. Ensuite, sélectionnez le fichier de licence du logiciel sauvegardé à cette fin. Lorsque vous avez terminé, l'emplacement du fichier de licence du logiciel sélectionné est ajouté juste en-dessous du bouton **Importer une licence**.
5. Cliquez sur **OK**. Vous êtes maintenant prêt à enregistrer le SLC. Voir Enregistrer le code de licence du logiciel (á la page 34).

À propos des plages d'adresses IP locales

Lorsqu'un client, tel que XProtect Smart Client, se connecte à un système de surveillance, une quantité de communication de données initiales, y compris l'échange d'adresses de contact, se poursuit en arrière-plan. Cela s'effectue automatiquement de façon transparente pour les utilisateurs.

Les clients peuvent se connecter depuis le réseau local ainsi que depuis internet, et dans chaque cas le système de surveillance doit pouvoir fournir les adresses adéquates pour que les clients aient accès aux vidéos en direct et enregistrées à partir des serveurs d'enregistrement :

- Lorsque les clients se connectent localement, le système de surveillance doit communiquer avec les adresses locales et les numéros de port.

- Lorsque les clients se connectent depuis Internet, le système de surveillance doit répondre avec l'adresse publique du serveur d'enregistrement, c'est-à-dire l'adresse du pare-feu ou du routeur NAT (traduction d'adresses réseau), et souvent aussi un numéro de port différent (qui est ensuite redirigé jusqu'aux serveurs d'enregistrement).

Le système de surveillance doit par conséquent pouvoir déterminer si un client appartient à une plage IP locale ou à Internet. À cette fin, vous pouvez définir une liste de plages IP que le système de surveillance doit reconnaître comme provenant d'un réseau local.

Installer les clients

Installer XProtect Smart Client silencieusement

Vous avez la possibilité de déployer XProtect Smart Client ou votre logiciel de surveillance vers les ordinateurs d'autres utilisateurs à l'aide d'outils tels que Microsoft Systems Management Server (SMS). Ce type d'outil vous permet de créer des bases de données des matériels et des logiciels sur des réseaux locaux. Les bases de données peuvent alors, entre autres, être utilisées pour distribuer et installer des logiciels, comme XProtect Smart Client, sur des réseaux locaux.

1. Localisez le fichier du programme d'installation du Smart Client (.exe) - *XProtect Smart Client 2016 R3 Installer.exe* ou *XProtect Smart Client 2016 R3 Installer x64.exe* pour les versions 32 et 64 bits, respectivement. Vous trouverez le fichier dans un sous-dossier du dossier **httpdocs**. Le dossier **httpdocs** est situé dans le dossier dans lequel votre logiciel de surveillance Milestone est installé.

   Le chemin d'accès est généralement :
   C:\Program Files\Milestone\XProtect Management Server\IIS\httpdocs\XProtect Smart Client Installer\[version number] [bit-version]\All Languages\en-US

   Par exemple :
   C:\Program Files\Milestone\XProtect Management Server\IIS\httpdocs\XProtect Smart Client Installer\2016 (32-bit)\All Languages\en-US

2. Lance une installation silencieuse avec l'une des deux options suivantes :

   a Exécuter avec les paramètres par défaut :

   pour exécuter une installation silencieuse à l'aide des valeurs par défaut pour tous les paramètres, lancez une invite de commande (cmd.exe) dans le répertoire dans lequel se trouve le programme d'installation et exécutez la commande suivante :

   >XProtect Smart Client 2016 R3 Installer.exe --quiet

   Cela effectue une installation silencieuse de XProtect Smart Client en utilisant les valeurs par défaut pour des paramètres tels que le répertoire cible et ainsi de suite. Voir ci-dessous pour modifier les paramètres par défaut.

   b Personnaliser les paramètres par défaut à l'aide d'un fichier d'argument xml comme entrée :

   Pour personnaliser les paramètres d'installation par défaut, fournissez un fichier xml aux valeurs modifiées comme entrée. Pour générer le fichier xml avec les valeurs par défaut, ouvrez une invite de commande dans le répertoire dans lequel se trouve le programme d'installation et exécutez la commande suivante :

>XProtect Smart Client 2016 R3 Installer.exe --generateargsfile=[path]

Ouvrez le fichier Arguments.xml ainsi généré, par exemple à l'aide du bloc-notes de Windows, et effectuez toutes les modifications nécessaires. Ensuite, pour effectuer une installation silencieuse à l'aide de ces valeurs modifiées, exécutez la commande suivante dans le même répertoire.

>XProtect Smart Client 2016 R3 Installer.exe --arguments=args.xml --quiet

Installer le serveur Milestone Mobile

Une fois le serveur Milestone Mobile installé, vous pouvez utiliser le client Milestone Mobile et XProtect Web Client avec votre système. Pour réduire l'usage général des ressources du système sur l'ordinateur exécutant le serveur de gestion, installez le serveur Milestone Mobile sur un ordinateur séparé.

Le serveur de gestion est doté d'une page web d'installation publique. À partir de cette page web, les administrateurs et utilisateurs finaux peuvent télécharger et installer les composants requis du système XProtect à partir du serveur de gestion ou de tout autre ordinateur du système.

Pour accéder à la page web d'installation :

1. Saisissez l'URL suivante dans votre navigateur : http://[adresse *du serveur de gestion]/installation/admin*

   [adresse du serveur de gestion] est l'adresse IP ou le nom d'hôte du serveur de gestion.

2. Cliquez sur **Toutes les langues** pour l'installateur du serveur Milestone Mobile.

3. Lancez le fichier téléchargé. Cliquez sur **Oui** pour tous les avertissements. Le déballage commence.

4. Choisissez la langue du programme d'installation. Cliquez sur **Continuer**.

5. Lisez et acceptez le contrat de licence. Cliquez sur **Continuer**.

6. Sélectionnez le type d'installation. Cliquez sur **Typique** pour l'installer avec les sélections par défaut.

7. Spécifiez le serveur primaire du système de surveillance :

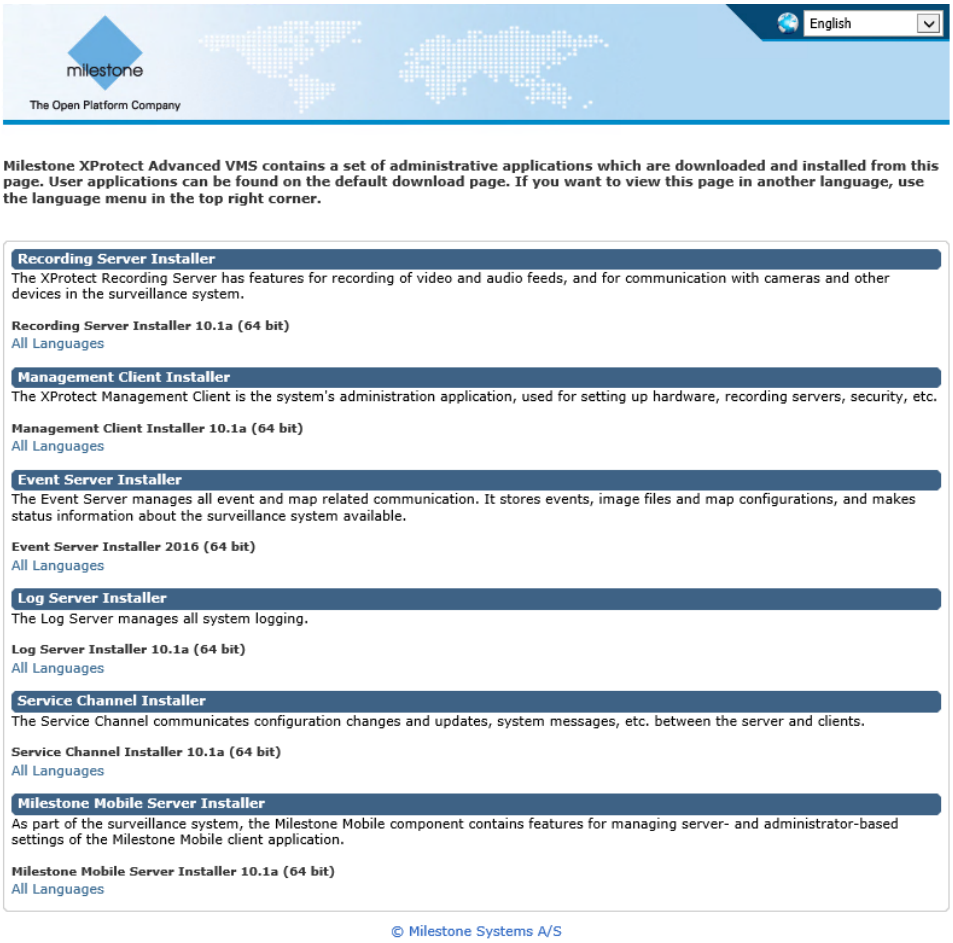
   - URL du serveur de gestion
   - Connexion
   - Nom d'utilisateur et mot de passe. Cliquez sur **Continuer**.

8. Sélectionnez l'emplacement du fichier et la langue du produit. Cliquez sur **Installer**. Une fois l'installation terminée, une liste de composants correctement installés s'affiche. Cliquez sur **Fermer.**

Êtes-vous prêt pour la configuration de Milestone Mobile (voir "Configuration Milestone Mobile" á la page 375).

Download Manager/page web de téléchargement.

Le serveur de gestion est doté d'une page web intégrée. Cette page web permet aux administrateurs et aux utilisateurs finaux de télécharger et d'installer les composants requis du système XProtect à partir de n'importe quel emplacement, localement ou à distance.



La page web est capable d'afficher deux groupes de contenu, tous deux dans une langue qui, par défaut, correspond à la langue d'installation du système :

- Une page web est destinée aux **administrateurs** et leur permet de télécharger et d'installer les principaux composants du système. La plupart du temps, la page web est automatiquement chargée à la fin de l'installation du serveur de gestion et le contenu par défaut s'affiche. Sur le serveur de gestion, vous pouvez accéder à la page web à partir du menu **Démarrer** de Windows. Sélectionnez **Programmes** > **Milestone** > **Page d'installation administrative**. Sinon, vous pouvez saisir l'URL :

  http://[adresse *du serveur de gestion]:[port]/installation/admin/*

  [adresse serveur de gestion] est l'adresse IP ou le nom d'hôte du serveur de gestion, et [port] correspond au numéro de port pour lequel vous avez configuré IIS pour l'utiliser sur le serveur de gestion. Si l'accès à la page Web n'a pas lieu sur le serveur de gestion, connectez-vous à partir d'un compte qui possède des droits d'administrateur sur le serveur de gestion.

- L'autre page web est destinée aux **utilisateurs** finaux et leur permet d'accéder aux applications client dans leur configuration par défaut. Sur le serveur de gestion, vous pouvez accéder à la page web à partir du menu **Démarrer** de Windows. Sélectionnez **Programmes** > **Milestone** > **Page d'installation publique**. Sinon, vous pouvez saisir l'URL :

  http://[adresse *du serveur de gestion]:[port]/installation/*

  [adresse serveur de gestion] est l'adresse IP ou le nom d'hôte du serveur de gestion, et [port] correspond au numéro de port pour lequel vous avez configuré IIS pour l'utiliser sur le serveur de gestion.

Les deux pages web ont des contenus par défaut et peuvent ainsi être utilisées immédiatement après le processus d'installation. Cependant, en tant qu'administrateur, vous pouvez personnaliser les éléments apparaissant sur les pages web à l'aide du Download Manager. Vous pouvez également déplacer des composants entre les deux versions de la page web. Pour déplacer un composant, cliquez dessus à l'aide du bouton droit de votre souris et sélectionnez tout simplement la version de la page web vers laquelle vous souhaitez déplacer le composant.

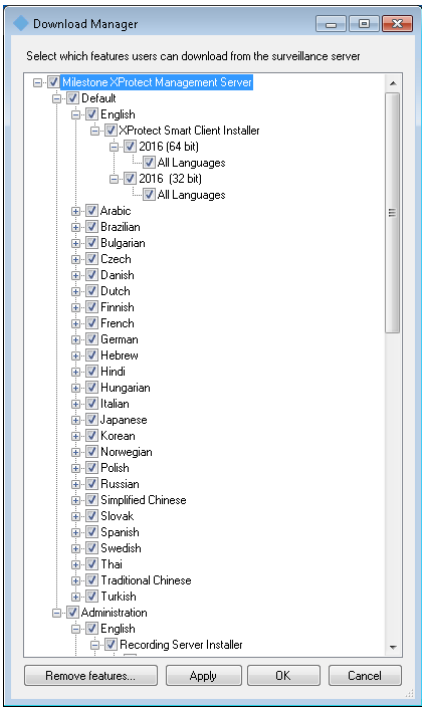
Même si vous pouvez contrôler les composants que les utilisateurs peuvent télécharger et installer dans Download Manager, vous ne pouvez pas l'utiliser en tant qu'outil de gestion des droits des utilisateurs. Ces droits sont déterminés par les rôles définis dans le Management Client.

Sur le serveur de gestion, vous pouvez accéder au XProtect Download Manager à partir du menu **Démarrer** de Windows. Sélectionnez **Programmes** > **Milestone** > **XProtect Download Manager**.

Configuration du Download Manager par défaut

Le Download Manager a une configuration par défaut. Ceci vous permet de vous assurer que les utilisateurs de votre organisation peuvent accéder aux composants standard dès le début.

La configuration par défaut offre aux administrateurs une configuration par défaut avec accès au téléchargement de composants supplémentaires ou facultatifs. Vous accédez généralement à la page web à partir de l'ordinateur du serveur de gestion, mais vous pouvez également accéder à la page web à partir d'autres ordinateurs.



- Le premier niveau : Se rapporte à votre produit XProtect.
- Le deuxième niveau : Se rapporte aux deux versions ciblées de la page web. **Par défaut** se rapporte à la version de la page web visualisée par les utilisateurs finaux. **Administration** se rapporte à la version de la page web visualisée par les administrateurs du système.
- Le troisième niveau : Se rapporte aux langues dans lesquelles la page web est disponible.
- Le quatrième niveau : Se rapporte aux composants qui sont (ou peuvent être mis) à la disposition des utilisateurs.
- Le cinquième niveau : Se rapporte aux versions particulières de chaque composant qui sont (ou peuvent être mises) à la disposition des utilisateurs.
- Le sixième niveau : Se rapporte aux versions linguistiques des composants qui sont (ou peuvent être mises) à la disposition des utilisateurs.

Le fait que seules les composants standard soient disponibles au départ - et ce uniquement dans la même langue que le système lui-même - permet de réduire la durée d'installation et d'économiser de l'espace sur le serveur. Il est tout simplement inutile d'avoir un composant ou une langue disponible sur le serveur si personne ne s'en sert.

Vous pouvez mettre à disposition davantage de composants ou de langues selon les besoins et vous pouvez masquer ou supprimer les composants ou langues indésirables.

Installateurs standard du Download Manager (utilisateur)

Par défaut, les composants suivants sont disponibles sur la page web de téléchargement du serveur de gestion destinée aux utilisateurs (contrôlée par le Download Manager) à des fins d'installation séparée :

- Serveurs d'enregistrement, y compris les serveurs d'enregistrement de redondance. Les serveurs d'enregistrement de redondance sont initialement téléchargés et installés en tant que serveurs d'enregistrement et c'est au cours du processus d'installation que vous spécifiez que vous souhaitez installer un serveur d'enregistrement de redondance.
- Management Client
- XProtect Smart Client
- Serveur d'événements, utilisé en lien avec la fonctionnalité de plans
- Serveur de journaux, utilisé afin d'offrir les fonctions nécessaires pour journaliser les informations du système
- Canal de service, permet de communiquer automatiquement et en toute transparence les paramètres entre différents serveurs et clients
- Serveur Milestone Mobile - **disponible uniquement ici**
- De plus amples options peuvent être disponibles pour votre entreprise.

Pour l'installation des **pilotes de périphériques**, reportez-vous à l'Installateur de pilotes de périphériques - doit être téléchargé (á la page 54).

Ajouter/publier les composants de l'installateur Download Manager

Vous devez exécuter deux procédures pour mettre les composants non standard et les nouvelles versions à disposition sur la page de téléchargement du serveur de gestion.

Tout d'abord, **ajoutez les nouveaux composants et/ou les composants non standard sur le Download Manager**. Vous l'utilisez ensuite pour **affiner les composants qui doivent être disponibles** dans les diverses langues de la page web.

Si le Download Manager est ouvert, fermez-le avant d'installer de nouveaux composants.

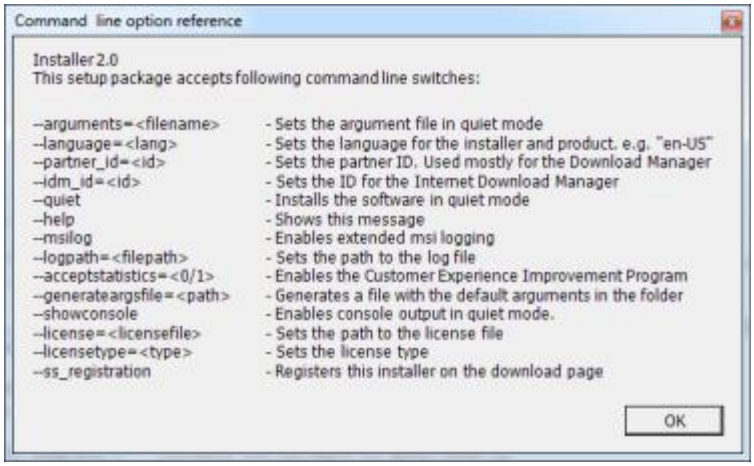
Ajouter de nouveaux fichiers/des fichiers non standard sur le Download Manager :

1. Sur l'ordinateur sur lequel vous avez téléchargé le(s) composant(s), allez dans le menu **Démarrer** de Windows et saisissez une *invite de commande*.
2. Dans l'*invite de commande*, exécutez le nom du fichier (*.exe*) avec :[espace]--*ss_registration*

   Exemple : *RecordingServer_setup_x64.exe --ss_registration*

   Le fichier est maintenant ajouté au Download Manager mais n'est **pas** installé sur l'ordinateur actuel.

Pour obtenir une vue d'ensemble des commandes de l'installateur, dans la fenêtre d'*Invite de commande*, saisissez [espace]*--aide* pour faire apparaître la fenêtre suivante :



Une fois les nouveaux composants installés, ceux-ci sont sélectionnés par défaut dans le Download Manager et sont immédiatement mis à disposition des utilisateurs par le biais de la page web. Vous pouvez toujours afficher ou masquer les fonctions sur la page web en cochant ou en décochant des cases de l'arborescence du Download Manager.

Vous pouvez modifier la séquence d'affichage des composants sur la page web. Dans l'arborescence du Download Manager, faites glisser les composants et déposez-les à l'emplacement désiré.

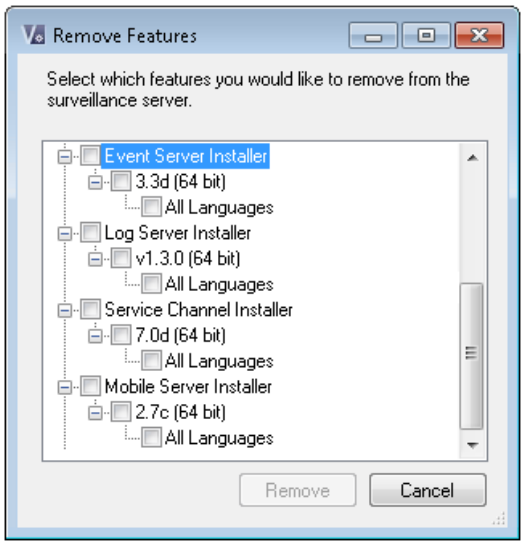
Masquer/supprimer les composants de l'installateur Download Manager

Trois options s'offrent à vous :

- **Masquer des fonctions** depuis la page web en décochant des cases de l'arborescence Download Manager. Les composants sont tout de même installés sur le serveur de gestion, mais en cochant des cases de l'arborescence du Download Manager, vous pourrez rapidement rendre les composants à nouveau disponibles.
- **Supprimer l'installation des composants** sur le serveur de gestion. Les composants disparaissent du Download Manager, mais les fichiers d'installation des composants restent sur *C:\Program Files (x86)\Milestone\XProtect Download Manager*. Vous pourrez donc les réinstaller ultérieurement si nécessaire.

1. Dans le Download Manager, cliquez sur **Supprimer fonctions**.

2. Dans la fenêtre **Supprimer fonctions**, sélectionnez la ou les fonction(s) à supprimer.



3. Cliquez sur **OK** et **Oui**.

- **Supprimer les fichiers d'installation de fonctions non désirées** depuis le serveur de gestion. Ceci permet d'économiser de l'espace disque sur le serveur si vous savez que votre entreprise n'utilisera pas certaines fonctions.

Installateur de pilotes de périphériques - doit être téléchargé

Les pilotes de périphériques inclus dans votre installation d'origine ne sont pas inclus sur le site web de téléchargement. Ainsi, si vous devez réinstaller les pilotes de périphériques ou mettre l'installateur de pilotes de périphériques à disposition, vous devez tout d'abord ajouter ou publier le tout dernier installateur de pilotes de périphériques sur le Download Manager en procédant comme suit :

1. Vous pouvez obtenir les pilotes de périphériques les plus récents à partir de la page de téléchargement sur le site web http://www.milestonesys.com/downloads de Milestone.

2. Ajoutez/publiez-le sur le Download Manager en l'appelant à l'aide de la commande --*ss_registration*.

Si vous n'avez pas de connexion réseau, vous pouvez réinstaller l'ensemble du serveur d'enregistrement à partir de Download Manager. Les fichiers d'installation du serveur d'enregistrement sont sauvegardés localement sur votre ordinateur. Ainsi, vous bénéficiez d'une réinstallation automatique du pilote de périphérique.

Mise à niveau

À propos de la mise à niveau

Ces informations ne sont pertinentes que si vous mettez à niveau une installation XProtect précédente.

Important : Votre système XProtect ne prend plus en charge Microsoft Windows XP.

Lorsque vous procédez à la mise à niveau, tous les composants à l'exception de la base de données du serveur de gestion sont automatiquement supprimés et remplacés. Cela inclut vos pilotes de périphériques.

La base de données du serveur de gestion contient l'ensemble de la configuration du système (configurations des serveurs d'enregistrement, configurations des caméras, règles, etc.). Tant que vous ne supprimez pas la base de données du serveur de gestion, votre système de surveillance ne requiert aucune reconfiguration, même si vous pouvez configurer certaines nouvelles fonctions présentes dans la nouvelle version si vous le souhaitez.

La compatibilité rétrospective avec les serveurs d'enregistrement provenant de versions de XProtect antérieures à la présente version est limitée. Vous pouvez toujours accéder aux enregistrements sur ces serveurs d'enregistrement plus anciens, mais pour que puissiez modifier leur configuration, ils doivent être de la même version que celui-ci. Milestone recommande que vous mettiez à niveau tous les serveurs d'enregistrement de votre système.

Lorsque vous mettez vos serveurs d'enregistrement à niveau, vous devez indiquer si vous souhaitez **mettre à jour** ou **conserver** vos pilotes de périphériques vidéo. Si vous choisissez de les mettre à jour, vos périphériques matériels prendront peut-être quelques minutes pour contacter les nouveaux pilotes de périphériques vidéo après avoir redémarré votre système. Cela peut être à cause des nombreuses vérifications internes qui ont lieu sur les pilotes qui viennent tout juste d'être installés.

Conditions préalables de mise à niveau

- Assurez-vous d'avoir votre **fichier de licence du logiciel** (voir "**À propos des licences**" á la page 22) (.lic) à disposition.

  - **Mise à jour du Service Pack** : Au cours de l'installation du serveur de gestion, l'assistant vous demandera peut-être de préciser l'emplacement du fichier de la licence du logiciel. Vous pouvez utiliser le fichier de la licence du logiciel que vous avez reçu après l'achat de votre système (ou après la dernière mise à jour) ou celui que vous avez reçu suite à la dernière activation de votre licence.

  - **Mise à jour de la version :** Après avoir acheté la nouvelle version, vous recevrez un nouveau fichier de licence du logiciel. Au cours de l'installation du serveur de gestion, l'assistant vous demandera de préciser l'emplacement du fichier de la licence du logiciel.

  Le système vérifie votre fichier de licence avant que vous puissiez poursuivre. Les périphériques déjà ajoutés nécessitant une licence passent en période de grâce. Si vous n'avez pas activé l'activation automatique des licences (voir "À propos de l'activation automatique des licences" á la page 71), n'oubliez pas d'activer vos licences manuellement avant l'expiration de la période de grâce. Si vous n'avez pas de fichier de licence, veuillez contacter votre revendeur XProtect.

- Assurez-vous d'avoir le logiciel de la **nouvelle version de votre produit** à disposition. Si vous n'avez pas acheté le logiciel sur un DVD, vous pouvez le télécharger sur la page de téléchargement du site internet http://www.milestonesys.com/downloads de Milestone.

- N'oubliez pas de sauvegarder la configuration de votre système (voir "À propos de la sauvegarde et de la restauration de la configuration de votre système" á la page 416).

  Le serveur de gestion sauvegarde la configuration de votre système dans une base de données. La base de données de la configuration système peut être enregistrée de deux manières différentes :

1. Dans une base de données SQL Server Express Edition sur le serveur de gestion proprement dit.

   2. Dans une base de données sur un serveur SQL existant sur votre réseau.

   Si vous utilisez l'option 2), vous devez disposer de **droits d'administrateur sur le serveur SQL** lorsque vous souhaitez créer, déplacer ou actualiser la base de données de configuration du système du serveur de gestion sur le serveur SQL. Une fois les processus de création, de déplacement ou d'actualisation terminés, le statut de propriétaire de la base de données de configuration du système du serveur de gestion sur le serveur SQL est suffisant.

Lorsque vous êtes prêt à commencer la mise à niveau, suivez les procédures indiquées dans Mise à jour des meilleures pratiques (á la page 56).

Mise à jour des meilleures pratiques

Consultez les conditions préalables de mise à niveau (á la page 55), y compris la sauvegarde de la base de données SQL, avant de démarrer la mise à niveau.

Si vous disposez d'un système à un seul serveur, il vous suffit d'installer le nouveau logiciel XProtect Advanced VMS en plus de l'installation existante.

Dans un système Milestone Interconnect ou Milestone Federated Architecture, vous devez mettre à jour le site central et les sites distants.

Effectuez la mise à jour dans cet ordre :

1. Mettez à jour le serveur de gestion avec l'option **Distribué** dans l'installateur.

   1. Sur la page de l'assistant où vous choisissez les composants, tous les composants des serveurs de gestion sont présélectionnés.

   2. Précisez votre serveur SQL et choisissez de garder la base de données.

   Lorsque vous démarrez l'installation, vous perdez la fonction de serveur de redondance.

2. Mise à jour des serveurs de redondance. Installez le serveur d'enregistrement à partir de la page web de téléchargement de votre serveur de gestion (contrôlée par le Download Manager).

   À ce stade, la fonction de serveur de redondance est à nouveau disponible.

3. Mettre à niveau les serveurs d'enregistrement. Vous pouvez installer les serveurs d'enregistrement à l'aide de l'assistant d'installation (voir "Installer le serveur d'enregistrement" á la page 38) ou en installation silencieuse (voir "Installation silencieuse d'un serveur d'enregistrement" á la page 39). L'avantage d'une installation silencieuse est qu'elle peut être effectuée à distance.

4. Mise à jour du serveur d'évènements. Installez le serveur d'événements à partir de la page web de téléchargement de votre serveur de gestion.

Continuez ces étapes pour les autres sites de votre système.

Mise à niveau alternative pour les groupes de travail

Si vous avez recours non pas à une configuration de domaine mais à une configuration de groupe de travail, procédez comme suit lors de la mise à niveau :

1. Sur le serveur d'enregistrement, créez un utilisateur Windows local.

2. À partir du **Panneau de contrôle** Windows, trouvez le **service Data Collector Milestone XProtect**. Faites un clic droit dessus, sélectionnez **Propriétés** et sélectionnez l'onglet **Connexion**. Configurez le service Data Collector de façon à l'exécuter en tant que l'utilisateur Windows local que vous venez de créer sur le serveur d'enregistrement.
3. Sur le serveur de gestion, créez le même utilisateur Windows local (avec le même nom d'utilisateur et le même mot de passe).
4. Dans le Management Client, ajoutez cet utilisateur Windows local au groupe d'**Administrateur**s.

Pour les installations avec groupes de travail, reportez-vous à la section Installation alternative pour les groupes de travail (voir "Installation pour les groupes de travail" á la page 43).

Première utilisation

Meilleures pratiques

Protection des bases de données d'enregistrement contre la corruption

Vous pouvez sélectionner la mesure à prendre en cas de corruption de la base de données d'une caméra. Ces mesures comprennent plusieurs options de réparation de base de données. Bien que ces options soient utiles, Milestone vous recommande de prendre des mesures pour veiller à ce que les bases de données de vos caméras ne soient pas corrompues.

Panne de disque dur : protégez vos lecteurs

Les lecteurs de disque dur sont des périphériques mécaniques, et sont donc sensibles aux facteurs externes. Voici des exemples de facteurs externes qui peuvent endommager les lecteurs de disque dur et entraîner une corruption des bases de données des caméras :

- Vibration (veillez à ce que le serveur du système de surveillance et son environnement soient stables)
- Forte chaleur (veillez à ce que le serveur soit correctement ventilé)
- Champs magnétiques forts (à éviter)
- Pannes de courant (veillez à utiliser un onduleur)
- Électricité statique (veillez à assurer une liaison à la terre si vous manipulez un lecteur de disque dur).
- Incendie, inondation, etc. (à éviter)

Windows Task Manager : attention à la fermeture des processus

Lorsque vous travaillez sous Windows Task Manager, prenez garde à ne pas mettre un terme aux processus qui ont un impact sur le système de surveillance. Si vous arrêtez une application ou un périphérique système en cliquant sur **Fermer le processus** dans le Windows Task Manager, le processus ne pourra pas enregistrer son état ni ses données avant de fermer. Cela peut entraîner des bases de données caméras corrompues.

En règle générale, Windows Task Manager affiche un avertissement si vous tentez de fermer un processus. Sauf si vous êtes absolument certain que mettre un terme au processus n'affectera aucunement le système de surveillance, cliquez sur **Non** lorsque le message d'avertissement vous demande si vous désirez vraiment fermer le processus.

Coupures de courant : utilisation d'un onduleur

La raison la plus courante de corruption des bases de données est l'arrêt brutal du serveur d'enregistrement, sans sauvegarde des fichiers et sans fermeture correcte du système

d'exploitation. Ceci peut arriver en raison de pannes d'alimentation, dues à un débranchement accidentel du câble d'alimentation du serveur ou autre.

Le meilleur moyen de protéger vos serveurs d'enregistrement contre l'arrêt brutal consiste à équiper chacun de vos serveurs d'enregistrement d'un onduleur (alimentation de secours).

L'onduleur fonctionne comme une source d'alimentation secondaire sur batterie et fournit l'alimentation nécessaire pour sauvegarder les fichiers ouverts et déconnecter votre système en toute sécurité en cas d'irrégularités d'alimentation. Les onduleurs peuvent avoir une sophistication différente les uns des autres, mais la plupart des onduleurs intègrent un logiciel permettant de sauvegarder automatiquement les fichiers ouverts, d'alerter les administrateurs, etc.

Le choix du bon type d'onduleur pour l'environnement de votre entreprise est un processus individuel. Lorsque vous évaluez vos besoins, n'oubliez pas la quantité de durée d'exécution dont vous aurez besoin pour que l'onduleur puisse fonctionner en cas de panne d'alimentation. La sauvegarde des fichiers ouverts et la fermeture correcte d'un système d'exploitation peuvent prendre plusieurs minutes.

À propos de l'heure d'été

L'heure d'été est la pratique qui consiste à avancer les horloges afin que les soirées bénéficient de plus de lumière du jour et les matins de moins. L'utilisation de l'heure d'été varie entre les pays/régions.

Lorsque vous travaillez avec un système de surveillance, qui est évidemment sensible à l'heure, il est important que vous sachiez comment le système gère l'heure d'été.

Printemps : Passage de l'heure standard à l'heure d'été

Le passage de l'heure standard à l'heure d'été ne pose pas vraiment de problème car on avance d'une heure.

Exemple :

L'horloge passe de 2 h 00 (heure standard) à 3 h 00 (heure d'été), et la journée compte 23 heures. Dans ce cas, il n'y a aucune donnée entre 2 h 00 et 3 h 00 du matin parce que cette heure de cette journée n'a pas existé.

Automne : Passage de l'heure d'été à l'heure standard

Lorsque vous passez de l'heure d'été à l'heure standard à l'automne, vous reculez d'une heure.

Exemple :

L'horloge passe de 2 h 00 (heure d'été) à 1 h 00 (heure standard), en répétant une heure, et la journée compte 25 heures. Vous allez jusqu'à 01:59:59, puis revenez immédiatement à 01:00:00. Si le système ne réagit pas, il va réenregistrer cette heure, ainsi la première instance de 01:30 sera écrasée par la seconde instance de 01:30.

Pour éviter qu'une telle situation ne se produise, votre système archive la vidéo en cours au cas où l'heure du système changerait de plus de cinq minutes. Vous ne pouvez pas consulter la première instance de l'heure 01 h 00 directement dans l'un de nos clients, mais les données sont enregistrées et conservées en sécurité. Vous pouvez parcourir cette vidéo dans XProtect Smart Client en ouvrant directement la base de données archivée.

À propos des serveurs de temps

Dès que votre système reçoit les images, elles sont immédiatement horodatées. Les caméras sont des unités distinctes qui peuvent avoir des périphériques de réglage de l'heure distincts. L'heure de

la caméra et l'heure de votre système peuvent par conséquent ne pas correspondre exactement. Cela peut parfois prêter à confusion. Si les horodateurs sont pris en charge par vos caméras, Milestone vous recommande de synchroniser automatiquement l'heure de la caméra et du système via un serveur de temps pour une synchronisation cohérente.

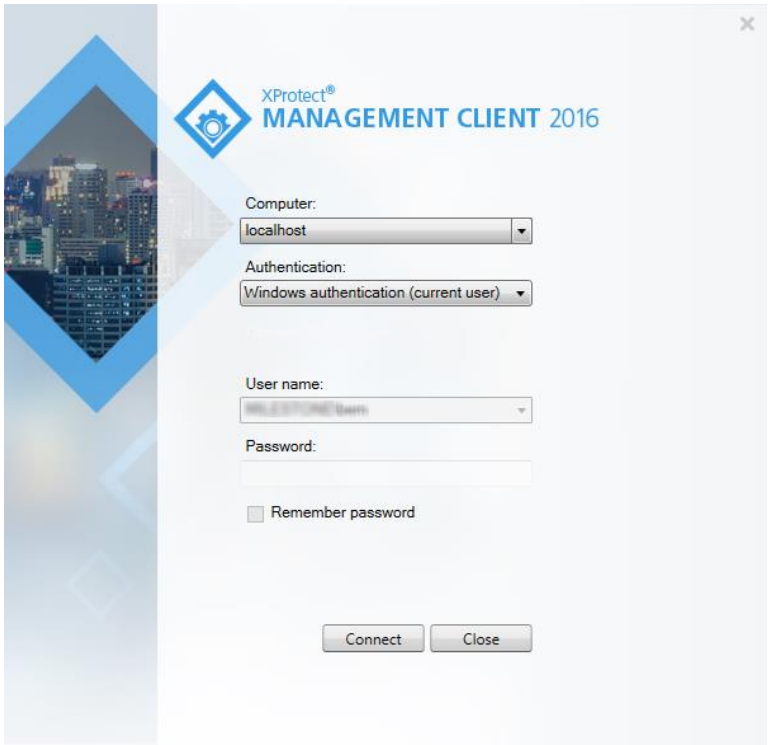
Pour de plus amples informations sur la configuration d'un serveur de temps, effectuez des recherches sur www.microsoft.com http://www.microsoft.com/ en saisissant les mots-clés **serveur de temps**, **service de temps** ou d'autres termes similaires.

Vue d'ensemble Management Client

Vue d'ensemble de la connexion

Lors du lancement du Management Client, vous devez tout d'abord saisir vos informations sur l'ouverture de session pour vous connecter au système.

Lorsque XProtect Corporate 2016 ou XProtect Expert 2016 ou plus récent est installé, vous pouvez vous connecter aux systèmes exécutant des versions plus anciennes du produit en installant un correctif. Les versions prises en charge sont XProtect Corporate 2013 et XProtect Expert 2013 ou toute autre version plus récente.



À propos de l'autorisation d'ouverture de session

Le système permet aux administrateurs de configurer des utilisateurs de façon à ce qu'ils ne puissent se connecter à un système que si un deuxième utilisateur bénéficiant de droits suffisants autorise leur connexion. Dans ce cas, XProtect Smart Client ou le Management Client demande cette deuxième autorisation au cours de la procédure d'ouverture de session.

Un utilisateur associé au rôle intégré d'**Administrateurs** a toujours la permission d'autoriser et ne reçoit pas de demande de deuxième connexion, à moins que l'utilisateur ne soit associé à un autre rôle nécessitant une deuxième connexion.

Pour associer l'autorisation de connexion à un rôle :

- Définissez l'**Autorisation de connexion requise** pour le rôle sélectionné dans l'onglet **Info** (voir "**Onglet Info (rôles)**" á la page 219) dans **Rôles**, de façon à ce que l'utilisateur reçoive une demande d'autorisation supplémentaire au cours de la connexion.
- Définissez **Autoriser des utilisateurs** pour le rôle sélectionné dans l'onglet **Sécurité globale** (voir "**Onglet Sécurité globale (rôles)**" á la page 221) dans **Rôles**, de sorte que l'utilisateur puisse autoriser les connexions d'autres utilisateurs.

Vous pouvez choisir les deux options pour le même utilisateur. Autrement dit, l'utilisateur reçoit une demande d'autorisation supplémentaire au cours de la connexion, mais peut également autoriser les connexions d'autres utilisateurs, à l'exception de ses propres connexions.

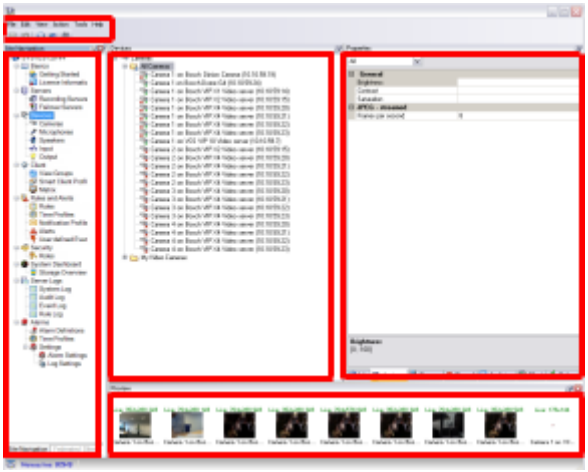
Vue d'ensemble de la fenêtre Management Client

La fenêtre Management Client est divisée en plusieurs volets. Le nombre de volets et la mise en page dépendent de vos :

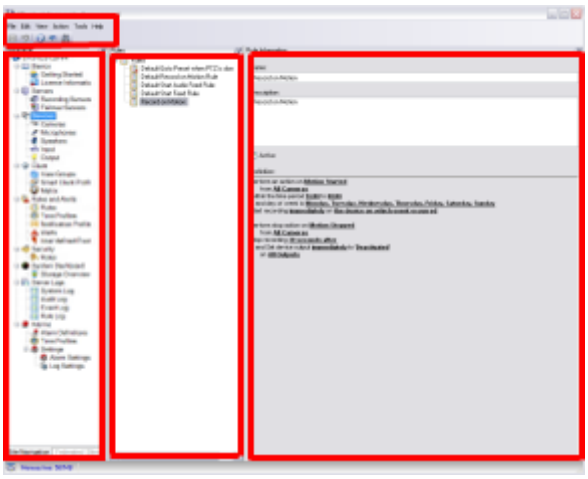
- configuration système
- tâche
- fonctions disponibles.

Vous trouverez ci-après quelques exemples de mises en page typiques :

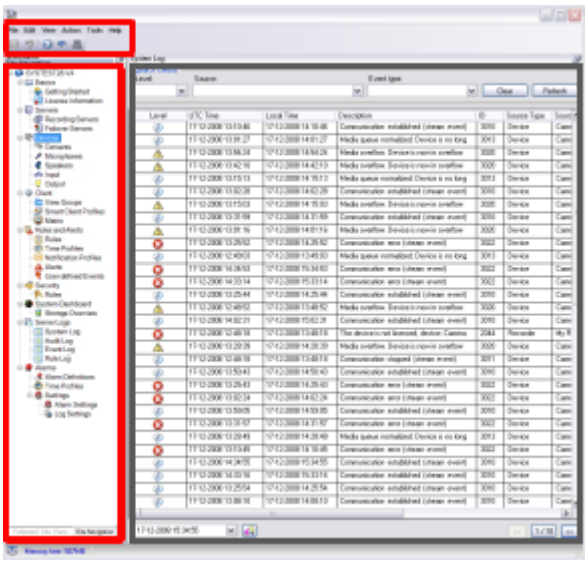
- Lorsque vous travaillez avec des serveurs d'enregistrement et des périphériques :



- Lorsque vous travaillez avec des règles, des profils de temps et de notification, des utilisateurs, des rôles :

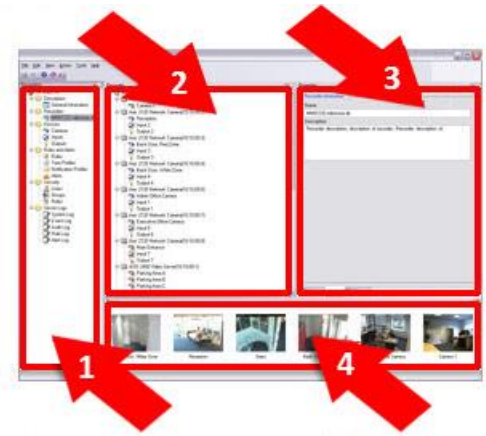


- Lorsque vous affichez des journaux :



Vue d'ensemble des volets

L'illustration représente une mise en page typique de fenêtre. Vous pouvez personnaliser la mise en page afin qu'elle soit différente sur votre ordinateur.



1. Volet Navigation sur le site et volet Hiérarchie des sites fédérés
2. Volet Vue d'ensemble
3. Volet Propriétés
4. Volet Aperçu

Volet Navigation sur le site : Il s'agit du composant principal de navigation dans le Management Client. Il contient le nom, les paramètres et les configurations du site auquel vous êtes connecté. Le nom du site est visible dans la partie supérieure du volet. Les fonctions sont regroupées en catégories reflétant les fonctionnalités du logiciel.

Volet Hiérarchie des sites fédérés : Il s'agit de votre élément de navigation dédié à l'affichage de tous les sites Milestone Federated Architecture dans une hiérarchie de sites parents/enfants.

Vous pouvez sélectionner n'importe quel site, vous y connecter, et lancer ainsi le Management Client correspondant à ce site. Le site auquel vous êtes connecté est toujours en haut de la hiérarchie du site.

Volet Vue d'ensemble : Fournit une vue d'ensemble de l'élément que vous avez sélectionné dans le volet **Navigation sur le site**, par exemple sous forme de liste détaillée. Lorsque vous sélectionnez un élément dans le volet **Vue d'ensemble**, il affiche généralement les propriétés correspondantes dans le volet **Propriétés**. Lorsque vous cliquez avec le bouton droit de la souris dans le volet **Vue d'ensemble**, vous accédez aux fonctionnalités de gestion.

Volet Propriétés : Affiche les propriétés de l'élément sélectionné dans le volet **Vue d'ensemble**. Les propriétés apparaissent dans plusieurs onglets dédiés :

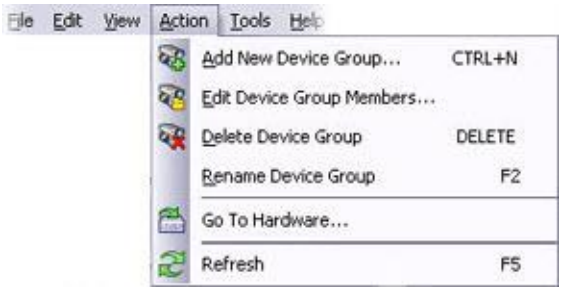
Exemple de propriétés affichées sur les onglets

Volet Aperçu : Le volet **Aperçu** apparaît lorsque vous travaillez avec des serveurs d'enregistrement et des périphériques. Il affiche des images d'aperçu venant des caméras sélectionnées ou des informations sur l'état du périphérique. L'exemple illustré présente une image d'aperçu de caméra avec des informations concernant la résolution et le débit de diffusion du flux en direct de la caméra.

Par défaut, les informations affichées avec les images d'aperçu de la caméra se rapportent à des flux en direct. Cet état est visible par le biais du texte en vert au-dessus de l'aperçu. Si vous souhaitez obtenir des informations sur les flux d'enregistrement à la place (en rouge), sélectionnez **Vue** > **Montrer les flux d'enregistrement** dans le menu.

La performance peut être affectée par le volet **Aperçu** lorsque celui-ci affiche des images d'aperçu provenant de plusieurs caméras avec un grand nombre d'images par seconde. Pour contrôler le nombre d'images d'aperçu et leur nombre d'images par seconde, sélectionnez **Options** > **Général** dans le menu.

Vue d'ensemble des menus



Il s'agit d'un exemple uniquement ; certains menus varient selon le contexte.

Menu Fichier

Vous pouvez enregistrer les modifications apportées à la configuration et quitter l'application. Vous pouvez également sauvegarder votre configuration, voir À propos de la sauvegarde et de la restauration de la configuration de votre système (á la page 416).

Menu Modifier

Vous pouvez annuler les modifications.

Menu Vue

Nom	Description
Réinitialiser la présentation de l'application	Réinitialisez la présentation des différents volets du Management Client à leurs paramètres par défaut.
Fenêtre Aperçu	Activez ou désactivez le volet **Aperçu** lorsque vous travaillez avec des serveurs d'enregistrement et des périphériques.

Nom	Description
Afficher les flux d'enregistrement	Par défaut, les informations affichées avec les images d'aperçu dans le volet **Aperçu** se rapportent aux flux en direct des caméras. Si vous souhaitez plutôt obtenir de plus amples informations sur les flux d'enregistrement, sélectionnez **Afficher flux d'enregistrement**.
Hiérarchie des sites fédérés	Par défaut, le volet **Hiérarchie des sites fédérés** est activé.
Navigation sur le site	Par défaut, le volet **Navigation sur le site** est activé.

Menu Action

Le contenu du menu **Action** dépend de l'élément sélectionné dans le volet **Navigation sur le site**. Les actions disponibles sont identiques lorsque vous cliquez avec le bouton droit de la souris sur l'élément. Les éléments sont décrits dans Éléments du Management Client (voir "Éléments Management Client" á la page 67).

Nom	Description
Actualiser	Est toujours disponible et recharge les informations requises à partir du serveur de gestion.

Menu Outils

Nom	Description
Services enregistrés	Gérez les services enregistrés. Voir À propos du canal de service (á la page 438).
Serveurs Enterprise	Ajoutez les serveurs XProtect Enterprise à votre système et gérez l'intégration des serveurs ajoutés. Voir À propos des serveurs XProtect Enterprise (á la page *411*). Vous pouvez également utiliser cette fonction pour migrer d'un système XProtect Enterprise vers XProtect Corporate. Cette procédure est décrite dans un document séparé. Uniquement pris en charge si votre système : - exécute XProtect Corporate - utilise IPv4 - travaille avec les serveurs XProtect Enterprise s'exécutant dans la version XProtect Enterprise 6.0 et plus
Rôles effectifs	Affichez tous les rôles d'un utilisateur ou groupe sélectionné. Pertinent uniquement si vous exécutez XProtect Corporate.
Options	Ouvre la boîte de dialogue Options, qui vous permet de définir et de modifier les paramètres généraux du système. Pertinent uniquement si vous exécutez XProtect Corporate.

Menu Aide

Vous pouvez accéder au système d'aide et aux informations relatives à la version du Management Client.

Éléments Management Client

Bases

Renseignements sur la licence

Vous pouvez suivre les licences qui partagent les mêmes fichiers de licence du logiciel sur ce site et tous les autres sites et votre abonnement Milestone Care. Vous pouvez ainsi décider comment activer vos licences. Pour les informations de base à propos des licences XProtect, consultez À propos des licences (á la page 22).

Licence attribuée à

Coordonnées du propriétaire de la licence que vous avez saisi au cours de l'enregistrement du logiciel. Cliquez sur **Modifier les détails** pour modifier les informations relatives au propriétaire de la licence. Vous trouverez également un lien vers le contrat de licence utilisateur final que vous avez accepté avant l'installation.

Milestone Care

Vous trouverez ici des informations relatives au niveau actuel de Milestone Care™. Lors de l'achat de votre système, vous avez également pris un abonnement Milestone Care Plus de deux ans. Votre installation est toujours couverte par Milestone Care Basic qui vous donne accès à différents types de documents tels que des articles, guides et tutoriels sur notre site internet d'Assistance http://www.milestonesys.com/support. Un abonnement Milestone Care Plus vous donne accès à des mises à jour. Vous avez également accès au service Customer dashboard (Tableau de bord client), à la fonction Smart Connect et à toutes les notifications push. La date d'expiration de votre abonnement Milestone Care Plus est visible dans le tableau **Produits installés**. Si vous disposez d'un abonnement Milestone Care Premium, vous pouvez également contacter l'assistance Milestone pour demander de l'aide. Lorsque vous contactez l'assistance Milestone, n'oubliez pas de préciser les informations concernant votre identifiant Milestone Care. La date d'expiration de votre abonnement Milestone Care Premium est visible. Pour en savoir plus à propos de Milestone Care, suivez les liens. Si vous décidez d'acheter ou de renouveler votre abonnement Milestone Care après l'installation de votre système, vous devrez activer votre licence pour que les bonnes informations Milestone Care apparaissent.

Produits installés

Liste des informations relatives à toutes les licences de base installées pour XProtect VMS et les produits complémentaires qui partagent le même fichier de licence du logiciel :

- Produits et versions
- Le code de licence du logiciel (SLC) des produits.
- Date d'expiration de votre SLC. Généralement illimité.
- La date d'expiration de votre abonnement Milestone Care Plus.

- La date d'expiration de votre abonnement Milestone Care Premium.

Installed Products

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 2016	M01-C01-100-01-	Unlimited	01-10-2016	01-10-2016
Milestone XProtect Smart Wall	M01-P03-023-01-	Unlimited	Unlimited	
Milestone XProtect Access 2016 v10.0a	M01-P01-011-01-	Unlimited	Unlimited	
Milestone XProtect Transact 2016	M01-P08-100-01-	Unlimited	Unlimited	

Aperçu de la licence - Tous les sites

Nombre de licences de périphérique activées ou autres licences dans le fichier de licence de votre logiciel et nombre total de licences disponibles sur votre système. Vous pouvez facilement voir s'il est possible d'agrandir votre système sans acheter de licences supplémentaires.

Pour un aperçu détaillé de l'état de vos licences activées sur d'autres sites, cliquez sur le lien **Détails de la licence - Tous les sites**. Consultez la rubrique **Détails de la licence - Site actuel** ci-dessous pour plus d'informations.

License Overview - All sites License Details - All Sites...

License Type	Activated
Hardware Device	51 out of 100
Milestone Interconnect Camera	0 out of 100
Access control door	9 out of 2002
Transaction source	1 out of 101

Si vous possédez des licences pour des produits complémentaires, vous pouvez afficher des détails supplémentaires sous les nœuds spécifiques du produit complémentaire dans le **volet de Navigation du site**.

Détails de la licence - Site actuel

La colonne **Activées** énumère le nombre de licences de périphérique activées ou d'autres licences sur ce site.

Vous pouvez également afficher le nombre de changements apportés aux périphériques sans activation (voir "À propos des changements apportés aux périphériques sans activation" á la page 69) et combien vous en possédez par an dans la colonne **Changements sans activation**.

Si vous disposez de licences que vous n'avez pas encore activées et qui sont dans la période de grâce, elles s'afficheront dans la colonne **En période de grâce**. La date d'expiration de la première licence à expirer apparaît en rouge sous le tableau.

Si vous oubliez d'activer les licences avant la fin de la période de grâce, vous ne recevrez plus de vidéo dans le système. Ces licences s'affichent dans la colonne **Période de grâce expirée**. Voir également Activer des licences après la période de grâce (á la page 73).

Si vous utilisez plus de licences que vous ne possédez, elles s'afficheront dans la colonne **Sans licence** et vous ne pourrez pas les utiliser dans votre système. Voir également Obtenir des licences supplémentaires (á la page 73).

Si vous avez des licences en période de grâce, en fin de période de grâce ou sans licence, un message de rappel apparaitra à chaque connexion sur votre Management Client.

License Details - Current Site: SYS

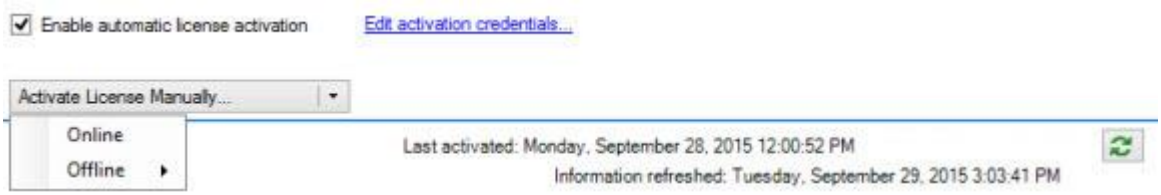
License Type	Activated	Changes without activation	In Grace Period	Grace Period Expired	Without License
Hardware Device	32	0 out of 10	0	0	0
Milestone Interconnect Camera	11	N/A	0	0	0
Access control door	9	N/A	0	0	0
Transaction source	1	N/A	0	0	0

Les périphériques sans licences sont identifiés par un point d'exclamation dans le Management Client. Veuillez noter que le point d'exclamation est aussi utilisé pour d'autres raisons. Placez votre curseur sur le point d'exclamation pour plus de précisions.

Fonctions pour activer les licences

Sous les trois tableaux, vous trouverez

- une case à cocher pour activer l'activation automatique des licences et un lien pour modifier les identifiants utilisateur pour l'activation automatique. Pour plus d'informations, voir À propos de l'activation automatique des licences (á la page 71) et Activer l'activation automatique des licences (á la page 71). Si l'activation automatique échoue, un message apparaitra en rouge. Pour plus d'information, veuillez cliquer sur le lien **Détails**.
- Liste déroulante pour activer manuellement les licences en ligne ou hors ligne. Pour plus d'informations, voir Activer les licences en ligne (voir "Activation des licences en ligne" á la page 72) et Activer les licences hors ligne (voir "Activation des licences hors ligne" á la page 72).
- Dans le coin en bas à gauche, vous pouvez voir la date de la dernière activation de vos licences (automatique ou manuelle) et la date d'actualisation des informations de la page. Les données d'horodatage proviennent du serveur et non pas de l'ordinateur local.



À propos des changements apportés aux périphériques sans activation

Sur la page **Bases** > **Renseignements sur la licence**, la colonne **Changements sans activation** affiche le nombre de périphériques pouvant être remplacés ou ajoutés sans avoir à activer la licence et le nombre de changements apportés depuis la dernière activation. Les périphériques ajoutés dans le cadre de vos changements sans activation fonctionnent comme avec des licences entièrement activées. Un an après la dernière activation de votre licence, le nombre de **changements apportés aux périphériques sans activation** est automatiquement remis à zéro. Après cette remise à zéro, vous pouvez continuer d'ajouter et remplacer des périphériques sans en activer les licences.

Le nombre de changements apportés aux périphériques sans activation varie d'une installation à l'autre et est calculé d'après plusieurs variables. Pour une description plus détaillée, voir Calcul du nombre de changements apportés aux périphériques sans activation (á la page 70).

Si votre système de surveillance reste hors ligne pendant des périodes prolongées, par exemple à bord d'un bateau en croisière ou dans un endroit reculé sans accès à internet, vous pouvez

contacter votre revendeur Milestone et lui demander un nombre plus élevé de changements apportés aux périphériques sans activation.

Il vous faudra lui expliquer pourquoi vous méritez un nombre plus élevé de changements apportés aux périphériques sans activation. Milestone prendra une décision au cas par cas. Si on vous accorde un nombre plus élevé de changements apportés aux périphériques sans activation, vous devrez activer vos licences afin d'enregistrer le nombre plus élevé sur votre système XProtect.

Calcul du nombre de changements apportés aux périphériques sans activation

Les changements apportés aux périphériques sans activation sont calculés d'après trois variables. Si vous disposez de plusieurs installations du logiciel Milestone, les variables s'appliquent séparément à chacune d'elle. Les variables sont les suivantes :

- **C%** est un pourcentage fixe du nombre total de licences activées.
- **Cmin** est la valeur minimum fixe du nombre de changements apportés aux périphériques sans activation.
- **Cmax** est la valeur maximum fixe du nombre de changements apportés aux périphériques sans activation.

Le nombre de changements apportés aux périphériques sans activation ne peut pas être inférieur à **Cmin** ni supérieur à **Cmax**. La valeur calculée d'après la variable **C%** change en fonction du nombre de périphériques activés sur chaque installation de votre système. La variable **C%** ne compte pas les périphériques ajoutés dans le cadre des changements sans activation comme étant activés.

Milestone définit les valeurs des trois variables et ces dernières peuvent être modifiées sans préavis. Les valeurs des variables varient selon le produit.

Pour plus d'informations à propos des valeurs par défaut de votre produit, rendez-vous sur My Milestone http://www.milestonesys.com/device-change-calculation.

Exemples basés sur C% = 15 %, Cmin = 10 et Cmax = 100

Un client achète 100 licences de périphériques. Il ajoute 100 caméras à son système. À moins qu'il n'active l'activation automatique des licences, il ne dispose d'aucun changement sans activation. Il active ses licences et dispose alors de 15 changements sans activation.

Un client achète 100 licences de périphériques. Il ajoute 100 caméras à son système et active ses licences. Il dispose désormais de 15 changements sans activation. Le client décide de supprimer un périphérique de son système. Il dispose désormais de 99 périphériques activés et son nombre de changements sans activation passe à 14.

Un client achète 1000 licences de périphériques. Il ajoute 1000 caméras et active ses licences. Il dispose désormais de 100 changements sans activation. D'après la variable **C%**, il devrait avoir 150 changements sans activation, mais la variable **Cmax** ne lui permet d'avoir que 100 changements sans activation.

Un client achète 10 licences de périphériques. Il ajoute 10 caméras à son système et active ses licences. Son nombre de changements sans activation passe à 10, étant donné la variable **Cmin.** Si le nombre avait été calculé d'après la variable **C%,** le client n'aurait eu qu'un seul changement (15 % de 10 = 1,5 arrondi à 1).

Un client achète 115 licences de périphériques. Il ajoute 100 caméras à son système et active ses licences. Il dispose désormais de 15 changements sans activation. Il ajoute 15 caméras de plus sans les activer et utilise la totalité des 15 changements sans activation. Il supprime 50 caméras du système et le nombre de changements sans activation passe à 7. Cela signifie que 8 de ses caméras ajoutées dans le cadre des 15 changements sans activation passent en période de grâce.

Le client ajoute alors 50 nouvelles caméras. Vu que le client a activé 100 caméras sur son système lors de l'activation de ses licences, le nombre de changements sans activation repasse à 15 et les 8 caméras en période de grâce sont à nouveau considérées comme des changements sans activation. Les 50 nouvelles caméras passent en période de grâce.

Afficher la vue d'ensemble des licences

Vous pouvez accéder à une vue d'ensemble des licences qui sont activées, dans un période de grâce, expirées et manquantes pour tous les sites dotés d'une licence à l'aide du même fichier de licence du logiciel.

- Cliquez sur **Vue d'ensemble des licences**.

Si le site n'est pas un site fédéré ou si la connexion est en panne, vous pouvez uniquement afficher le nombre de licences activées. Le message N/A apparaît pour les licences dans une période de grâce, expirées et manquantes.

À propos de l'activation automatique des licences

Pour une maintenance plus aisé et une meilleure adaptabilité, Milestone recommande l'activation automatique des licences (voir "Activer l'activation automatique des licences" á la page 71) pour vous faciliter la tâche. L'activation automatique des licences nécessite bien sûr que votre serveur de gestion soit en ligne.

Une fois ces conditions préalables remplies, le système active vos périphériques ou autres licences quelques minutes après les avoir ajoutés, supprimés ou remplacés ou après tout changement ayant un impact sur l'utilisation de vos licences. De ce fait, vous n'avez plus besoin de démarrer l'activation manuelle des licences. Le nombre de changements apportés aux périphériques sans activation reste nul et aucun périphérique ne passe en période de grâce et ne risque d'expirer. Par mesure de précaution, si l'une de vos licences de base expire au bout de 14 jours, votre système XProtect tentera automatiquement d'activer votre licence toutes les nuits.

Vous n'avez besoin d'activer manuellement vos licences que lorsque vous avez acheté des licences supplémentaires (voir "Obtenir des licences supplémentaires" á la page 73), que vous voulez les mettre à jour (voir "Conditions préalables de mise à niveau" á la page 55), que vous avez acheté ou renouvelé un abonnement Milestone Care (voir "Renseignements sur la licence" á la page 67), ou lorsque Milestone vous a accordé un nombre plus élevé de changements apportés aux périphériques sans activation (voir "À propos des changements apportés aux périphériques sans activation" á la page 69).

Activer l'activation automatique des licences

1. Sur la page des **Renseignements sur la licence**, sélectionnez **Activer l'activation automatique des licences**.
2. Saisissez le nom d'utilisateur et le mot de passe que vous souhaitez utiliser avec l'activation automatique des licences. Les identifiants sont enregistrés dans un fichier sur le serveur de gestion.
   - Si vous êtes un utilisateur existant, saisissez votre nom d'utilisateur et mot de passe pour vous identifier sur le système d'enregistrement des logiciels.
   - Si vous êtes un nouvel utilisateur, cliquez sur le lien **Créer nouvel utilisateur** pour configurer un nouveau compte d'utilisateur puis suivez la procédure d'enregistrement. Si vous n'avez pas encore enregistré votre code de licence du logiciel (SLC), vous devez le faire.
3. Cliquez sur **OK**.

Si vous voulez modifier ultérieurement votre nom d'utilisateur et/ou le mot de passe pour l'activation automatique, cliquez sur le lien **Modifier les identifiants d'activation**.

Désactiver l'activation automatique des licences

Désactiver l'activation automatique des licences tout en gardant le mot de passe pour une utilisation ultérieure

- Sur la page des **Renseignements sur la licence**, désélectionnez **Activer l'activation automatique des licences**. Le mot de passe et nom d'utilisateur sont toujours enregistrés sur le serveur de gestion.

Désactiver l'activation automatique des licences et supprimer le mot de passe

- Sur la page des **Renseignements sur la licence**, cliquez sur **Modifier les identifiants d'activation**.
- Cliquez sur **Supprimer le mot de passe**.
- Confirmez la suppression du mot de passe et du nom d'utilisateur sur le serveur de gestion.

Activation des licences en ligne

Activez vos licences en ligne si l'ordinateur qui exécute le serveur de gestion est doté d'une connexion Internet.

1. Sur le nœud **Renseignements sur la licence**, sélectionnez **Activer licence manuellement** puis **En ligne**.
2. La boîte de dialogue **Activer en ligne** s'ouvre.
   - Si vous êtes un utilisateur existant, saisissez votre nom d'utilisateur et mot de passe.
   - Si vous êtes un nouvel utilisateur, cliquez sur le lien **Créer nouvel utilisateur** pour configurer un nouveau compte d'utilisateur. Si vous n'avez pas encore enregistré votre code de licence du logiciel (SLC), vous devez le faire.
3. Cliquez sur **OK**.

Si vous recevez un message d'erreur pendant l'activation en ligne, suivez les instructions à l'écran pour résoudre le problème. Si vous avez suivi les instructions et ne pouvez toujours pas accéder à l'activation en ligne https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx , contactez le service d'assistance de Milestone.

Activation des licences hors ligne

Si l'ordinateur qui exécute le serveur de gestion n'est pas doté d'une connexion Internet, vous pouvez activer les licences hors ligne.

1. Sir le nœud **Renseignements sur la licence**, sélectionnez **Activer votre licence manuellement** -> **Hors ligne** -> **Exporter une licence pour activation** pour exporter un fichier de demande de licence (.lrq) contenant des informations sur les périphériques ajoutés.
2. Le nom du fichier de demande de licence (.lrq) est le même que votre SLC. Si vous avez plusieurs sites, n'oubliez pas de créer des noms de fichier uniques pour pouvoir facilement identifier à quel site appartient quel fichier.

3. Copiez le fichier de demande de licence sur un ordinateur avec connexion Internet et connectez-vous à votre site internet http://online.milestonesys.com pour obtenir le fichier de licence du logiciel activée (.lic).
4. Copiez sur votre ordinateur le fichier .lic avec le même nom que votre fichier de demande de licence avec Management Client.
5. Sur la page **Renseignements sur la licence** de Management Client, sélectionnez **Activer licence hors ligne** > **Importer une licence activée**, et sélectionnez le fichier de licence du logiciel activée pour l'importer et ainsi activer vos licences.
6. Cliquez sur **Terminer** pour conclure le processus d'activation.

Activer des licences après la période de grâce

Si vous n'activez pas une licence (périphérique, caméra Milestone Interconnect ou licence de contrôle d'accès de porte) dans la période de grâce, le périphérique devient indisponible et ne peut pas envoyer de données au système de surveillance.

- Le périphérique, sa configuration et les autres paramètres ne sont pas supprimés de la configuration du système.
- Afin de pouvoir recevoir des données de votre périphérique expiré, il vous suffit d'activer la licence. Pour plus d'informations, voir Activer les licences hors ligne (voir "Activation des licences hors ligne" á la page 72) et Activer les licences en ligne (voir "Activation des licences en ligne" á la page 72).

Obtenir des licences supplémentaires

Si vous souhaitez ajouter, ou si vous avez déjà ajouté, plus de périphériques matériels, de systèmes Milestone Interconnect ou de portes que vous ne possédez actuellement de licences, vous devez acheter des licences supplémentaires pour permettre aux périphériques d'envoyer des données à votre système.

- Pour obtenir des licences supplémentaires pour votre système, contactez votre revendeur de produits XProtect.

Nouvelles licences pour la version existante de votre système de surveillance :

- Il vous suffit d'activer vos licences manuellement pour accéder aux nouvelles licences. Pour plus d'informations, voir Activer les licences hors ligne (voir "Activation des licences hors ligne" á la page 72) et Activer les licences en ligne (voir "Activation des licences en ligne" á la page 72).

Nouvelles licences et nouvelle version de votre système de surveillance :

- Vous recevrez un nouveau fichier de licence du logiciel (.**lic**) (voir "À propos des licences" á la page 22) avec de nouvelles licences et une nouvelle version. Vous devez utiliser le nouveau fichier de licence du logiciel au cours de l'installation de la nouvelle version. Pour en savoir plus, consultez la rubrique Conditions préalables de mise à niveau (á la page 55).

Licences et remplacement de périphériques matériels

Vous pouvez remplacer un périphérique doté d'une licence, tel qu'une caméra, par un nouveau périphérique dans votre système, activer le nouveau périphérique et transférer la licence.

Si vous retirez un périphérique d'un serveur d'enregistrement, vous libérez par la même occasion une licence de périphérique.

Si vous remplacez une caméra par une caméra similaire (fabricant, marque et modèle) et que vous affectez la même adresse IP à la nouvelle caméra, vous conservez votre accès à toutes les bases de données de cette caméra. Dans ce cas, vous transférez le câble de réseau de l'ancienne caméra à la nouvelle sans changer les paramètres du Management Client.

Si vous remplacez un périphérique par un modèle différent, vous devez utiliser l'assistant **Remplacer le matériel** (voir Remplacer le matériel (á la page 425)) pour cartographier toutes les bases de données pertinentes des caméras, microphones, entrées, sorties et paramètres.

Si vous avez activé l'activation automatique des licences (voir "Activer l'activation automatique des licences" á la page 71), le nouveau périphérique sera automatiquement activé. Si vous avez utilisé tous vos changements apportés aux périphériques sans activation (voir "À propos des changements apportés aux périphériques sans activation" á la page 69), vous devrez activer manuellement vos licences. Pour plus d'informations, voir Activer les licences hors ligne (voir "Activation des licences hors ligne" á la page 72) et Activer les licences en ligne (voir "Activation des licences en ligne" á la page 72).

Renseignements sur le site

Vous pouvez ajouter des informations complémentaires à un site pour faciliter l'identification de chaque site, par exemple dans une configuration Milestone Federated Architecture de grande envergure. Mis à part le nom du site, vous pouvez décrire :

- Adresse/emplacement
- Administrateur(s)
- Informations complémentaires

Mettre à jour les renseignements sur le site

Pour mettre à jour les renseignements sur le site :

1. Sélectionnez **Modifier**.
2. Sélectionnez une balise.
3. Saisissez des informations dans le champ **Valeur**.
4. Cliquez sur **OK**.

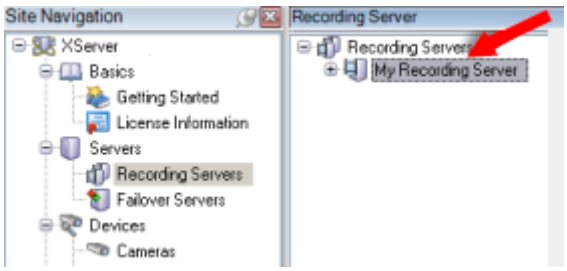
Serveurs et matériel

Serveurs d'enregistrement

À propos des serveurs d'enregistrement

Vous utilisez les serveurs d'enregistrement pour enregistrer des flux vidéo et pour communiquer avec des caméras et d'autres périphériques. Un système de surveillance est généralement constitué de plusieurs serveurs d'enregistrement.

Les serveurs d'enregistrement sont des ordinateurs sur lesquels vous avez installé le logiciel du serveur d'enregistrement et configurés afin de communiquer avec un serveur de gestion. Vous pouvez consulter vos serveurs d'enregistrement dans le volet **Vue d'ensemble** lorsque vous développez le dossier **Serveurs** et sélectionnez **Serveurs d'enregistrement**.



Serveur d'enregistrement répertorié dans le volet Vue d'ensemble

La compatibilité rétrospective avec les versions du serveur d'enregistrement antérieures à la présente version du serveur de gestion est limitée. Vous pouvez toujours accéder aux enregistrements sur des serveurs d'enregistrement dotés de versions plus anciennes, mais si vous souhaitez modifier leur configuration, veillez à ce qu'ils correspondent à cette version du serveur de gestion. Milestone vous recommande de mettre à niveau tous les serveurs d'enregistrement de votre système à la même version que celle de votre serveur de gestion.

Vous disposez de plusieurs options en matière de gestion de vos serveurs d'enregistrement :

- Autoriser un serveur d'enregistrement (á la page 75)
- Ajouter matériel (á la page 104)
- Déplacer du matériel (á la page 107)
- Supprimer tous les périphériques matériels (voir "Supprimer tous les périphériques matériels sur un serveur d'enregistrement" á la page 95)
- Supprimer un serveur d'enregistrement (á la page 95)

Important : Lorsque le service Recording Server est en cours de fonctionnement, il est très important de ne pas laisser Windows Explorer ou d'autres programmes accéder à des fichiers ou répertoires de la base de données multimédia associés à la configuration de votre système. S'ils y accèdent, le serveur d'enregistrement ne pourra probablement pas renommer ou déplacer les fichiers multimédia en question. Ceci pourrait entraîner l'arrêt du serveur d'enregistrement. Pour redémarrer un serveur d'enregistrement arrêté, arrêter le service Recording Server, fermer le programme accédant au(x) fichier(s) ou répertoire(s) multimédia en question, et redémarrer tout simplement le service Recording Server.

Autoriser un serveur d'enregistrement

Lorsque vous utilisez le système pour la première fois, ou lorsque vous avez ajouté de nouveaux serveurs d'enregistrement au système, vous devez autoriser les nouveaux serveurs d'enregistrement.

Lorsque vous autorisez un serveur d'enregistrement, vous le configurez pour qu'il se connecte à votre serveur de gestion.

1. Faites un clic droit sur le serveur d'enregistrement concerné dans le volet **Vue d'ensemble**.
2. Sélectionnez **Autoriser le serveur d'enregistrement** :

3. Après quelques instants, le serveur d'enregistrement est autorisé et prêt pour une configuration complémentaire via les onglets. Vous pouvez également Ajouter du matériel (voir "Ajouter matériel" á la page 104).

Modifier/vérifier la configuration de base d'un serveur d'enregistrement

Si votre Management Client ne répertorie pas tous les serveurs d'enregistrement que vous avez installés, la raison la plus probable est que vous avez mal configuré les paramètres de configuration (par exemple, l'adresse IP ou le nom d'hôte du serveur de gestion) pendant l'installation.

Vous n'avez pas besoin de réinstaller les serveurs d'enregistrement pour spécifier les paramètres des serveurs de gestion, mais vous pouvez modifier/vérifier sa configuration de base :

1. Sur l'ordinateur hébergeant le serveur d'enregistrement, cliquez sur l'icône **Serveur d'enregistrement** avec le bouton droit de votre souris dans la zone de notification.
2. Sélectionnez **Arrêter le service Recording Server**.
3. Cliquez avec le bouton droit à nouveau sur l'icône **Serveur d'enregistrement** et sélectionnez **Modifier les paramètres**.

   La fenêtre **Paramètres du serveur d'enregistrement** s'affiche.
4. Vérifiez/modifiez les paramètres suivants :
   - **Adresse IP/nom d'hôte du serveur de gestion** : spécifiez l'adresse IP ou le nom d'hôte du serveur de gestion auquel le serveur d'enregistrement devrait être connecté.
   - **Port du serveur de gestion** : spécifiez le numéro de port à utiliser lors de la communication avec le serveur de gestion. Le port par défaut est 9993. Vous pouvez le modifier si nécessaire, mais le numéro de port doit toujours correspondre au numéro de port configuré sur le serveur de gestion.
5. Cliquez sur **OK**.
6. Pour redémarrer le service Recording Server, cliquez sur l'icône **Serveur d'enregistrement** avec le bouton droit de la souris et sélectionnez **Démarrer le service Recording Server**.

Important : L'arrêt du service Recording Server vous empêche d'enregistrer et de lire des vidéos en direct pendant que vous vérifiez/modifiez la configuration de base du serveur d'enregistrement.

Icônes d'état du serveur d'enregistrement

Le Management Client utilise les icônes suivantes pour indiquer l'état des serveurs d'enregistrement individuels :

Icône	Description
	**Le serveur d'enregistrement est en cours de fonctionnement**
	**Le serveur d'enregistrement est en cours de communication**
	**Le serveur d'enregistrement requiert votre attention :** Cette icône s'affiche généralement parce que le service Recording Server est arrêté. 1) Cliquez sur l'icône du serveur d'enregistrement avec le bouton droit de la souris dans la zone de notification. 2) Démarrez/arrêtez le service Recording Server et visualisez les messages d'état du serveur d'enregistrement.
	**Le serveur d'enregistrement doit être autorisé :** S'affiche lorsque vous chargez le serveur d'enregistrement pour la première fois. Lorsque vous utilisez un serveur d'enregistrement pour la première fois, vous devez l'autoriser : 1) Faites un clic droit sur l'icône de serveur d'enregistrement souhaitée. 2) Sélectionnez **Autoriser le serveur d'enregistrement** : Après quelques instants, le serveur d'enregistrement est autorisé et prêt pour une configuration complémentaire.
	**Réparation de la base de données en cours :** S'affiche lorsque les bases de données sont corrompues, par exemple en raison d'une panne de courant, et que le serveur d'enregistrement les répare. Le processus de réparation peut prendre un certain temps si les bases de données sont de grande taille. Reportez-vous à la section Protection des bases de données d'enregistrement contre la corruption (á la page 58) pour savoir comment éviter les bases de données corrompues. **Important :** Pendant la réparation d'une base de données au démarrage, vous ne pouvez pas enregistrer une vidéo à partir des caméras connectées au serveur d'enregistrement. Seul le visionnage en direct est disponible. Une réparation de base de données pendant le fonctionnement normal n'affecte pas les enregistrements.

Onglet Info (serveur d'enregistrement)

Vous pouvez vérifier ou modifier le nom et la description d'un serveur d'enregistrement sélectionné dans l'onglet **Info**.

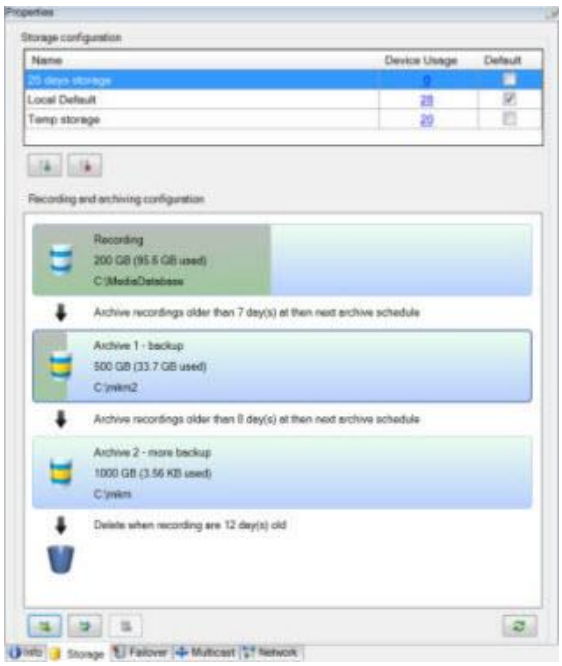
L'onglet **Info** affichant des informations au sujet d'un serveur d'enregistrement.

Propriétés de l'onglet Info

Nom	Description
Nom	Utilisé lorsque le serveur d'enregistrement est répertorié dans le système et les clients. Le nom ne doit pas nécessairement être unique. Lorsque vous renommez un serveur d'enregistrement, son nom est modifié de manière globale dans le Management Client.
Description	La description apparaît dans plusieurs listes au sein du système. Il n'est pas obligatoire de saisir une description.
Nom de l'hôte	Affiche le nom de l'hôte du serveur d'enregistrement.
URL du serveur web	Affiche l'URL du serveur web du serveur d'enregistrement. Vous utilisez le serveur web, par exemple, pour gérer les commandes des caméras PTZ et les demandes en direct et de consultation de XProtect Smart Client. L'URL inclut le numéro de port utilisé pour la communication avec le serveur web (généralement le port 7563).
Fuseau horaire	Affiche le fuseau horaire dans lequel le serveur d'enregistrement est situé.

Onglet Stockage (serveur d'enregistrement)

Dans l'onglet **Stockage**, vous pouvez configurer, gérer et visualiser des emplacements de stockage pour les serveurs d'enregistrement sélectionnés.



À propos du stockage et de l'archivage

Lorsqu'une caméra effectue un enregistrement vidéo ou audio, tous les enregistrements spécifiés sont stockés par défaut dans l'emplacement de stockages défini pour ce périphérique. Chaque emplacement de stockage sauvegarde les enregistrements dans la base de données **Enregistrement.** Un emplacement de stockage n'a pas d'archive(s) par défaut, mais vous pouvez les créer.

Pour éviter que la base de données d'enregistrement devienne pleine, vous pouvez créer des emplacements de stockage supplémentaires (voir "Ajouter un nouvel emplacement de stockage d'enregistrement" á la page 82). Vous pouvez également créer des archives (voir "Créer une archive dans un emplacement de stockage" á la page 82) dans chaque emplacement de stockage et lancer un processus d'archivage pour stocker les données.

L'archivage est le transfert automatique des enregistrements de la base de données d'enregistrement d'une caméra à un autre emplacement, par exemple. Ainsi, la quantité d'enregistrements que vous pouvez stocker n'est pas limitée par la taille de la base de données d'enregistrement. Avec l'archivage, vous pouvez également sauvegarder vos enregistrements sur un autre support.

Vous configurez le stockage et l'archivage sur la base d'un serveur d'enregistrement.

À condition que vous stockiez les enregistrements archivés localement ou sur des disques réseau accessibles, vous pouvez utiliser XProtect Smart Client pour les visualiser. C'est également ainsi que vous visualisez les enregistrements stockés dans les bases de données ordinaires d'une caméra.

Les mentions suivantes font principalement référence aux caméras et à la vidéo, mais les haut-parleurs, les microphones, l'audio et le son s'appliquent également.

Important : Milestone vous recommande d'utiliser un disque dur dédié pour la base de données du serveur d'enregistrement afin de prévenir toute mauvaise performances du disque. Lors du

formatage du disque dur, il est important de changer son paramètre **Taille d'unité d'allocation** de 4 à 64 kilo-octets. Ceci permet d'améliorer de façon significative les performances d'enregistrement du disque dur. Vous pouvez obtenir de plus amples informations sur les tailles d'unités d'allocation sur le site web de Microsoft http://support.microsoft.com/kb/140365/en-us.

Important : Les plus anciennes données d'une base de données seront toujours auto-archivées (ou supprimées si aucune archive suivante n'est définie) dès qu'il y a moins de 5 Go d'espace libre. S'il y a moins de 1 Go d'espace libre, les données seront supprimées. Une base de données a toujours besoin de 250 Mo d'espace libre. Si vous atteignez cette limite parce que les données ne sont pas supprimées assez rapidement, aucune autre donnée ne sera ajoutée à la base de données tant que vous n'aurez pas libéré suffisamment d'espace. La taille maximum réelle de votre base de données est la quantité de giga-octets que vous spécifiez, moins 5 Go.

Relier des périphériques à un emplacement de stockage

Une fois que vous avez configuré les paramètres de stockage et d'archivage d'un serveur d'enregistrement, vous pouvez activer le stockage et l'archivage pour chaque caméra ou pour un groupe de caméras. Cette opération peut être effectuée à partir des périphériques individuels ou à partir du groupe de périphériques. Voir Relier un périphérique ou un groupe de périphériques à un emplacement de stockage (á la page 82).

Archivage efficace

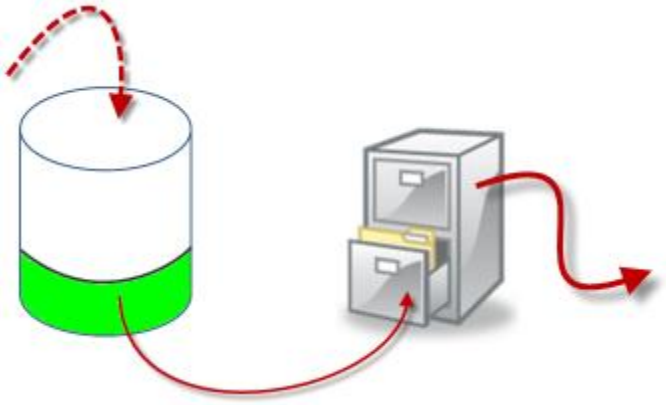
Lorsque vous activez l'archivage d'une caméra ou d'un groupe de caméras, le contenu de la base de données de la caméra est automatiquement déplacé vers une archive à des intervalles que vous définissez.

Selon vos exigences, vous pouvez configurer une ou plusieurs archives pour chacune de vos bases de données. Les archives peuvent être situées soit sur l'ordinateur du serveur d'enregistrement, soit dans un autre emplacement que le système peut atteindre, comme par exemple un disque réseau.

Si nécessaire, vous pouvez organiser et affiner l'usage de l'emplacement de stockage de votre base de données en paramétrant votre archivage de façon efficace. Bien souvent, vous souhaitez minimiser la taille des enregistrements archivés afin qu'ils prennent le moins de place possible, tout spécialement à long terme où il est même possible de diminuer un peu la qualité de l'image. Vous pouvez optimiser l'efficacité de l'organisation et de l'affinage à partir de l'onglet **Stockage** d'un serveur d'enregistrement en réglant plusieurs paramètres interdépendants :

- Durée de rétention de la base de données d'enregistrement
- Taille de la base de données d'enregistrement
- Durée de rétention des archives
- Taille de l'archive
- Calendrier d'archivage
- CryptageImages par seconde (Frames per second - FPS)

Les champs de taille définissent la taille de la base de données de la caméra, comme illustré par ce cylindre et sa/ses archive(s) respective(s) :



Cheminement des enregistrements de la base de données d'enregistrement aux archives et jusqu'à leur suppression

En termes de durée de rétention et de paramètre de taille pour la base de données d'enregistrement, illustrés par la zone blanche du cylindre, vous définissez l'âge que les enregistrements doivent atteindre avant leur archivage. Dans notre exemple illustré, vous archivez les enregistrements lorsqu'ils sont assez anciens pour être archivés.

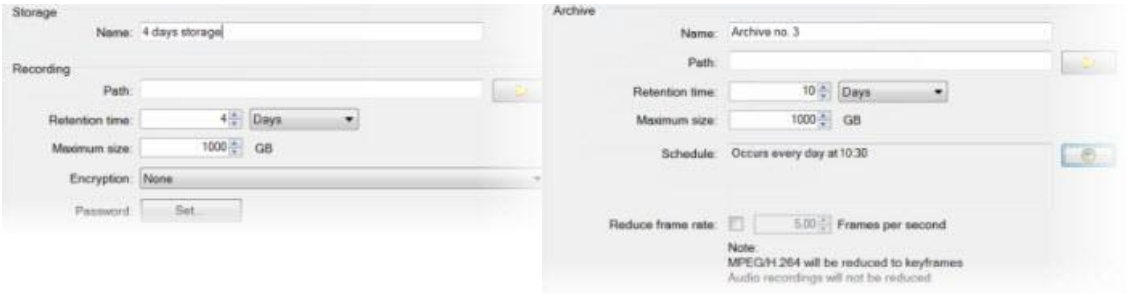
La durée de rétention et le paramétrage de taille des archives définissent la durée pendant laquelle les enregistrements demeurent dans l'archive. Les enregistrements demeurent dans l'archive pendant la période spécifiée, ou jusqu'à ce que l'archive atteigne la limite de taille spécifiée. Lorsque ces paramètres sont remplis, le système commence à remplacer les anciens enregistrements de l'archive.

Le calendrier d'archivage définit la fréquence et l'horaire d'archivage.

Le FPS détermine la taille des données dans les bases de données.

Pour archiver vos enregistrements, vous devez régler tous ces paramètres les uns par rapport aux autres. Cela signifie que la durée de rétention de la prochaine archive entrante doit toujours être plus longue que la durée de rétention d'une archive ou base de données d'enregistrement actuelle. En effet, le nombre de jours de rétention indiqué pour une archive inclut toute rétention mentionnée précédemment dans le processus. De plus, l'archivage doit toujours avoir lieu plus fréquemment que ne le permet la durée de rétention. Autrement, vous risquez de perdre des données. Si votre durée de rétention est de 24 heures, toute donnée vieille de plus de 24 heures sera effacée. Ainsi, pour transférer vos données vers l'archive suivante en toute sécurité, il est important d'effectuer l'archivage plus fréquemment que toutes les 24 heures.

> **Exemple** : Ces emplacements de stockage (image à gauche) ont une durée de rétention de 4 jours alors que l'archive suivante (image à droite) a une durée de rétention de 10 jours. L'archivage est réglé de façon à se produire tous les jours à 10 h 30, permettant un archivage des données bien plus fréquent que la durée de rétention.



Vous pouvez également contrôler l'archivage au moyen de règles et d'événements.

Ajouter un nouvel emplacement de stockage d'enregistrement

Vous créez toujours un emplacement de stockage avec une base de données d'enregistrement prédéfinie appelée **Enregistrement**. Vous ne pouvez pas la renommer. Hormis une base de données d'enregistrement, un emplacement de stockage peut contenir un certain nombre d'archives.

1. Pour ajouter plus de stockage à un serveur d'enregistrement sélectionné, cliquez sur le bouton  situé en dessous de la liste de **Configuration du stockage**. Celui-ci ouvre la boîte de dialogue **Paramètres de stockage et d'enregistrement**.
2. Spécifiez les paramètres (voir "Propriétés des paramètres de stockage et d'enregistrement" á la page 86) pertinents pour continuer.
3. Cliquez sur **OK**.

Si besoin, vous êtes maintenant prêt à créer une ou des archive(s) à l'intérieur de votre nouvel emplacement de stockage. Voir Créer une archive dans un emplacement de stockage (á la page 82).

Créer une archive dans un emplacement de stockage

Un emplacement de stockage ne comporte aucune archive par défaut lorsqu'il est créé.

1. Pour créer une archive, sélectionnez l'emplacement de stockage pertinent dans la liste **Configuration d'enregistrement et d'archivage**.
2. Cliquez sur le bouton  situé sous la liste **Configuration d'enregistrement et d'archivage**.
3. Dans la boîte de dialogue **Paramètres d'archive**, spécifiez les paramètres requis (voir Propriétés des paramètres d'archive (á la page 87)).
4. Cliquez sur **OK**.

Relier un périphérique ou un groupe de périphériques à un emplacement de stockage

Une fois qu'un répertoire d'enregistrements est configuré pour un serveur d'enregistrement, vous pouvez l'activer pour des périphériques individuels tels que des caméras, micros ou haut-parleurs ou un groupe de périphériques. Vous pouvez également sélectionner quels répertoires d'enregistrements d'un serveur d'enregistrement vous souhaitez utiliser pour le périphérique individuel ou le groupe de périphériques.

1. Agrandissez **Périphériques** et sélectionnez **Caméras**, **Microphones** ou **Haut-parleurs** selon les besoins.
2. Sélectionnez le périphérique ou un groupe de périphériques.
3. Sélectionnez l'onglet **Enregistrer**.
4. Dans la zone **Stockage**, sélectionnez **Sélectionner**.
5. Dans la boîte de dialogue qui apparaît, sélectionnez la base de données qui doit stocker les enregistrements du périphérique, puis cliquez sur **OK**.
6. Dans la boîte à outils, cliquez sur **Enregistrer**.

Lorsque vous cliquez sur le numéro d'utilisation du périphérique pour le répertoire d’enregistrements de l'onglet Stockage du serveur d'enregistrement, le périphérique est visible dans le rapport des messages qui apparaît.

Modifier les paramètres d'un emplacement de stockage ou d'une archive sélectionné(e)

1. Pour modifier un emplacement de stockage, sélectionnez sa base de données d'enregistrement dans la liste **Configuration d'enregistrement et d'archivage**. Pour modifier une archive, sélectionnez la base de données de l'archive.

2. Cliquez sur le bouton **Modifier stockage d'enregistrement**  situé sous la liste **Configuration d'enregistrement et d'archivage**.

3. Modifiez une base de données d'enregistrement ou modifiez une archive.

Si vous modifiez la taille maximale d'une base de données, le système archive automatiquement les enregistrements qui dépassent la nouvelle limite. Il archive automatiquement les enregistrements dans l'archive suivante ou les supprime selon les paramètres d'archivage.

Sauvegarde des enregistrements archivés

De nombreuses organisations souhaitent sauvegarder leurs enregistrements, au moyen de lecteurs de bande ou de tout autre lecteur similaire. La façon dont vous y parvenez est hautement personnalisée et dépend des supports de sauvegarde utilisés par votre entreprise. Cependant, il est prudent de garder les informations suivantes à l'esprit :

Sauvegardez les archives plutôt que les bases de données des caméras

Créez toujours des sauvegardes basées sur le contenu des archives et non sur les bases de données des caméras individuelles. Si vous créez des sauvegardes basées sur le contenu des bases de données d'une caméra individuelle, vous pouvez provoquer des violations de partage ou d'autres dysfonctionnements.

Lorsque vous prévoyez de faire une copie de sauvegarde, assurez-vous que l’opération de sauvegarde ne chevauche pas vos horaires d'archivage spécifiés. Pour visualiser le calendrier d'archivage de chaque serveur d'enregistrement dans chacun des répertoires d’enregistrements d'un serveur d'enregistrement, reportez-vous à l'onglet Stockage.

Familiarisez-vous avec votre structure d'archive pour pouvoir cibler les sauvegardes

Lorsque vous archivez des enregistrements, ils sont stockés dans une certaine structure de sous-répertoires au sein de l'archive.

Dans le cadre d'une utilisation ordinaire de votre système, la structure de sous-répertoires est entièrement transparente aux utilisateurs du système lorsqu'ils parcourent tous les enregistrements avec le XProtect Smart Client. Ceci est valable pour les enregistrements archivés et non archivés. Il est judicieux de connaître la structure de sous-répertoires si vous souhaitez sauvegarder vos enregistrements archivés. Voir À propos de la structure d'archive (á la page 83) et Sauvegarder et restaurer la configuration (voir "Sauvegarde et restauration de la configuration du système" á la page 416).

À propos de la structure d'archive

Lorsque vous archivez des enregistrements, ils sont stockés dans une certaine structure de sous-répertoires au sein de l'archive.

Dans le cadre d'une utilisation ordinaire de votre système, la structure de sous-répertoires est entièrement transparente aux utilisateurs du système lorsqu'ils parcourent tous les

enregistrements avec le XProtect Smart Client, que ces enregistrements soient archivés ou non. Une bonne connaissance de votre structure de sous-répertoires est particulièrement intéressante si vous souhaitez sauvegarder vos enregistrements archivés.

Dans chaque répertoire d'archivage du serveur d'enregistrement, le système crée automatiquement des sous-répertoires séparés. Ces sous-répertoires sont désignés par le nom du périphérique et de la base de données d'archivage.

Puisque vous pouvez stocker des enregistrements provenant de différentes caméras dans la même archive, et puisque l'archivage de chaque caméra est probablement exécuté à des intervalles réguliers, des sous-répertoires supplémentaires sont également ajoutés automatiquement.

Ces sous-répertoires représentent environ une heure d'enregistrements chacun. La coupure horaire permet de supprimer uniquement des parties relativement petites des données d'une archive si vous atteignez la taille maximale permise pour l'archive.

Les sous-répertoires sont désignés par le nom du périphérique, puis par une indication du lieu de provenance des enregistrements (caméra locale ou via SMTP, **puis** par la date et l'heure de l'enregistrement le plus récent de la base de données contenu dans le sous-répertoire.

Structure de désignation :

```
...[Chemin de stockage]\[Nom de l'espace de stockage]\[nom du périphérique] -
 plus la date et l'heure de l'enregistrement le plus récent]\
```

Si les données proviennent d'une caméra locale :

```
...[Chemin de stockage]\[Nom de l'espace de stockage]\[nom du périphérique]
(Edge) - plus la date et l'heure de l'enregistrement le plus récent]\
```

Si les données proviennent de SMTP :

```
...[Chemin de stockage]\[Nom de l'espace de stockage]\[nom du périphérique]
(SMTP) - plus la date et l'heure de l'enregistrement le plus récent]\
```

Exemple réel :

```
...F:\OurArchive\Archive1\Camera 1 sur Axis Q7404 Video Server(10.100.50.137)
- 2011-10-05T11:23:47+02:00\
```

Sous-répertoires :

D'autres sous-répertoires sont également ajoutés automatiquement. La quantité et la nature de ces sous-répertoires dépend de la nature des enregistrements. Par exemple, plusieurs sous-répertoires différents doivent être ajoutés si les enregistrements sont techniquement divisés en séquences. Ceci est souvent le cas si vous avez utilisé la détection du mouvement pour déclencher les enregistrements.

- **Média** : Ce répertoire contient les média, qui sont soit vidéo, soit audio (mais pas les deux).
- **NiveauMouvement** : Ce répertoire contient des grilles de niveau de mouvement générées à partir des données vidéo à l'aide d'un algorithme de détection du mouvement. Ces données permettent à la fonction Recherche avancée de XProtect Smart Client d'effectuer des recherches très rapides.
- **Signature** : Ce répertoire contient les signatures générées pour les données multimédia (dans le répertoire Média). Avec ces informations, vous pouvez vérifier que les données multimédia n'ont pas été falsifiées depuis leur enregistrement.
- **Mouvement** : Dans ce répertoire, le système stocke des séquences de mouvement. Une séquence de mouvement est une tranche horaire pour laquelle un mouvement a été détecté dans les données vidéo. Par exemple, ces informations sont utilisées dans la chronologie de XProtect Smart Client.

- **Enregistrement** : Dans ce répertoire, le système stocke des séquences d'enregistrement. Une séquence d'enregistrement est une tranche horaire pour laquelle il existe des enregistrements cohérents de données multimédia. Par exemple, ces informations sont utilisées pour afficher la chronologie dans XProtect Smart Client.

Si vous souhaitez sauvegarder vos archives, vous pouvez cibler vos sauvegardes si vous connaissez les fondamentaux de la structure des sous-répertoires.

Exemples de sauvegarde :

Pour sauvegarder le contenu entier d'une archive, sauvegardez le répertoire de l'archive requis ainsi que son contenu complet. Par exemple, tout le contenu de :

```
...F:\OurArchive\
```

Pour sauvegarder les enregistrements d'une caméra particulière pour une période particulière, sauvegardez uniquement le contenu des sous-répertoires pertinents. Par exemple, tout le contenu de :

```
...F:\OurArchive\Archive1\Camera 1 sur Axis Q7404 Video Server(10.100.50.137)
- 2011-10-05T11:23:47+02:00\
```

Supprimer une archive d'un espace de stockage

1. Sélectionnez l'archive dans la liste **Configuration d'enregistrement et d'archivage**.

   Il est uniquement possible de supprimer la dernière archive de la liste. Il n'est pas nécessaire que l'archive soit vide.

2. Cliquez sur le bouton  situé sous la liste **Configuration d'enregistrement et d'archivage**.

3. Cliquez sur **Oui**.

Suppression d'un espace de stockage

Vous ne pouvez pas supprimer le ou les espace(s) de stockage par défaut que les périphériques utilisent pour le stockage des enregistrements en direct.
Cela signifie que vous devrez peut-être déplacer des périphériques (voir "Déplacer du matériel" á la page 107) et tout enregistrement qui n'a pas encore été archivé vers un autre espace de stockage avant de supprimer l'espace de stockage.

1. Pour consulter la liste des périphériques qui utilisent cet espace de stockage, cliquez sur le numéro d'utilisation du périphérique.

   Si l'espace de stockage comporte des données provenant de périphériques ayant été déplacés vers un autre serveur d'enregistrement, un avertissement s'affiche. Cliquez sur le lien pour consulter la liste de périphériques.

2. Suivez les étapes présentées dans Déplacer les enregistrements non archivés d'un emplacement de stockage à un autre (voir "Déplacer les enregistrements non archivés d'un espace de stockage à un autre" á la page 86).

3. Continuez jusqu'à ce que vous ayez déplacé tous les périphériques.

4. Sélectionnez l'espace de stockage que vous souhaitez supprimer.

5. Cliquez sur le bouton  situé sous la liste **Configuration de stockage**.
6. Cliquez sur **Oui**.

Déplacer les enregistrements non archivés d'un espace de stockage à un autre

Vous déplacez des enregistrements d'une base de données d'enregistrement en direct à une autre à partir de l'onglet **Enregistrer** du périphérique.

1. sélectionnez le type de périphérique. Dans le volet **Vue d'ensemble**, sélectionnez le périphérique.
2. Cliquez sur l'onglet **Enregistrer**. Dans la partie supérieure de la zone **Stockage**, cliquez sur **Sélectionner**.
3. Dans la boîte de dialogue **Sélectionner stockage**, sélectionnez la base de données.
4. Cliquez sur **OK**.
5. Dans la boîte de dialogue **Action d'enregistrement**, indiquez si vous souhaitez déplacer des enregistrements existants mais **non-archivés** vers le nouvel espace de stockage ou si vous souhaitez les supprimer.
6. Cliquez sur **OK**.

Propriétés des paramètres de stockage et d'enregistrement

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

Dans la fenêtre de dialogue des **Paramètres de stockage et d'enregistrement**, indiquez les éléments suivants :

Nom	Description
Nom	Renommez l'emplacement de stockage si nécessaire. Les noms doivent être uniques.
Chemin	Spécifiez le chemin jusqu'au répertoire dans lequel vous sauvegardez les enregistrements dans cet emplacement de stockage. L'emplacement de stockage ne doit pas nécessairement être situé sur l'ordinateur du serveur d'enregistrement. Si le répertoire n'existe pas, vous pouvez le créer. Les disques réseau doivent être indiqués à l'aide du format UNC (Universal Naming Convention), par exemple : \\serveur\volume\répertoire\.

Nom	Description
Durée de rétention	Précisez la durée pendant laquelle les enregistrements doivent demeurer dans l'archive avant d'être supprimés ou déplacés dans l'archive suivante (en fonction des paramètres de l'archive). La durée de rétention doit toujours être plus longue que la durée de rétention de l'archive précédente ou de la base de données d'enregistrement par défaut. En effet, le nombre de jours de rétention indiqué pour une archive inclut toutes les périodes de rétention mentionnées précédemment dans le processus.
Taille maximum	Sélectionnez le nombre maximum de giga-octets de données d'enregistrement à enregistrer dans la base de données d'enregistrement. Les données d'enregistrement supérieures au nombre de giga-octets spécifié seront déplacées automatiquement dans la première archive de la liste - si des archives sont spécifiées - ou supprimées. **Important** : S'il y a moins de 5 Go d'espace libre, le système archive toujours automatiquement (ou supprime si aucune archive suivante n'est définie) les plus anciennes données d'une base de données. S'il y a moins de 1 Go d'espace libre, les données seront supprimées. Une base de données a toujours besoin de 250 Mo d'espace libre. Si vous atteignez cette limite (si les données ne sont pas supprimées assez rapidement), aucune autre donnée ne sera ajoutée à la base de données tant que vous n'aurez pas libéré suffisamment d'espace. La taille maximum réelle de votre base de données est la quantité de giga-octets que vous spécifiez, moins 5 Go.
Signature	Active une signature numérique pour les enregistrements. Par exemple, cela signifie que le système confirme qu'une vidéo exportée n'a pas été modifiée ou manipulée lors de la lecture.
Cryptage	Sélectionnez le niveau de cryptage des enregistrements : • **Aucun** • **Faible (utilisation du processeur moindre)** • **Fort (utilisation du processeur supérieure)** Si vous choisissez d'activer le cryptage, vous devez également spécifier un mot de passe pour les utilisateurs autorisés à consulter les données chiffrées.
Mot de passe	Saisissez un mot de passe.

Propriétés des paramètres d'archive

Dans les **Paramètres d'archive**, spécifiez les éléments suivants :

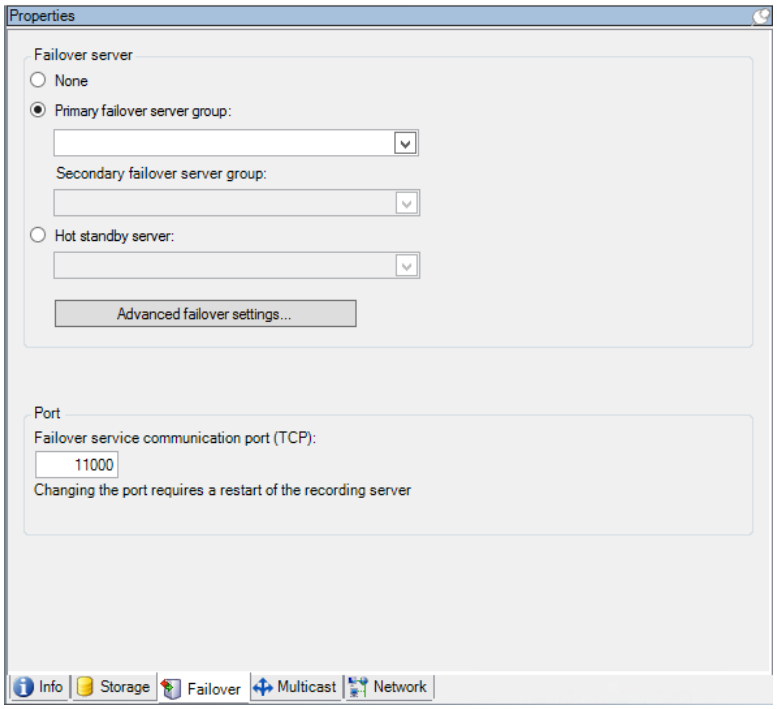
Nom	Description
Nom	Renommez l'emplacement de stockage si nécessaire. Les noms doivent être uniques.
Chemin	Spécifiez le chemin jusqu'au répertoire dans lequel vous sauvegardez les enregistrements dans cet emplacement de stockage. L'emplacement de stockage ne doit pas nécessairement être situé sur l'ordinateur du serveur d'enregistrement. Si le répertoire n'existe pas, vous pouvez le créer. Les disques réseau doivent être indiqués à l'aide du format UNC (Universal Naming Convention), par exemple : \\server\volume\directory\.
Durée de rétention	Précisez la durée pendant laquelle les enregistrements doivent demeurer dans l'archive avant d'être supprimés ou déplacés dans l'archive suivante (en fonction des paramètres de l'archive). La durée de rétention doit toujours être plus longue que la durée de rétention de l'archive précédente ou de la base de données d'enregistrement par défaut. En effet, le nombre de jours de rétention indiqué pour une archive inclut toutes les périodes de rétention mentionnées précédemment dans le processus.
Taille maximum	Sélectionnez le nombre maximum de giga-octets de données d'enregistrement à enregistrer dans la base de données d'enregistrement. Les données d'enregistrement supérieures au nombre de giga-octets spécifié seront déplacées automatiquement dans la première archive de la liste - si des archives sont spécifiées - ou supprimées. **Important** : S'il y a moins de 5 Go d'espace libre, le système archive toujours automatiquement (ou supprime si aucune archive suivante n'est définie) les plus anciennes données d'une base de données. S'il y a moins de 1 Go d'espace libre, les données seront supprimées. Une base de données a toujours besoin de 250 Mo d'espace libre. Si vous atteignez cette limite (si les données ne sont pas supprimées assez rapidement), aucune autre donnée ne sera ajoutée à la base de données tant que vous n'aurez pas libéré suffisamment d'espace. La taille maximum réelle de votre base de données est la quantité de giga-octets que vous spécifiez, moins 5 Go.
Calendrier	Spécifiez un calendrier d'archivage qui définit les intervalles dans lesquels le processus d'archivage doit commencer. Vous pouvez archiver très fréquemment (en principe chaque heure toute l'année) ou très rarement (par exemple, chaque premier lundi tous les 36 mois).

Nom	Description
Réduire la fluidité d'image	Pour réduire le FPS lors de l'archivage, sélectionnez la case à cocher **Réduire la fluidité d'image** et configurez un nombre d'images par seconde (FPS). La réduction de la fluidité d'image d'un nombre d'images par seconde sélectionné permet de faire en sorte que vos enregistrements prennent moins de place dans l'archive, mais réduit également la qualité de votre archive. MPEG-4/H.264/H.265 réduit automatiquement aux images clés comme minimum. 0,1 = 1 image par 10 secondes.

Onglet Redondance (serveur d'enregistrement)

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

Si votre organisation utilise des serveurs d'enregistrement de redondance, utilisez l'onglet **Redondance** pour affecter des serveurs de redondance aux serveurs d'enregistrement, voir Propriétés de l'onglet Redondance (voir "Propriétés de l'onglet basculement" á la page 90).



Pour obtenir des informations plus détaillées sur les serveurs d'enregistrement de redondance, l'installation et les paramètres, les groupes de redondance et leurs paramètres, reportez-vous au paragraphe À propos des serveurs d'enregistrement de redondance (ordinaires et à affectation unique) (voir "À propos des serveurs d'enregistrement de redondance" á la page 95).

Affecter des serveurs d'enregistrement de redondance

Dans l'onglet **Redondance** d'un serveur d'enregistrement, vous pouvez choisir parmi 3 différents types de configurations de redondance :

a Pas de configuration de redondance

b Une configuration de redondance primaire/secondaire

c Une configuration à affectation unique.

Si vous sélectionnez **b** et **c**, vous devez sélectionner le serveur/les groupes spécifique(s). Avec **b**, vous pouvez également sélectionner un groupe de redondance secondaire. En cas d'indisponibilité du serveur d'enregistrement, un serveur d'enregistrement de redondance du groupe de redondance primaire prend le relais. Si vous avez également sélectionné un groupe de redondance secondaire, un serveur d'enregistrement de redondance du groupe secondaire prend le relais si tous les serveurs d'enregistrement de redondance du groupe de redondance primaire sont occupés. De cette façon, votre risque se limite à l'absence d'une solution de redondance dans le rare cas où tous les serveurs d'enregistrement de redondance des groupes de redondance primaire et secondaire sont occupés.

1. Dans le volet **Navigation du site**, sélectionnez **Serveurs** > **Serveurs d'enregistrement**. Cette commande ouvre une liste de serveurs d'enregistrement.
2. Dans le volet **Vue d'ensemble**, sélectionnez le serveur d'enregistrement souhaité puis allez sur l'onglet **Redondance**.
3. Pour choisir le type de configuration de redondance, sélectionnez **Aucun**, **Groupe de serveurs de redondance primaire**/**groupe de serveurs de redondance secondaire**ou **Serveur de redondance à affectation unique**. Vous ne pouvez pas choisir le même groupe de redondance comme groupe de redondance primaire et secondaire ni sélectionner des serveurs de redondance ordinaires qui font déjà partie d'un groupe de redondance en tant que serveurs de redondance à affectation unique.
4. Ensuite, cliquez sur **Paramètres de redondance avancés**. Ceci ouvre la fenêtre **Paramètres de redondance avancés**, qui répertorie tous les périphériques rattachés au serveur d'enregistrement sélectionné. Si vous avez sélectionné **Aucun**, les Paramètres de redondance avancés sont disponibles. Toute sélection est conservée pour toute configuration de redondance ultérieure.
5. Afin de spécifier le niveau de soutien de redondance, sélectionnez **Soutien complet**, **Uniquement en direct** ou **Désactivé** pour chaque périphérique de la liste. Cliquez sur **OK**.
6. Dans le champ **Port de communication avec le service de redondance (TCP)**, modifiez le numéro de port si nécessaire.

Propriétés de l'onglet basculement

Nom	Description
aucun	Sélectionnez une configuration sans basculement
Groupe de serveurs de basculement primaire / groupe de serveurs de basculement secondaire	Sélectionnez une configuration de basculement ordinaire avec un groupe de serveurs de basculement primaire, et potentiellement un groupe secondaire.

Nom	Description
Serveur de basculement à affectation unique	Sélectionnez une configuration à affectation unique dotée d'un serveur d'enregistrement dédié en tant que serveur de redondance à affectation unique.
Paramètres de basculement avancés	Ouvre la fenêtre **Paramètres de basculement avancés**. • **Soutien complet** : Sélectionnez cette option pour que le périphérique bénéficie d'un soutien de redondance complet. • **Uniquement en direct** : Sélectionnez cette option pour que le périphérique bénéficie d'un soutien de redondance en direct. • **Désactivé** : Sélectionnez cette option pour désactiver le soutien de redondance pour le périphérique.
Port de communication avec le service de basculement (TCP)	Par défaut, le numéro de port est 11000. Vous utilisez ce port pour les communications entre les serveurs d'enregistrement et les serveurs d'enregistrement de redondance. Si vous modifiez le port, le serveur d'enregistrement **doit** être en cours de fonctionnement et **doit** être connecté au serveur de gestion.

Onglet Multicast (serveur d'enregistrement)

Votre système prend en charge le multicast de diffusions en continu et en direct à partir de serveurs d'enregistrement. Si de multiples utilisateurs de XProtect Smart Client souhaitent visualiser des vidéos en direct à partir de la même caméra, le multicast contribue à économiser une quantité considérable de ressources du système. Ainsi, le multicast est particulièrement utile si vous utilisez la fonction Matrix, où de multiples clients requièrent la diffusion en direct d'une vidéo provenant de la même caméra.

Le multicast est possible uniquement pour les diffusions en direct, et non pour les enregistrements vidéo/audio.

Si un serveur d'enregistrement possède plus d'une carte d'interface réseau, il est uniquement possible de procéder à un multicast sur l'une d'entre elles. Vous pouvez spécifier laquelle utiliser par le biais du Management Client.

La mise en œuvre fructueuse du multicast nécessite également la configuration des équipements de votre réseau pour pouvoir relayer des paquets de données au groupe de destinataires requis uniquement. Sinon, le multicast ne diffèrera pas de la diffusion ordinaire, qui peut ralentir les communications de votre réseau de façon significative.

À propos du multicast

Dans une communication réseau standard, chaque paquet de données est envoyé par un expéditeur unique à un destinataire unique ; on l'appelle unicast. Cependant, avec le multicast, vous pouvez envoyer un seul paquet de données (à partir d'un serveur) à des destinataires multiples (clients) au sein d'un groupe. Le multicast peut contribuer à économiser de la bande passante.

- Lorsque vous utilisez l'**unicast**, la source doit transmettre un flux de données pour chaque destinataire.

- Lorsque vous utilisez le **multicast**, un seul flux de données suffit sur chaque segment du réseau.

Le multicast tel qu'il est décrit ici ne s'apparente **pas** à la diffusion de vidéos d'une caméra vers des serveurs, mais de serveurs vers des clients.

Avec le multicast, vous travaillez avec un groupe de destinataires défini, basé sur des options telles que les plages d'adresses IP, la possibilité d'activer/désactiver le multicast pour des caméras individuelles, la possibilité de définir la plus grande taille de paquet de données acceptable (MTU), le nombre maximum de routeurs entre lesquels un paquet de données peut être transféré (TTL), etc.

Le multicast ne doit pas être confondu avec la **diffusion**, qui envoie des données à toute personne connectée au réseau, même si les données ne sont pas pertinentes pour tous :

Nom	Description
Unicast	envoie des données d'une source unique à un destinataire unique.
Multicast	envoie des données d'une source unique à des destinataires multiples au sein d'un groupe clairement défini.
Diffusion	Envoie des données d'une source unique à toutes les personnes d'un réseau. La diffusion peut donc ralentir considérablement la communication du réseau.

Activation du multicast

Pour utiliser le multicast, votre infrastructure réseau doit prendre en charge l'IGMP (Internet Group Management Protocol) standard de multicast IP.

- Dans l'onglet **Multicast**, sélectionnez la case **Multicast**.

Si la plage d'adresses IP complète pour le multicast est déjà en cours d'utilisation sur un ou plusieurs serveurs d'enregistrement, vous devez libérer tout d'abord certaines adresses IP multicast avant de pouvoir activer le multicast sur des serveurs d'enregistrement supplémentaires.

Affectation de la plage d'adresses IP

Spécifiez la plage que vous souhaitez affecter en tant qu'adresses pour les flux multicast à partir du serveur d'enregistrement sélectionné. Les clients se connectent à ces adresses lorsque les utilisateurs visionnent une vidéo en multicast à partir du serveur d'enregistrement.

Pour chaque envoi de la caméra en multicast, la combinaison d'adresse IP et de port doit être unique (exemple IPv4 : 232.0.1.0:6000). Vous pouvez utiliser une adresse IP et de nombreux ports, ou de nombreuses adresses IP et moins de ports. Par défaut, le système suggère une seule adresse IP et une plage de 1 000 ports, mais vous pouvez le modifier selon les besoins.

Les adresses IP pour le multicast doivent être dans la plage définie pour l'affectation d'hôte dynamique par IANA. IANA est l'autorité qui supervise l'affectation globale des adresses IP.

Nom	Description
Adresse IP	Dans le champ **Début**, indiquez la première adresse IP de la plage désirée. Ensuite, indiquez la dernière adresse IP de la plage dans le champ **Fin**.

Nom	Description
Port	Dans le champ **Début**, indiquez le premier numéro de port de la plage désirée. Ensuite, indiquez le dernier numéro de port de la plage dans le champ **Fin**.
Adresse IP source pour tous les flux multicast	Vous pouvez uniquement multidiffuser sur une carte d'interface réseau, donc ce champ est pertinent si votre serveur d'enregistrement possède plus d'une carte d'interface réseau ou s'il possède une carte d'interface réseau comptant plus d'une adresse IP. Pour utiliser l'interface par défaut du serveur d'enregistrement, laissez la valeur 0.0.0.0 (IPv4) ou :: (IPv6) dans le champ. Si vous souhaitez utiliser une autre carte d'interface réseau, ou une adresse IP différente sur la même carte d'interface réseau, indiquez l'adresse IP de l'interface désirée. • IPv4 : 224.0.0.0 à 239.255.255.255. • IPv6, la plage est décrite sur le site IANA http://www.iana.org.

Spécification des options de datagramme

Spécifiez les paramètres relatifs aux paquets de données (datagrammes) transmis par le biais du multicast.

Nom	Description
MTU	unité de transmission maximum, la plus grande taille de paquet de données physique autorisée (mesurée en octets). Les messages supérieurs à la MTU spécifiée sont divisés en paquets plus petits avant d'être envoyés. La valeur par défaut est 1500, ce qui est également la valeur par défaut sur la plupart des ordinateurs Windows et des réseaux Ethernet.
TTL	durée de vie, le plus grand nombre de bonds autorisé qu'un paquet de données devrait pouvoir parcourir avant d'être jeté ou renvoyé. Un bond est un point entre deux dispositifs de réseau, généralement un routeur. La valeur par défaut est 128.

Activation du multicast pour des caméras individuelles

Le multicast ne fonctionne que lorsque vous l'activez pour les caméras requises :

1. Sélectionnez le serveur d'enregistrement et sélectionnez la caméra requise dans le volet **Vue d'ensemble**.
2. Dans l'onglet **Client**, sélectionnez la case **Multicast en direct**. Répétez l'opération pour toutes les caméras requises.

Onglet Réseau (serveur d'enregistrement)

Vous définissez l'adresse IP publique d'un serveur d'enregistrement dans l'onglet **Réseau**.

Pourquoi utiliser une adresse publique ?

Lorsqu'un client d'accès, tel qu'un XProtect Smart Client, se connecte à un système de surveillance, une quantité de communication de données initiales, y compris l'échange d'adresses de contact, est partagée en arrière-plan. Cela s'effectue automatiquement, et est totalement transparent pour les utilisateurs.

Les clients peuvent se connecter depuis le réseau local ainsi que depuis Internet, et dans les deux cas, le système de surveillance doit fournir les adresses adéquates pour que les clients aient accès aux vidéos en direct et enregistrées à partir des serveurs d'enregistrement :

- Lorsque les clients se connectent localement, le système de surveillance doit communiquer avec les adresses locales et les numéros de port.
- Lorsque les clients se connectent depuis Internet, le système de surveillance doit répondre avec l'adresse publique du serveur d'enregistrement, c'est-à-dire l'adresse du pare-feu ou du routeur NAT (Network Address Translation), et souvent aussi un numéro de port différent. L'adresse et le port peuvent ensuite être redirigés à l'adresse locale et au port du serveur.

  Pour donner accès au système de surveillance depuis l'extérieur d'un pare-feu NAT (Network Address Translation), vous pouvez utiliser des adresses publiques et la redirection du port. Les clients situés à l'extérieur du pare-feu peuvent ainsi se connecter aux serveurs d'enregistrement sans utiliser de VPN (Virtual Private Network, réseau privé virtuel). Chaque serveur d'enregistrement peut être configuré sur un port spécifique et le port peut être redirigé à travers le pare-feu jusqu'à l'adresse interne du serveur.

Définition de l'adresse publique et du port

1. Pour activer l'accès public, sélectionnez la case à cocher **Activer l'accès public**.
2. Définissez l'adresse publique du serveur d'enregistrement. Saisissez l'adresse du pare-feu ou du routeur NAT pour que les clients qui accèdent au système de surveillance depuis Internet puissent se connecter aux serveurs d'enregistrement.
3. Spécifiez un numéro de port public. Il est toujours judicieux que les numéros de ports utilisés sur le pare-feu ou le routeur NAT soient différents de ceux utilisés localement.

Si vous utilisez un accès public, configurez le pare-feu ou le routeur NAT de façon à ce que les demandes envoyées à l'adresse et au port publics soient redirigées à l'adresse et au port locaux des serveurs d'enregistrement pertinents.

Affectation de plages IP locales

Vous définissez une liste de plages IP locales que le système de surveillance doit reconnaître comme provenant d'un réseau local.

- Dans l'onglet **Réseau**, cliquez sur **Configurer**.

Supprimer un serveur d'enregistrement

Important : Si vous supprimez un serveur d'enregistrement, toute la configuration spécifiée dans le Management Client est supprimée du serveur d'enregistrement, y compris **tout** le matériel associé au serveur d'enregistrement (caméras, périphériques d'entrée, etc.).

1. Faites un clic droit sur le serveur d'enregistrement que vous souhaitez supprimer dans le volet **Vue d'ensemble**.
2. Sélectionnez **Supprimer le serveur d'enregistrement**.
3. Si vous êtes sûr de vous, cliquez sur **Oui**.
4. Le serveur d'enregistrement et tout son matériel associé sont supprimés.

Supprimer tous les périphériques matériels sur un serveur d'enregistrement

Important : Lorsque vous supprimez du matériel, toutes les données enregistrées associées au matériel sont supprimées de façon permanente.

1. Faites un clic droit sur le serveur d'enregistrement sur lequel vous souhaitez supprimer tout le matériel.
2. Sélectionnez **Supprimer tous les périphériques matériels**.
3. Confirmez la suppression.

Serveurs de redondance

À propos des serveurs d'enregistrement de redondance

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

Un serveur d'enregistrement de redondance est un serveur d'enregistrement supplémentaire qui peut prendre le relais d'un serveur d'enregistrement normal si celui-ci devient indisponible. Vous pouvez configurer un serveur d'enregistrement de redondance de deux façons, en tant que **serveur d'enregistrement de redondance ordinaire** ou en tant que **serveur de redondance à affectation unique**.

Vous installez les serveurs d'enregistrement de redondance comme des serveurs d'enregistrement ordinaires. Une fois que vous avez installé les serveurs d'enregistrement de redondance, ils sont visibles dans le Management Client. Vous devez installer tous les serveurs d'enregistrement de redondance sur des ordinateurs séparés. Veillez à configurer les serveurs d'enregistrement de redondance avec l'adresse IP/nom d'hôte corrects du serveur de gestion et à vérifier que le compte d'utilisateur dans lequel le service Failover Server fonctionne a accès à votre système avec des droits d'administrateur.

Vous pouvez spécifier quel type d'assistance de redondance vous souhaitez pour chaque périphérique. Pour chaque périphérique d'un serveur d'enregistrement, vous pouvez sélectionner une assistance complète, uniquement en direct ou aucune assistance de redondance. Ceci vous aide à accorder une priorité à vos ressources de redondance et, par exemple, à ne configurer de

système de redondance que pour la vidéo et non pour l'audio, ou encore à n'avoir de système de redondance que pour les caméras essentielles et non pour les caméras de moindre importance.

Important : Lorsque votre système est en mode de redondance, vous ne pouvez pas remplacer ou déplacer du matériel, mettre le serveur d'enregistrement à jour, ou modifier les configurations des périphériques, et notamment les paramètres de stockage ou les paramètres de flux vidéo.

Serveurs de redondance ordinaires

Dans une configuration de serveur de redondance ordinaire, vous pouvez regrouper un serveur d'enregistrement de redondance avec d'autres serveurs d'enregistrement de redondance dans un groupe de redondance. L'ensemble du groupe de redondance se consacre à prendre le relais de plusieurs serveurs d'enregistrement présélectionnés au cas où ceux-ci ne seraient plus disponibles.

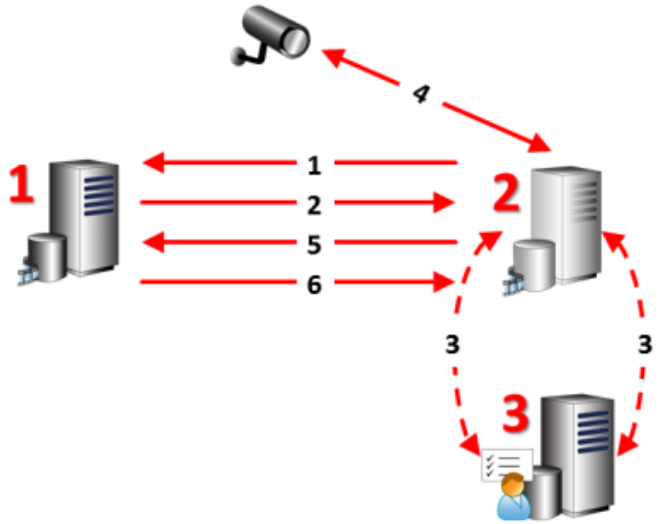
Un groupe de redondance peut contenir un ou plusieurs autres serveurs d'enregistrement de redondance. Le regroupement a un avantage évident : par la suite, lorsque vous spécifiez les serveurs d'enregistrement de redondance devant prendre le relais d'un serveur d'enregistrement, vous sélectionnez un groupe de serveurs d'enregistrement de redondance. Si le groupe choisi contient plus d'un serveur d'enregistrement de redondance, vous savez que vous avez plus d'un serveur d'enregistrement de redondance à disposition si jamais un serveur d'enregistrement était indisponible. Vous pouvez créer autant de groupes de redondance que nécessaire et les regrouper en fonction de vos besoins. Un serveur d'enregistrement de redondance peut uniquement faire partie d'un seul groupe à la fois.

Les serveurs d'enregistrement de redondance d'un groupe de redondance sont classés de façon séquentielle. Cette séquence détermine dans quel ordre les serveurs d'enregistrement de redondance doivent prendre le relais d'un serveur d'enregistrement. Par défaut, cette séquence reflète l'ordre dans lequel vous avez incorporé les serveurs d'enregistrement de redondance dans le groupe de redondance : l'ordre du premier arrivé. Vous pouvez le modifier si nécessaire.

Serveurs d'enregistrement de redondance à affectation unique

Dans une configuration de serveur d'enregistrement à affectation unique, vous pouvez dédier un serveur d'enregistrement de redondance pour qu'il prenne le relais d'**un** seul serveur d'enregistrement. Pour cette raison, le système peut conserver ce serveur d'enregistrement de redondance en mode « veille », ce qui signifie qu'il démarre déjà avec la configuration correcte/actuelle du serveur d'enregistrement auquel il est dédié et qu'il peut prendre le relais plus rapidement qu'un serveur d'enregistrement de redondance ordinaire. Comme mentionné précédemment, vous affectez les serveurs à affectation unique à un seul serveur d'enregistrement et vous ne pouvez pas le regrouper. Vous ne pouvez pas choisir d'utiliser des serveurs de redondance qui font déjà partie d'un groupe de redondance en tant que serveurs d'enregistrement à affectation unique.

À propos des étapes de redondance



Serveurs impliqués (numéros en rouge) :

1. Serveur d'enregistrement
2. Serveur d'enregistrement de redondance
3. Serveur de gestion

Étapes de redondance pour les configurations de **Redondance ordinaire** :

1. Pour vérifier si elle fonctionne ou non, un serveur d'enregistrement de redondance dispose d'une connexion permanente avec le serveur d'enregistrement.
2. Cette connexion est interrompue.
3. Le serveur d'enregistrement de redondance demande la configuration actuelle du serveur d'enregistrement à partir du serveur de gestion. Le serveur de gestion envoie la configuration requise, le serveur d'enregistrement de redondance reçoit la configuration, démarre et commence à enregistrer pour le compte du serveur d'enregistrement.
4. Le serveur d'enregistrement de redondance et la/les caméra(s) échangent des données vidéo.
5. Le serveur d'enregistrement de redondance essaie continuellement de rétablir la connexion avec le serveur d'enregistrement.
6. Lorsque la connexion au serveur d'enregistrement est rétablie, le serveur d'enregistrement de redondance s'éteint et le serveur d'enregistrement recherche les données vidéo (le cas échéant) enregistrées pendant sa coupure et les données vidéo sont fusionnées dans la base de données du serveur d'enregistrement.

Étapes de redondance pour les configurations **à affectation unique** :

1. Pour vérifier si elle fonctionne ou non, un serveur de redondance à affectation unique dispose d'une connexion permanente avec le serveur d'enregistrement auquel il est assigné.
2. Cette connexion est interrompue.
3. À partir du serveur de gestion, le serveur de redondance à affectation unique connaît déjà la configuration actuelle de son serveur d'enregistrement assigné et commence à enregistrer pour son compte.
4. Le serveur de redondance à affectation unique et la ou les caméra(s) pertinente(s) échangent des données vidéo.
5. Le serveur de redondance à affectation unique essaie continuellement de rétablir la connexion avec le serveur d'enregistrement.
6. Lorsque la connexion au serveur d'enregistrement est rétablie et que le serveur de redondance à affectation unique retourne en mode veille, le serveur d'enregistrement récupère les données

vidéo (le cas échéant) enregistrées pendant sa coupure et les données vidéo sont fusionnées dans la base de données du serveur d'enregistrement.

À propos de la fonctionnalité du serveur d'enregistrement de redondance

- Un serveur d'enregistrement de redondance vérifie l'état des serveurs d'enregistrement concernés toutes les 0,5 secondes. Si un serveur d'enregistrement ne répond pas sous 2 secondes, le serveur d'enregistrement est considéré comme indisponible et le serveur d'enregistrement de redondance prend le relais.

- Un serveur d'enregistrement de redondance ordinaire prend le relais du serveur d'enregistrement qui est devenu indisponible après 5 secondes plus le temps qu'il faut au service Recording Server du serveur d'enregistrement de redondance pour démarrer, plus le temps nécessaire à la connexion aux caméras. Par contre, un serveur d'enregistrement à affectation unique prend le relais plus rapidement car le service Recording Server fonctionne déjà avec la bonne configuration et n'a qu'à démarrer ses caméras pour diffuser les flux. Pendant la période de démarrage, vous ne pouvez pas stocker d'enregistrements ni visionner des vidéos en direct à partir des caméras concernées.

- Lorsqu'un serveur d'enregistrement redevient disponible, il prend automatiquement le relais du serveur d'enregistrement de redondance ou à affectation unique. Les enregistrements stockés par le serveur d'enregistrement de redondance ou à affectation unique sont automatiquement fusionnés dans les bases de données du serveur d'enregistrement standard. Le temps que le processus de fusion prend dépend de la quantité d'enregistrements à fusionner, de la capacité du réseau, etc. Pendant le processus de fusion, vous ne pouvez pas parcourir les enregistrements à partir de la période pendant laquelle le serveur d'enregistrement de redondance ou à affectation unique a pris le relais.

- Si un serveur d'enregistrement de redondance doit prendre le relais d'un autre serveur d'enregistrement pendant le processus de fusion dans une configuration de serveur d'enregistrement de redondance ordinaire, il reporte le processus de fusion avec le serveur d'enregistrement A, et prend le relais du serveur d'enregistrement B. Lorsque le serveur d'enregistrement B redevient disponible, le serveur d'enregistrement de redondance ordinaire reprend le processus de fusion avec le serveur d'enregistrement A, après quoi il commence la fusion avec le serveur d'enregistrement B.
  Dans une configuration à affectation unique, un serveur de redondance à affectation unique ne peut pas prendre le relais d'un autre serveur d'enregistrement car il n'est affecté qu'à un seul serveur d'enregistrement. Mais si ce serveur d'enregistrement subit une nouvelle défaillance, le serveur à affectation unique prend à nouveau le relais et conserve les enregistrements de la période précédente. Le serveur d'enregistrement conserve les enregistrements jusqu'à leur fusion avec l'enregistreur primaire ou jusqu'à ce que le serveur d'enregistrement de redondance n'ait plus d'espace disponible sur le disque.

- Une solution de redondance n'offre pas une redondance intégrale. Elle peut uniquement servir de moyen fiable pour minimiser les temps d'arrêt. Si un serveur d'enregistrement redevient disponible, le service Failover Server s'assure que le serveur d'enregistrement est prêt à sauvegarder de nouveau les enregistrements. Alors seulement la responsabilité de sauvegarder les enregistrements revient au serveur d'enregistrement standard. Par conséquent, la perte des enregistrements à ce stade du processus est très improbable.

- Les utilisateurs clients remarquent à peine qu'un serveur d'enregistrement de redondance prend le relais. Une brève coupure se produit, généralement pendant quelques secondes seulement, au moment où le serveur d'enregistrement de redondance prend le relais. Au cours de cette interruption, les utilisateurs n'ont pas accès à la vidéo du serveur d'enregistrement concerné. Les utilisateurs clients peuvent reprendre le visionnage des

vidéos en direct dès que le serveur d'enregistrement de redondance a pris le relais. Comme les enregistrements récents sont stockés sur le serveur d'enregistrement de redondance, ils peuvent lire les enregistrements effectués après la prise de relais par le serveur d'enregistrement de redondance. Les clients ne peuvent pas lire les enregistrements plus anciens sauvegardés uniquement sur le serveur d'enregistrement touché tant que ce serveur d'enregistrement ne fonctionne pas de nouveau, et a pris le relais du serveur d'enregistrement de redondance. Vous ne pouvez pas accéder aux enregistrements archivés. Lorsque le serveur d'enregistrement fonctionne de nouveau, un processus de fusion a lieu. Au cours de ce processus, les enregistrements du serveur de redondance sont fusionnés dans la base de données du serveur d'enregistrement. Pendant ce processus, vous ne pouvez pas lire les enregistrements de la période pendant laquelle le serveur d'enregistrement de redondance a pris le relais.

- Dans une configuration de redondance ordinaire, la configuration d'un serveur d'enregistrement de redondance en soutien d'un autre serveur d'enregistrement de redondance n'est pas nécessaire. La raison est que vous n'attribuez pas de serveurs d'enregistrement de redondance particuliers pour prendre le relais d'un serveur d'enregistrement standard. Mais vous attribuez plutôt des groupes de redondance. Un groupe de redondance doit comprendre au moins un serveur d'enregistrement de redondance, mais vous pouvez ajouter autant de serveurs d'enregistrement de redondance que nécessaire. À condition qu'un groupe de redondance contienne plusieurs serveurs d'enregistrement de redondance, plusieurs serveurs d'enregistrement de redondance peuvent prendre le relais. Dans une configuration à affectation unique, vous ne pouvez pas configurer un serveur d'enregistrement de redondance ou un serveur à affectation unique pour un serveur de redondance à affectation unique.

Installer un serveur d'enregistrement de redondance

Important : Au cours du processus d'installation, il vous est demandé de spécifier un compte utilisateur sous lequel le **service Failover Server** doit fonctionner. Ce compte d'utilisateur doit disposer de droits d'administrateur dans le système. Veuillez également noter que si vous gérez des groupes de travail, vous devez ignorer les instructions normales d'installation des serveurs d'enregistrement et utiliser la méthode alternative d'installation pour les groupes de travail.

Une fois que vous avez installé le serveur de gestion à l'aide de l'installateur commun, téléchargez l'installateur du serveur d'enregistrement séparé à partir de la page web du serveur de gestion. Dans cet installateur, vous pouvez spécifier si vous souhaitez installer un serveur d'enregistrement standard ou un serveur d'enregistrement de basculement.

1. Allez sur la page web de téléchargement du serveur de gestion et sélectionnez l'installateur de Recording Server. Sauvegardez l'installateur dans un emplacement approprié et exécutez-le à partir de là ou directement sur la page web.

2. Sélectionnez la **Langue** que vous souhaitez utiliser pendant l'installation. Cliquez sur **Continuer**.

3. Dans la liste de sélection, sélectionnez **Basculement** pour installer un serveur d'enregistrement en tant que serveur d'enregistrement de basculement.

4. Spécifiez les propriétés du serveur d'enregistrement de basculement. Cliquez sur **Continuer**.

5. Lors de l'installation d'un serveur d'enregistrement de basculement, vous devez utiliser le compte d'utilisateur particulier appelé **Ce compte**. Si nécessaire, saisissez un mot de passe et confirmez-le. Cliquez sur **Continuer**.

6. Sélectionnez l'**Emplacement des fichiers** pour le fichier du programme. Dans **Langue du produit**, sélectionnez la langue dans laquelle votre système doit être installé. Cliquez sur **Installer**.

7. Le logiciel procède maintenant à l'installation. Une fois l'installation terminée, une liste des composants installés correctement s'affiche. Cliquez sur **Fermer.**

   Une fois que vous avez installé le serveur d'enregistrement de basculement, vous pouvez vérifier son état à partir de l'icône **Service Failover Server**.

Configurer et activer des serveurs d'enregistrement de redondance

Important : Si vous avez désactivé le serveur d'enregistrement de redondance, vous devez l'activer avant qu'il puisse prendre le relais des serveurs d'enregistrement ordinaires.

Suivez la procédure suivante pour activer un serveur d'enregistrement de redondance et modifier ses propriétés de base :

1. Dans le volet **Navigation du site**, sélectionnez **Serveurs** > **Serveurs de redondance**. Ceci ouvre une liste des serveurs d'enregistrement de redondance et des groupes de redondance installés.
2. Dans le volet **Vue d'ensemble**, sélectionnez le serveur d'enregistrement de redondance requis.
3. Faites un clic droit et sélectionnez **Activé**. Le serveur d'enregistrement de redondance est maintenant activé.
4. Pour modifier les propriétés du serveur d'enregistrement de redondance, allez dans l'onglet **Info** :
5. Une fois que vous avez terminé, allez dans l'onglet **Réseau**. Ici, vous pouvez entre autres définir l'adresse IP publique du serveur d'enregistrement de redondance. Cela vous concerne si vous utilisez NAT (Network Address Translation) et la redirection du port. Reportez-vous à l'onglet **Réseau** du serveur d'enregistrement standard pour de plus amples informations.

Pour voir l'état d'un serveur d'enregistrement de redondance, passez votre souris sur l'icône dans la barre d'état système. Une infobulle apparaît. Celle-ci contient le texte saisi dans le champ Description du serveur d'enregistrement de redondance. Cela peut vous aider à déterminer le serveur d'enregistrement duquel le serveur d'enregistrement de redondance est censé prendre le relais.

Important : Le serveur d'enregistrement de redondance pingue le serveur de gestion à intervalles réguliers afin de vérifier qu'il est bien en ligne et capable de demander et de recevoir la configuration des serveurs d'enregistrement standard en fonction des besoins. Si vous bloquez le ping, le serveur d'enregistrement de redondance n'est pas en mesure de prendre le relais des serveurs d'enregistrement standard.

Regrouper des serveurs d'enregistrement de redondance

1. Sélectionnez **Serveurs** > **Serveurs de redondance**. Ceci ouvre une liste des serveurs d'enregistrement de redondance et des groupes de redondance installés.
2. Dans le volet **Vue d'ensemble**, faites un clic droit sur le nœud supérieur **Groupes de redondance** et sélectionnez **Ajouter groupe**.
3. Spécifiez un nom (dans cet exemple *Groupe de redondance 1*) et une description (facultative) de votre nouveau groupe. Cliquez sur **OK**.

4. Faites un clic droit sur le groupe (*Groupe de redondance 1*) que vous venez de créer. Sélectionnez **Modifier les membres du groupe**. La fenêtre **Sélectionner les membres du groupe** s'ouvre.
5. Utilisez les boutons ou votre souris pour déplacer le(s) serveur(s) d'enregistrement de redondance du côté gauche au côté droit. Cliquez sur **OK**. Le(s) serveur(s) d'enregistrement de redondance appartiennent maintenant au groupe (*Groupe de redondance 1*) que vous venez de créer.
6. Allez dans l'onglet **Séquence**. Cliquez sur **Haut** et **Bas** pour configurer la séquence interne des serveurs d'enregistrement de redondance ordinaires dans le groupe.

Lire les icônes d'état du serveur d'enregistrement de redondance

Les icônes suivantes représentent l'état des serveurs d'enregistrement de redondance (les icônes sont visibles dans le volet **Vue d'ensemble**) :

Icône	Description
	Le serveur d'enregistrement de redondance est en attente ou « en surveillance ». Lorsqu'il est en attente, le serveur d'enregistrement de redondance n'est pas configuré pour prendre le relais d'un quelconque serveur d'enregistrement. Lorsqu'il est « en surveillance », le serveur d'enregistrement de redondance est configuré pour surveiller un ou plusieurs serveurs d'enregistrement.
	Le serveur d'enregistrement de redondance a pris le relais du serveur d'enregistrement désigné. Si vous placez votre curseur sur l'icône du serveur, vous voyez une infobulle. Utilisez cette infobulle pour identifier le serveur d'enregistrement duquel le serveur d'enregistrement de redondance a pris le relais.
	La connexion au serveur d'enregistrement de redondance est interrompue.

Propriétés du serveur d'enregistrement de redondance

Spécifiez les propriétés du serveur d'enregistrement de redondance suivantes :

Nom	Description
Nom	Le nom du serveur d'enregistrement de redondance tel qu'il apparaît dans le Management Client, les journaux et autres.
Description	Un champ facultatif que vous pouvez utiliser pour décrire le serveur d'enregistrement de redondance, par exemple de quel serveur d'enregistrement il prend le relais.
Nom de l'hôte	Affiche l'adresse réseau du serveur d'enregistrement de redondance. Vous ne pouvez pas le modifier.
Port UDP	Le numéro de port utilisé pour la communication entre les serveurs d'enregistrement de redondance. Par défaut, le système utilise le port 8844.

Nom	Description
Emplacement de la base de données	Spécifiez le chemin conduisant à la base de données utilisée par le serveur d'enregistrement de redondance pour le stockage des enregistrements. Vous ne pouvez pas modifier le chemin de la base de données lorsque le serveur d'enregistrement de redondance prend le relais d'un serveur d'enregistrement. Le système applique les modifications lorsque le serveur d'enregistrement de redondance ne prend plus le relais du serveur d'enregistrement.
Activer ce serveur de redondance	Décochez la case pour désactiver le serveur d'enregistrement de redondance (cochée par défaut). Veuillez noter que vous devez désactiver les serveurs d'enregistrement de redondance avant qu'ils puissent prendre le relais des serveurs d'enregistrement.

Propriétés des groupes de redondance

L'onglet **Info** :

Champ	Description
Nom	Le nom du groupe de redondance tel qu'il apparaît dans le Management Client, les journaux et autres.
Description	Une description facultative, par exemple l'emplacement physique du serveur.

L'onglet **Séquence** :

Champ	Description
Spécifier la séquence de redondance	Utilisez **Haut** et **Bas** pour configurer la séquence désirée des serveurs d'enregistrement de redondance ordinaires au sein du groupe.

À propos des services Failover Recording Server

Un serveur d'enregistrement de redondance comprend deux services installés :

- Un service Failover Server, qui traite les processus de prise en charge du serveur d'enregistrement. Ce service fonctionne toujours et vérifie en permanence l'état des serveurs d'enregistrement concernés.
- Un service Failover Recording Server, qui permet au serveur d'enregistrement de redondance d'agir comme un serveur d'enregistrement.

  Dans une configuration de groupe de redondance, ce service n'est démarré que lorsqu'il est requis, c'est-à-dire lorsque le serveur d'enregistrement de redondance ordinaire doit prendre le relais du serveur d'enregistrement. Le démarrage de ce service prend généralement quelques secondes, mais peut prendre plus longtemps selon les paramètres de sécurité et d'autres éléments.

Dans une configuration à serveur de secours, ce service est toujours en fonctionnement et permet au serveur de redondance à affectation unique de prendre le relais plus rapidement que le serveur d'enregistrement de redondance ordinaire.

Voir les messages d'état

1. Sur le serveur d'enregistrement de redondance, faites un clic droit sur l'icône **Service Failover server** de **Milestone**.
2. Sélectionnez **Afficher les messages d'état**. La fenêtre **Messages d'état du serveur de redondance** apparaît, listant les messages d'état horodatés.

Modifier l'adresse du serveur de gestion

Le serveur d'enregistrement de redondance doit pouvoir communiquer avec le serveur de gestion de votre système. Vous spécifiez l'adresse IP/nom d'hôte du serveur de gestion lors de l'installation du serveur d'enregistrement de redondance. Si vous souhaitez modifier l'adresse du serveur de gestion, procédez comme suit :

1. Sur le serveur d'enregistrement de redondance, arrêtez le service Failover Recording Server.
2. Cliquez à nouveau sur l'icône du service Failover Recording Server de la zone de notification avec le bouton droit.
3. Sélectionnez **Modifier les paramètres**. La fenêtre **Paramètres du serveur d'enregistrement de redondance** apparaît pour que vous puissiez spécifier l'adresse IP ou le nom d'hôte du serveur de gestion avec lequel le serveur d'enregistrement de redondance doit communiquer.

Voir les informations sur la version

Connaître la version exacte de votre **service Failover Recording Server** est un avantage s'il vous faut contacter l'assistance du produit.

1. Sur le serveur d'enregistrement de redondance, faites un clic droit sur l'icône **service Failover Recording Server** de **Milestone**.
2. Sélectionnez **À propos**.
3. Une petite boîte de dialogue s'ouvre. Elle affiche la version exacte de votre **service Failover Recording Server.**

Matériel et serveurs distants

À propos du matériel

Le matériel représente :

- l'unité physique qui se connecte directement au serveur d'enregistrement du système de surveillance via IP, par exemple une caméra, un encodeur vidéo, un module E/S ou

- un serveur d'enregistrement sur un site distant dans une configuration Milestone Interconnect.

Reportez-vous au paragraphe Ajouter un matériel (voir "Ajouter matériel" á la page 104) pour savoir comment ajouter un matériel à votre système.

Ajouter matériel

Vous avez plusieurs possibilités pour ajouter du matériel pour chaque serveur d'enregistrement que vous avez autorisé sur votre système.

Important : Si votre matériel se situe derrière un routeur compatible NAT ou un pare-feu, il se peut que vous deviez préciser un numéro de port différent et configurer le routeur/pare-feu de façon à ce qu'il cartographie le port et les adresses IP que le matériel utilise.

L'assistant d'installation **Ajout de matériel** vous aide à détecter le matériel tel que les caméras et les encodeurs vidéo sur votre réseau et à les ajouter aux serveurs d'enregistrement sur votre système. L'assistant vous aide également à ajouter des serveurs d'enregistrement à distance pour les configurations Milestone Interconnect. Ajoutez uniquement du matériel à **un serveur d'enregistrement** à la fois.

1. Pour accéder à l'assistant **Ajout de matériel**, faites un clic droit sur le serveur d'enregistrement requis et sélectionnez **Ajout de matériel**.
2. Sélectionnez l'une des options de l'assistant (voir ci-dessous) et suivez les instructions qui s'affichent à l'écran.
3. Une fois l'installation terminée, vous pouvez voir le matériel et ses périphériques dans le volet **Vue d'ensemble**.

Nom	Description
Rapide (Recommandé)	Le système recherche automatiquement les nouveaux matériels disponibles sur le réseau local du serveur d'enregistrement. Cochez la case **Afficher le matériel exécuté sur d'autres serveurs d'enregistrement** pour voir si le matériel détecté fonctionne sur d'autres serveurs d'enregistrement. Vous pouvez sélectionner cette option chaque fois que vous ajoutez un nouveau matériel sur votre réseau et souhaitez l'utiliser dans votre système. Vous ne pouvez pas utiliser cette option pour ajouter des systèmes à distance dans les configurations Milestone Interconnect.

Nom	Description
Analyse de la plage d'adresses	Le système recherche les matériels et les systèmes à distance Milestone Interconnect pertinents sur votre réseau en fonction de vos spécifications de : • noms d'utilisateur et mots de passe des matériels. Ils ne sont pas nécessaires si vos matériels utilisent les noms d'utilisateur et mots de passe par défaut configurés en usine. • pilotes • plages IP (IPv4 uniquement) • numéro de port (port par défaut 80) Vous pouvez sélectionner cette option lorsque vous souhaitez seulement analyser une partie de votre réseau, par exemple lors d'une expansion de votre système.
Manuelle	Précisez les détails concernant chaque matériel et système à distance Milestone Interconnect séparément. Il peut s'agir d'un choix judicieux si vous souhaitez ajouter uniquement quelques matériels et que vous connaissez leurs adresses IP, les noms d'utilisateur et mots de passe concernés ou si une caméra ne prend pas en charge la fonction de détection automatique.
Matériel de connexion à distance	Le système recherche les matériels connectés au moyen d'un serveur connecté à distance. Vous pouvez utiliser cette option si vous avez installé des serveurs pour, par exemple, la Connexion à la caméra Axis One-click. Vous ne pouvez pas utiliser cette option pour ajouter des systèmes à distance dans les configurations Milestone Interconnect.

Désactiver/activer le matériel

Le matériel ajouté est **activé** par défaut.

Vous pouvez voir si le matériel est activé ou désactivé de cette façon :

 Activé
 Désactivé

Pour désactiver le matériel ajouté, à des fins d'activation de licence ou de performance, par exemple :

1. Agrandissez le serveur d'enregistrement et faites un clic droit sur le matériel que vous souhaitez désactiver.
2. Sélectionnez **Activé** pour le supprimer ou le sélectionner.

Éditer le matériel

Vous pouvez modifier des paramètres de base, tels que l'adresse IP/le nom d'hôte, pour le matériel ajouté :

1. Agrandissez le serveur d'enregistrement et faites un clic droit sur le matériel que vous souhaitez éditer.
2. Sélectionnez **Modifier le matériel**. Ceci ouvre la fenêtre **Modifier le matériel**, dans laquelle vous pouvez modifier les propriétés pertinentes.
3. Cliquez sur **OK**.

Activer/désactiver des périphériques individuels

Les caméras sont **activées** par défaut.

Les microphones, haut-parleurs, métadonnées, entrées et **sorties** sont **désactivés** par défaut.

Cela signifie que les microphones, haut-parleurs, métadonnées, entrées et sorties doivent être activés individuellement avant de pouvoir être utilisés sur le système. Cela s'explique par le fait que les systèmes de surveillance reposent intrinsèquement sur les caméras, alors que l'utilisation de microphones, etc. dépend beaucoup des besoins de chaque entreprise.

Vous pouvez voir si les périphériques sont activés ou désactivés (les exemples montrent une sortie) :

Désactivé
Activé

La même méthode d'activation/désactivation est utilisée pour les caméras, les microphones, les haut-parleurs, les métadonnées, les entrées et les sorties.

1. Agrandissez le serveur d'enregistrement et le périphérique. Faites un clic droit sur le périphérique que vous souhaitez activer.
2. Sélectionnez **Activé** pour le supprimer ou le sélectionner.

Configurer une connexion sécurisée avec le matériel

Vous pouvez configurer une connexion HTTPS sécurisée avec SSL (Secure Sockets Layer) entre le matériel et le serveur d'enregistrement.

Consultez votre fournisseur de caméras pour obtenir un certificat pour votre matériel et le télécharger sur le matériel, avant de continuer avec les étapes ci-dessous :

1. Dans le volet **Vue d'ensemble**, faites un clic droit sur le serveur d'enregistrement et sélectionnez le matériel.

Sélectionner le matériel sous un serveur d'enregistrement

2. Dans l'onglet **Paramètres**, activez HTTPS. Cela n'est pas activé par défaut.
3. Saisissez le port du serveur d'enregistrement auquel la connexion HTTPS est raccordée. Le numéro du port doit correspondre au port configuré sur la page d'accueil du périphérique.
4. Apportez les changements nécessaires et enregistrez.

Déplacer du matériel

À propos du déplacement de matériel

Vous pouvez déplacer du matériel d'un serveur d'enregistrement à un autre dans la mesure où ils appartiennent au même site. Après tout déplacement, le matériel et ses périphériques fonctionnent sous le nouveau serveur d'enregistrement et les nouveaux enregistrements sont stockés sur ce serveur. Le déplacement est transparent pour les utilisateurs du client.

Les enregistrements stockés sur l'ancien serveur d'enregistrement y restent jusqu'à ce que :

- Le système les supprime à l'expiration de la durée de rétention. Les enregistrements que quelqu'un a protégés à l'aide de la protection des preuves (voir "À propos de la protection des preuves" á la page 254) ne sont pas supprimés tant que la durée de rétention de la protection des preuves n'a pas expiré. C'est vous qui définissez la durée de rétention de la protection des preuves lorsque vous la créez. La durée de rétention des preuves peut potentiellement ne jamais expirer.
- Vous les supprimez du nouveau serveur d'enregistrement de chaque périphérique dans l'onglet **Enregistrer**.

Si vous essayez de supprimer un serveur d'enregistrement contenant encore des enregistrements, vous recevez un avertissement.

Si vous déplacez du matériel vers un serveur d'enregistrement sur lequel aucun matériel n'est ajouté, les utilisateurs du client doivent se déconnecter et se reconnecter afin de recevoir des données des périphériques en question.

Vous pouvez utiliser la fonction Déplacer du matériel pour :

- **Équilibrer les charges** : Si, par exemple, le disque du serveur d'enregistrement est surchargé, vous pouvez ajouter un nouveau serveur d'enregistrement et déplacer une partie de votre matériel.
- **Mettre à jour** : Par exemple, si vous devez remplacer le serveur hébergeant le serveur d'enregistrement par un nouveau modèle, vous pouvez installer un nouveau serveur d'enregistrement et déplacer le matériel de l'ancien serveur vers le nouveau serveur.

- **Remplacer un serveur d'enregistrement défectueux** : Si, par exemple, le serveur est hors ligne et ne va jamais revenir en ligne, vous pouvez déplacer le matériel vers d'autres serveurs d'enregistrement et ainsi permettre au système de continuer à fonctionner. Vous ne pouvez pas accéder aux anciens enregistrements. Voir également Remplacer un serveur d'enregistrement (voir "Remplacer un serveur d'enregistrement" á la page 428).

Enregistrements à distance

Lorsque vous déplacez du matériel vers un autre serveur d'enregistrement, le système annule les récupérations en cours ou planifiées à partir des sites interconnectés ou des espaces de stockage externe sur les caméras. Les enregistrements ne sont pas supprimés, mais les données ne sont pas récupérées et sauvegardées dans les bases de données comme escompté. Si tel est le cas, vous recevrez un avertissement. Pour l'utilisateur XProtect Smart Client qui avait entamé une récupération lorsque vous avez lancé le déplacement du matériel, la récupération échoue. L'utilisateur XProtect Smart Client en est informé et peut réessayer ultérieurement.

Si quelqu'un a déplacé du matériel sur un site distant, vous devez synchroniser manuellement le site central à l'aide de l'option **Mettre le matériel à jour** afin de refléter la nouvelle configuration du site distant. Si vous ne procédez pas à cette synchronisation, les caméras déplacées restent déconnectées sur le site central.

Voir également

Déplacer du matériel (Assistant) (á la page 108)

Déplacer du matériel (Assistant)

Pour déplacer du matériel d'un serveur d'enregistrement vers un autre, exécutez l'assistant **Déplacer du matériel**. L'assistant vous guide tout au long des étapes nécessaires pour déplacer un ou plusieurs périphériques matériels.

Conditions préalables
Avant de lancer l'assistant :

- Assurez-vous que le nouveau serveur d'enregistrement peut accéder à la caméra physique par le biais du réseau.
- Installez le serveur d'enregistrement (voir "Installer le serveur d'enregistrement" á la page 38) sur lequel vous souhaitez déplacer le matériel.
- Autorisez-le (voir "Autoriser un serveur d'enregistrement" á la page 75) et vérifiez qu'il est en ligne.
- Installez la même version des pilotes de périphériques (voir "À propos des pilotes de périphériques vidéo" á la page 429) sur le nouveau serveur d'enregistrement que sur le serveur existant.

Dans un système interconnecté, vous devez synchroniser manuellement le site central après avoir déplacé du matériel sur un site distant pour refléter les changements que vous ou un autre administrateur du système avez apporté au site distant.

Pour exécuter l'assistant :

1. Dans le volet **Navigation du site**, sélectionnez **Serveurs d'enregistrement**.
2. Dans le volet **Vue d'ensemble**, effectuez un clic droit sur le serveur d'enregistrement à partir duquel vous souhaitez déplacer du matériel ou effectuez un clic droit sur un périphérique spécifique.
3. Sélectionnez **Déplacer du matériel**.

Si le serveur d'enregistrement à partir duquel vous déplacez du matériel est déconnecté, un message d'erreur s'affiche. Vous ne devriez déplacer du matériel à partir d'un serveur d'enregistrement déconnecté que si vous êtes certain qu'il ne sera plus jamais en ligne. Si vous choisissez quand même de déplacer du matériel et que le serveur est remis en ligne, vous risquez d'observer un comportement inattendu de la part du système, car le même matériel fonctionnera sur deux serveurs d'enregistrement pendant un certain temps. Par exemple, vous pourriez rencontrer des problèmes tels que des erreurs de licence ou des événements adressés au mauvais serveur d'enregistrement.

4. Si vous avez lancé l'assistant au niveau du serveur d'enregistrement, la page **Sélectionnez le matériel que vous souhaitez déplacer** s'affiche. Sélectionnez les périphériques que vous souhaitez déplacer.
5. Sur la page **Sélectionnez le serveur d'enregistrement vers lequel vous souhaitez déplacer le matériel**, faites votre choix dans la liste de serveurs d'enregistrement installés sur ce site.
6. Sur la page **Sélectionnez le stockage que vous souhaitez utiliser pour les enregistrements futurs**, la barre d'utilisation du stockage indique l'espace libre restant dans la base de données d'enregistrement pour les enregistrements en direct uniquement, et non pour les archives. La durée de rétention totale est la période de rétention combinée de la base de données d'enregistrement et des archives.
7. Le système traite votre demande.
8. Si le déplacement a abouti, cliquez sur **Fermer**. Si vous sélectionnez le serveur d'enregistrement dans le Management Client, vous pouvez voir le matériel déplacer et les enregistrements sont maintenant stockés sur ce serveur.

   Si le déplacement a échoué, vous pouvez diagnostiquer le problème ci-dessous.

Diagnostic des problèmes de déplacement du matériel

Si un déplacement a échoué, il est possible que l'une des raisons suivantes en soient la cause :

Type d'erreur	Dépannage
Le serveur d'enregistrement n'est pas connecté ou est en mode de redondance.	Assurez-vous que le serveur d'enregistrement est bien en ligne. Vous devrez peut-être l'autoriser. Si le serveur est en mode de redondance, patientez et réessayez.
Le serveur d'enregistrement n'est pas la version la plus récente.	Mettez le serveur d'enregistrement à jour de façon à ce qu'il utilise la même version que le serveur de gestion.
Impossible de trouver le serveur d'enregistrement dans la configuration.	Assure-vous de bien avoir autorisé le serveur d'enregistrement ou vérifiez qu'il n'a pas été supprimé.
Échec de mise à jour de la configuration ou de communication avec la base de données de configuration.	Assurez-vous que votre serveur SQL est connecté et qu'il fonctionne.

Type d'erreur	Dépannage
Échec d'arrêt du matériel sur le serveur d'enregistrement actuel.	Il est possible qu'un autre processus ait verrouillé le serveur d'enregistrement ou que le serveur d'enregistrement soit en mode erreur. Assurez-vous que le serveur d'enregistrement fonctionne et réessayez.
Le matériel n'existe pas.	Assurez-vous que le matériel que vous essayez de déplacer n'a pas été simultanément supprimé du système par un autre utilisateur. Ce scénario est relativement improbable.
Le serveur d'enregistrement à partir duquel le matériel a été déplacé est à nouveau en ligne, mais vous avez choisi d'ignorer cette possibilité lorsqu'il était en ligne.	Vous avez sans doute accepté que l'ancien serveur d'enregistrement ne serait plus jamais en ligne lorsque vous avez lancé l'assistant **Déplacer du matériel** mais, au cours du déplacement, le serveur est revenu en ligne. Redémarrez l'assistant et sélectionnez **Non** lorsqu'on vous demande de confirmer si le serveur va être en ligne à nouveau.

Gérer le matériel

Onglet Info (matériel)

Pour des informations sur l'onglet **Info** pour les serveurs distants, consultez l' Onglet Info (serveur distant) (á la page 113).

Onglet Info (matériel)

Nom	Description
Nom	Indiquez un nom. Le système utilise le nom partout où le matériel est répertorié dans le système et les clients. Le nom ne doit pas nécessairement être unique. Lorsque vous renommez un matériel, son nom est modifié de manière globale dans le Management Client.
Description	Saisissez une description du matériel (facultatif). La description apparaît dans plusieurs listes au sein du système. Par exemple, lorsque vous arrêtez le curseur de la souris sur le nom du matériel dans le volet **Vue d'ensemble :**  Exemple d'une caméra.
Modèle	Identifie le modèle du périphérique.

Nom	Description
Version	Affiche la version firmware du système, comme spécifiée par le fabricant.
Numéro de série	Numéro de série du matériel tel que spécifié par le fabricant. Le numéro de série est souvent, mais pas toujours, identique à l'adresse MAC.
Pilote	Identifie le pilote prenant en charge la connexion au matériel.
IE	Ouvre la page d'accueil par défaut du fournisseur du matériel. Vous pouvez utiliser cette page à des fins d'administration du matériel.
Adresse	Le nom d'hôte ou l'adresse IP.
Adresse MAC	Indique l'adresse de contrôle d'accès aux médias (MAC) du matériel du système. Une adresse MAC est un nombre hexadécimal à 12 caractères qui identifie spécifiquement chacun des périphériques d'un réseau.

Onglet Paramètres (matériel)

Dans l'onglet **Paramètres**, vous pouvez vérifier ou modifier les paramètres du matériel.

Le contenu de l'onglet **Paramètres** est déterminé par le matériel sélectionné et varie selon le type de matériel. Pour certains types de matériel, l'onglet **Paramètres** n'affiche aucun contenu ou un contenu en lecture seule.

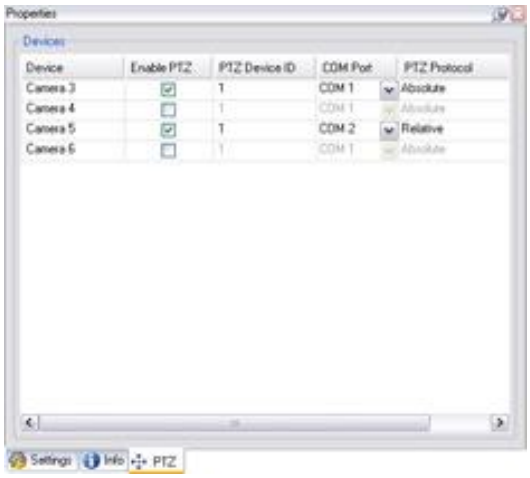
Pour en savoir plus sur l'onglet **Paramètres** pour les serveurs distants, consultez l' onglet Paramètres (serveur distant) (á la page 114).

Onglet PTZ (encodeurs vidéo)

Dans l'onglet **PTZ**, vous pouvez activer PTZ (pan-tilt-zoom) pour les encodeurs vidéo. L'onglet est disponible si le périphérique sélectionné est un encodeur vidéo ou si le pilote prend en charge à la fois les caméras non PTZ et PTZ.

Vous devez activer l'utilisation de PTZ séparément pour chacun des canaux de l'encodeur vidéo dans l'onglet **PTZ** avant de pouvoir utiliser les fonctions PTZ des caméras PTZ fixées à l'encodeur vidéo.

L'utilisation de caméras PTZ n'est pas prise en charge par tous les encodeurs vidéo. Même les encodeurs vidéo qui prennent en charge l'utilisation de caméras PTZ peuvent nécessiter une configuration avant que les caméras PTZ puissent être utilisées. Il s'agit généralement de l'installation de pilotes supplémentaires par le biais d'une interface de configuration basée sur navigateur sur l'adresse IP du périphérique.



Onglet **PTZ**, avec activation PTZ pour deux canaux d'un encodeur vidéo

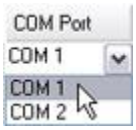
Activer PTZ sur un encodeur vidéo

Pour activer l'utilisation de caméras PTZ sur un encodeur vidéo, procédez comme suit dans l'onglet **PTZ** :

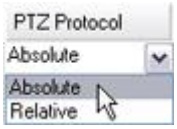
1. Dans la liste des périphériques connectés à l'encodeur vidéo, cochez la case **Activer PTZ** pour les caméras concernées :

2. Dans la colonne **ID du périphérique PTZ**, vérifiez l'ID de chaque caméra.

3. Dans la colonne **Port COM**, sélectionnez quels ports COM (communication série) de l'encodeur vidéo utiliser pour contrôler la fonctionnalité PTZ :



4. Dans la colonne **Protocole PTZ**, sélectionnez quel plan de positionnement vous souhaitez utiliser :



   - **Absolu :** Lorsque les opérateurs utilisent les commandes PTZ de la caméra, elle est ajustée par rapport à une position fixe, souvent appelée position de base de la caméra.
   - **Relative :** Quand les opérateurs utilisent les commandes PTZ de la caméra, elle est ajustée par rapport à sa position actuelle.

Le contenu de la colonne **Protocole PTZ** varie beaucoup en fonction du matériel. Certains possèdent 5 à 8 protocoles différents. Voir également la documentation de la caméra.

5. Dans la boîte à outils, cliquez sur **Enregistrer**.

   Vous êtes maintenant prêt à configurer les positions prédéfinies et la patrouille de chaque caméra PTZ :

   - Ajouter une position prédéfinie (type 1) (á la page 139)
   - Ajouter un profil de patrouille (á la page 147)

Gérer les serveurs distants

Onglet Info (serveur distant)

Nom	Description
Nom	Le système utilise le nom partout où le serveur distant est répertorié dans le système et les clients. Le nom ne doit pas nécessairement être unique. Lorsque vous renommez un serveur, son nom est modifié de manière globale dans le Management Client.
Description	Saisissez une description du serveur distant (facultatif). La description apparaît dans plusieurs listes au sein du système. Par exemple, lorsque vous arrêtez le curseur de la souris sur le nom du matériel dans le volet **Vue d'ensemble**.
Modèle	Affiche le produit XProtect installé sur le site distant.
Version	Affiche la version du système à distance.
Code de licence du logiciel	Code de licence du logiciel du système à distance.
Pilote	Identifie le pilote prenant en charge la connexion au serveur distant.
Adresse	Le nom d'hôte ou l'adresse IP.
IE	(S'applique uniquement au matériel fonctionnant sous Milestone Arcus™) Ouvre la page d'accueil par défaut du fournisseur du matériel. Vous pouvez utiliser cette page à des fins d'administration des matériels ou du système.
ID du système à distance	L'ID unique du système du site distant utilisée par XProtect pour gérer les licences, par exemple.
Nom d'utilisateur Windows	Saisissez le nom d'utilisateur Windows pour accéder par le biais du bureau distant. Ne s'applique pas au matériel fonctionnant sous Milestone Arcus.
Mot de passe Windows	Saisissez le mot de passe Windows pour accéder par le biais du bureau distant. Ne s'applique pas au matériel fonctionnant sous Milestone Arcus.

Nom	Description
Connecter	Ouvre une connexion à distance avec le site distant (sur approbation des certificats Windows). Ne s'applique pas au matériel fonctionnant sous Milestone Arcus.

Onglet Paramètres (serveur distant)

Dans l'onglet **Paramètres**, vous pouvez visualiser le nom du système à distance.

Onglet Événements (serveur distant)

Vous pouvez ajouter des événements à partir du système à distance à votre site central afin de créer des règles et ainsi de répondre immédiatement aux événements à partir du système à distance. Le nombre d'événements dépend des événements configurés dans le système à distance. Vous ne pouvez pas supprimer les événements par défaut.

Si la liste semble incomplète :

1. Faites un clic droit sur le serveur distant concerné dans le volet **Vue d'ensemble** et sélectionnez **Mettre le matériel à jour**.
2. La boîte de dialogue répertorie tous les changements (périphériques supprimés, mis à jour et ajoutés) dans le système à distance depuis que vous avez établi ou actualisé pour la dernière fois la configuration Milestone Interconnect. Cliquez sur **Confirmer** pour mettre votre site central à jour avec ces changements.

Onglet Rappel à distance

Dans l'onglet **Rappel à distance**, vous pouvez gérer les paramètres de rappel d'enregistrement à distance pour le site distant dans une configuration Milestone Interconnect :

Spécifiez les propriétés suivantes :

Nom	Description
Rappeler les enregistrements au max	Détermine la bande passante maximale (en Kbits/s) à utiliser pour rappeler des enregistrements à partir d'un site distant. Cochez la case pour activer la fonction de limitation des rappels.

Nom	Description
Rappeler les enregistrements entre	Détermine que le rappel d'enregistrements à partir d'un site distant doit être limité à un intervalle de temps spécifique. Les travaux non terminés à l'heure de fin se poursuivent jusqu'à leur achèvement, donc si l'heure de fin est critique, vous devez la régler plus tôt pour permettre aux travaux non terminés de s'achever. Si le système reçoit un rappel automatique ou une demande de rappel à partir du XProtect Smart Client en dehors de l'intervalle de temps, il est accepté, mais n'est pas commencé avant d'avoir atteint l'intervalle de temps sélectionné. Vous pouvez visualiser les tâches de rappel d'enregistrement à distance en instance déclenchées par les utilisateurs à partir du **Tableau de bord système** -> **Tâches actuelles**.
Rappeler sur des périphériques en parallèle	Détermine le nombre maximum de périphériques sur lesquels des enregistrements peuvent être récupérés simultanément. Modifiez la valeur par défaut si vous avez besoin de plus ou moins de capacité en fonction des capacités de votre système.

Lorsque vous modifiez les paramètres, plusieurs minutes peuvent être nécessaires pour que les modifications apparaissent dans le système.

Aucune des informations ci-dessus ne s'applique à la lecture directe des enregistrements distants. Toutes les caméras configurées pour être lues directement sont disponibles pour une lecture en direct et utilisent la bande passante selon les besoins.

Périphériques

Les périphériques apparaissent dans le Management Client lorsque vous ajoutez du matériel à l'aide de l'assistant **Ajouter du matériel**.

Vous avez la possibilité de gérer les périphériques par le biais de groupes de périphériques s'ils disposent des mêmes propriétés, voir À propos des groupes de périphériques (á la page 116).

Vous pouvez également gérer les périphériques individuellement :

- Caméras
- Microphones
- Haut-parleurs
- Métadonnées
- Entrées
- Sorties

Voir À propos des périphériques (á la page 119).

Travailler avec des groupes de périphériques

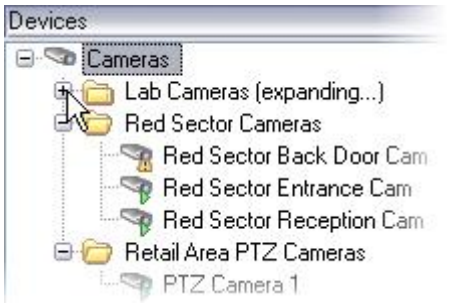
À propos des groupes de périphériques

Le regroupement de périphériques en groupes de périphériques est contenu dans l'assistant **Ajouter du matériel**, mais vous avez toujours la possibilité de modifier les groupes et d'en ajouter d'autres le cas échéant.

Le regroupement de différents types de périphériques (caméras, microphones, haut-parleurs, métadonnées, entrées et sorties) de votre système constitue un avantage :

- Les groupes de périphériques vous aident à garder une vue d'ensemble intuitive des périphériques de votre système.
- Les périphériques peuvent être présents dans plusieurs groupes.
- Vous pouvez créer des sous-groupes et d'autres sous-groupes dans ces sous-groupes.
- Vous pouvez spécifier des propriétés communes pour tous les périphériques d'un groupe de périphériques en une seule fois.
- Les propriétés de périphériques définies par le biais du groupe ne sont pas enregistrées pour le groupe, mais pour chaque périphérique individuel.
- Lorsque vous traitez de rôles, vous pouvez spécifier des paramètres de sécurité communs pour tous les périphériques d'un groupe de périphériques en une seule fois.
- Lorsque vous traitez de règles, vous pouvez appliquer une règle pour tous les périphériques d'un groupe de périphériques en une seule fois.

Vous pouvez ajouter autant de groupes de périphériques que nécessaire. En revanche, vous ne pouvez pas mélanger différents types de périphériques (par exemple des caméras et des haut-parleurs) dans un groupe de périphériques.



Exemple : caméras regroupées dans des groupes de périphériques

Créez des groupes de périphériques avec **moins** de 400 périphériques afin de pouvoir afficher et modifier toutes les propriétés.

Si vous supprimez un groupe de périphériques, vous supprimez uniquement le groupe de périphériques à proprement parler. Si vous souhaitez supprimer un périphérique, par exemple une caméra, de votre système, faites-le au niveau du serveur d'enregistrement.

Les exemples suivants sont basés sur le regroupement de caméras dans des groupes de périphériques, mais le principe s'applique également à tous les périphériques :

Ajouter un groupe de périphériques (á la page 117)

Spécifier les périphériques à inclure dans un groupe de périphériques (á la page 117)

Spécifier les propriétés communes pour tous les périphériques d'un groupe de périphériques (á la page 118)

Ajouter un groupe de périphériques

1. Dans le volet **Vue d'ensemble**, faites un clic droit sur le type de périphérique sous lequel vous souhaitez créer un groupe de périphériques.
2. Sélectionnez **Ajouter un groupe de périphériques**.
3. Dans la boîte de dialogue **Ajouter un groupe de périphériques**, spécifiez un nom et une description pour le nouveau groupe de périphériques :

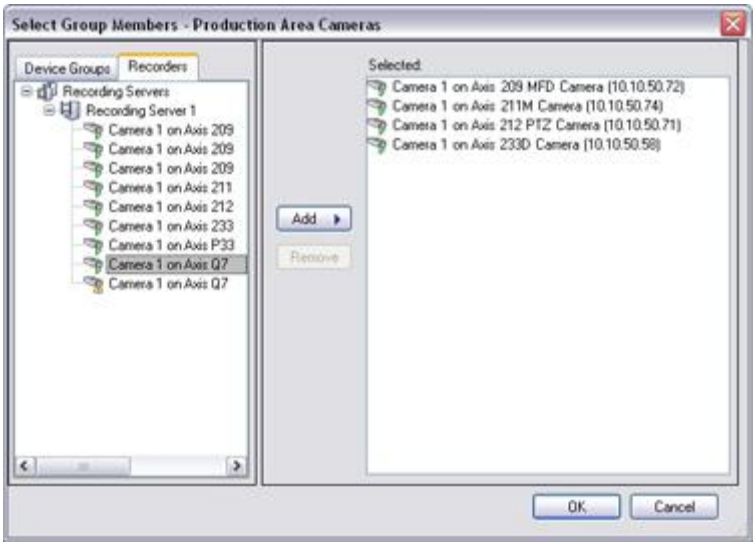
   la description s'affiche lorsque vous survolez le groupe de périphériques dans la liste des périphériques avec le curseur de la souris.
4. Cliquez sur **OK**. Un dossier représentant le nouveau groupe de périphériques apparaît dans la liste.
5. Continuez avec l'étape Spécifier les périphériques à inclure dans un groupe de périphériques (á la page 117).

Spécifier les périphériques à inclure dans un groupe de périphériques

1. Dans le volet **Vue d'ensemble**, faites un clic droit sur le dossier du groupe de périphériques concerné.
2. Sélectionnez **Modifier les membres du groupe de périphériques**.
3. Dans la fenêtre **Sélectionner les membres du groupe**, sélectionnez l'un des onglets pour trouver le périphérique.

   Un périphérique peut être membre de plusieurs groupes de périphériques.

4. Sélectionnez les périphériques que vous souhaitez inclure et cliquez sur **Ajouter** ou double-cliquez sur le périphérique :



5. Cliquez sur **OK**.

6. Si la limite de 400 périphériques est dépassée dans un groupe, vous pouvez ajouter les groupes de périphériques sous formes de sous-groupes dans d'autres groupes de périphériques :

Spécifier les propriétés communes pour tous les périphériques d'un groupe de périphériques

Pour les groupes de périphériques, vous pouvez spécifier les propriétés communes pour tous les périphériques d'un groupe de périphériques donné :

1. Dans le volet **Vue d'ensemble**, cliquez sur le groupe de périphériques.

   Dans le volet **Propriétés**, toutes les propriétés **qui sont disponibles sur tous les périphériques du groupe de périphériques** sont répertoriées et groupées dans des onglets.

2. Indiquez les propriétés communes pertinentes.

   Dans l'onglet **Paramètres**, vous pouvez basculer entre les paramètres pour **tous** les périphériques et ceux de périphériques individuels.

3. Dans la boîte à outils, cliquez sur **Enregistrer**. Ces paramètres sont enregistrés sur les périphériques individuels, pas dans le groupe de périphériques.

Travailler avec des périphériques

À propos des périphériques

Le matériel a un certain nombre de dispositifs que vous pouvez gérer individuellement, par exemple :

- Une caméra physique dispose de périphériques qui représentent les parties de la caméra (objectifs) ainsi que les microphones, les haut-parleurs, les métadonnées, les entrées et les sorties reliés ou intégrés.
- Un encodeur vidéo dispose de plusieurs caméras analogiques connectées qui apparaissent dans une liste de périphériques qui représentent les parties de la caméra (objectifs) ainsi que les microphones, les haut-parleurs, les métadonnées, les entrées et les sorties reliés ou intégrés.
- Un module d'entrée/sortie comporte des dispositifs qui représentent les canaux d'entrée et de sortie pour les lumières, par exemple.
- Un module dédié à l'audio comporte des dispositifs qui représentent les entrées et les sorties des microphones et des haut-parleurs.
- Dans une configuration Milestone Interconnect, le système distant apparaît comme un matériel présentant tous les périphériques du système à distance énumérés dans une liste.

Le système ajoute automatiquement les périphériques du matériel lorsque vous ajoutez un matériel.

Pour plus d'informations sur le matériel pris en charge, voir la page du matériel supporté sur le site Internet de Milestone. https://www.milestonesys.com/supported-hardware.

Les sections suivantes décrivent chaque type de périphérique avec des liens vers les onglets que vous pouvez utiliser pour les gérer.

À propos des périphériques de la caméra

Les périphériques de la caméra sont ajoutés automatiquement lorsque vous ajoutez un matériel sur le système et qu'ils sont activés par défaut.

Les périphériques de caméra offrent un flux vidéo au système que les utilisateurs du client peuvent utiliser pour afficher la vidéo en direct ou que le système peut enregistrer pour une lecture ultérieure par les utilisateurs du client. Les rôles déterminent le droit des utilisateurs à visualiser la vidéo.

Pour plus d'informations sur le matériel pris en charge, voir la page du matériel supporté sur le site Internet de Milestone. https://www.milestonesys.com/supported-hardware.

Le système est fourni avec une règle de flux de démarrage par défaut qui garantit que les flux audio de toutes les caméras connectées soient automatiquement transmis au système. Comme les autres règles, la règle par défaut peut être désactivée et/ou modifiée selon les besoins.

Activer/désactiver et renommer les périphériques individuels s'effectue au niveau du matériel du serveur d'enregistrement. Voir Activer/désactiver des périphériques par le biais des groupes de périphériques (á la page 125).

Pour toute autre configuration et gestion des caméras, développez **Périphériques** dans le volet Navigation du site, puis sélectionnez **Caméras**. Dans le volet Vue d'ensemble, vous regroupez vos

caméras pour une vue d'ensemble aisée de vos caméras. Le regroupement initial est effectué dans le cadre de l'assistant **Ajout de matériel**.

Suivez cet ordre de configuration pour effectuer les tâches les plus courantes liées à la configuration d'un périphérique de caméra :

1. Configurer les paramètres de la caméra (voir onglet Paramètres (voir "Onglet Paramètres (périphériques)" á la page 127)).
2. Configurez le flux (voir onglet Flux (voir "Onglet Flux (périphériques)" á la page 129)).
3. Configurez le mouvement (voir onglet Mouvement (voir "Onglet Mouvement (périphériques)" á la page 157)).
4. Configurer l'enregistrement (voir onglet Enregistrement (voir "Onglet Enregistrement (périphériques)" á la page 131)).
5. Configurez les autres paramètres selon vos besoins.

À propos des périphériques de micros

Vous pouvez relier des micros externes sur de nombreux périphériques. Certains périphériques sont équipés de micros intégrés.

Les périphériques de micros sont ajoutés automatiquement lorsque vous ajoutez un matériel sur le système. Ils sont par défaut désactivés, vous devez donc les réactiver avant utilisation, soit avec l'assistant **Ajout de matériel** soit par la suite. Les micros ne nécessitent aucune licence distincte. Vous pouvez utiliser autant de microphones que nécessaire sur votre système.

Vous pouvez utiliser des microphones entièrement indépendamment des caméras.

Les périphériques de micros offrent un flux audio au système que les utilisateurs du client peuvent utiliser pour écouter en direct ou que le système peut enregistrer pour une lecture ultérieure par les utilisateurs du client. Vous pouvez configurer le système pour recevoir des événements spécifiques de microphone qui déclenchent des actions pertinentes.

Pour plus d'informations sur le matériel pris en charge, voir la page du matériel supporté sur le site Internet de Milestone. https://www.milestonesys.com/supported-hardware.

Les rôles déterminent le droit des utilisateurs d'écouter les microphones. Vous ne pouvez pas écouter les micros depuis le Management Client.

Le système est fourni avec une règle de flux de démarrage audio par défaut qui garantit que les flux audio de tous les micros connectés soient automatiquement transmis au système. Comme les autres règles, la règle par défaut peut être désactivée et/ou modifiée selon les besoins.

Activer/désactiver et renommer les périphériques individuels s'effectue au niveau du matériel du serveur d'enregistrement. Voir Activer/désactiver des périphériques par le biais des groupes de périphériques (á la page 125).

Pour toute autre configuration et gestion des caméras, développez **Périphériques** dans le volet Navigation du site de Management Client, puis sélectionnez **Microphones**. Dans le volet de vue d'ensemble, vous regroupez vos micros pour pouvoir les examiner plus facilement. Le regroupement initial est effectué dans le cadre de l'assistant **Ajout de matériel**.

Vous pouvez configurer les périphériques de microphones sur ces onglets :

- Onglet Infos (voir "Onglet Info (périphériques)" á la page 126)
- Onglet Paramètres (voir "Onglet Paramètres (périphériques)" á la page 127)
- Onglet Enregistrement (voir "Onglet Enregistrement (périphériques)" á la page 131)

- Onglet Événements (voir "Onglet Événements (périphériques)" á la page 151)

À propos des périphériques de haut-parleurs

Vous pouvez relier des haut-parleurs externes sur de nombreux périphériques. Certains périphériques disposent de haut-parleurs intégrés.

Les périphériques de haut-parleurs sont ajoutés automatiquement lorsque vous ajoutez un matériel sur le système. Ils sont par défaut désactivés, vous devez donc les réactiver avant utilisation, soit avec l'assistant **Ajout de matériel** soit par la suite. Les haut-parleurs ne nécessitent aucune licence distincte. Vous pouvez utiliser autant de haut-parleurs que nécessaire sur votre système.

Vous pouvez utiliser des haut-parleurs entièrement indépendamment des caméras.

Pour plus d'informations sur le matériel pris en charge, voir la page du matériel supporté sur le site Internet de Milestone. https://www.milestonesys.com/supported-hardware.

Le système envoie un flux audio vers les haut-parleurs lorsque l'utilisateur appuie sur le bouton de conversation dans XProtect Smart Client. L'audio des haut-parleurs n'est enregistré que lorsque l'utilisateur parle. Les Rôles déterminent le droit des utilisateurs de parler dans les haut-parleurs. Vous ne pouvez pas parler dans les haut-parleurs depuis le Management Client.

Si deux utilisateurs veulent parler en même temps, les rôles déterminent le droit des utilisateurs à parler dans les haut-parleurs. Dans le cadre de la définition des rôles, vous pouvez spécifier la priorité d'un haut-parleur de très haute à très basse. Si deux utilisateurs veulent parler en même temps, l'utilisateur dont le rôle possède la priorité la plus haute remporte la possibilité de parler. Si deux utilisateurs avec le même rôle souhaitent parler en même temps, la règle du premier arrivé premier servi s'applique.

Le système est livré avec une règle de flux audio de démarrage par défaut qui lance le dispositif afin que l'appareil soit prêt à envoyer l'audio activé par l'utilisateur vers les haut-parleurs. Comme les autres règles, la règle par défaut peut être désactivée et/ou modifiée selon les besoins.

Activer/désactiver et renommer les périphériques individuels s'effectue au niveau du matériel du serveur d'enregistrement. Voir Activer/désactiver des périphériques par le biais des groupes de périphériques (á la page 125).

Pour toute autre configuration et gestion des caméras, développez **Périphériques** dans le volet de navigation du site, puis sélectionnez **Microphones**. Dans le volet de vue d'ensemble, vous regroupez vos haut-parleurs pour pouvoir les examiner plus facilement. Le regroupement initial est effectué dans le cadre de l'assistant **Ajout de matériel**.

Vous pouvez configurer les périphériques de haut-parleurs sur les onglets suivants :

- Onglet Infos (voir "Onglet Info (périphériques)" á la page 126)
- Onglet Paramètres (voir "Onglet Paramètres (périphériques)" á la page 127)
- Onglet Enregistrement (voir "Onglet Enregistrement (périphériques)" á la page 131)

À propos des périphériques de métadonnées

Les périphériques de métadonnées fournissent des flux de données au système que les utilisateurs du client peuvent utiliser pour afficher des informations sur les données, par exemple, des données qui décrivent l'image vidéo, le contenu ou les objets de l'image, ou la localisation de l'endroit où l'image a été enregistrée. Les métadonnées peuvent être reliées à des caméras, des microphones, ou à des haut-parleurs.

Les métadonnées peuvent être générées par :

- Le périphérique lui-même en fournissant les données, par exemple la caméra diffusant la vidéo.
- Un système tiers ou une intégration via un pilote de métadonnées générique.

Les métadonnées générées par un périphérique sont automatiquement liées à un ou plusieurs périphériques sur le même matériel.

Pour plus d'informations sur le matériel pris en charge, voir la page du matériel supporté sur le site Internet de Milestone. https://www.milestonesys.com/supported-hardware.

Les rôles déterminent le droit des utilisateurs à visualiser les métadonnées.

Le système est fourni avec une règle de flux de démarrage par défaut qui garantit que les flux de métadonnées de tout matériel connecté qui prend en charge les métadonnées soient automatiquement transmis au système. Comme les autres règles, la règle par défaut peut être désactivée et/ou modifiée selon les besoins.

Activer/désactiver et renommer les périphériques individuels s'effectue au niveau du matériel du serveur d'enregistrement. Voir Activer/désactiver des périphériques par le biais des groupes de périphériques (á la page 125).

Pour toute autre configuration et gestion des périphériques de métadonnées, développez **Périphériques** dans le volet Navigation du site, puis sélectionnez **Métadonnées**. Dans le volet de vue d'ensemble, vous regroupez vos périphériques de métadonnées pour pouvoir les examiner plus facilement. Le regroupement initial est effectué dans le cadre de l'assistant **Ajout de matériel**.

Vous pouvez configurer les périphériques de métadonnées sur les onglets suivants :

- Onglet Infos (voir "Onglet Info (périphériques)" á la page 126)
- Onglet Paramètres (voir "Onglet Paramètres (périphériques)" á la page 127)
- Onglet Enregistrement (voir "Onglet Enregistrement (périphériques)" á la page 131)

À propos des périphériques d'entrée

Sur de nombreux périphériques, il est possible de connecter des appareils externes aux ports d'entrée du périphérique. Les unités d'entrée sont généralement des capteurs externes. Vous pouvez utiliser ces capteurs externes pour détecter si les portes, les fenêtres ou les portes sont ouvertes, par exemple. Les entrées de ces unités d'entrée externes sont traitées comme des événements par le système.

Vous pouvez utiliser ces événements dans les règles. Vous pourriez par exemple créer une règle spécifiant qu'une caméra devrait commencer à enregistrer lorsqu'une entrée est activée et arrêter d'enregistrer 30 secondes après la désactivation de l'entrée.

Vous pouvez utiliser des périphériques d'entrée de façon entièrement indépendante des caméras.

Avant de définir l’utilisation d’unités externes d’entrée sur un périphérique, vérifiez que le fonctionnement du détecteur est reconnu par le périphérique. La plupart des périphériques peuvent indiquer ceci dans leur interface de configuration ou via les commandes de script Common Gateway Interface (CGI).

Les périphériques d'entrée sont ajoutés automatiquement lorsque vous ajoutez un matériel sur le système. Ils sont par défaut désactivés, vous devez donc les réactiver avant utilisation, soit avec l'assistant **Ajout de matériel** soit par la suite. Les périphériques d'entrée ne nécessitent aucune licence distincte. Vous pouvez utiliser autant de périphériques d'entrée que nécessaire sur votre système.

Pour plus d'informations sur le matériel pris en charge, voir la page du matériel supporté sur le site Internet de Milestone. https://www.milestonesys.com/supported-hardware.

Activer/désactiver et renommer les périphériques individuels s'effectue au niveau du matériel du serveur d'enregistrement. Voir Activer/désactiver des périphériques par le biais des groupes de périphériques (á la page 125).

Pour toute autre configuration et gestion des caméras, développez **Périphériques** dans le volet Navigation du site, puis sélectionnez **Entrée**. Dans le volet de vue d'ensemble, vous regroupez vos périphériques d'entrée pour pouvoir les examiner plus facilement. Le regroupement initial est effectué dans le cadre de l'assistant **Ajout de matériel**.

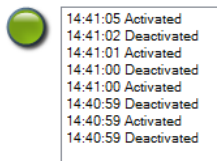
Vous pouvez configurer les périphériques d'entrée sur les onglets suivants :

- Onglet Infos (voir "Onglet Info (périphériques)" á la page 126)
- Onglet Paramètres (voir "Onglet Paramètres (périphériques)" á la page 127)
- Onglet Événements (voir "Onglet Événements (périphériques)" á la page 151)

Activer une entrée manuellement pour la tester

Avec la fonction de règles, vous définissez les règles permettant d'activer ou de désactiver automatiquement une entrée. Vous pouvez également les activer manuellement et vérifier le résultat dans le Management Client.

1. Dans le volet **Vue d'ensemble**, sélectionnez le périphérique d'entrée concerné.
2. Activez l'entrée sur le périphérique physique.
3. Dans le volet **Aperçu**, vérifiez si les témoins d'indication s'allument en vert. Cela signifie que le périphérique d'entrée fonctionne.



À propos des périphériques de sortie

Sur de nombreux périphériques, il est possible de connecter des appareils externes aux ports de sortie du périphérique. Cela vous permet d'activer/désactiver les voyants lumineux, les sirènes, etc. par le biais du système

Vous pouvez utiliser les sorties au moment de créer des règles. Vous pouvez créer des règles qui activent ou désactivent automatiquement les sorties, et des règles qui déclenchent des actions lorsque l'état d'une sortie est modifié.

Les sorties peuvent également être déclenchées manuellement à partir du Management Client et de XProtect Smart Client.

Avant de définir l'utilisation d'unités externes de sortie sur un périphérique, vérifiez que le dispositif peut lui-même contrôler le périphérique connecté à la sortie. La plupart des périphériques peuvent indiquer ceci dans leur interface de configuration ou via les commandes de script Common Gateway Interface (CGI).

Les périphériques de sortie sont ajoutés automatiquement lorsque vous ajoutez un matériel sur le système. Ils sont par défaut désactivés, vous devez donc les réactiver avant utilisation, soit avec l'assistant **Ajout de matériel** soit par la suite. Les périphériques de sortie ne nécessitent aucune

licence distincte. Vous pouvez utiliser autant de périphériques de sortie que nécessaire sur votre système.

Pour plus d'informations sur le matériel pris en charge, voir la page du matériel supporté sur le site Internet de Milestone. https://www.milestonesys.com/supported-hardware.

Activer/désactiver et renommer les périphériques individuels s'effectue au niveau du matériel du serveur d'enregistrement. Voir Activer/désactiver des périphériques par le biais des groupes de périphériques (á la page 125).

Pour toute autre configuration et gestion des caméras, développez **Périphériques** dans le volet Navigation du site, puis sélectionnez **Sortie**. Dans le volet de vue d'ensemble, vous regroupez vos périphériques d'entrée pour pouvoir les examiner plus facilement. Le regroupement initial est effectué dans le cadre de l'assistant **Ajout de matériel**.

Vous pouvez configurer les périphériques de sortie sur les onglets suivants :

- Onglet Infos (voir "Onglet Info (périphériques)" á la page 126)
- Onglet Paramètres (voir "Onglet Paramètres (périphériques)" á la page 127)

Activer une sortie manuellement pour la tester

Avec la fonction de règles, vous définissez les règles permettant d'activer ou de désactiver automatiquement une sortie. Vous pouvez également les activer manuellement depuis un client.

Vous pouvez activer une sortie manuellement depuis le Management Client afin de tester la fonctionnalité :

1. Dans le volet **Vue d'ensemble**, sélectionnez le périphérique de sortie concerné.
2. Les éléments suivants sont généralement représentés pour chaque sortie dans le volet **Aperçu** :

3. Sélectionnez/décochez la case pour activer/désactiver la sortie sélectionnée. Lorsqu'une sortie est activée, l'indicateur devient vert :

4. Vous pouvez également cliquer sur le bouton rectangulaire pour activer la sortie pendant la durée définie dans le paramètre **Durée de déclenchement de la sortie** de l'onglet **Paramètres** (il se peut que cette fonction/ce paramètre ne soit pas disponible pour toutes les sorties). Après la durée définie, la sortie est automatiquement désactivée.

Activer/désactiver des périphériques par le biais des groupes de périphériques

Vous pouvez activer/désactiver des périphériques uniquement par le biais du matériel configuré. Les périphériques de caméra sont par défaut activés et tous les autres appareils sont par défaut désactivés, sauf s'ils sont activés/désactivés manuellement dans l'assistant d'ajout de matériel.

Pour trouver un périphérique à activer ou désactiver par le biais des groupes de périphériques :

1. Dans le volet **Navigation sur le site**, sélectionnez le périphérique.
2. Dans le volet **Vue d'ensemble**, développez le groupe correspondant et cherchez le périphérique.
3. Faites un clic droit sur le périphérique, puis sélectionnez **Accéder au matériel**.
4. Cliquez sur le nœud plus pour voir tous les appareils sur le matériel.
5. Faites un clic droit sur le périphérique que vous souhaitez activer ou désactiver, puis sélectionnez **Activé**.

Icônes de statut des périphériques

Lorsque vous sélectionnez un périphérique, les informations relatives à son statut actuel apparaissent dans le volet **Aperçu**.
Les icônes suivantes indiquent l'état des périphériques :

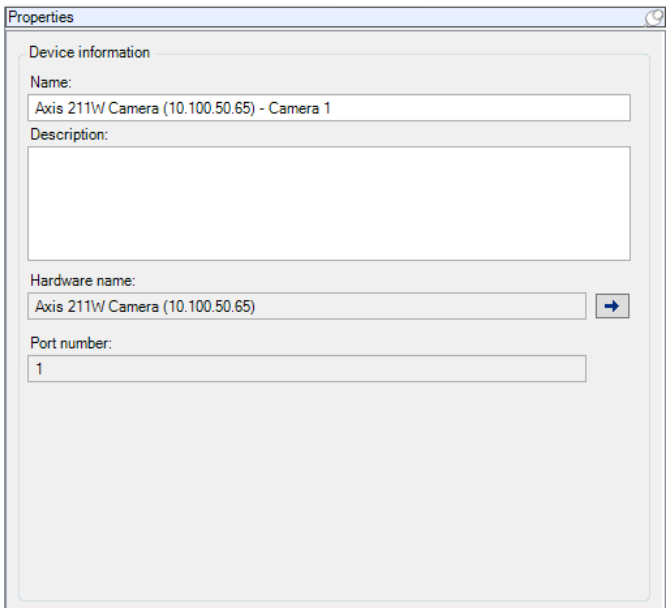
Cam-éra	Micro-phone	Haut-parleur	Méta données	En-trée	Sor-tie	Description
						**Périphérique activé et récupération de données :** le périphérique est activé et vous récupérez un flux en direct.
						**Périphérique en cours d'enregistrement :** le périphérique enregistre des données sur le système.
						**Périphérique temporairement arrêté ou sans alimentation :** Une fois arrêté, aucune information n'est transférée au système. S'il s'agit d'une caméra, vous ne pouvez pas afficher la vidéo en direct. Un périphérique arrêté peut toujours communiquer avec le serveur d'enregistrement pour récupérer des événements, configurer des paramètres, etc., contrairement à un périphérique désactivé.
						**Périphériques désactivés :** ne peut pas être activé automatiquement au moyen d'une règle et ne peut pas communiquer avec le serveur d'enregistrement. Si une caméra est désactivée, vous ne pouvez pas afficher le direct ou la vidéo enregistrée.
						**Base de données du périphérique en cours de réparation.**

Cam-éra	Micro-phone	Haut-parleur	Méta données	En-trée	Sor-tie	Description
						**Périphériques nécessitant de l'attention** : le périphérique ne fonctionne pas correctement. Survolez l'icône du périphérique avec le curseur de la souris pour obtenir une description du problème dans l'infobulle.
						**État inconnu** : le statut du périphérique n'est pas connu, par exemple si le serveur d'enregistrement est hors ligne.
						Notez que certaines icônes peuvent être associées comme dans cet exemple dans lequel **Périphérique activé et récupération de données** est associé avec **Périphérique en cours d'enregistrement**.

Onglet Info (périphériques)

À propos de l'onglet Infos

L'onglet **Infos** vous permet d'afficher et de modifier les informations de base concernant un périphérique dans un certain nombre de champs.
Tous les périphériques possèdent un onglet **Infos**.



Exemple d'onglet **Infos** d'une caméra.

Propriétés de l'onglet Info

Nom	Description
Nom	Le nom est utilisé partout où le périphérique apparaît dans une liste sur le système et les clients. Si vous renommez un périphérique, son nom est modifié de manière globale dans le Management Client.
Description	Saisissez une description du périphérique (facultatif). La description apparaît dans plusieurs listes au sein du système. Par exemple, lorsque vous survolez le nom de l'élément dans le volet **Vue d'ensemble** avec le curseur de la souris.
Nom du matériel	Affiche le nom du matériel avec lequel le périphérique est connecté. Le champ n'est pas modifiable à partir d'ici, mais peut être modifié en cliquant sur le bouton **Atteindre** situé à côté de lui. Vous serez dirigé vers les informations relatives au matériel, où le nom est modifiable.
Numéro de port	Affiche le port sur lequel le périphérique est raccordé au matériel. Pour du matériel à un seul périphérique, le numéro de port sera généralement de **1**. Pour du matériel à plusieurs périphériques, tel que les serveurs vidéo comptant plusieurs chaînes, le nombre de port indique généralement le canal sur lequel le périphérique est connecté, par exemple **3**.

Onglet Paramètres (périphériques)

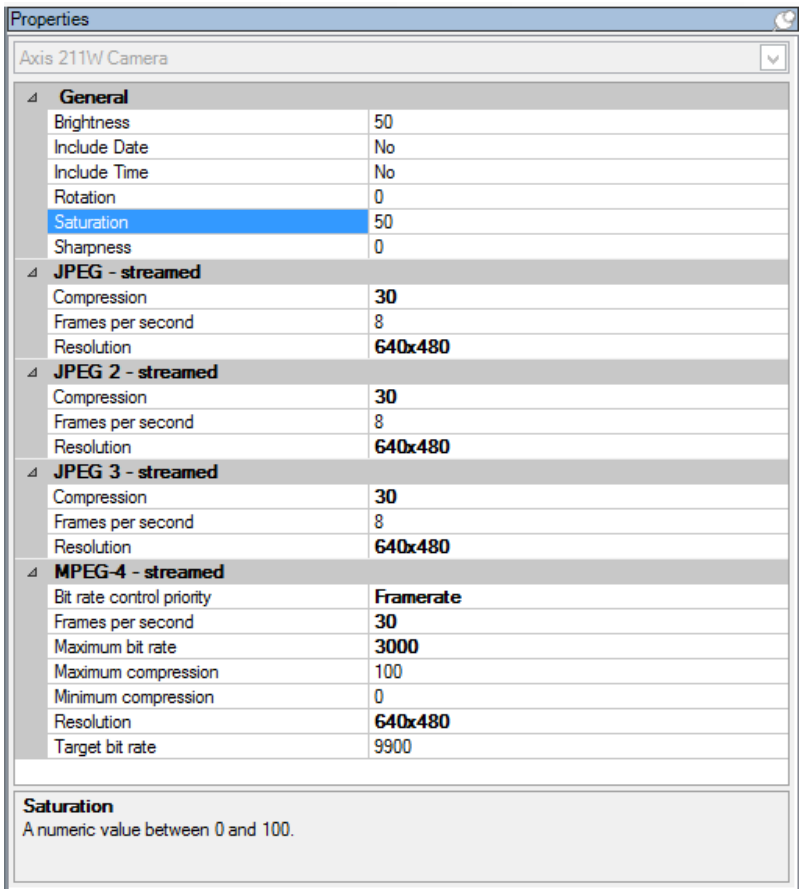
À propos de l'onglet Paramètres

L'onglet **Paramètres** vous permet d'afficher et de modifier les paramètres d'un périphérique dans un certain nombre de champs.
Tous les périphériques possèdent un onglet **Paramètres**.

Les valeurs dans le tableau sont modifiables ou en lecture seule. Après avoir modifié un paramètre au profit d'une valeur autre que la valeur par défaut, la valeur apparaît **en gras**.

Le contenu du tableau dépend du pilote de périphérique.

Les plages autorisées sont visibles dans la zone d'informations sous le tableau des paramètres :



Onglet **Paramètres**, exemple à partir de la **caméra**.

À propos des paramètres de la caméra

Vous pouvez afficher ou modifier des paramètres tels que :

- Fluidité d'image par défaut
- Résolution
- Compression
- Nombre maximal d'images entre les images-clés
- Affichage sur écran du texte/de l'heure/de la date pour une caméra sélectionnée ou pour toutes les caméras d'un groupe de périphériques.

Les pilotes des caméras définissent le contenu de l'onglet **Paramètres**. Les pilotes varient en fonction du type de caméra.

Pour les caméras prenant en charge plus d'un type de flux, par exemple MPEG-4/H.264/H.265, vous pouvez utiliser la diffusion multiflux, voir À propos de la diffusion multiflux (á la page 129).

Si vous modifiez un paramètre, vous pouvez rapidement vérifier les effets de votre modification si votre volet **Aperçu** est activé. Vous ne pouvez pas utiliser le volet **Aperçu** pour voir les effets des modifications de fluidité d'image parce que les images miniatures dans le volet **Aperçu** utilisent un nombre d'images par seconde différent, défini dans la boîte de dialogue **Options**.

La modification des paramètres de **Images max. entre les images-clés** et **Images max. entre les modes images-clés** peut réduire la performance de certaines fonctionnalités dans XProtect Smart Client. XProtect Smart Client nécessite par exemple la présence d'une image-clé pour lancer la lecture d'une vidéo. Ainsi, une période plus longue entre les images-clés prolonge le démarrage de XProtect Smart Client.

Onglet Flux (périphériques)

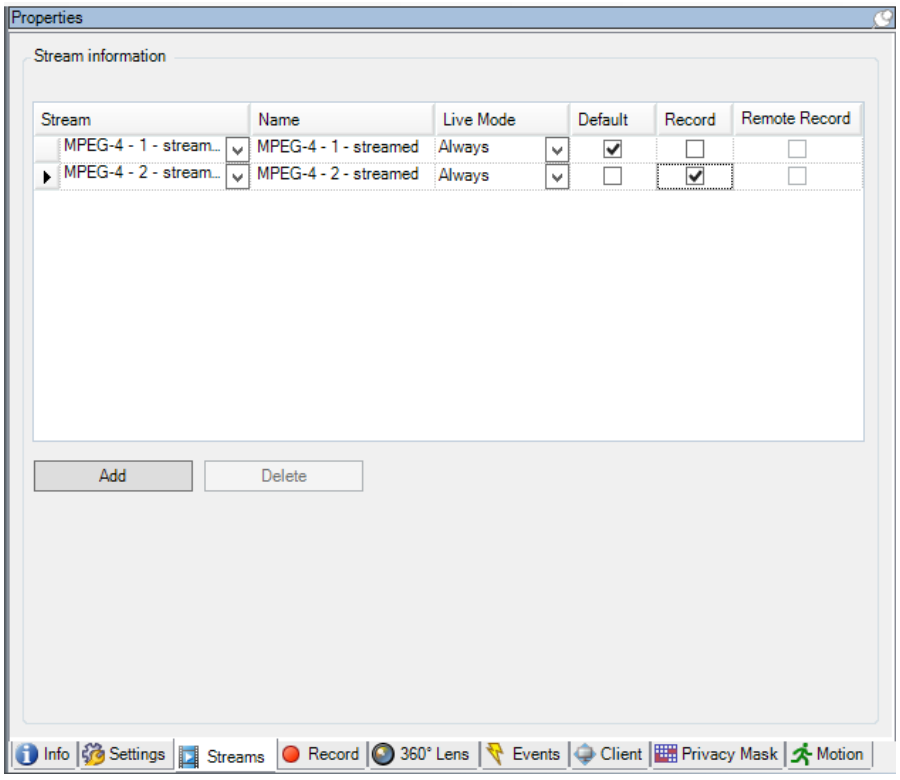
À propos de l'onglet Flux

Les périphériques suivants possèdent un onglet **Flux** :

- Caméras

L'onglet **Flux** répertorie un flux unique par défaut. Il s'agit du flux par défaut de la caméra sélectionnée, utilisée pour le direct et les vidéos enregistrées.

Pour la diffusion en direct, vous pouvez configurer et utiliser autant de flux en direct que le nombre pris en charge par la caméra. En revanche, vous ne pouvez sélectionner qu'un seul flux pour l'enregistrement simultané. Pour modifier le flux à utiliser pour l'enregistrement, cochez la case **Enregistrement** du flux à enregistrer.



À propos de la diffusion multiflux

La lecture d'une vidéo enregistrée ou l'affichage de la vidéo en direct ne nécessite pas obligatoirement la même qualité vidéo et la même fluidité d'image pour obtenir un résultat optimal. Vous pouvez choisir **soit** un flux pour le visionnage en direct et un autre à des fins de lecture **soit** deux flux séparés en direct, mais avec une résolution, un codage et une fluidité d'image différents.

Exemple 1, vidéo en direct et enregistrée :

- Pour le visionnage d'une vidéo **en direct**, votre société peut préférer le format MPEG4 avec une fluidité d'image élevée.
- Pour la lecture d'une vidéo **enregistrée**, votre société peut préférer le format MJPEG avec une fluidité d'image inférieure car cela aide à préserver de l'espace disque.

Exemple 2, plusieurs vidéos en direct :

- Pour le visionnage **d'une vidéo en direct à partir d'un point de fonctionnement local**, votre société peut préférer le format MPEG4 avec une fluidité d'image élevée afin d'obtenir la meilleure qualité vidéo disponible.
- Pour le visionnage **d'une vidéo en direct à partir d'un point de fonctionnement connecté à distance**, votre société peut préférer le format MPEG avec une fluidité d'image et une qualité inférieures afin de préserver la bande passante du réseau.

Même lorsque les caméras prennent en charge la diffusion multiflux, les capacités individuelles en termes de lecture en direct multiple peuvent varier entre différentes caméras. Consultez la documentation de la caméra pour plus d'informations.

Pour voir si une caméra offre différents types de flux, consultez l'onglet **Paramètres**.

Ajouter un flux

1. Dans l'onglet **Flux**, cliquez sur **Ajouter**. Cette action ajoute un second flux à la liste.
2. Dans la colonne **Nom**, modifiez le nom du flux. Le nom s'affiche dans XProtect Smart Client.
3. Dans la colonne **Mode en direct**, sélectionnez quand la diffusion en direct est requise.
   - **Toujours** : le flux s'exécute même si aucun utilisateur XProtect Smart Client ne le demande.
   - **Jamais** : le flux est désactivé. Utilisez cette fonction uniquement pour les flux d'enregistrement, par exemple si vous souhaitez des enregistrements de qualité supérieure et avez besoin de la largeur de bande.
   - **Si nécessaire** : le flux est lancé lorsqu'un utilisateur XProtect Smart Client le demande.
4. Dans la colonne **Par défaut**, sélectionnez le flux par défaut.
5. Dans la colonne **Enregistrement**, cochez la case si vous souhaitez enregistrer ce flux ou décochez-la si vous souhaitez uniquement l'utiliser pour des vidéos en direct.
6. Dans la colonne **Enregistrement à distance**, cochez la case si vous souhaitez utiliser ce flux d'enregistrement pour la récupération des enregistrements à distance et décentralisés.
7. Cliquez sur **Enregistrer**.

Important : Si vous réglez un flux sur **Défaut** ou **Enregistrer**, le flux fonctionne toujours indépendamment du paramètre **Mode En direct**. La sélection de **En cas de besoin** et **Toujours** a le même effet dans le système. Si vous sélectionnez **Jamais**, le flux fonctionne mais ne peut pas être visionné en direct.

Si vous ne souhaitez pas que les flux fonctionnent du tout à moins que quelqu'un ne consulte la vidéo en direct, vous pouvez modifier la **Règle de démarrage des flux par défaut** pour les démarrer à la demande avec l'événement prédéfini **Flux client en direct requis**.

Onglet Enregistrement (périphériques)

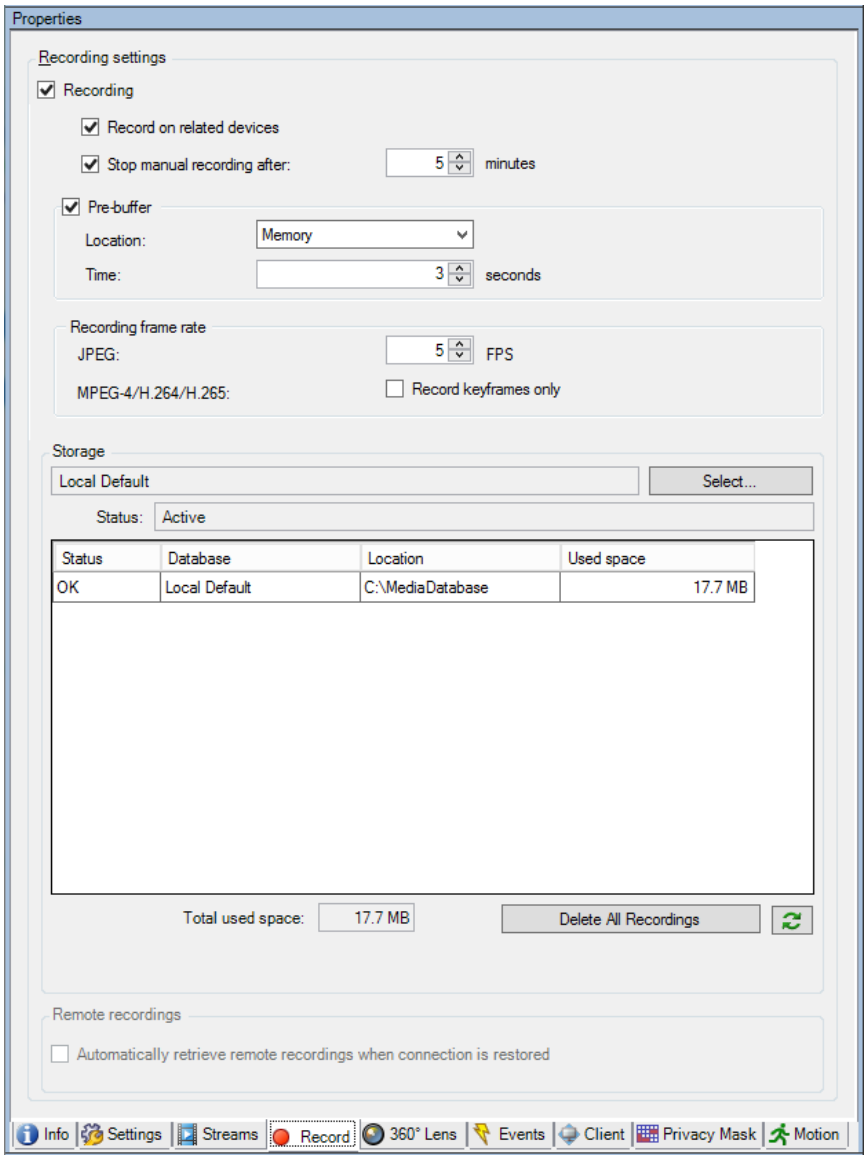
À propos de l'onglet Enregistrer

Les périphériques suivants possèdent un onglet **Enregistrer** :

- Caméras
- Microphones
- Haut-parleurs
- Métadonnées

Les enregistrements d'un périphérique sont uniquement sauvegardés dans la base de données une fois que vous avez activé l'enregistrement et que les critères de la règle associée aux enregistrements sont remplis.

Les paramètres qui ne peuvent pas être configurés pour un périphérique apparaissent en grisé.



Onglet **Enregistrement**, exemple à partir de la **caméra**

Activer/désactiver l'enregistrement

Par défaut, l'enregistrement est activé. Pour activer/désactiver l'enregistrement :

1. Dans le volet **Navigation du site**, sélectionnez **Serveurs d'enregistrement**.
2. Sélectionnez le périphérique requis dans le volet **Vue d'ensemble** :
3. Dans l'onglet **Enregistrer**, cochez ou décochez la case **Enregistrement**.

Vous devez activer l'enregistrement pour le périphérique afin d'enregistrer des données de la caméra. Une règle indiquant les circonstances d'enregistrement d'un périphérique ne fonctionnera pas si vous avez désactivé l'enregistrement pour le périphérique.

Activer l'enregistrement sur les périphériques connexes

Pour les caméras, vous pouvez activer l'enregistrement pour les périphériques connexes connectés au même serveur d'enregistrement, tels que les microphones ou les haut-parleurs, par exemple. Cela signifie que les périphériques connexes enregistrent lorsque la caméra enregistre.

L'enregistrement sur les périphériques connexes est activé par défaut pour les nouvelles caméras, mais vous pouvez désactiver et activer cette fonction selon vos besoins. Pour les caméras existantes du système, la case est décochée par défaut.

1. Dans le volet **Navigation du site**, sélectionnez **Serveurs d'enregistrement**.
2. Sélectionnez le périphérique caméra requis dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Enregistrer**, cochez ou décochez la case **Enregistrer sur des périphériques associés**.
4. Dans l'onglet **Client**, spécifiez les périphériques associés à cette caméra.

Si vous souhaitez activer l'enregistrement sur des périphériques connexes connectés à un autre serveur d'enregistrement, vous devez créer une règle.

À propos de la mise en mémoire-tampon préalable

La mise en mémoire-tampon préalable représente la capacité d'enregistrer de l'audio ou de la vidéo avant la survenue de l'événement de déclenchement. Elle s'avère utile lorsque vous souhaitez enregistrer des données audio ou vidéo qui précèdent l'événement de déclenchement de l'enregistrement, par exemple l'ouverture d'une porte.

La mise en mémoire-tampon préalable est possible dans la mesure où le système reçoit continuellement des flux audio et vidéo depuis les périphériques connectés et les enregistre de manière temporaire pendant la période de mise en mémoire-tampon préalable définie.

- Si une règle d'enregistrement est déclenchée, les enregistrements temporaires sont rendus permanents pendant la durée de pré-enregistrement configurée pour cette règle.
- Si aucune règle d'enregistrement n'est déclenchée, les enregistrements temporaires dans la mémoire-tampon préalable sont automatiquement supprimés après la durée de mise en mémoire-tampon préalable définie.

Pour utiliser la fonction de mémoire-tampon préalable, les périphériques doivent être activés et envoyer un flux au système.

Stockage des enregistrements temporairement en mémoire-tampon

Vous pouvez choisir l'emplacement de stockage des enregistrements temporairement en mémoire-tampon :

- Dans la mémoire ; la durée de mémoire-tampon est limitée à 15 secondes.
- Sur le disque (dans la base de données multimédia) ; vous pouvez choisir toutes les valeurs.

Le stockage dans la mémoire au lieu du disque améliore les performances du système, mais est uniquement possible pendant des durées de mémoire-tampon plus courtes.

Lorsque des enregistrements sont stockés dans la mémoire et si vous rendez des enregistrements temporaires permanents, les enregistrements temporaires restants sont supprimés et ne peuvent

pas être restaurés. Si vous devez pouvoir conserver les enregistrements restants, stockez les enregistrements sur le disque.

Périphériques prenant la mise en mémoire-tampon préalable en charge

Les caméras, microphones et haut-parleurs prennent la mise en mémoire-tampon préalable en charge. Concernant les haut-parleurs, les flux sont envoyés uniquement si l'utilisateur XProtect Smart Client se sert de la fonction **Parler au haut-parleur**. En d'autres termes, cela signifie qu'en fonction de la façon dont les flux de votre haut-parleur sont déclenchés, vous disposez d'une petite mise en mémoire-tampon préalable ou d'aucune mise en mémoire-tampon préalable.

Dans la plupart des cas, les haut-parleurs sont configurés de sorte à enregistrer lorsque l'utilisateur XProtect Smart Client se sert de la fonction **Parler au haut-parleur**. Dans ces cas, aucune mémoire-tampon préalable du haut-parleur n'est disponible.

Gérer la mise en mémoire-tampon préalable

Activer et désactiver la mise en mémoire-tampon préalable :

la mise en mémoire-tampon préalable est activée par défaut avec une durée de trois secondes et un stockage en mémoire.

1. Pour activer/désactiver la mise en mémoire-tampon préalable, cochez/décochez la case **Pré-enregistrement**.

Précisez l'emplacement de stockage et la durée de mise en mémoire-tampon :

Les enregistrements temporairement en mémoire-tampon sont stockés dans la mémoire ou sur le disque :

1. Pour **Emplacement**, sélectionnez **Mémoire** ou **Disque** et précisez le nombre de secondes.

   Le nombre de secondes saisi doit être suffisamment grand pour correspondre à vos exigences dans les différentes règles d'enregistrement définies.

   Si vous avez besoin d'une durée de mise en mémoire-tampon supérieure à 15 secondes, sélectionnez **Disque**.

2. Si vous changez l'emplacement par **Mémoire**, le système réduit la durée à 15 secondes automatiquement.

Utiliser la mise en mémoire-tampon dans les règles :

lorsque vous créez des règles destinées à déclencher l'enregistrement, vous pouvez choisir de lancer les enregistrements un peu avant l'événement actuel (mémoire-tampon préalable).

Exemple : La règle ci-après indique que l'enregistrement doit commencer sur la caméra 5 secondes avant la détection du mouvement sur la caméra.

Détail d'une règle s'appuyant sur la mise en mémoire-tampon préalable

Pour utiliser la fonction d'enregistrement avec mise en mémoire-tampon préalable dans la règle, vous devez activer la mise en mémoire-tampon préalable sur le périphérique en cours

d'enregistrement et définir la durée de la mise en mémoire-tampon préalable afin qu'elle soit au minimum égale à celle spécifiée dans la règle.

Gérer l'enregistrement manuel

Arrêter l'enregistrement manuel après : est activé par défaut avec une durée d'enregistrement de cinq minutes. Ceci permet de s'assurer que le système arrête automatiquement tous les enregistrements commencés par les utilisateurs deXProtect Smart Client.

1. Pour activer et désactiver l'enregistrement manuel à arrêter automatiquement par le système, cochez/décochez la case **Arrêter l'enregistrement manuel après :**.
2. Lorsque vous l'activez, précisez une durée d'enregistrement. Le nombre de minutes que vous spécifiez doit être suffisamment grand pour correspondre aux exigences des divers enregistrements manuels sans surcharger le système.

Ajouter des rôles :

Vous devez accorder le droit de démarrer et d'arrêter l'enregistrement manuel aux utilisateurs du client sur chaque caméra dans **Rôles**, dans l'onglet **Périphérique**.

Utilisation dans les règles :

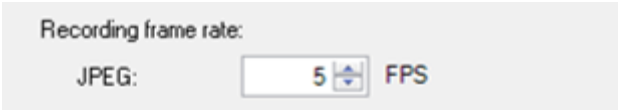
Les événements que vous pouvez utiliser lorsque vous créez des règles associées à l'enregistrement manuel sont :

- **Enregistrement manuel démarré**
- **Enregistrement manuel arrêté**

Spécifier la fluidité d'image de l'enregistrement

Vous pouvez spécifier la fluidité d'image de l'enregistrement pour le format JPEG.

- Sélectionnez ou saisissez la fluidité d'image (en nombre d'images par seconde) de l'enregistrement dans la case **Fluidité d'image d'enregistrement : (JPEG)**.



Spécification d'une fluidité d'image d'enregistrement particulière

Activer l'enregistrement des images-clés

Vous pouvez activer l'enregistrement des images-clés pour les flux MPEG-4/H.264/H.265. Cela signifie que le système alterne entre l'enregistrement des images-clés uniquement et l'enregistrement de toutes les images selon les paramètres de vos règles.

Vous pouvez par exemple laisser le système enregistrer des images-clés lorsqu'il n'y a aucun mouvement dans la vue et passer à toutes les images en cas de détection de mouvement pour économiser de l'espace de stockage.

1. Cochez la case **Enregistrer les images-clés uniquement**.

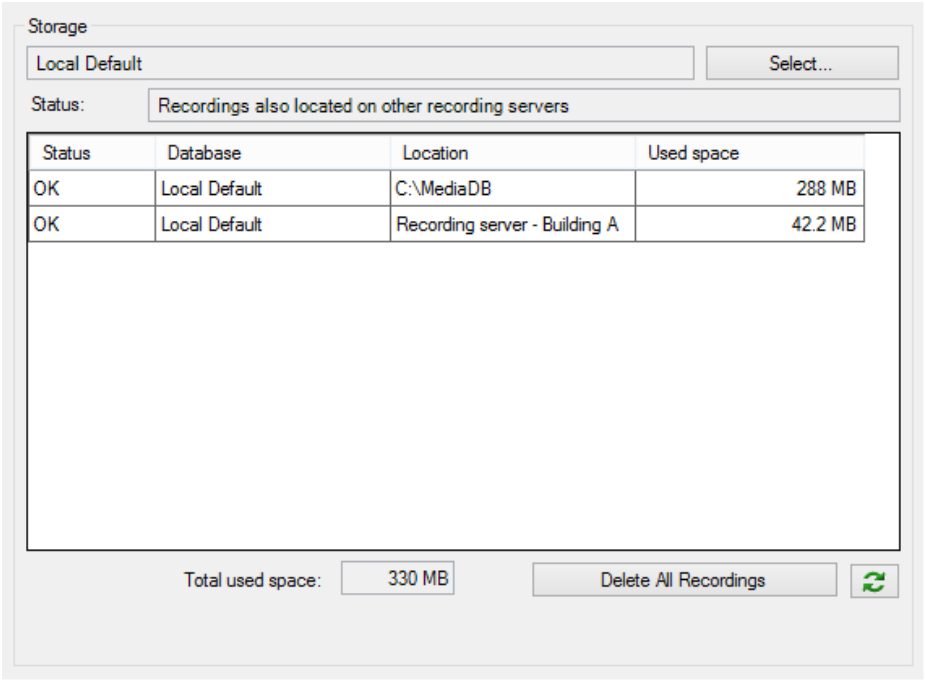
Activation de l'enregistrement des images-clés

2. Créez une règle qui active la fonction, voir À propos des actions et des actions d'arrêt (á la page 175).

À propos du stockage

Dans **Stockage**, vous pouvez surveiller et gérer les bases de données pour un périphérique ou un groupe de périphériques ajoutés au même serveur d'enregistrement.

Au-dessus du tableau, vous voyez la base de données sélectionnée et son statut. Dans cet exemple, la base de données sélectionnée est la base de données par défaut, **Locale par défaut** et son statut est **Des enregistrements sont également situés sur d'autres serveurs d'enregistrement**. L'autre serveur est le serveur d'enregistrement du bâtiment A.



Possibles statuts pour la base de données sélectionnée :

Nom	Description
Des enregistrements sont également situés sur d'autres serveurs d'enregistrement	La base de données est active et en fonctionnement et contient également des enregistrements dans des espaces de stockage situés sur d'autres serveurs d'enregistrement.

Nom	Description
Archives également situées sur l'ancien stockage	La base de données est active et en fonctionnement et possède aussi des archives situées dans d'autres espaces de stockage.
Activé	La base de données est active et en fonctionnement.
Les données des périphériques choisis sont actuellement déplacées vers un autre emplacement	La base de données est active et en fonctionnement et le système déplace des données d'un ou plusieurs périphériques sélectionnés dans un groupe depuis un emplacement vers un autre.
Les données du périphérique sont actuellement déplacées vers un autre emplacement	La base de données est active et en fonctionnement et le système déplace des données du périphérique sélectionné d'un emplacement vers un autre.
Informations non disponibles en mode redondant	Le système ne peut pas recueillir d'informations d'état au sujet de la base de données lorsque la base de données est en mode de redondance.

Plus bas dans la fenêtre, vous pouvez apercevoir le statut individuel de chaque base de données (**OK**, **Hors ligne** ou **Ancien stockage**), l'emplacement de chaque base de données et l'espace utilisé par chaque base de données.

Si tous les serveurs sont en ligne, vous pouvez voir l'espace total utilisé pour l'intégralité du stockage dans le champ **Espace total utilisé**.

Avec le bouton **Supprimer tous enregistrements**, vous pouvez supprimer tous les enregistrements pour le périphérique ou le groupe de périphériques si vous avez ajouté tous les périphériques du groupe sur le même serveur.

Pour obtenir des informations sur la configuration du stockage, reportez-vous à À propos du stockage et de l'archivage (á la page 79).

À propos de l'enregistrement à distance

L'option d'enregistrement à distance n'est disponible que si la caméra sélectionnée prend en charge le stockage décentralisé ou s'il s'agit d'une caméra avec une configuration Milestone Interconnect.

Pour garantir la sauvegarde de tous les enregistrements en cas de problèmes réseau, sélectionnez **Récupérer automatiquement les enregistrements à distance lors de la restauration des connexions**. Ainsi, les enregistrements sont récupérés automatiquement lorsque la connexion est rétablie.

Le type de matériel sélectionné détermine l'emplacement à partir duquel les enregistrements sont récupérés :

- Pour une caméra dotée d'un espace de stockage local des enregistrements, les enregistrements sont récupérés à partir de l'espace de stockage local des enregistrements.
- Pour un système à distance Milestone Interconnect, les enregistrements sont récupérés à partir des serveurs d'enregistrement du système à distance.

Vous pouvez utiliser la fonctionnalité ci-après indépendamment de la récupération automatique :

- Enregistrement manuel.
- La règle **Récupérer et stocker les enregistrements à distance à partir des <périphériques>**.

- La règle **Récupérer et stocker les enregistrements à distance entre <heure de début et de fin> sur <périphériques>**.

Onglet Préréglages (périphériques)

À propos de l'onglet Préréglages

Les périphériques suivants possèdent un onglet **Préréglages** :

- Caméras PTZ prenant en charge les positions prédéfinies.

L'onglet **Préréglages** vous permet de créer ou d'importer des positions prédéfinies, par exemple :

- Dans les règles pour le déplacement d'une caméra PTZ (pan-tilt-zoom) vers une position prédéfinie spécifique lorsqu'un événement survient.
- Dans la patrouille, pour le déplacement automatique d'une caméra PTZ entre plusieurs positions prédéfinies.
- Pour l'activation manuelle par les utilisateurs XProtect Smart Client.

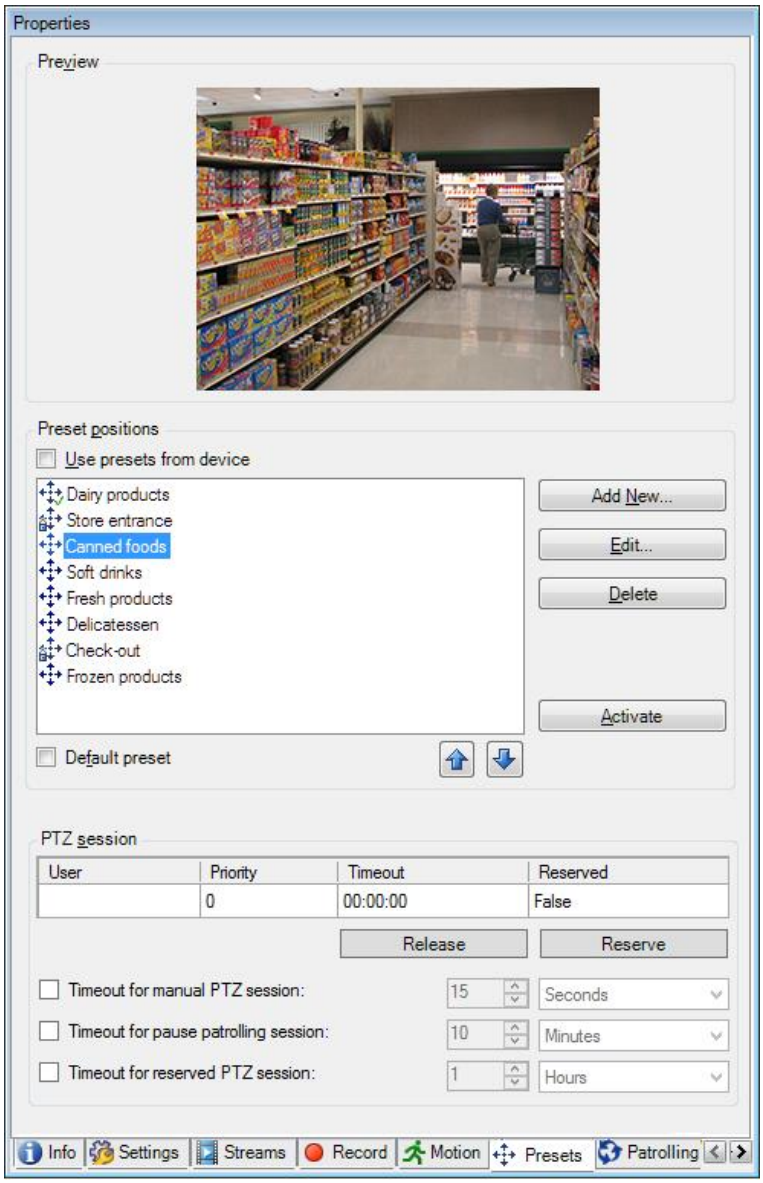
Vous pouvez verrouiller une position prédéfinie si vous souhaitez empêcher les utilisateurs de XProtect Smart Client ou les utilisateurs dotés de droits de sécurité limités de mettre à jour ce préréglage. Les préréglages verrouillés sont indiqués par l'icône  .

Les administrateurs dotés de droits de sécurité suffisants pour exécuter une session PTZ réservée (voir "À propos des sessions PTZ réservées" á la page 143) peuvent exécuter la caméra PTZ dans ce mode. Ceci évite que d'autres utilisateurs prennent le contrôle de la caméra. Avec des droits suffisants, vous pouvez libérer les sessions PTZ réservées d'autres utilisateurs (voir "Libérer une session PTZ" á la page 144).

Vous assignez la permission PTZ aux rôles de l'onglet sécurité globale (voir "Onglet Sécurité globale (rôles)" á la page 221) ou de l'onglet PTZ (voir "Onglet PTZ (rôles)" á la page 243).

Vous pouvez surveiller le système pour savoir s'il est actuellement en patrouille ou si un utilisateur en a pris le contrôle dans l'espace de la **session PTZ** (voir "**Propriétés des sessions PTZ**" á la page 145).

Vous pouvez également y modifier les périodes d'expiration des sessions PTZ pour la caméra.

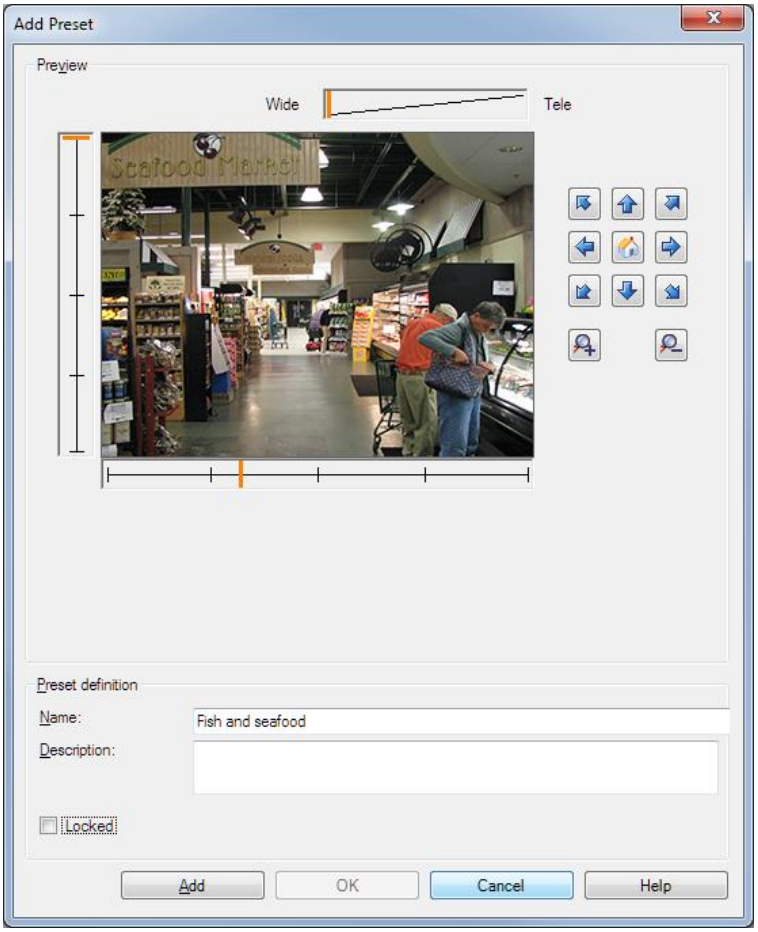


L'onglet **Préréglages** avec des positions prédéfinies définies

Ajouter une position prédéfinie (type 1)

Pour ajouter une position prédéfinie pour la caméra :

1. Cliquez sur **Ajouter nouveau**. La fenêtre **Ajouter un préréglage** s'ouvre :



2. la fenêtre **Ajouter un préréglage** affiche une image d'aperçu en direct depuis la caméra. Utilisez les boutons de navigation et/ou les curseurs pour déplacer la caméra jusqu'à la position souhaitée.
3. Précisez un nom en ce qui concerne la position prédéfinie, dans le champ **Nom**.
4. Facultativement, saisissez une description de la position prédéfinie dans le champ **Description**.
5. Sélectionnez **Verrouillé** si vous souhaitez verrouiller la position prédéfinie. Seuls les utilisateurs dotés des droits suffisants peuvent déverrouiller la position par la suite.
6. Cliquez sur **Ajouter** pour spécifier des préréglages. Continuez à les ajouter jusqu'à ce que vous disposiez de tous les préréglages souhaités.
7. Cliquez sur **OK**. La fenêtre **Ajouter un préréglage** se ferme et ajoute la position à la liste des positions prédéfinies de l'onglet **Préréglages** de la caméra.

Utiliser les positions prédéfinies de la caméra (type 2)

En alternative à la spécification des positions prédéfinies dans le système, vous pouvez prérégler ces positions pour certaines caméras PTZ directement sur la caméra. Pour ce faire, vous devrez généralement vous connecter à un site Internet de configuration spécifique au produit.

1. Importez les préréglages dans le système en sélectionnant **Utiliser les préréglages à partir du périphérique**.

   Tous les préréglages précédemment définis pour la caméra sont supprimés, ce qui a une influence sur les règles et les calendriers de patrouille définis et supprime également les préréglages disponibles pour les utilisateurs XProtect Smart Client.

2. Cliquez sur **Supprimer** pour supprimer les préréglages dont vos utilisateurs n'ont pas besoin.

3. Cliquez sur **Modifier** pour changer le nom du préréglage (voir "Modifier le nom d'une position prédéfinie (type 2 seulement)" á la page 142).

4. Si vous souhaitez ensuite modifier ces préréglages définis sur le périphérique, modifiez-les sur la caméra, puis réimportez-les.

Assigner une position prédéfinie par défaut

Si nécessaire, vous pouvez assigner l'une des positions prédéfinies d'une caméra PTZ à la position prédéfinie par défaut de la caméra.

Avoir une position prédéfinie par défaut peut s'avérer utile car cela vous permet de définir les règles indiquant que la caméra PTZ doit être mise en position prédéfinie par défaut dans des circonstances particulières, par exemple après que la caméra PTZ a été utilisée manuellement.

1. Pour assigner une position prédéfinie par défaut, sélectionnez le préréglage concerné dans votre liste de positions prédéfinies.

2. Cochez la case **Préréglage par défaut** sous la liste.

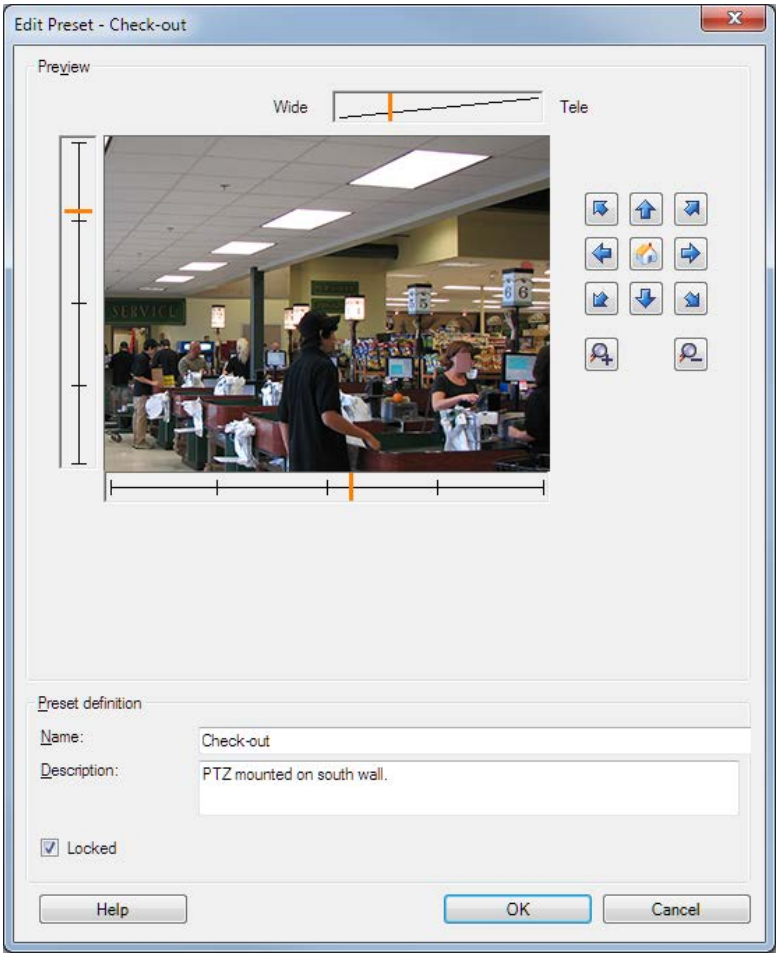
Seule une position prédéfinie peut être définie comme position prédéfinie par défaut.

Modifier une position prédéfinie (type 1 seulement)

Pour modifier une position prédéfinie existante, définie dans le système :

1. Sélectionnez la position prédéfinie requise dans la liste de l'onglet **Préréglages** des positions prédéfinies à disposition pour la caméra.

2. Cliquez sur **Modifier**. Cela ouvre la fenêtre **Modifier un préréglage** :



Exemple seulement. Les fonctionnalités dépendent de la caméra.

3. La fenêtre **Modifier un préréglage** affiche la vidéo en direct depuis la position prédéfinie. Utilisez les boutons de navigation et/ou les curseurs pour modifier la position prédéfinie en fonction de vos besoins.

4. Changez le nom/le numéro et la description de la position prédéfinie si nécessaire.

5. Sélectionnez **Verrouillé** si vous souhaitez verrouiller la position prédéfinie. Seuls les utilisateurs dotés des droits suffisants peuvent déverrouiller la position par la suite.

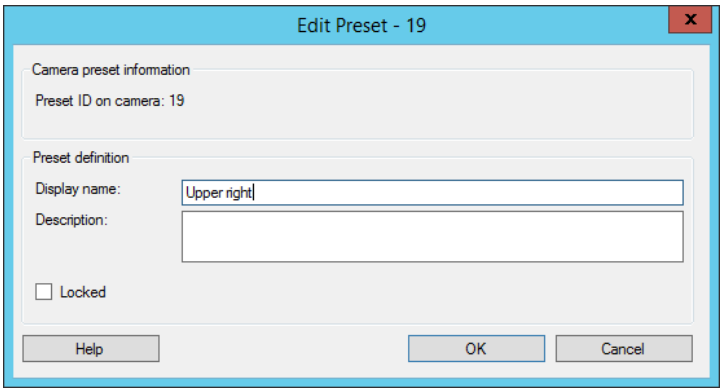
6. Cliquez sur **OK**.

Modifier le nom d'une position prédéfinie (type 2 seulement)

Pour modifier le nom d'une position prédéfinie dans la caméra :

1. Sélectionnez la position prédéfinie requise dans la liste de l'onglet **Préréglages** des préréglages à disposition pour la caméra.

2. Cliquez sur **Modifier**. Cela ouvre la fenêtre **Modifier un préréglage** :



Exemple d'un préréglage dans la caméra

3. Modifiez le nom et ajoutez une description de la position prédéfinie si nécessaire.
4. Sélectionnez **Verrouillé** si vous souhaitez verrouiller le nom du préréglage. Vous pouvez verrouiller un nom de préréglage si vous souhaitez empêcher les utilisateurs de XProtect Smart Client ou les utilisateurs dotés de droits de sécurité limités de mettre à jour le nom du préréglage ou de le supprimer. Les préréglages verrouillés sont indiqués par l'icône . Seuls les utilisateurs dotés des droits suffisants peuvent déverrouiller le nom du préréglage par la suite.
5. Cliquez sur **OK**.

Verrouiller une position prédéfinie

Vous pouvez verrouiller une position prédéfinie si vous souhaitez empêcher les utilisateurs de XProtect Smart Client ou les utilisateurs dotés de droits de sécurité limités de mettre à jour ou de supprimer un préréglage. Les préréglages verrouillés sont indiqués par l'icône .

Vous pouvez verrouiller des préréglages dans le cadre d'un ajout (voir "Ajouter une position prédéfinie (type 1)" á la page 139) et d'une modification (voir "Modifier une position prédéfinie (type 1 seulement)" á la page 141).

Tester une position prédéfinie (type 1 seulement)

1. Sélectionnez la position prédéfinie requise dans la liste de l'onglet **Préréglages** des positions prédéfinies à disposition pour la caméra.
2. Cliquez sur **Activer**.
3. La caméra se déplace vers la position prédéfinie sélectionnée.

À propos des sessions PTZ réservées

En fonction de votre système de surveillance, vous pouvez réserver des sessions PTZ.

Les administrateurs dotés de droits de sécurité suffisants pour exécuter une session PTZ réservée peuvent exécuter la caméra PTZ dans ce mode. Ceci évite que d'autres utilisateurs prennent le contrôle de la caméra. Dans une session PTZ réservée, le système de priorité PTZ standard est ignoré pour éviter que les utilisateurs dotés d'une priorité PTZ plus élevée n'interrompent la session.

Vous pouvez contrôler la caméra dans une session PTZ réservée à partir du XProtect Smart Client et du Management Client.

La réservation d'une session PTZ peut s'avérer utile lorsque vous avez besoin de procéder à des mises à jour ou des opérations de maintenance urgentes sur une caméra PTZ ou sur ses préréglages sans être interrompu par d'autres utilisateurs.

Vous ne pouvez pas démarrer une session PTZ réservée si un utilisateur ayant une priorité supérieure à la vôtre contrôle la caméra ou si un autre utilisateur a déjà réservé la caméra.

Libérer une session PTZ

Le bouton **Libérer** vous permet de libérer votre session PTZ actuelle de façon à ce qu'un autre utilisateur puisse contrôler la caméra. Lorsque vous cliquez sur **Libérer**, la session PTZ prend immédiatement fin et est mise à la disposition du premier utilisateur qui fera fonctionner la caméra.

Des administrateurs dotés de la permission de sécurité **Libérer la session PTZ** ont le droit de libérer des sessions PTZ réservées par d'autres utilisateurs à tout moment. Ceci peut s'avérer utile lorsque vous avez besoin de procéder à la maintenance de la caméra PTZ ou de ses préréglages par exemple, ou si d'autres utilisateurs ont accidentellement bloqué la caméra dans des situations d'urgence.

Spécifier les périodes d'expiration des sessions PTZ

Les utilisateurs Management Client et XProtect Smart Client dotés des droits d'utilisateurs nécessaires peuvent interrompre manuellement la patrouille des caméras PTZ.

Vous pouvez indiquer combien de temps doit s'écouler avant que le programme de patrouille habituel reprenne pour toutes les caméras PTZ de votre système :

1. Sélectionnez **Outils** > **Options**.
2. Dans l'onglet **Général** de la fenêtre **Options**, sélectionnez la durée dans :
   - la liste **Période d'inactivité pour les sessions PTZ manuelles** (la valeur par défaut est de 15 secondes).
   - la liste **Période d'inactivité pour la mise en pause des sessions PTZ** (la valeur par défaut est de 10 minutes).
   - la liste **Période d'inactivité pour les sessions PTZ réservées** (la valeur par défaut est de 1 heure).

   Les paramètres s'appliquent à toutes les caméras PTZ de votre système.

Vous pouvez modifier les délais individuellement pour chaque caméra.

1. Dans le volet **Navigation sur le site**, cliquez sur **caméra**.
2. Dans le volet Vue d'ensemble, sélectionnez la caméra.
3. Dans l'onglet **Préréglages**, sélectionnez la durée dans :
   - la liste **Période d'inactivité pour la session PTZ manuelle** (la valeur par défaut est de 15 secondes).
   - la liste **Période d'inactivité pour la mise en pause de la session PTZ** (la valeur par défaut est de 10 minutes).

- la liste **Période d'inactivité pour la session PTZ réservée** (la valeur par défaut est de 1 heure).

Les paramètres s'appliquent uniquement à cette caméra.

Propriétés des sessions PTZ

Le tableau **session PTZ** présente l'état actuel de la caméra PTZ.

Nom	Description
Utilisateur	Affiche l'utilisateur qui a appuyé sur le bouton **Réservé** et contrôle la caméra PTZ à présent. Si une session de patrouille est activée par le système, **Patrouille en cours** s'affiche.
Priorité	Affiche la priorité PTZ de l'utilisateur. Vous ne pouvez prendre le contrôle que de sessions PTZ d'utilisateurs ayant une priorité inférieure à la vôtre.
Délai de réponse dépassé	Affiche le temps restant de la session PTZ actuelle.
Réservé	Indique si la session actuelle est une session PTZ réservée ou non. • **Vrai** : Réservé. • **Faux** : Non réservé.

Vous pouvez modifier les délais suivants pour chaque caméra PTZ.

Nom	Description
Période d'inactivité pour la session PTZ manuelle	Spécifiez la période d'inactivité pour les sessions PTZ manuelles sur cette caméra si vous souhaitez que le délai soit différent de la période par défaut. Vous pouvez spécifier la période par défaut dans le menu **Outils** sous **Options**.
Délai de mise en pause d'un session PTZ en patrouille	Spécifiez le délai de mise en pause des sessions PTZ en patrouille sur cette caméra si vous souhaitez que le délai soit différent de la période par défaut. Vous pouvez spécifier la période par défaut dans le menu **Outils** sous **Options**.
Période d'inactivité pour les sessions PTZ réservées	Spécifiez la période d'inactivité pour les sessions PTZ réservées sur cette caméra si vous souhaitez que le délai soit différent de la période par défaut. Vous pouvez spécifier la période par défaut dans le menu **Outils** sous **Options**.

Onglet Patrouilles (périphériques)

À propos de l'onglet Patrouille

Les périphériques suivants possèdent un onglet **Patrouille** :

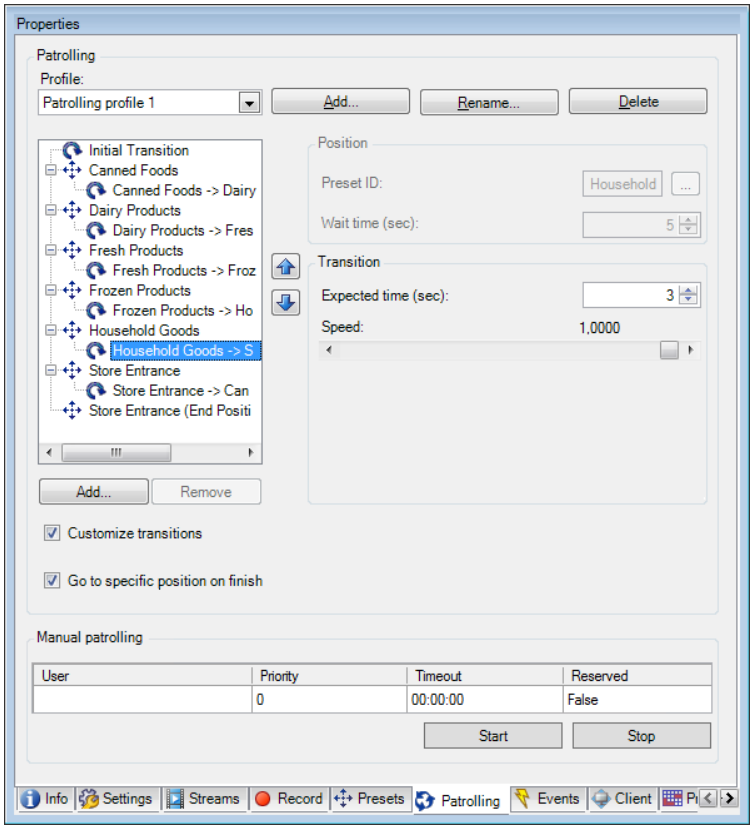
- Caméras PTZ

Dans l'onglet **Patrouille** vous permet de créer des profils de patrouille, c'est-à-dire le mouvement automatique d'une caméra PTZ (pan-tilt-zoom) entre plusieurs positions prédéfinies.
Avant de pouvoir vous servir de la fonction Patrouille, vous devez saisir au moins deux positions prédéfinies pour la caméra dans l'onglet **Préréglages**.

Les profils de patrouilles définissent la façon dont une patrouille doit avoir lieu. En font notamment partie l'ordre dans lequel la caméra doit se déplacer entre les positions prédéfinies et la durée pendant laquelle elle doit rester à chaque position. Vous pouvez créer un nombre illimité de profils de patrouille et les utiliser dans vos règles. Par exemple, vous pouvez créer une règle spécifiant qu'un profil de patrouille doit être utilisé pendant les heures d'ouverture de jour et un autre pendant la nuit.

Avant d'appliquer un profil de patrouille dans une règle, par exemple, vous pouvez tester le profil de patrouille à l'aide de la patrouille manuelle. Vous pouvez également utiliser la patrouille manuelle pour prendre le contrôle de la patrouille d'un autre utilisateur ou d'une patrouille activée par des règles, dans la mesure où vous disposez d'une priorité PTZ plus élevée.

Vous pouvez surveiller le système pour savoir s'il est actuellement en patrouille ou si un utilisateur en a pris le contrôle dans l'espace de la **Patrouille manuelle**.



L'onglet **Patrouille**, affichant un profil de patrouille avec des transitions personnalisées

Ajouter un profil de patrouille

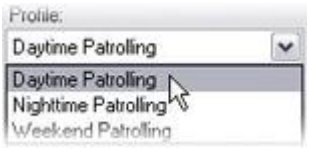
Ajoutez le profil souhaité, à utiliser dans une règle :

1. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter profil** s'ouvre.
2. Dans la boîte de dialogue **Ajouter profil**, donnez un nom au profil de patrouille.
3. Cliquez sur **OK**. Le bouton est désactivé si le nom n'est pas unique.

   Le nouveau profil de patrouille est ajouté à la liste **Profil**. Vous pouvez désormais préciser les positions prédéfinies et autres paramètres pour le profil de patrouille.

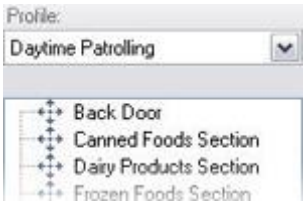
Spécifier des positions prédéfinies dans un profil de patrouille

1. Sélectionnez le profil de patrouille dans la liste **Profil** :



2. Cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Sélectionner prédéfinition**, sélectionnez les positions prédéfinies de votre profil de patrouille :

4. Cliquez sur **OK**. Les positions prédéfinies sélectionnées sont ajoutées à la liste de positions prédéfinies du profil de patrouille :



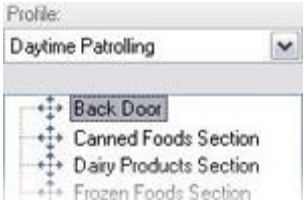
5. la caméra utilise la position prédéfinie la plus haute dans la liste comme premier arrêt lorsqu'elle patrouille en suivant le profil de patrouille. La position prédéfinie suivante depuis le haut constitue le second arrêt, et ainsi de suite.

Spécifier la durée à chaque position prédéfinie

Lors d'une patrouille, la caméra PTZ reste par défaut pendant 5 secondes sur chaque position prédéfinie indiquée dans le profil de patrouille.

Pour modifier le nombre de secondes :

1. Sélectionnez le profil de patrouille dans la liste **Profil**.
2. Sélectionnez la position prédéfinie pour laquelle vous souhaitez modifier la durée :



3. Indiquez la durée dans le champ **Durée en position (sec)** :
4. Si nécessaire, recommencez pour d'autres positions prédéfinies.

Personnaliser les transitions

Par défaut, la durée nécessaire au déplacement de la caméra d'une position prédéfinie à une autre, appelée **transition**, est estimée à trois secondes. Durant cette durée, par défaut, la détection du mouvement est désactivée sur la caméra, car un mouvement non pertinent est sinon susceptible d'être détecté alors que la caméra se déplace entre les positions prédéfinies.

La personnalisation des vitesses lors des transitions est uniquement prise en charge si votre caméra accepte le balayage PTZ et si elle est du type où les positions prédéfinies sont configurées et stockées sur le serveur de votre système (caméra PTZ type 1). Sinon, le curseur **vitesse** est grisé.

Vous pouvez personnaliser les éléments suivants :

- La durée de transition estimée.
- La vitesse à laquelle la caméra se déplace lors d'une transition.

Pour personnaliser les transitions entre les différentes positions prédéfinies :

1. Sélectionnez le profil de patrouille dans la liste **Profil**.
2. Cochez la case **Personnaliser transitions** :

   Les indications relatives à la transition sont ajoutées dans la liste des positions prédéfinies.

3. Dans la liste, sélectionnez la transition :

4. Indiquez la durée de transition estimée (en secondes) dans le champ **Temps escompté (sec.)** :

5. Utilisez le curseur **Vitesse** afin de préciser la vitesse de transition. Lorsque le curseur est complètement à droite, la caméra se déplace à sa vitesse par défaut. Plus vous déplacez le curseur sur la gauche, plus la caméra se déplacera lentement durant la transition choisie.

6. Répétez la procédure le cas échéant pour les autres transitions.

Spécifier une position de fin

Vous pouvez indiquer que la caméra doit se déplacer vers une position prédéfinie particulière lors d'une patrouille, conformément aux fins sélectionnées du profil de patrouille.

1. Sélectionnez le profil de patrouille dans la liste **Profil**.

2. Cochez la case **Atteindre une position spécifique à la fin**. Cela ouvre la boîte de dialogue **Sélectionner le préréglage**.

3. Sélectionnez la position de fin, puis cliquez sur **OK**.

   Vous pouvez sélectionner n'importe quelle position prédéfinie de la caméra comme position finale, vous n'avez pas à vous limiter aux positions prédéfinies utilisées dans le profil de patrouille.

4. La nouvelle position finale est ajoutée à la liste des profils.

   Lors d'une patrouille conformément aux fins sélectionnées du profil de patrouille, la caméra se déplace en position finale indiquée.

À propos des patrouilles manuelles

Lorsque vous avez conçu un profil de patrouille, vous pouvez le tester avec une patrouille manuelle avant de l'appliquer au système. Utilisez les boutons **Démarrer** et **Arrêter** pour lancer et arrêter la patrouille manuelle.

Si la caméra est déjà en patrouille ou contrôlée par un autre utilisateur, vous ne pouvez démarrer la patrouille manuelle que si vous disposez d'une priorité supérieure.

Si vous démarrez une patrouille manuelle alors que la caméra exécute une patrouille du système activée par des règles, le système reprend cette patrouille lorsque vous arrêtez votre patrouille manuelle. Si un autre utilisateur exécute une patrouille manuelle mais que vous disposez d'une priorité plus élevée et que vous démarrez votre patrouille manuelle, la patrouille manuelle de l'autre utilisateur ne reprendra pas.

Si vous n'arrêtez pas votre patrouille manuelle de vous-même, celle-ci se poursuivra jusqu'à ce qu'une patrouille basée sur des règles ou un utilisateur doté d'une priorité supérieure prenne le contrôle. Lorsque la patrouille du système basée sur des règles s'arrête, le système reprend votre patrouille manuelle. Si un autre utilisateur démarre une patrouille manuelle, votre patrouille manuelle s'arrête et ne reprendra pas.

Lorsque vous arrêtez votre patrouille manuelle et que vous avez défini une position finale pour votre profil de patrouille à l'aide de **Atteindre une position spécifique à la fin**, la caméra revient à cette position.

Propriétés des patrouilles manuelles

Le tableau **Patrouille manuelle** présente l'état actuel de la caméra PTZ.

Nom	Description
Utilisateur	Affiche l'utilisateur qui a réservé la session PTZ ou démarré une patrouille manuelle et contrôle actuellement la caméra. Si une session de patrouille est activée par le système, **Patrouille en cours** s'affiche.
Priorité	Affiche la priorité PTZ de l'utilisateur. Vous ne pouvez prendre le contrôle que de sessions PTZ d'utilisateurs ou de profils de patrouille ayant une priorité inférieure à la vôtre.
Délai de réponse dépassé	Affiche le temps restant des sessions PTZ manuelles ou réservées actuelles.
Réservé	Indique si la session actuelle est une session PTZ réservée ou non. • **Vrai** : Réservé. • **Faux** : Non réservé.

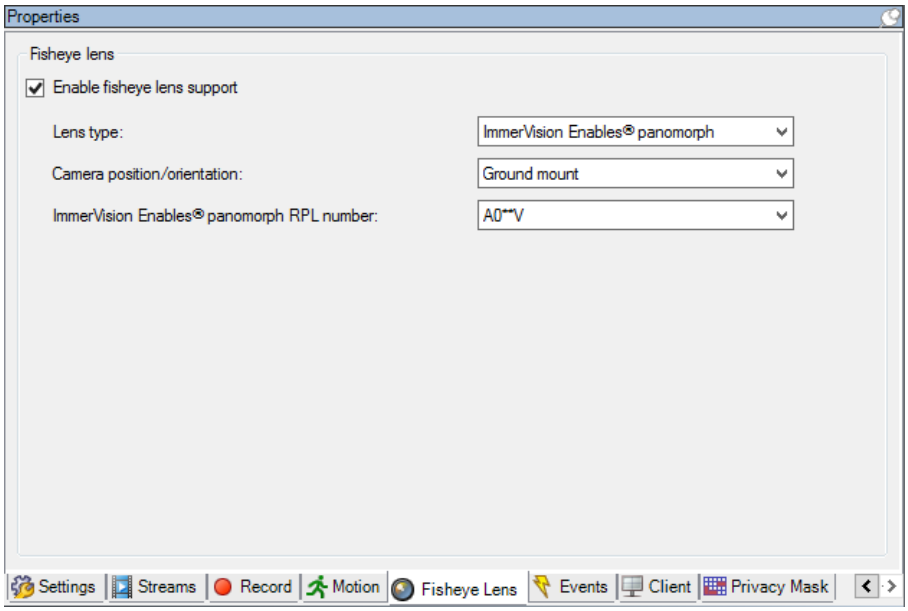
Onglet Lentille fisheye (périphériques)

À propos de l'onglet Lentille fisheye

Les périphériques suivants possèdent un onglet **Lentille fisheye** :

- Caméras fixes avec une lentille fisheye

L'onglet **Lentille fisheye** vous permet d'activer et de configurer la prise en charge fisheye de la caméra sélectionnée.



Activer et désactiver la prise en charge fisheye

La prise en charge fisheye est désactivée par défaut.

Pour l'activer ou la désactiver, cochez ou décochez la case **Activer le support fisheye** de l'onglet **Lentille fisheye**.

Spécifier les paramètres de la lentille fisheye

Pour activer la prise en charge de la lentille fisheye :

1. Sélectionnez le type de lentille.
2. Indiquez la position physique / l'orientation de la caméra dans la liste **Position/orientation de la caméra**.
3. Sélectionnez un numéro de lentille Panomorphe enregistrée (Registered Panomorph Lens, RPL) dans la liste **Numéro RPL ImmerVision Enables® Panomorph**.

   Ceci permet d'identifier et de corriger la configuration de la lentille utilisée avec la caméra. Le numéro RPL se trouve généralement sur la lentille elle-même ou sur la boîte dans laquelle elle vous a été fournie. Pour plus d'informations sur ImmerVision, les lentilles Panomorph et les RPL, consultez site web d'Immervision https://www.immervisionenables.com/**.**

Onglet Événements (périphériques)

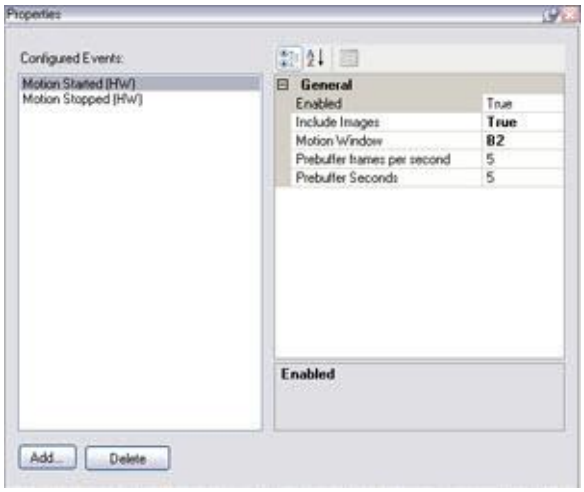
À propos de l'onglet Événements

Les périphériques suivants possèdent un onglet **Événements** :

- Caméras

- Microphones
- Entrées

Outre les événements du système, certains périphériques peuvent être configurés pour déclencher des événements. Vous pouvez utiliser ces événements lors de la création de règles basées sur des événements dans le système. Ils se produisent techniquement sur le matériel/périphérique et non sur le système de surveillance.



Onglet **Événement**, exemple de la **caméra**

Lorsque vous supprimez un événement, cela affecte toutes les règles qui utilisent l'événement.

- Ajouter un événement (á la page 152)
- Spécifier les propriétés des événements (á la page 152)
- Utiliser plusieurs instances d'un événement (á la page 153)

Ajouter un événement

1. Dans le volet **Vue d'ensemble**, sélectionnez un périphérique.
2. Sélectionnez l'onglet **Événements** et cliquez sur **Ajouter**. La fenêtre **Sélectionner un événement pilote** s'ouvre.
3. Sélectionner un événement. Vous pouvez uniquement sélectionner un événement à la fois.
4. Cliquez sur **OK**.
5. Dans la boîte à outils, cliquez sur **Enregistrer**.

Spécifier les propriétés des événements

Vous pouvez spécifier les propriétés pour chaque événement que vous avez ajouté. Le nombre de propriétés dépend du périphérique et de l'élément. Afin que l'événement fonctionne comme prévu, vous devez spécifier une partie ou la totalité des propriétés de la même façon sur le périphérique ainsi que sur cet onglet.

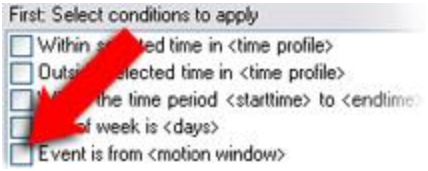
Utiliser plusieurs instances d'un événement

Pour pouvoir spécifier différentes propriétés pour différentes instances d'un événement, vous pouvez ajouter un événement plus d'une fois.

L'exemple suivant est spécifique aux **caméras**.

Exemple : Vous avez configuré la caméra avec deux fenêtres de mouvement appelées A1 et A2. Vous avez ajouté deux instances de l'événement **Mouvement démarré (HW)**. Dans les propriétés de l'une des instances, vous avez précisé l'utilisation de la fenêtre de mouvement A1. Dans les propriétés de l'autre instance, vous avez précisé l'utilisation de la fenêtre de mouvement A2.

Lorsque vous utilisez l'événement dans une règle, vous pouvez spécifier que l'événement doit être basé sur le mouvement détecté dans une fenêtre de mouvement spécifique afin que la règle soit déclenchée :



Exemple : Spécifier une fenêtre de mouvement spécifique
dans le cadre des conditions d'une règle

Onglet événement (propriétés)

Nom	Description
Événements configurés	Les événements que vous sélectionnez et ajoutez dans la liste d'**Événements configurés** sont entièrement déterminés par le périphérique et sa configuration. Pour certains types de périphériques, la liste est vide.
Généralités	La liste de propriétés dépend du périphérique et de l'élément. Afin que l'événement fonctionne comme prévu, vous devez spécifier une partie ou la totalité des propriétés de la même façon sur le périphérique ainsi que sur cet onglet.

Onglet Client (périphériques)

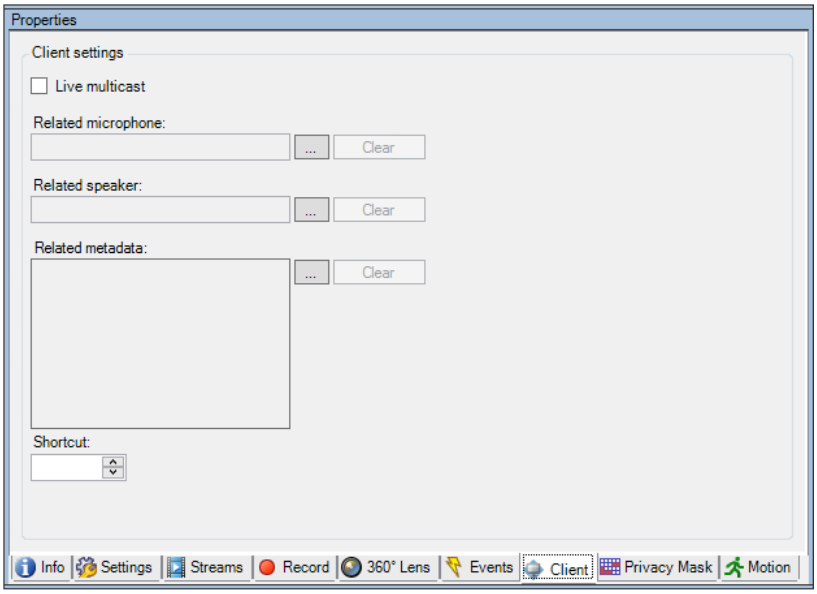
À propos de l'onglet Client

Les périphériques suivants possèdent un onglet **Client** :

- Caméras

Dans l'onglet **Client**, vous pouvez préciser quels autres périphériques sont vus et entendus lorsque vous utilisez la caméra dans XProtect Smart Client.

Les périphériques connexes enregistrent aussi lorsque la caméra enregistre, voir Activer l'enregistrement sur les périphériques connexes (á la page 133).



Propriétés de l'onglet Client

Nom	Description
Multicast en direct	Le système prend en charge le multicast de flux en direct depuis le serveur d'enregistrement vers XProtect Smart Client. Pour activer le multicast des flux en direct depuis la caméra sélectionnée, cochez la case correspondante. Vous devez également configurer le mode multicast pour le serveur d'enregistrement. Voir À propos du multicast (á la page 91). Si les diffusions en multicast ne fonctionnent pas, par exemple en raison de restrictions sur le réseau ou de clients individuels, le système revient en mode unicast.
Microphone connexe	Spécifiez depuis quel microphone de la caméra les utilisateurs XProtect Smart Client reçoivent la radio par défaut. L'utilisateur XProtect Smart Client peut choisir l'écoute par un autre microphone manuellement le cas échéant**.** Les microphones connexes enregistrent lorsque la caméra enregistre.
Haut-parleur connexe	Spécifiez depuis quels haut-parleurs de la caméra les utilisateurs XProtect Smart Client parlent par défaut. L'utilisateur XProtect Smart Client peut sélectionner un autre haut-parleur manuellement le cas échéant. Les haut-parleurs connexes enregistrent lorsque la caméra enregistre.

Nom	Description
Métadonnées connexes	Indiquez un ou plusieurs périphériques métadonnées sur la caméra à partir desquels les utilisateurs XProtect Smart Client reçoivent des données. Les dispositifs de métadonnées connexes lorsque la caméra enregistre.
Raccourci	Pour faciliter la sélection des caméras pour les utilisateurs XProtect Smart Client, définissez des raccourcis clavier pour les caméras. • Créez chaque raccourci de sorte qu'il identifie de manière unique les caméras. • Le numéro de raccourci d'une caméra ne peut pas avoir plus de quatre chiffres.

Onglet Masque de confidentialité (périphériques)

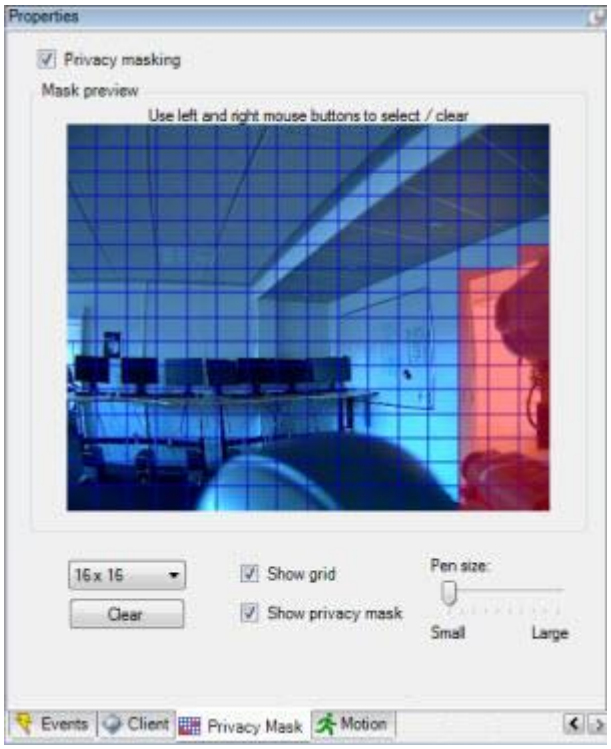
À propos de l'onglet Masque de confidentialité

Les périphériques suivants possèdent un onglet **Masque de confidentialité** :

- Caméras

L'onglet **Masque de confidentialité** vous permet d'activer et de configurer le masque de confidentialité de la caméra sélectionnée. Vous pouvez définir les zones de l'image à masquer avant la distribution. Par exemple, si une caméra de surveillance filme une rue, afin de protéger la vie privée des résidents, vous pouvez masquer certaines zones d'un bâtiment (peut-être les fenêtres et les portes) à l'aide du masque de confidentialité.

Lors de leur affichage via XProtect Smart Client ou un autre média, les zones avec un masquage de confidentialité apparaissent dans une zone noire qui ne peut être supprimée par personne.



Les zones en rouge illustrent les zones masquées pour confidentialité.

Lorsque vous utilisez des masques de confidentialité avec des caméras PTZ et que ces caméras peuvent être orientées, inclinées et agrandies, la zone sélectionnée pour la confidentialité ne se déplace **pas** car elle est verrouillée en fonction de l'image de la caméra. Pour combler ce défaut, certaines caméras PTZ prennent en charge l'activation d'une position en fonction du masque de confidentialité sur la caméra en elle-même.

Dans une configuration Milestone Interconnect, le site central ignore le masquage de confidentialité défini dans un site distant. Si vous souhaitez utiliser le même masquage de confidentialité, vous devez le redéfinir sur le site central.

Activer/désactiver le masquage de confidentialité

La fonction de masquage de confidentialité est désactivée par défaut.

Pour activer/désactiver la fonction de masquage de confidentialité pour une caméra :

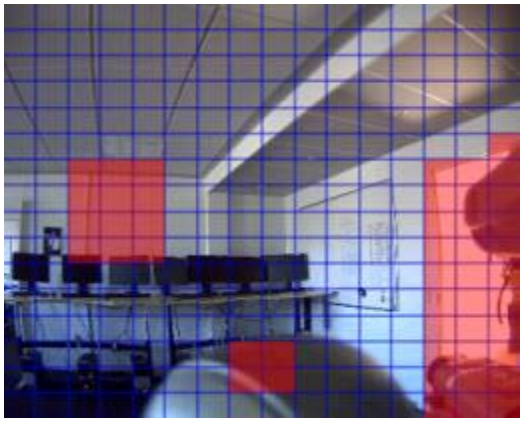
- Cochez/décochez la case **Masquage de confidentialité** dans l'onglet **Masque de confidentialité**.

Spécifier les paramètres du masque de confidentialité

Lorsque vous activez le masquage de confidentialité, l'image de l'aperçu est partagée sous forme de grille en sections à sélectionner.

1. Pour définir les zones à masquer, faites glisser le pointeur de la souris sur la zone choisie dans l'image de l'aperçu. Appuyez sur le bouton gauche de la souris pour sélectionner une partie de la grille. Le bouton droit de la souris permet d'annuler la zone sélectionnée.

2. Vous pouvez définir autant de zones de masque de confidentialité que nécessaire. Les zones du masque de confidentialité sont indiquées en rouge.



Trois zones du masque de confidentialité sont définies dans la fenêtre de l'aperçu. Dans ce cas, la grille est visible.

Les indications du masque de confidentialité en rouge apparaissent également dans l'image de l'aperçu sur l'onglet **Mouvement**.

Onglet Masque de confidentialité (propriétés)

Nom	Description
Taille de grille	La valeur sélectionnée dans la liste de la **taille de grille** détermine la densité de la grille, que la grille soit visible ou non. Les valeurs disponibles sont 8×8, 16×16, 32×32 ou 64×64.
Afficher la grille	Cochez la case **Afficher la grille** pour afficher le quadrillage.
Afficher le masque de confidentialité	Lorsque vous cochez la case **Afficher le masque de confidentialité** (par défaut), les régions sélectionnées sont mises en surbrillance en rouge dans l'image de l'aperçu. Masquer les zones peut fournir une vue moins obscurcie de l'image de l'aperçu. Milestone vous recommande de laisser la case **Afficher le masque de confidentialité** cochée afin d'éviter l'existence de régions sans que ou vos collègues en soyez conscients.
Taille du pinceau	Utilisez le curseur de **taille du pinceau** afin d'indiquer la taille des sélections que vous souhaitez effectuer lorsque vous cliquez et déplacez la grille sur les zones sélectionnées. Par défaut, la taille est définie sur petite, ce qui équivaut à un carré de la grille.

Onglet Mouvement (périphériques)

À propos de l'onglet Mouvement

Les périphériques suivants possèdent un onglet **Mouvement** :

- Caméras

L'onglet **Mouvement** vous permet d'activer et de configurer la détection du mouvement pour la caméra sélectionnée. La configuration de la détection du mouvement est un élément clé de votre système : Votre configuration de la détection de mouvement définit le moment où le système génère des événements de mouvement et généralement aussi lorsqu'une vidéo est enregistrée.

Le temps passé à chercher la meilleure configuration possible en termes de configuration de détection de mouvement vous aide plus tard à éviter les enregistrements inutiles par exemple. En fonction de l'emplacement physique de la caméra, il peut s'avérer utile de tester les paramètres de détection du mouvement dans plusieurs conditions physiques différentes comme par ex. de jour/nuit ou par temps venteux/calme.

Avant de configurer la détection du mouvement pour une caméra, Milestone vous recommande de configurer au préalable les paramètres de qualité d'image de la caméra, tels que la résolution, le codec vidéo et les paramètres de flux dans l'onglet **Paramètres**. Si vous changez plus tard les paramètres de qualité d'image, vous devez toujours tester la configuration de détection du mouvement par la suite.

Propriétés des caméras : Onglet **Mouvement** avec déflexion rouge sur la barre d'indication de mouvement

Vous pouvez configurer tous les paramètres d'un groupe de caméras, mais il est en général préférable de régler les zones à exclure par caméra.

- Activer et désactiver la détection du mouvement (á la page 159)
- Spécifier les paramètres de détection de mouvement (á la page 159)

Activer et désactiver la détection du mouvement

Vous spécifiez le paramètre par défaut de la détection du mouvement dans l'onglet **Outils** > **Options** > **Général**.

Pour activer ou désactiver la détection du mouvement par la suite pour une caméra :

- Cochez ou décochez la case **Détection du mouvement** dans l'onglet **Mouvement**.

Important : lorsque la détection du mouvement d'une caméra est désactivée, aucune des règles de la caméra associées à la détection du mouvement ne fonctionne.

Spécifier les paramètres de détection de mouvement

Vous pouvez spécifier des paramètres relatifs à la quantité de changement requise dans la vidéo d'une caméra afin que le changement soit considéré comme un mouvement. Vous pouvez par exemple spécifier des intervalles entre les analyses de détection du mouvement et des zones d'une image dans lesquelles les mouvements doivent être ignorés.

À propos de la sensibilité dynamique

La détection du mouvement est configurée par défaut pour la sensibilité dynamique. Pour régler le niveau de sensibilité manuellement, reportez-vous à la section Activer la sensibilité manuelle (á la page 159).

Milestone vous recommande de ne pas activer la sensibilité manuelle pour les raisons suivantes :

- Avec la sensibilité manuelle, le système calcule et optimise le niveau de sensibilité automatiquement et supprime les détections de mouvement provenant du bruit dans les images.
- La sensibilité dynamique améliore la détection du mouvement la nuit, lorsque le bruit dans les images déclenche souvent de faux mouvements.
- Le système n'est pas surchargé par des enregistrements excessifs.
- Il ne manque pas de résultats aux utilisateurs en raison d'une quantité trop faible d'enregistrements.

Activer la sensibilité manuelle

Le paramètre de sensibilité détermine **dans quelle mesure chaque pixel** de l'image doit changer avant que l'on considère qu'il y a mouvement.

1. Cochez la case **Sensibilité manuelle** dans l'onglet **Mouvement**.
2. Faites glisser le curseur vers la gauche pour un plus grand niveau de sensibilité et vers la droite pour un niveau de sensibilité moindre.

   Plus le niveau de sensibilité est **élevé**, et moins les changements requis dans chaque pixel pour constituer un mouvement sont importants.

   Plus le niveau de sensibilité est **faible**, et plus les changements requis dans chaque pixel pour constituer un mouvement sont importants.

Les pixels dans lesquels un mouvement est détecté sont surlignés en vert dans l'image de l'aperçu.

3. Sélectionnez une position du curseur dans laquelle seuls les changements détectés que vous considérez comme des mouvements sont mis en surbrillance.

Mouvement mis en surbrillance dans l'image de l'aperçu

Vous pouvez comparer et définir le paramètre de sensibilité exact entre les caméras à l'aide du numéro à droite du curseur.

Spécifier le seuil

Le seuil de détection du mouvement détermine **combien de pixels** de l'image doivent changer avant que l'on considère qu'il y a mouvement.

1. Faites glisser le curseur vers la gauche pour un plus grand niveau de mouvement et vers la droite pour un niveau de mouvement moindre.

2. Sélectionnez une position du curseur dans laquelle seuls les changements détectés que vous considérez comme des mouvements sont détectés.

La ligne noire verticale dans la barre d'indication de mouvement indique le seuil de détection du mouvement : quand le mouvement détecté est au-dessus du niveau du seuil de détection sélectionné, la barre passe du vert au rouge, ce qui indique une détection positive.

Barre d'indication de mouvement : passe du vert au rouge lorsque le seuil est dépassé, indiquant la détection positive d'un mouvement

Sélectionner les paramètres des images-clés

Détermine si la détection du mouvement est réalisée uniquement sur les images-clés ou sur l'ensemble du flux vidéo. S'applique uniquement à MPEG-4/H.264/H.265.

La détection du mouvement sur les images-clés réduit la quantité de puissance de traitement utilisée pour l'analyse.

Cochez la case **Images-clés uniquement (MPEG-4/H.264/H.265)** pour procéder à la détection du mouvement uniquement sur les images-clés.

Sélectionner l'intervalle de traitement des images

Vous pouvez sélectionner la fréquence avec laquelle le système procède à une analyse de détection du mouvement.

Dans la liste **Traiter l'image tous les (msec)** :

- Sélectionnez l'intervalle. Par exemple, toutes les 1000 millisecondes correspondent à une fois par seconde. La valeur par défaut est de 500 millisecondes.

L'intervalle est appliqué si la fluidité d'image actuelle est supérieure à l'intervalle défini à cet endroit.

Spécifier la méthode de détection

Vous permet d'optimiser la performance de détection du mouvement en analysant uniquement un pourcentage sélectionné de l'image, par exemple 25 %. En analysant 25 % par exemple, seul un quart des pixels de l'image est analysé au lieu de tous les pixels.

L'utilisation de la détection optimisée réduit la quantité de puissance du processeur utilisée pour effectuer l'analyse, mais se traduit également par une détection de mouvement moins précise.

- Dans la boîte déroulante **Méthode de détection**, sélectionnez la méthode de détection voulue.

À propos de la production de données de mouvement pour la recherche intelligente

Lorsque la fonction **Générer des données de mouvement pour la recherche intelligente**est activée, le système génère des données de mouvement pour les images utilisées pour la détection du mouvement. Par exemple, si vous sélectionnez la détection du mouvement sur les images-clés uniquement, les données de mouvement sont également produites pour les images-clés uniquement.

Les données de mouvement supplémentaires permettent à l'utilisateur du client, via la fonction de recherche avancée, de rechercher rapidement les enregistrements concernés sur la base du mouvement dans la zone sélectionnée de l'image. Les données de mouvement ne sont pas générées pour les zones dotées de masques de confidentialité.

Le seuil de détection du mouvement et les zones à exclure n'influencent pas les données de mouvement générées.

Vous spécifiez le paramètre par défaut de la génération de données de recherche intelligente dans l'onglet **Outils** > **Options** > **Général**.

Spécifier l'exclusion de zones

Vous pouvez désactiver la détection du mouvement dans des zones spécifiques de la vision d'une caméra.

Le fait désactiver la détection du mouvement dans des zones spécifiques vous aide à éviter la détection de mouvement inutile, par exemple si la caméra couvre une zone où un arbre bouge dans le vent ou un endroit où des voitures passent régulièrement en arrière-plan.

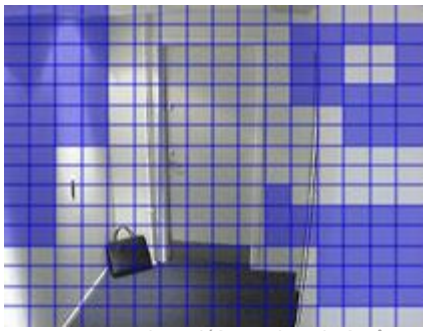
Lorsque vous utilisez l'exclusion de zones avec des caméras PTZ et que cette caméra peut être orientée, inclinée et agrandie, l'exclusion de zone ne se déplace **pas** car est verrouillée en fonction de l'image de la caméra et pas de l'objet.

1. Pour utiliser l'exclusion de zones, cochez la case **Utiliser l'exclusion de zones**.

   Une grille divise l'image de l'aperçu en zones à sélectionner.

2. Pour définir les régions à exclure, faites glisser le curseur de la souris sur les zones requises dans l'image de l'aperçu pendant que vous appuyez sur le bouton gauche de la souris. Le bouton droit de la souris permet d'annuler la zone sélectionnée.

Vous pouvez définir autant de zones à exclure que nécessaire. Les zones exclues apparaissent en bleu.



Trois zones exclues définies dans la fenêtre d'aperçu. Dans ce cas, la grille est visible.

Les zones à exclure bleues apparaissent uniquement dans l'image d'aperçu de l'onglet **Mouvement**, et non dans les autres images d'aperçu du Management Client ou des clients d'accès.

Client

À propos des clients

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

La section Client du Management Client est composée des éléments suivants :

Nom	Description
XProtect Smart Wall	XProtect Smart Wall est un produit complémentaire qui vous permet de visualiser du contenu venant de XProtect Smart Client sur un mur vidéo dédié. Pour obtenir des informations plus détaillées sur XProtect Smart Wall, consultez À propos de XProtect Smart Wall (á la page 305).
Groupes de vues	La façon dont la vidéo des caméras s'affiche s'appelle une vue. Pour contrôler qui peut voir quoi dans XProtect Smart Client, vous pouvez créer des groupes de vues pour grouper les vues en entités logiques. Vous pouvez assigner un accès à ces groupes de vues par le biais de rôles et ainsi limiter l'accès à certains groupes de vues à des rôles spécifiques. Sélectionnez **Groupes de vues** pour créer et travailler avec des groupes de vues pour répondre à vos besoins en matière de surveillance.
Profils Smart Client	Pour pouvoir différencier les utilisateurs XProtect Smart Client, vous pouvez créer des profils Smart Client, les rendre prioritaires et les personnaliser en fonction de vos besoins pour les différentes tâches à effectuer.
Profils Management Client	Pour pouvoir différencier les utilisateurs administrateurs Management Client, vous pouvez créer des profils Management Client, les rendre prioritaires et les personnaliser en fonction de vos besoins pour les différentes tâches à effectuer.

Nom	Description
Matrix	Matrix est une fonctionnalité qui permet d'envoyer les vidéos à distance. Lorsque vous utilisez Matrix, vous pouvez déplacer la vidéo d'une caméra au choix sur le réseau de votre système vers un XProtect Smart Client en marche.

Groupes de vues

À propos des groupes de vues

La façon dont le système présente les vidéos d'une ou plusieurs caméras dans les clients est appelée « vue ». Un groupe de vues est un conteneur d'un ou de plusieurs groupes logiques de telles vues. Dans les clients, un groupe de vues se présente comme un fichier extensible à partir duquel les utilisateurs peuvent sélectionner le groupe et la vue qu'ils souhaitent afficher :

Exemple de XProtect Smart Client : La flèche indique un groupe de vues, qui contient un groupe logique (appelé Amenities), qui à son tour contient 3 vues.

À propos des groupes de vues et des rôles

Par défaut, chaque rôle que vous définissez dans le Management Client est également créé comme un groupe de vues. Lorsque vous ajoutez un rôle dans le Management Client, le rôle s'affiche par défaut comme un groupe de vues dans les clients.

- Vous pouvez assigner un groupe de vues en fonction d'un rôle à des utilisateurs/groupes possédant le rôle en question. Vous pouvez changer les droits du groupe de vues en configurant le rôle ultérieurement.
- Un groupe de vues basé sur un rôle prend le nom de ce rôle.

  Exemple : si vous créez un rôle avec le nom **Personnel de sécurité Immeuble A**, par défaut, il apparaît dans XProtect Smart Client en tant que groupe de vues intitulé **Personnel de sécurité Immeuble A**.

  En complément des groupes de vues obtenus lorsque vous ajoutez des rôles, vous pouvez en créer autant que vous le souhaitez. Vous pouvez également supprimer des groupes de vues, y compris ceux qui sont automatiquement créés lorsque des rôles sont ajoutés.
- Même si un groupe de vues est créé à chaque fois que vous ajoutez un rôle, les groupes de vues ne doivent pas nécessairement correspondre aux rôles. Vous pouvez ajouter, renommer ou supprimer chacun de vos groupes de vues si nécessaire.

Veuillez noter que, si vous renommez un groupe de vues, les utilisateurs des clients déjà connectés doivent se déconnecter et se reconnecter avant que le changement de nom soit visible.

Ajouter un groupe de vues

1. Faites un clic droit dans **Groupes de vues**, puis sélectionnez **Ajouter groupe de vues**. La boîte de dialogue **Ajouter groupe de vues** s'ouvre.
2. Saisissez le nom et une description facultative du nouveau groupe de vues, puis cliquez sur **OK**.

Remarque : aucun rôle n'a le droit d'utiliser le groupe de vues nouvellement ajouté tant que ces droits n'ont pas été précisés. Si vous avez précisé les rôles qui doivent être capables d'utiliser le groupe de vues nouvellement ajouté, les utilisateurs clients déjà connectés avec les rôles pertinents doivent se déconnecter et se reconnecter avant de pouvoir voir le groupe de vues.

Profils Smart Client

À propos des profils Smart Client

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

Les profils Smart Client permettent aux administrateurs système de contrôler l'apparence et le comportement de XProtect Smart Client, ainsi que les fonctions et volets auxquels les utilisateurs XProtect Smart Client ont accès. Vous pouvez configurer les droits de l'utilisateur pour : les volets et les options, les options de réduction/agrandissement, le contrôle de la durée d'inactivité, le rappel d'un mot de passe ou non, la vue affichée après la connexion, la mise en page de rapports d'impression, le chemin d'exportation, et beaucoup d'autres choses encore.

Pour gérer les profils Smart Client dans le système, développez **Client**, puis sélectionnez **Profils Smart Client**. Vous pouvez également en savoir plus sur la relation entre les profils Smart Client, les rôles et les profils de temps et comment les utiliser ensemble (voir "Créer et configurer des profils Smart Client, rôles et profils de temps" á la page 165).

Ajouter et configurer un profil Smart Client

Vous devez créer un profil Smart Client avant de pouvoir le configurer.

1. Faites un clic droit sur **Profils Smart Client**.
2. Sélectionnez **Ajouter profil Smart Client**.
3. Dans la boîte de dialogue **Ajouter profil Smart Client**, saisissez le nom et la description du nouveau profil, puis cliquez sur **OK**.
4. Dans le volet **Vue d'ensemble**, cliquez sur le profil que vous venez tout juste de créer pour le configurer.
5. Ajustez les paramètres sur l'un ou plusieurs, voire tous les onglets disponibles, et cliquez sur **OK**.

Copier un profil Smart Client

Si vous possédez un profil Smart Client avec des paramètres ou des droits compliqués et avez besoin d'un profil semblable, il peut s'avérer plus simple de copier un profil déjà existant et d'apporter des petits ajustements à la copie plutôt que de créer un tout nouveau profil.

1. Cliquez sur **Profils Smart Client,** faites un clic droit sur le profil dans le volet **Vue d'ensemble**, sélectionnez **Copier profil Smart Client**.

2. Dans la boîte de dialogue qui s'ouvre, donnez au profil copié un nouveau nom et une description uniques. Cliquez sur **OK**.

3. Dans le volet **Vue d'ensemble**, cliquez sur le profil que vous venez tout juste de créer pour le configurer. Cela est effectué en ajustant les paramètres sur l'un, plusieurs voire tous les onglets disponibles. Cliquez sur **OK**.

Créer et configurer des profils Smart Client, rôles et profils de temps

Lors de l'utilisation de profils Smart Client, il est important de comprendre l'interaction entre profils Smart Client, rôles et profils de temps.

- Les profils Smart Client traitent les paramètres des droits d'utilisateur dans XProtect Smart Client.
- Les rôles concernent les paramètres de sécurité dans les clients, MIP SDK et bien plus encore
- Les profils de temps gèrent les aspects temporels des deux types-profils.

Ces trois fonctionnalité ensemble, assurent un contrôle et des possibilités de personnalisation uniques par rapport aux droits de l'utilisateur XProtect Smart Client.

> **Exemple** : Vous avez besoin d'un utilisateur dans votre configuration XProtect Smart Client qui doit uniquement être autorisé à voir la vidéo en direct (pas de lecture) de caméras choisies, et seulement durant les heures ouvrées normales (8 h 00 à 16 h 00). Une manière de configurer pourrait être comme suit :

1. Créez un profil Smart Client et donnez-lui un nom, par exemple **Direct uniquement**.

2. Précisez les paramètres de lecture/direct nécessaires sur **Direct uniquement**.

3. Créez un profil de temps et donnez-lui un nom, par exemple **Journée uniquement**.

4. Indiquez la période de temps nécessaire sur **Journée uniquement**.

5. Créez un nouveau rôle et donnez-lui un nom, par exemple **Gardien (caméras sélectionnées).**

6. Précisez les caméras utilisées par le **Gardien (caméras sélectionnées)**.

7. Attribuez le profil Smart Client **Direct uniquement** et le profil de temps **Journée uniquement** au rôle **Gardien (caméras sélectionnées)** pour connecter les trois éléments.

Vous disposez désormais d'une combinaison de trois fonctions créant le résultat souhaité et vous donnant la possibilité d'apporter des ajustements et de procéder à des réglages de précision. Remarquez également qu'il est possible d'effectuer la configuration dans un ordre différent, par exemple, en créant d'abord le rôle, puis le profil Smart Client et ensuite le profil de temps, ou dans un ordre différent.

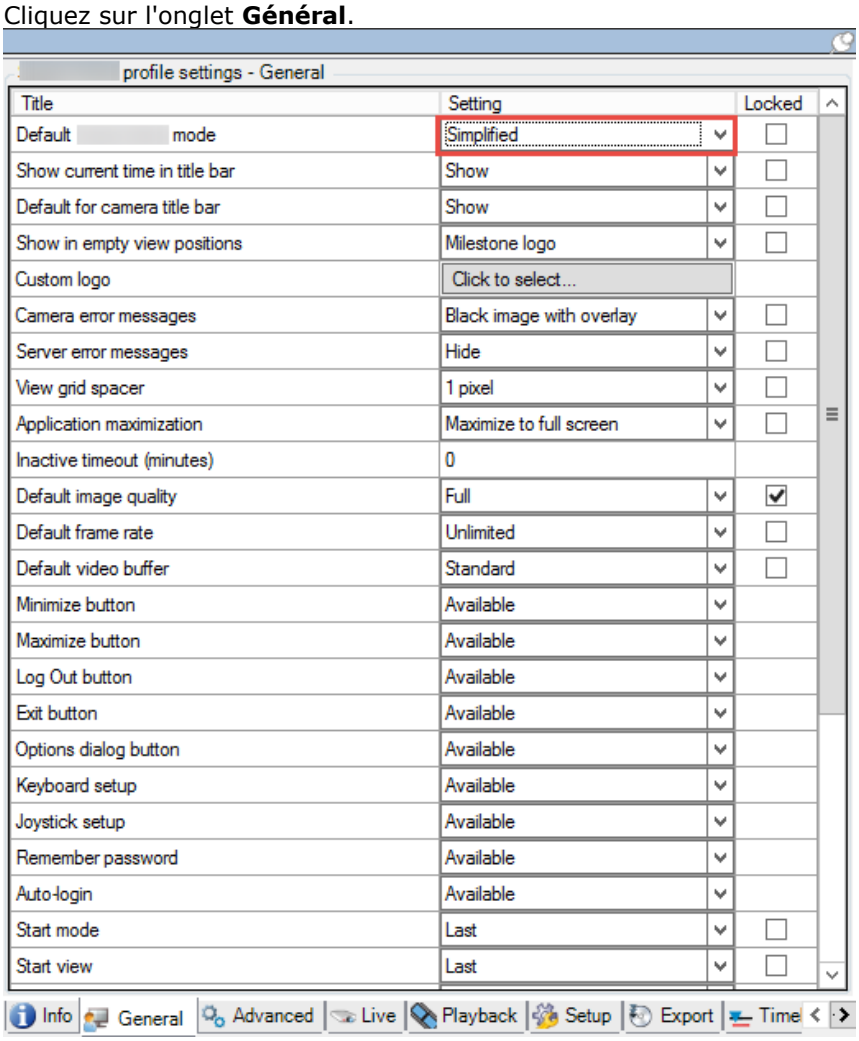
Définir le mode simplifié comme le mode par défaut

Par l'intermédiaire des profils Smart Client, vous pouvez configurer votre système pour qu'il ouvre automatiquement XProtect Smart Client en mode simplifié avec un ensemble limitée de

fonctionnalités et d'onglets. Par défaut XProtect Smart Client s'ouvre en mode avancé avec l'ensemble complet de fonctionnalités et d'onglets.

Si l'opérateur XProtect Smart Client décide de passer à un mode différent que le mode par défaut, XProtect Smart Client se souviendra de ce paramètre la prochaine fois que l'opérateur ouvrira le programme.

1. Dans Management Client, déroulez le nœud **Client**.
2. Sélectionnez le profil Smart Client pertinent.
3. Cliquez sur l'onglet **Général**.



4. Dans la liste **Mode Smart Client par défaut**, sélectionnez **Simplifié**. XProtect Smart Client s'ouvre à présent en mode simplifié pour les utilisateurs associés au profil Smart Client actuel.

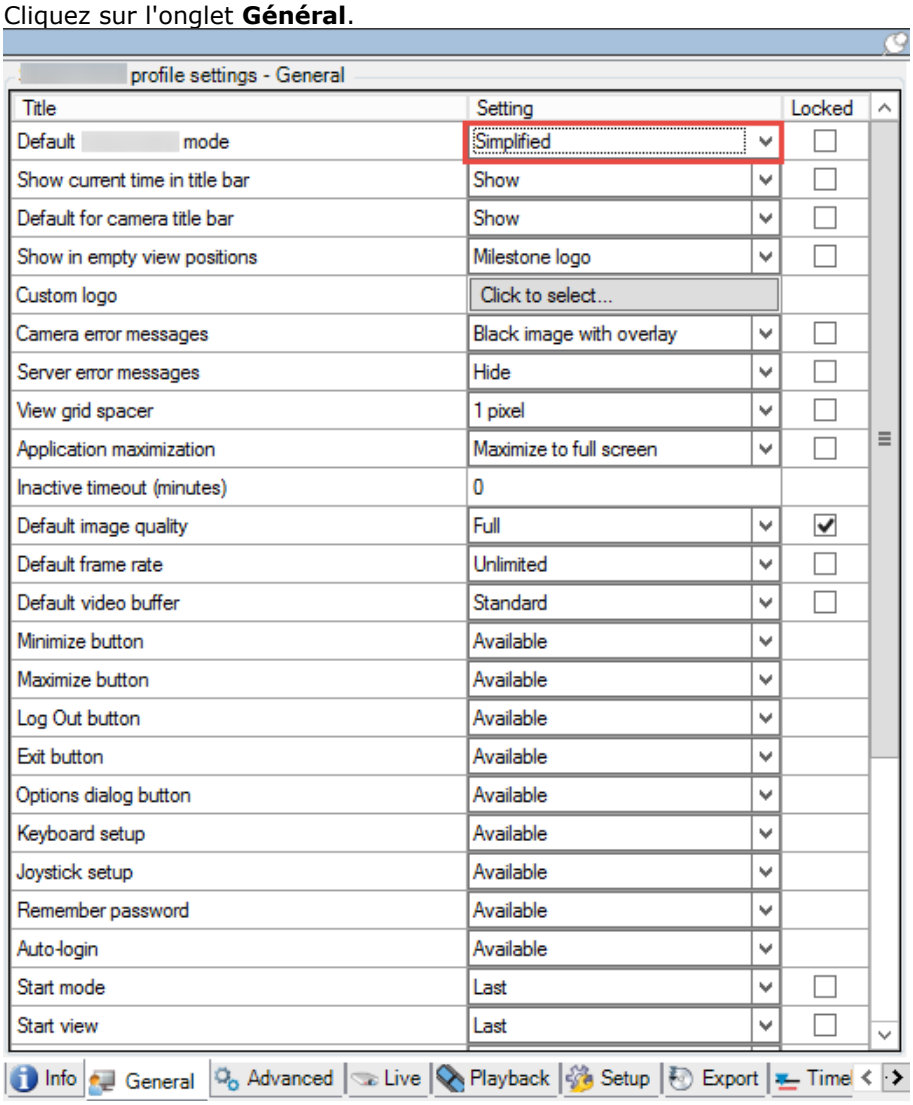
Voir également

Empêcher des opérateurs de permuter entre mode simple et avancé (á la page 167)

Empêcher des opérateurs de permuter entre mode simple et avancé

Dans XProtect Smart Client, les opérateurs peuvent permuter entre le mode simple et le mode avancé. Toutefois, vous pouvez empêcher les opérateurs XProtect Smart Client de permuter entre les deux modes. Techniquement, vous devez verrouiller les paramètres déterminant si XProtect Smart Client s'ouvre en mode simple ou avancé.

1. Dans Management Client, déroulez le nœud **Client**.
2. Sélectionnez le profil Smart Client pertinent.
3. Cliquez sur l'onglet **Général**.



4. Vérifiez que la liste **Mode Smart Client par défaut** a la valeur appropriée. Si **Activé**, XProtect Smart Client s'ouvre en mode simple.
5. Cochez la case **Verrouillé.** Le bouton Changer de mode dans XProtect Smart Client est masqué.

Voir également

Définir le mode simple comme le mode par défaut (voir "Définir le mode simplifié comme le mode par défaut" á la page 165)

Propriétés du profil Smart Client

Les onglets suivants vous permettent de spécifier les propriétés de chaque profil Smart Client. Vous pouvez verrouiller les paramètres dans le Management Client le cas échéant, de façon à ce que les utilisateurs de XProtect Smart Client ne puissent pas les modifier :

Onglet	Description
Informations	Le nom et la description, la priorité de modification des profils existants et un aperçu des rôles utilisés avec quel profil. Si un utilisateur est membre de plus d'un rôle, chacun avec leur profil Smart Client individuel, l'utilisateur a le profil Smart Client au niveau de priorité le plus élevé.
Généralités	Paramètres tels que afficher/masquer et minimiser et maximiser les paramètres des menus, connecter/déconnecter, démarrer, période d'inactivité, infos et options de messagerie et paramètres de l'Explorateur de séquences.
Avancée	Paramètres avancés tels que ceux des fils de décodage maximum, du désentrelacement et des fuseaux horaires. **Fils de décodage maximum** détermine combien de fils de décodage sont utilisés pour décoder les flux vidéo. Cela peut participer à améliorer la performance sur des ordinateurs multicoeurs aussi bien en mode direct qu'en mode de lecture. L'amélioration exacte de la performance dépend du flux vidéo. Cela est surtout pertinent lors de l'emploi de flux vidéo haute résolution lourdement codés tels que H.264/H.265, pour lesquels le potentiel d'amélioration de la performance peut être significatif et moins pertinent lors de l'utilisation, par exemple, de JPEG ou MPEG-4. Avec le **désentrelacement**, vous convertissez la vidéo en format non entrelacé. L'entrelacement détermine la manière dont une image est rafraîchie à l'écran. L'image est rafraîchie tout d'abord en analysant les lignes irrégulières de l'image puis les lignes régulières. Cela permet de disposer d'un taux de rafraîchissement plus rapide, car il y a moins d'informations à traiter à chaque analyse. Toutefois, l'entrelacement peut causer des fluctuations ou les changements dans la moitié des lignes de l'image peuvent être remarqués.
En direct	Disponibilité des volets/onglets de direct, des boutons de recouvrement et de lecture de la caméra, des cadres de sélection et du module d'extension MIP associé au direct.
Lecture	Disponibilité des onglets/volets de relecture, de l'agencement des rapports d'impression, de la relecture indépendante, des signets, des cadres de sélection et des modules d'extension MIP associés à la lecture.

Onglet	Description
Configuration	Disponibilité de la configuration générale/des volets/boutons, du module d'extension MIP associé à la configuration et des droits de modification d'une carte et de la modification de la zone tampon de vidéo en direct.
Exportations	Les chemins d'accès, les masques de confidentialité, les formats d'images et de vidéos et ce qu'il faut inclure lors de leur exportation, les formats d'exportation pour XProtect Smart Client – Player et bien plus encore.
Chronologie	S'il faut inclure l'audio ou non, la visibilité de l'indication de l'heure et du mouvement et enfin, comment traiter les écarts de lecture.
Intégration du	Sélectionnez si les notifications de demande d'accès doivent apparaître sur l'écran XProtect Smart Client quand elles sont déclenchées par des événements.
Plan intelligent	Saisissez une clé pour un API Bing Maps ou une clé privée et un ID de client pour l'API Google Static Maps. Vous pouvez également préciser à quelle fréquence vous voulez que le système supprime les copies des plans sur votre ordinateur. Pour aider XProtect Smart Client à afficher le Plan intelligent, le client enregistre une copie du plan dans le cache de votre ordinateur. Avec le temps ceci pourrait ralentir votre ordinateur.

Profils Management Client

À propos des profils Management Client

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

Les profils Management Client permettent aux administrateurs de systèmes de modifier l'interface utilisateur Management Client pour d'autres utilisateurs. Associez des profils Management Client à des rôles pour limiter l'interface utilisateur afin de représenter les fonctions disponibles pour chaque rôle d'administrateur.

Pour associer un rôle à un profil Management Client, voir l'onglet Info (voir "Onglet Info (rôles)" á la page 219) des paramètres de rôles. Veuillez noter que les profils Management Client ne traitent que la représentation visuelle des fonctions du système, et non l'accès à celles-ci. Pour limiter l'accès global d'un rôle aux fonctions du système, consultez l'onglet Sécurité Globale (voir "Onglet Sécurité globale (rôles)" á la page 221) des paramètres de rôles.

Vous pouvez modifier les paramètres relatifs à la visibilité de tous les éléments Management Client. Par défaut, le profil Management Client peut voir toutes les fonctions du Management Client.

- Pour limiter la visibilité d'une fonction, décochez les cases correspondant à la fonction pertinente afin de supprimer la représentation visuelle de la fonction dans le Management Client pour tout utilisateur de Management Client ayant un rôle associé à ce profil Management Client.

Outre le rôle intégré d'administrateur, seuls les utilisateurs associés à un rôle bénéficiant des permissions **Gérer la sécurité** pour le serveur de gestion dans l'onglet **Sécurité globale**, peuvent ajouter, modifier et supprimer des profils Management Client.

Ajouter et configurer un profil Management Client

Si vous ne souhaitez pas utiliser le profil par défaut, vous pouvez créer un profil Management Client avant de pouvoir le configurer.

1. Faites un clic droit sur **Profils Management Client**.
2. Sélectionnez **Ajouter profil Management Client**.
3. Dans la boîte de dialogue **Ajouter profil Management Client**, saisissez le nom et la description du nouveau profil, puis cliquez sur **OK**.
4. Dans le volet **Vue d'ensemble**, cliquez sur le profil que vous venez tout juste de créer pour le configurer.
5. Dans l'onglet **Profil**, sélectionnez ou effacez la fonction du profil Management Client.

Copier un profil Management Client

Si vous possédez un profil Management Client avec des paramètres ou des droits compliqués et avez besoin d'un profil semblable, il peut s'avérer plus simple de copier un profil déjà existant et d'apporter des petits ajustements à la copie plutôt que de créer un tout nouveau profil.

1. Cliquez sur **Profil Management Client,** faites un clic droit sur le profil dans le volet **Vue d'ensemble**, sélectionnez **Copier profil Management Client**.
2. Dans la boîte de dialogue qui s'ouvre, donnez au profil copié un nouveau nom et une description uniques. Cliquez sur **OK**.
3. Dans le volet **Vue d'ensemble**, cliquez sur le profil et allez dans l'onglet **Info** ou dans l'onglet **Profil** pour configurer le profil.

Propriétés du profil Management Client

Onglet Info (Profils Management Client)

Dans l'onglet **Info**, vous pouvez configurer les éléments suivants pour les profils Management Client :

Composant	Exigences
Nom	Saisissez un nom pour le profil Management Client.
Priorité	Utilisez les flèches haut et bas pour accorder une priorité au profil Management Client.
Description	Saisissez une description pour le profil. Cette option est facultative.
Rôles utilisant le profil Management Client	Ce champ affiche les rôles que vous avez associés au profil Management Client. Vous ne pouvez pas modifier ce champ.

Onglet Profil (Profils Management Client)

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

Dans l'onglet **Profil**, vous pouvez activer ou désactiver la visibilité des éléments suivants à partir de l'interface utilisateur Management Client :

Navigation

Dans cette rubrique, décidez si un utilisateur administrateur associé au profil Management Client est autorisé à voir les diverses fonctions et fonctionnalités situées dans le volet **Navigation**.

Élément de navigation	Description
Bases	Permet à l'utilisateur administrateur associé au profil Management Client de voir les **Informations sur les licences** et les **informations sur le site**.
Services de connexion à distance	Permet à l'utilisateur administrateur associé au profil Management Client de voir la **Connexion** à la **Caméra Axis One-click**.
Serveurs	Permet à l'utilisateur administrateur associé au profil Management Client de voir les **Serveurs d'enregistrement** et les **Serveurs de redondance**.
Périphériques	Permet à l'utilisateur administrateur associé au profil Management Client de voir les **Caméras**, **Microphones**, **Haut-parleurs**, **Métadonnées**, **Entrée** et **Sortie**.
Client	Permet à l'utilisateur administrateur associé au profil Management Client de voir les **Smart Wall**, **Groupes de vues**, **Profils Smart Client**, **Profils Management Client** et **Matrix**.
Règles et évènements	Permet à l'utilisateur administrateur associé au profil Management Client de voir les **Règles**, **Profils de temps**, **Profils de notification** , **Événements définis par les utilisateurs**, **Événements analytiques** et **Événements génériques**.
Sécurité	Permet à l'utilisateur administrateur associé au profil Management Client de voir les **Rôles** et les **Utilisateurs basiques**.
Tableau de bord système	Permet à l'utilisateur administrateur associé au profil Management Client de voir le **Moniteur système**, les **Seuils du moniteur système**, le **Verrouillage des preuves**, les **Tâches en cours** et les **Rapports de configuration**.
Journaux des serveurs	Permet à l'utilisateur administrateur associé au profil Management Client de voir le **Journal système**, le **Journal d'audit**, et le **Journal de règles**.
Intégration du	Permet à l'utilisateur administrateur associé au profil Management Client de voir les fonctions de **Contrôle d'accès**, si vous avez ajouté des modules d'intégration ou d'extension au système de contrôle d'accès dans votre système.

Détails

Dans cette rubrique, décidez si un utilisateur administrateur associé au profil Management Client est autorisé à voir les divers onglets correspondant à un canal de périphérique spécifique, comme par exemple l'onglet **Paramètres** ou l'onglet **Enregistrement** pour les caméras.

Canal du périphérique	Description
Caméras	Permet à l'utilisateur administrateur associé au profil Management Client de voir le une partie ou l'intégralité des paramètres et onglets associés aux caméras.
Microphones	Permet à l'utilisateur administrateur associé au profil Management Client de voir le une partie ou l'intégralité des paramètres et onglets associés aux microphones.
Haut-parleurs	Permet à l'utilisateur administrateur associé au profil Management Client de voir le une partie ou l'intégralité des paramètres et onglets associés aux haut-parleurs.
Métadonnées	Permet à l'utilisateur administrateur associé au profil Management Client de voir le une partie ou l'intégralité des paramètres et onglets associés aux métadonnées.
Entrées	Permet à l'utilisateur administrateur associé au profil Management Client de voir le une partie ou l'intégralité des paramètres et onglets associés aux entrées.
Sortie	Permet à l'utilisateur administrateur associé au profil Management Client de voir le une partie ou l'intégralité des paramètres et onglets associés aux sorties.

Menu Outils

Dans cette rubrique, décidez si un utilisateur administrateur associé au profil Management Client est autorisé à voir les éléments faisant partie du menu **Outils**.

Option de menu Outil	Description
Services enregistrés	Permet à l'utilisateur administrateur associé au profil Management Client de voir les **Services enregistrés**.
Rôles effectifs	Permet à l'utilisateur administrateur associé au profil Management Client de voir les **Rôles effectifs**.
Options	Permet à l'utilisateur administrateur associé au profil Management Client de voir les **Options**.
Serveurs Enterprise	Permet à l'utilisateur administrateur associé au profil Management Client de voir les **Serveurs Enterprise**.

Sites fédérés

Dans cette rubrique, décidez si un utilisateur administrateur associé au profil Management Client est autorisé à voir le volet de **Hiérarchie des sites fédérés**.

Matrix

À propos de Matrix

Avec Matrix, vous pouvez envoyer une vidéo d'une caméra au choix sur un réseau opérant votre système aux destinataires Matrix. Un destinataire Matrix est un ordinateur capable d'afficher une vidéo déclenchée par Matrix. Il existe deux types de destinataires Matrix :

- Ordinateur exécutant une application Matrix dédiée et
- Ordinateur exécutant XProtect Smart Client

Afin de consulter la liste des destinataires Matrix configurés dans le Management Client, développez **Client** dans le volet **Navigation sur le site**, puis sélectionnez **Matrix.** Une liste des configurations Matrix est affichée dans le volet **Propriétés**.

Chaque destinataire Matrix, qu'il s'agisse d'un ordinateur avec Matrix Monitor ou XProtect Smart Client, doit être configuré en vue de recevoir la vidéo déclenchée par Matrix. Consultez la documentation Matrix Monitor et XProtect Smart Client pour de plus amples informations.

Ajouter des destinataires Matrix

Pour ajouter un destinataire Matrix existant (à savoir une installation Matrix Monitor ou XProtect Smart Client existante) par le biais de Management Client :

1. Agrandissez **Clients**, puis sélectionnez **Matrix**.
2. Faites un clic droit sur **Configurations Matrix** et sélectionnez **Ajouter Matrix**.
3. Remplissez les champs de la boîte de dialogue **Ajouter Matrix**.
4. Dans le champ **Adresse**, saisissez l'adresse IP ou le nom d'hôte du destinataire Matrix souhaité.
5. Dans le champ **Port**, saisissez le numéro du port employé par l'installation du destinataire Matrix. Vous trouverez le numéro du port et le mot de passe de la façon suivante : Dans le cas d'une application Matrix Monitor, allez dans la boîte de dialogue **Configuration** de Matrix Monitor. Pour XProtect Smart Client, reportez-vous aux documents séparés concernant XProtect Smart Client.
6. Cliquez sur **OK**.

Vous pouvez maintenant utiliser le destinataire Matrix dans les règles.

Remarque : Votre système ne vérifie pas si le numéro de port ou le mot de passe fourni est correct ou si le numéro de port, mot de passe ou type précisé correspond au destinataire Matrix réel. Veillez à saisir les informations correctes.

Définir les règles d'envoi de vidéos aux destinataires Matrix

Pour envoyer une vidéo aux destinataires Matrix vous devez inclure le destinataire Matrix dans une règle qui déclenche la transmission vidéo au destinataire Matrix associé. Pour cela :

1. Dans le volet **Navigation du site**, agrandissez **Règles et événements** > **Règles**. Faites un clic droit sur **Règles** pour ouvrir l'assistant **Gérer la règle**. Dans la première étape, sélectionnez un type de règle et dans la deuxième étape, une condition.

2. Dans l'étape 3 de **Gérer la règle** (**Étape 3 : Actions**), sélectionnez **Configurer Matrix pour consulter l'action <devices>**.
3. Cliquez sur le lien Matrix dans la description initiale de règle.
4. Dans la boîte de dialogue **Sélectionner configuration Matrix**, sélectionnez le destinataire Matrix pertinent et cliquez sur **OK**.
5. Cliquez sur le lien des **périphériques** dans la description de règle initiale et définissez à partir de quelle caméra vous souhaitez envoyer une vidéo au destinataire Matrix, puis cliquez sur **OK** pour confirmer votre sélection.
6. Cliquez sur **Finir** si la règle est complète ou définissez, le cas échéant, des actions supplémentaires et/ou une action d'arrêt.

Si vous supprimez un destinataire Matrix, toute règle qui inclut le destinataire Matrix arrêtera de fonctionner.

Envoyer la même vidéo à plusieurs vues XProtect Smart Client

Si le destinataire Matrix est XProtect Smart Client, vous pouvez envoyer la même vidéo aux positions Matrix dans plusieurs vues de XProtect Smart Client, à condition que les positions de vues de Matrix partagent les mêmes numéro de port et mot de passe.

1. Dans XProtect Smart Client, créez les vues pertinentes et les positions Matrix qui partagent les mêmes numéro de port et mot de passe.
2. Dans le Management Client, ajoutez le XProtect Smart Client pertinent comme destinataire Matrix.
3. Vous pouvez inclure le destinataire Matrix dans une règle.

Règles et événements

À propos des règles et événements

Les **règles** sont un élément central dans votre système. Les règles déterminent des paramètres très importants tels que le moment où une caméra doit enregistrer, où les caméras PTZ doivent patrouiller, quand les notifications doivent être envoyées, etc.

Exemple : Une règle qui précise qu'une caméra particulière doit commencer à enregistrer lorsqu'elle détecte un mouvement.

Les **événements** sont des éléments centraux lorsque vous utilisez l'assistant **Gérer la règle**. Dans l'assistant, les événements sont principalement utilisés pour déclencher des actions**.** Vous créez par

exemple une règle qui précise que si **l'événement** mouvement est détecté, le système de surveillance lance l'**action** qui consiste à enregistrer une vidéo à partir d'une caméra spécifique.

Deux types de conditions peuvent déclencher des règles :

Nom	Description
Événements	Lorsque des événements se produisent sur le système de surveillance (par exemple lorsque le mouvement est détecté, quand le système reçoit une entrée de détecteurs externes).
Heure	Quand vous saisissez des périodes précises de temps (par exemple) : `Jeudi 16 août 2007 de 7 h 00 à 7 h 59` ou `tous les samedis et dimanches.`

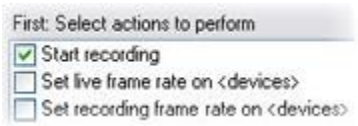
Vous pouvez travailler avec les éléments suivants sous **Règles et événements** :

- **Règles :** Les règles sont un élément central dans le système. Le comportement de votre système de surveillance est déterminé en grande partie par des règles. Lorsque vous créez une règle, vous pouvez travailler avec tous types d'événements.
- **Profils de temps :** Les profils de temps sont des périodes de temps définies dans le Management Client. Ils peuvent être utilisés lors de la création de règles dans le Management Client, par exemple lors de la création d'une règle spécifiant qu'une certaine action doit se dérouler dans un certain profil de temps.
- **Profils de notification :** Vous pouvez utiliser les profils de notification pour configurer des notifications par e-mail prêtes à l'emploi, qui peuvent être automatiquement déclenchées par une règle, par exemple lorsqu'un événement particulier se produit.
- **Événements définis par l'utilisateur :** Les événements définis par l'utilisateur sont des événements personnalisés qui font qu'il est possible pour les utilisateurs de déclencher manuellement des événements dans le système ou bien de réagir aux entrées du système.
- **Événements analytiques** : Les événements analytiques sont des données reçues de la part de fournisseurs d'analyse de contenu vidéo (VCA) tiers externes. Vous pouvez utiliser les événements analytiques comme base pour les alarmes.
- **Événements génériques :** Les événements génériques vous permettent de déclencher des actions sur le serveur d'événements XProtect en envoyant des chaînes simples via le réseau IP à votre système.

Voir Vue d'ensemble des événements (á la page 184) pour obtenir une liste des événements.

À propos des actions et des actions d'arrêt

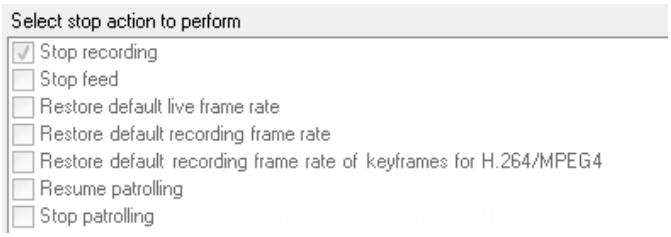
Lorsque vous ajoutez des règles (voir "Ajouter une règle" á la page 195) dans l'assistant **Gérer la règle**, vous pouvez choisir parmi différentes actions :



Exemple : Sélectionner une action

Certaines actions exigent une action d'arrêt. **Exemple** : Si vous sélectionnez l'action de **démarrage d'un enregistrement**, il commence et potentiellement continue indéfiniment. En conséquence, l'action de **démarrage d'un enregistrement** a une action d'arrêt obligatoire appelée **Arrêter d'enregistrer**.

L'assistant **Gérer la règle** s'assure que vous spécifiez des actions d'arrêt si nécessaire :



Sélection des actions d'arrêt. Dans l'exemple, remarquez l'action d'arrêt obligatoire (sélectionnée, grisée), les actions non pertinentes d'arrêt (grisées) et les actions d'arrêt en option (sélectionnables).

Chaque type d'action de votre système XProtect est décrit. Vous pouvez disposer de davantage d'actions si votre installation utilise des produits d'extension ou des plug-ins spécifiques au fournisseur. Pour chaque type d'action, les informations d'action d'arrêt sont également indiquées le cas échéant :

Action	Description
Démarrer l'enregistrement sur <devices>	Commencez l'enregistrement et la sauvegarde des données dans la base de données des périphériques choisis. En sélectionnant ce type d'action, l'assistant **Gérer la règle** vous invite à indiquer : À quel moment l'enregistrement doit commencer. Cela se produit immédiatement ou un certain nombre de secondes avant l'événement déclencheur/début de l'intervalle de temps de déclenchement et sur quels appareils l'action doit avoir lieu. Ce type d'action exige que vous ayez activé l'enregistrement sur les périphériques auxquels l'action est liée. Vous pouvez uniquement enregistrer les données précédant un intervalle de temps ou un événement si vous avez activé le pré-tampon pour les dispositifs concernés. L'enregistrement et la définition des paramètres de la mise en mémoire-tampon préalable d'un périphérique sont activés sur l'onglet **Enregistrement**. **Action d'arrêt requise** : Ce type d'action nécessite une ou plusieurs actions d'arrêt. Dans l'une des étapes suivantes, l'assistant vous invite automatiquement à spécifier l'action d'arrêt : **Arrêter l'enregistrement**. Sans cette action d'arrêt, un enregistrement pourrait potentiellement continuer indéfiniment. Vous pouvez aussi préciser d'autres actions d'arrêt.
Démarrer le flux sur <devices>	Lancer le flux de données des périphériques vers le système. Lorsque le flux à partir d'un périphérique a commencé, les données sont transférées depuis le périphérique jusqu'au système, auquel cas la visualisation et l'enregistrement sont possible selon le type de données. Lorsque vous sélectionnez ce type d'action, l'assistant **Gérer la règle** vous invite à indiquer sur quels périphériques les flux doivent être démarrés. Votre système dispose d'une règle par défaut qui assure que les flux soient toujours démarrés sur toutes les caméras. **Action d'arrêt requise** : Ce type d'action nécessite une ou plusieurs actions d'arrêt. Dans l'une des étapes suivantes, l'assistant vous invite

Action	Description
	automatiquement à spécifier l'action d'arrêt : **Arrêter un flux**. Vous pouvez également indiquer d'autres actions d'arrêt. Notez qu'utiliser l'action d'arrêt obligatoire **Arrêter un flux** pour arrêter un flux provenant d'un périphérique signifie que les données ne sont plus transférées depuis le périphérique jusqu'au système, auquel cas la visualisation et l'enregistrement de la vidéo, par exemple, ne sont plus possibles. Cependant, un périphérique sur lequel vous avez arrêté l'alimentation peut toujours communiquer avec le serveur d'enregistrement, et vous pouvez relancer l'alimentation automatiquement par le biais d'une règle, contrairement au moment où vous avez désactivé manuellement l'appareil. **Important :** Bien que ce type d'action donne accès aux flux de données de périphériques sélectionnés, il ne garantit pas que la vidéo soit enregistrée, car vous devez spécifier les paramètres d'enregistrement séparément.
Régler <Smart Wall> sur <preset>	Définit le XProtect Smart Wall à un préréglage sélectionné. Spécifier le préréglage sur l'onglet **vue prédéfinie Smart Wall**. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Régler le <monitor> du <Smart Wall> pour afficher des <caméras>	Règle un moniteur XProtect Smart Wall spécifique de façon à ce qu'il affiche la vidéo de caméras sélectionnées en direct sur ce site ou sur tout site enfant configuré dans Milestone Federated Architecture. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Régler le <monitor> du Smart Wall pour afficher le texte <messages>	Réglez un moniteur XProtect Smart Wall spécifique de sorte qu'il affiche un message défini par l'utilisateur d'une longueur maximale de 200 caractères. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Supprimer caméras du moniteur <monitor> <Smart Wall>	Arrête d'afficher la vidéo d'une caméra spécifique. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.

Action	Description
Définir la fluidité d'image en direct sur <devices>	Définit une fluidité d'image précise à utiliser lorsque le système affiche la vidéo en direct provenant de caméras choisies, qui remplace la fluidité d'image par défaut. Indiquez cela sur l'onglet **Paramètres**. Lors vous sélectionnez ce type d'action, l'assistant **Gérer la règle** vous invite à indiquer sur quelle fluidité d'image définir et sur quels périphériques. Vérifiez toujours que la fluidité d'image que vous spécifiez est disponible sur les caméras concernées. **Action d'arrêt requise** : Ce type d'action nécessite une ou plusieurs actions d'arrêt. Dans l'une des étapes suivantes, l'assistant vous invite automatiquement à spécifier l'action d'arrêt : **Rétablir la fluidité d'images en direct par défaut**. Sans cette action d'arrêt, il est possible que la fluidité d'image par défaut ne soit jamais restaurée. Vous pouvez aussi préciser d'autres actions d'arrêt.
Définir la fluidité d'image à l'enregistrement sur <devices>	Définit une fluidité d'image précise à utiliser lorsque le système sauvegarde la vidéo enregistrée provenant de caméras choisies dans la base de données, au lieu de la fluidité d'image d'enregistrement par défaut. Lors de la sélection de ce type d'action, l'assistant **Gérer la règle** vous invite à indiquer les fluidités d'image d'enregistrement à définir et sur quels caméras. Vous pouvez uniquement spécifier une fluidité d'image d'enregistrement pour JPEG, un codec vidéo avec lequel chaque image est compressée séparément dans une image JPEG. Ce type d'action exige également que l'enregistrement ait été activé sur les caméras auxquelles l'action est liée. Vous activez l'enregistrement d'une caméra sur l'onglet **Enregistrer**. La fluidité d'image maximum que vous pouvez préciser dépend des types de caméras concernés et de leur résolution d'image sélectionnée. **Action d'arrêt requise** : Ce type d'action nécessite une ou plusieurs actions d'arrêt. Dans l'une des étapes suivantes, l'assistant vous invite automatiquement à spécifier l'action d'arrêt : **Rétablir la fluidité d'images enregistrées par défaut**. Sans cette action d'arrêt, il est possible que la fluidité d'image d'enregistrement par défaut ne soit jamais restaurée. Vous pouvez aussi préciser d'autres actions d'arrêt.
Établir la fluidité d'images enregistrées pour tous les cadres pour MPEG-4/H.264/H.265 sur <devices>	Définit la fluidité d'images pour enregistrer toutes les images lorsque le système enregistre la vidéo enregistrée par les caméras sélectionnées dans la base de données, au lieu des images clés seulement. Activer les images clés d'enregistrement uniquement sur l'onglet **Enregistrement**. Lorsque vous sélectionnez ce type d'action, l'assistant **Gérer la règle** vous invite à choisir sur quels périphériques l'action doit être appliquée. Vous pouvez activer l'enregistrement des images-clés pour MPEG-4/H.264/H.265. Ce type d'action exige également que l'enregistrement ait été activé sur les caméras auxquelles l'action est liée. Vous activez l'enregistrement d'une caméra sur l'onglet **Enregistrer**. **Action d'arrêt requise** : Ce type d'action nécessite une ou plusieurs actions d'arrêt. Dans l'une des étapes suivantes, l'assistant vous invite automatiquement à spécifier l'action d'arrêt : **Rétablir la fluidité d'image à l'enregistrement par défaut des**

Action	Description
	images-clés pour MPEG-4/H.264/H.265 Sans cette action d'arrêt, il est possible que les paramètres par défaut ne soient jamais restaurés. Vous pouvez aussi préciser d'autres actions d'arrêt.
Début de la patrouille sur <device> à l'aide de <profile> avec priorité PTZ <priority>	Démarrer la patrouille PTZ selon un profil de patrouille particulier pour une caméra PTZ particulière avec une priorité particulière. Il s'agit de la définition exacte de la manière dont une patrouille doit avoir lieu, y compris la séquence des positions prédéfinies, les paramètres horaires, etc. Si vous avez actualisé votre système à partir d'une version plus ancienne du système, les anciennes valeurs (**très bas**, **bas**, **moyen**, **élevé** et **très élevé**) ont été traduites comme suit : • Très bas = 1000 • Bas = 2000 • Moyen = 3000 • Élevé = 4000 • Très élevé = 5000 Lorsque vous sélectionnez ce type d'action, l'assistant **Gérer la règle** vous invite à sélectionner un profil de patrouille. Vous pouvez uniquement sélectionner un profil de patrouille sur un périphérique et vous ne pouvez pas sélectionner plusieurs profils de patrouille. Ce type d'action exige que les dispositifs auxquels l'action est liée soient des dispositifs PTZ. Vous devez définir au moins un profil de patrouille pour le périphérique (ou les périphériques). Vous définissez les profils de patrouille pour une caméra PTZ sur l'onglet **Patrouille**. **Action d'arrêt requise** : Ce type d'action nécessite une ou plusieurs actions d'arrêt. Dans l'une des étapes suivantes, l'assistant vous invite automatiquement à spécifier l'action d'arrêt : **Arrêter la patrouille** Sans cette action d'arrêt, patrouiller pourrait éventuellement ne jamais s'arrêter. Vous pouvez également indiquer d'autres actions d'arrêt.
Mettre la patrouille en pause sur <devices>	Met la patrouille PTZ en pause. Lors de la sélection de ce type d'action, l'assistant **Gérer la règle** vous invite à indiquer sur quels périphériques la patrouille doit être mise sur pause. Ce type d'action exige que les dispositifs auxquels l'action est liée soient des dispositifs PTZ. Vous devez définir au moins un profil de patrouille pour le périphérique (ou les périphériques). Vous définissez les profils de patrouille pour une caméra PTZ sur l'onglet **Patrouille**. **Action d'arrêt requise** : Ce type d'action nécessite une ou plusieurs

Action	Description
	actions d'arrêt. Dans l'une des étapes suivantes, l'assistant vous invite automatiquement à spécifier l'action d'arrêt : **Réactiver la patrouille** Sans cette action d'arrêt, patrouiller pourrait éventuellement se mettre sur pause indéfiniment. Vous pouvez aussi préciser d'autres actions d'arrêt.
Adopter la position <preset> pour <device> avec la priorité PTZ <priority>	Déplace une caméra spécifique dans une position prédéfinie particulière, toutefois toujours conformément à la priorité. Lors de la sélection de ce type d'action, l'assistant **Gérer la règle** vous invite à sélectionner une position prédéfinie. Une seule position prédéfinie sur une caméra peut être sélectionnée. Il n'est pas possible de sélectionner plusieurs positions préréglées. Ce type d'action exige que les dispositifs auxquels l'action est liée soient des dispositifs PTZ. Cette action nécessite que vous ayez défini au moins une position prédéfinie pour ces dispositifs. Vous définissez des positions prédéfinies pour une caméra PTZ sur l'onglet **Positions prédéfinies**. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Adopter le paramètre prédéfini pour <devices> avec la priorité PTZ <priority>	Déplacer une caméra ou plusieurs caméras spécifiques sur leurs positions prédéfinies par défaut respectives, toutefois, toujours conformément à la priorité. Lorsque vous sélectionnez ce type d'action, l'assistant **Gérer la règle** vous invite à choisir sur quels périphériques l'action doit être appliquée. Ce type d'action exige que les dispositifs auxquels l'action est liée soient des dispositifs PTZ. Cette action nécessite que vous ayez défini au moins une position prédéfinie pour ces dispositifs. Vous définissez des positions prédéfinies pour une caméra PTZ sur l'onglet **Positions prédéfinies**. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Définir la sortie du périphérique sur <state>	Définit une sortie sur un périphérique sur un état particulier (activé ou désactivé). Lors de la sélection de ce type d'action, l'assistant **Gérer la règle** vous invitera à indiquer l'état à définir et sur quels périphériques. Ce type d'action exige que les périphériques auxquels l'action est liée aient chacun au moins une unité de sortie externe connectée à un port de sortie. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Créer le signet sur <device>	Crée un signet sur le flux en direct ou les enregistrements à partir d'un périphérique choisi. Un signet fait qu'il est aisé de retracer un certain événement ou une certaine période de temps. Les paramètres du signet sont contrôlés à partir de la boîte de dialogue **Options**. Lorsque vous sélectionnez ce type d'action, l'assistant **Gérer la règle** vous invite à préciser les détails du signet et à sélectionner les périphériques. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.

Action	Description
Envoyer la notification à <profile>	Envoie une notification par l'intermédiaire d'un profil de notification particulier. Lorsque vous sélectionnez ce type d'action, l'assistant **Gérer la règle** vous invite à choisir un profil de notification et à partir de quels périphériques inclure les images pré-alarme. Vous pouvez uniquement sélectionner un profil de notification et vous ne pouvez pas sélectionner plusieurs profils de notification. Notez qu'un seul profil de notification peut contenir plusieurs destinataires. Vous pouvez également créer d'autres règles pour le même événement et envoyer différentes notifications à chacun des profils de notification. Vous pouvez copier et réutiliser le contenu des règles par un clic droit sur une règle dans la liste des **Règles**. Ce type d'action nécessite que vous ayez défini au moins un profil de notification. Les images de pré-alarme sont uniquement incluses si vous avez activé l'option **Inclure les images** pour le profil de notification correspondant. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Créer une entrée <log entry>	Génère une entrée dans le journal des règles. Lors de la sélection de ce type d'action, l'assistant **Gérer la règle** vous invite à préciser un texte pour une entrée du journal. Lorsque vous indiquez le texte du journal, vous pouvez insérer rapidement des variables telles que **$DeviceName$, $EventName$**, dans le message de journalisation. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Démarrer le module d'extension sur <devices>	Lance un ou plusieurs modules d'extension. Lorsque vous sélectionnez ce type d'action, l'assistant **Gérer la règle** vous invite à sélectionner les modules d'extension nécessaires et sur quels périphériques lancer les modules d'extension. Ce type d'action exige que vous ayez au moins un ou plusieurs modules d'extension installés sur votre système. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Arrêter le module d'extension sur <devices>	Arrête un ou plusieurs modules d'extension. Lors de la sélection de ce type d'action, l'assistant **Gérer la règle** vous invitera à sélectionner les modules d'extension nécessaires et sur quels périphériques arrêter les modules d'extension. Ce type d'action exige que vous ayez au moins un ou plusieurs modules d'extension installés sur votre système. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.

Action	Description
Appliquer les nouveaux paramètres sur <devices>	Modifie les paramètres des périphériques sur un ou plusieurs périphériques. Lorsque vous sélectionnez ce type d'action, l'assistant **Gérer la règle** vous invite à sélectionner les périphériques concernés et vous pouvez définir les paramètres pertinents sur les périphériques que vous avez spécifiés. Si vous définissez des paramètres pour plus d'un périphérique, vous pouvez uniquement changer les paramètres qui sont disponibles pour tous les périphériques précisés. **Exemple** : Vous spécifiez que l'action doit être liée au Périphérique 1 et au Périphérique 2. Le Périphérique 1 a les paramètres A, B et C et le Périphérique 2 a les paramètres B, C et D. Dans ce cas, vous pouvez uniquement changer les paramètres disponibles pour les deux périphériques, à savoir les paramètres B et C. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Définir Matrix pour afficher <devices>	Fait apparaître des vidéos à partir des caméras choisies sur un ordinateur en mesure d'afficher une vidéo déclenchée par Matrix tel qu'un ordinateur sur lequel vous avez installé soit XProtect Smart Client, soit l'application Matrix Monitor. Lorsque vous sélectionnez ce type d'action, l'assistant **Gérer la règle** vous invite à sélectionner un destinataire Matrix et un ou plusieurs périphériques à partir desquels afficher une vidéo sur le destinataire Matrix choisi. Ce type d'action vous permet de sélectionner uniquement un seul destinataire Matrix à la fois. Si vous souhaitez que des vidéos provenant de périphériques sélectionnés apparaissent sur plus d'un destinataire Matrix, vous devriez créer une règle pour chaque destinataire Matrix requis ou utiliser la fonction XProtect Smart Wall. Le fait d'effectuer un clic droit sur une règle dans la liste des **Règles** vous permet de copier et de réutiliser le contenu des règles. De cette manière, vous pouvez éviter d'avoir à créer entièrement des règles presque identiques. En tant que partie de la configuration des destinataires Matrix eux-mêmes, les utilisateurs doivent spécifier le numéro de port et le mot de passe requis pour la communication avec le Matrix Veillez à ce que les utilisateurs aient accès à cette information. Généralement, les utilisateurs doivent aussi définir les adresses IP des hôtes autorisés à partir desquels les commandes relatives à l'affichage de la vidéo déclenchée par Matrix sont acceptées. Dans ce cas, les utilisateurs doivent également connaître l'adresse IP du serveur de gestion (ou tout autre routeur ou pare-feu utilisé.
Envoyer un trap SNMP	Génère un petit message qui journalise les événements sur les périphériques sélectionnés. Le texte des traps SNMP est auto-généré et ne peut pas être personnalisé. Il peut contenir généralement le type et le nom de source du périphérique sur lequel l'événement s'est produit. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.

Action	Description
Récupérer et stocker les enregistrements à distance à partir des <devices>	Récupère et stocke les enregistrements à distance provenant des périphériques sélectionnés (prenant en charge les enregistrements locaux) au cours d'une période spécifiée et après l'événement déclencheur. Veuillez noter que cette règle est indépendante du paramètre **Rappeler les enregistrements à distance automatiquement lorsque la connexion est rétablie**. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Récupérer et stocker les enregistrements à distance entre <start and end time> sur <devices>	Récupère et stocke les enregistrements à distance de périphériques choisis (qui prennent en charge l'enregistrement local) au cours d'une période spécifiée. Veuillez noter que cette règle est indépendante du paramètre **Rappeler les enregistrements à distance automatiquement lorsque la connexion est rétablie**. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Enregistrer une image jointe	Veille à ce que lorsqu'une image est reçue de l'événement Images reçues (envoyées via e-mail SMTP à partir d'une caméra), elle est sauvegardée pour usage ultérieur. À l'avenir, d'autres événements peuvent éventuellement déclencher cette action. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Activer l'archivage sur <archives>	Lance l'archivage d'une ou de plusieurs archives. Lors de la sélection de ce type d'action, l'assistant **Gérer la règle** vous invite à sélectionner les archives concernées. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Déclencher <user-defined event> sur <site>	Surtout pertinent au sein de Milestone Federated Architecture mais vous pouvez également l'utiliser dans la configuration d'un site unique. Utilisez la règle pour déclencher un événement défini par utilisateur sur un site, normalement un site à distance au sein d'une hiérarchie fédérée. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Envoyer au Customer dashboard (Tableau de bord client)	Envoie les informations système pertinentes au Customer dashboard (Tableau de bord client) Milestone. Vous ne pouvez envoyer des informations système au Customer Dashboard que si vous avez activé le système pour accéder au Customer dashboard dans l'onglet Customer dashboard (voir "Onglet Customer dashboard (Tableau de bord client)" á la page 274)

Action	Description
Afficher la <notification de demande d'accès>	Laisse les notifications de demande d'accès apparaître sur l'écran de XProtect Smart Client lorsque les critères pour les événements déclencheurs sont remplis. Milestone recommande que vous utilisiez des événements de contrôle d'accès en tant qu'événements déclencheurs pour cette action, car les notifications de demande d'accès sont généralement configurées pour une utilisation sur des commandes et caméras de contrôle d'accès connexes Ce type d'action exige que vous ayez au moins un plug-in de contrôle d'accès installé sur votre système. **Aucune action d'arrêt obligatoire** : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.

Vue d'ensemble des événements

Lorsque vous ajoutez une règle basée sur l'événement dans l'assistant **Gérer la règle**, vous pouvez effectuer une sélection entre différents types d'événements : Pour que vous puissiez avoir un bon aperçu, les événements que vous pouvez sélectionner apparaissent dans une liste établie par groupes selon s'ils sont :

Matériel :

Certains matériels peuvent créer eux-mêmes des événements, comme par exemple pour la détection du mouvement. Vous pouvez les utiliser en tant qu'événements mais vous devez les configurer sur le matériel avant de pouvoir les utiliser dans le système. Vous pourrez peut-être utiliser uniquement les événements énumérés sur certains périphériques car tous les types de caméras ne peuvent pas détecter la modification ou les changements de température.

Évènements configurables du matériel :

Les événements configurables sur les périphériques sont automatiquement importés à partir des pilotes de périphériques. Cela signifie qu'ils varient d'un matériel à l'autre et ne sont pas mentionnés ici. Les événements configurables ne sont pas déclenchés tant que vous ne les avez pas ajoutés au système et ne les avez pas configurés sur l'onglet **Événement** pour le matériel. Certains des événements configurables exigent également que vous configuriez la caméra (matériel).

Matériel - Évènements prédéfinis :

Événement	Description
Erreur de communication (Matériel)	Se produit lors de la perte d'une connexion à un matériel.
Communication démarrée (Matériel)	Se produit lorsqu'une tentative de communication avec un matériel réussit.
Communication arrêtée (Matériel)	Se produit lorsqu'une tentative d'arrêt de la communication avec un matériel réussit.

Périphériques - Évènements configurables :

Les événements configurables sur les périphériques sont automatiquement importés à partir des pilotes de périphériques. Cela signifie qu'ils varient d'un périphérique à l'autre et ne sont pas mentionnés ici. Les événements configurables ne sont pas déclenchés tant que vous ne les avez pas ajoutés au système et ne les avez pas configurés sur l'onglet **Événement** sur un périphérique.

Périphériques - Évènements prédéfinis :

Événement	Description
Référence de signet demandée	Se produit lorsqu'un signet est créé en mode direct ou lecture dans les clients. De plus, une exigence d'utilisation de la règle d'enregistrement sur signet
Erreur de communication (Périphérique)	A lieu lorsqu'une connexion à un périphérique est perdue, ou lorsqu'une tentative de communication avec un périphérique échoue.
Communication démarrée (Périphérique)	A lieu lorsqu'une tentative de communication avec un périphérique réussit.
Communication arrêtée (Périphérique)	A lieu lorsqu'une communication avec un périphérique est bien arrêtée.
Changement dans la protection de preuves	Se produit quand une preuve protégée est modifiée pour les périphériques par un utilisateur client ou via le SDK MIP.
Preuves protégées	Se produit quand une preuve protégée est créée pour les périphériques par un utilisateur client ou via le SDK MIP.
Preuves déverrouillées	Se produit quand la protection de la preuve est supprimée pour les périphériques par un utilisateur client ou via le SDK MIP.
Dépassement de la capacité d'alimentation démarré	Le dépassement de la capacité d'alimentation (dépassement de capacité multimédia) a lieu lorsqu'un serveur d'enregistrement ne peut pas traiter les données reçues aussi rapidement que l'indique la configuration et qu'il est par conséquent obligé d'ignorer certains enregistrements. Si le serveur est sain, le dépassement de la capacité d'alimentation se produit car le disque lent enregistre. Vous pouvez y remédier soit en réduisant la quantité de données écrites, soit en améliorant la performance de stockage du système. Réduit la quantité de données écrites en réduisant la fluidité d'image, la résolution ou la qualité d'image sur vos caméras, mais cela peut détériorer la qualité de l'enregistrement. Si cela ne vous intéresse pas, améliorez alors la performance de stockage de votre système en installant des pilotes supplémentaires pour partager la charge ou bien en installant des disques ou des contrôleurs plus rapides. Vous pouvez utiliser cet événement pour déclencher des actions qui vous aident à éviter le problème, par exemple, pour réduire la fluidité d'images d'enregistrement.
Dépassement de la capacité d'alimentation arrêtée	A lieu lorsque le dépassement de la capacité d'alimentation (consultez la description de l'événement **Dépassement de la capacité d'alimentation démarré**) se termine.

Événement	Description
Alimentation du Live Client demandée	A lieu lorsque des utilisateurs du client demandent un flux en direct à partir d'un périphérique. L'événement se produit à la demande, même si la demande de l'utilisateur client échoue par la suite, par exemple parce que l'utilisateur client ne possède pas les droits nécessaires pour voir le flux demandé en direct ou parce que le flux est arrêté pour une raison quelconque.
Alimentation du Live Client terminée	A lieu lorsque des utilisateurs du client ne demandent plus un flux en direct à partir d'un périphérique.
Enregistrement manuel démarré	Se produit quand un utilisateur client démarre une session d'enregistrement pour une caméra. L'événement est déclenché même si le périphérique est déjà en cours d'enregistrement via les actions de règles.
Enregistrement manuel arrêté	Se produit quand un utilisateur client arrête une session d'enregistrement pour une caméra. Si le système de règles a aussi commencé une session d'enregistrement, il continue d'enregistrer même après l'arrêt de l'enregistrement manuel.
Référence de données marquées demandée	Se produit quand la protection de la preuve est effectuée en mode lecture dans les clients ou via le MIP SDK. Un événement est créé et vous pouvez l'utiliser dans vos règles.
Mouvement démarré	A lieu lorsque le système détecte un mouvement dans la vidéo reçue des caméras. Ce type d'événement exige que la détection du mouvement du système soit activée en ce qui concerne les caméras auxquelles l'événement est lié. Outre la détection de mouvement du système, certaines caméras peuvent détecter le mouvement elles-mêmes et déclencher l'événement **Démarrage de mouvements (HW)**, mais cela dépend de la configuration du périphérique de caméra et du système. Voir **Matériel - Événements configurables** ci-dessus.
Mouvement arrêté	A lieu lorsque le mouvement n'est plus détecté dans la vidéo reçue. Consultez également la description de l'événement **Mouvement démarré**. Ce type d'événement exige que la détection du mouvement du système soit activée en ce qui concerne les caméras auxquelles l'événement est lié. Outre la détection de mouvement du système, certaines caméras peuvent détecter le mouvement elles-mêmes et déclencher l'événement Arrêt des mouvements (HW), mais cela dépend de la configuration du périphérique de caméra et du système. Voir **Matériel - Événements configurables** ci-dessus.

Événement	Description
Sortie activée	Se produit quand un port de sortie externe sur un périphérique est activé. Ce type d'événement exige qu'au moins un périphérique sur votre système prenne en charge les ports de sortie.
Sortie modifiée	Se produit quand l'état d'un port de sortie externe sur un périphérique est modifié. Ce type d'événement exige qu'au moins un périphérique sur votre système prenne en charge les ports de sortie.
Sortie désactivée	A lieu lorsqu'une unité de sortie externe connectée à un port de sortie sur un périphérique est désactivé. Ce type d'événement exige qu'au moins un périphérique sur votre système prenne en charge les ports de sortie.
Session manuelle PTZ démarrée	A lieu lorsqu'une session PTZ manuelle (à l'inverse d'une session PTZ basée sur une patrouille programmée ou automatiquement déclenchée par un événement) est déclenchée sur une caméra. Ce type d'action exige que les caméras auxquelles l'événement est lié soient des caméras PTZ.
Session manuelle PTZ arrêtée	A lieu lorsqu'une session PTZ manuelle (à l'inverse d'une session PTZ basée sur une patrouille programmée ou automatiquement déclenchée par un événement) est arrêtée sur une caméra. Ce type d'action exige que les caméras auxquelles l'événement est lié soient des caméras PTZ.
Enregistrement démarré	A lieu dès que l'enregistrement commence. Il existe un événement distinct pour le démarrage de l'enregistrement manuel.
Enregistrement arrêté	A lieu lorsque l'enregistrement est arrêté. Il existe un événement distinct pour l'arrêt de l'enregistrement manuel.
Paramètre modifié	A lieu lorsque des paramètres sur un périphérique sont correctement modifiés.
Erreur : paramètres modifiés	A lieu lorsqu'une tentative de modification des paramètres d'un périphérique échoue.

Événements externes - Événements prédéfinis :

Événement	Description
Demander le départ de l'enregistrement	Activé lorsque le démarrage des enregistrements est demandé via le MIP Software Development Kit (SDK). Au travers du kit de développement logiciel d'intégration MIP SDK, un vendeur tiers peut développer des modules d'extension personnalisés (par exemple, l'intégration à des systèmes de contrôle de l'accès externes ou d'autres services semblables) pour votre système.
Demande Arrêter l'enregistrement	Activé lorsque l'arrêt des enregistrements est demandé via le MIP SDK. Au travers du kit de développement logiciel d'intégration MIP SDK, un vendeur tiers peut développer des modules d'extension personnalisés (par exemple, l'intégration à des systèmes de contrôle de l'accès externes ou d'autres services semblables) pour votre système.

Événements externes - Événements génériques :

Les événements génériques vous permettent de déclencher des actions dans le système en envoyant des chaînes simples via le réseau IP au système. L'objectif des événements génériques est d'autoriser autant de sources externes que possible pour interagir avec le système.

Événements externes - événements définis par les utilisateurs :

Plusieurs événements personnalisés pour convenir à votre système peuvent éventuellement également être sélectionnés. Vous pouvez utiliser ces événements définis par l'utilisateur pour :

- Donner la possibilité aux utilisateurs du client de déclencher manuellement des évènements tout en visualisant une vidéo en direct dans les clients.
- D'innombrables autres objectifs. Par exemple, vous pouvez créer des événements définis par l'utilisateur qui ont lieu si un type particulier de données est reçu d'un périphérique.

  Voir À propos des événements définis par l'utilisateur (voir "À propos des évènements définis par l'utilisateur" á la page 204) pour plus d'informations.

Serveurs d'enregistrement :

Événement	Description
Archive disponible	A lieu lorsqu'une archive d'un serveur d'enregistrement est disponible après avoir été indisponible (consultez **Archive non disponible**).

Événement	Description
Archive non disponible	A lieu lorsqu'une archive pour un serveur d'enregistrement devient indisponible, par exemple la connexion avec une archive sur un volume connecté au réseau est perdue. Dans ce cas, vous ne pouvez pas archiver d'enregistrements. Vous pouvez utiliser l'événement, par exemple, pour déclencher une alarme ou un profil de notification afin qu'un e-mail de notification soit automatiquement envoyé aux personnes appropriées de votre organisation.
Archive non terminée	A lieu lorsqu'une archive d'un serveur d'enregistrement n'est pas terminée et quand le dernier archivage est fait lorsque le prochain est programmé pour commencer.
Disque de base de données saturé	A lieu lorsqu'un disque de base de données n'a plus d'espace libre. Un disque de base de données est considéré comme saturé lorsqu'il contient moins de 5 Go d'espace libre : Les plus anciennes données d'une base de données seront toujours auto-archivées (ou supprimées si aucune archive suivante n'est définie) dès qu'il y a moins de 5 Go d'espace libre. Si moins de 1 Go d'espace est disponible, les données sont supprimées, même si une archive suivante est définie. Une base de données a toujours besoin de 250 Mo d'espace libre. Si cette limite est atteinte (si les données ne sont pas supprimées assez rapidement), aucune autre donnée n'est ajoutée à la base de données tant que de l'espace n'a pas été libéré. La taille maximum réelle de votre base de données est la quantité de giga-octets que vous spécifiez, moins 5 Go.
Base de données pleine - Archivage automatique	A lieu lorsqu'une archive pour un serveur d'enregistrement est pleine et qu'elle a besoin d'un archivage automatique dans une archive de stockage.
Réparation de la base de données	A lieu lorsqu'une base de données est corrompue, auquel cas le système applique automatiquement deux méthodes différentes de réparation :
Stockage de base de données disponible	A lieu lorsque le stockage d'un serveur d'enregistrement est disponible après avoir été indisponible (consultez **Stockage de base de données non disponible** ensuite). Par exemple, vous pouvez utiliser l'événement pour lancer l'enregistrement s'il a été arrêté par l'événement **Stockage de base de données non disponible**.
Stockage de base de données non disponible	A lieu lorsque le stockage pour un serveur d'enregistrement devient indisponible, par exemple si la connexion à un stockage situé sur une unité de réseau est perdue. Dans ce cas, vous ne pouvez pas archiver d'enregistrements. Vous pouvez utiliser l'événement, par exemple, pour arrêter l'enregistrement, déclencher une alarme ou un profil de notification afin qu'un e-mail de notification soit automatiquement envoyé aux personnes appropriées de votre organisation.
Basculement commencé	A lieu lorsqu'un serveur d'enregistrement de basculement se substitue à un serveur d'enregistrement. Voir À propos des serveurs d'enregistrement de basculement (voir "À propos des serveurs d'enregistrement de redondance" á la page *95*).

Événement	Description
Basculement arrêté	A lieu lorsqu'un serveur d'enregistrement devient à nouveau disponible, et peut se substituer au serveur d'enregistrement de basculement.

Événements à partir des intégrations et des produits complémentaires :

Les événements à partir des intégrations et des produits complémentaires peuvent être utilisés dans le système de règles, par exemple :

- Les événements analytiques peuvent également être utilisés dans le système de règle.

Règles

À propos des règles

Les règles spécifient les actions à réaliser dans des conditions particulières. Exemple : Lorsqu'un mouvement est détecté (condition), une caméra doit commencer à enregistrer (action).

Voici des **exemples** de ce que vous pouvez faire avec les règles :

- Débuter et terminer un enregistrement
- Régler la fluidité d'images en direct (autre que par défaut)
- Régler la fluidité d'images enregistrées (autre que par défaut)
- Débuter et terminer une patrouille PTZ
- Mettre en pause et reprendre une patrouille PTZ
- Déplacer les caméras PTZ dans des positions spécifiques
- Activer/désactiver des sorties
- Envoyer des notifications par e-mail
- Journaliser des entrées
- Générer des événements
- Appliquer de nouveaux paramètres aux périphériques, par exemple une résolution différente sur une caméra
- Faire apparaître la vidéo dans les destinataires Matrix
- Activer et arrêter des modules d'extension
- Activer et arrêter des flux de périphériques

Le fait d'arrêter un périphérique signifie qu'aucune vidéo n'est plus transférée à partir du périphérique vers le système, auquel cas ni le visionnement en direct, ni l'enregistrement ne sont possibles. Au contraire, un périphérique sur lequel vous avez arrêté l'alimentation peut toujours communiquer avec le serveur d'enregistrement, et vous pouvez lancer l'alimentation automatiquement depuis le périphérique par le biais d'une règle, contrairement à l'arrêt manuel de l'appareil dans le Management Client.

Important : le contenu de certaines règles peut demander à ce que certaines fonctions soient activées pour les périphériques concernés. Par exemple, une règle qui précise qu'une caméra doit enregistrer, ne fonctionne pas comme souhaité si l'enregistrement n'est pas activé pour la caméra concernée. Avant de créer une règle, Milestone vous recommande donc vivement de vérifier que les périphériques impliqués sont capables de fonctionner conformément aux intentions.

À propos des règles par défaut

Votre système contient un certain nombre de règles par défaut que vous pouvez utiliser sans autre forme de configuration. Vous pouvez désactiver ou modifier les règles par défaut en fonction de vos besoins. Si vous modifiez ou désactivez les règles par défaut, votre système peut ne pas fonctionner selon vos souhaits, ni garantir que les flux vidéo ou audio arrivent automatiquement au système.

Règle par défaut	Description
Aller au préréglage en fin de PTZ	Veille à ce que les caméras PTZ se déplacent à leurs positions prédéfinies par défaut respectives après qu'elles ont été opérées manuellement. Cette règle n'est pas activée par défaut. Même lorsque la règle est activée, vous devez avoir des positions prédéfinies par défaut en ce qui concerne les caméras PTZ concernées pour que la règle fonctionne. Pour ce faire, allez dans l'onglet **Préréglages**.
Enregistrer sur signet	S'assure que la vidéo est enregistrée automatiquement lorsqu'un opérateur configure un signet dans XProtect Smart Client. Cette action n'est possible que si vous avez activé l'enregistrement des caméras concernées. Par défaut, l'enregistrement est activé. Pour cette règle, la durée d'enregistrement par défaut est fixée à trois secondes avant le positionnement du signet et 30 secondes après le positionnement du signet. Vous pouvez modifier les temps d'enregistrement par défaut dans la règle. Notez que la mise en mémoire-tampon préalable configurable dans l'onglet Enregistrement doit être identique ou supérieure à la durée de pré-enregistrement.
Enregistrer sur mouvement	Veille à ce que tant que le mouvement est détecté par les caméras, la vidéo est enregistrée, à condition que l'enregistrement soit activé pour les caméras en question. Par défaut, l'enregistrement est activé. Bien que la règle par défaut indique un enregistrement basé sur la détection du mouvement, elle ne garantit pas que la vidéo soit enregistrée par le système car vous pouvez avoir désactivé l'enregistrement d'une caméra individuelle pour une ou plusieurs caméras. Même lorsque l'enregistrement est activé, il ne faut pas oublier que la qualité des enregistrements peut être affectée par les paramètres d'enregistrement de chaque caméra.
Enregistrer sur demande	Veille à ce que la vidéo soit enregistrée automatiquement lorsqu'une demande externe survient, à condition que l'enregistrement soit activé pour les caméras en question. Par défaut, l'enregistrement est activé. La demande est toujours déclenchée par un système s'intégrant en externe avec votre système, et la règle est principalement utilisée par les intégrateurs de systèmes externes ou de modules d'extension.

Règle par défaut	Description
Activer le flux audio	Veille à ce que les flux audio de tous les microphones et haut-parleurs connectés soient automatiquement alimentés vers le système. Bien que la règle par défaut donne accès aux flux audio des microphones et haut-parleurs connectés immédiatement après installation du système, elle ne garantit pas que l'audio sera enregistré, car les paramètres d'enregistrement doivent être précisés séparément.
Activer le flux	Veille à ce que les flux vidéo de toutes les caméras connectées soient automatiquement alimentés vers le système. Bien que la règle par défaut donne accès aux flux vidéo des caméras connectées immédiatement après installation du système, elle ne garantit pas que la vidéo soit enregistrée, car les paramètres d'enregistrement des caméras doivent être précisés séparément.
Activer le flux de métadonnées	Veille à ce que les flux de données de toutes les caméras connectées soient automatiquement alimentés vers le système. Bien que la règle par défaut donne accès aux flux de données des caméras connectées immédiatement après installation du système, elle ne garantit pas que les données soient enregistrées, car les paramètres d'enregistrement des caméras doivent être précisés séparément.
Afficher la notification de demande d'accès	Veille à ce que tous les événements de contrôle d'accès classés comme « Demande d'accès », entraîne l'apparition d'une notification de demande d'accès sur XProtect Smart Client, à moins que la fonction de notification ne soit désactivée dans le profil Smart Client.

Recréer les règles par défaut

Si vous supprimez une règle par défaut sans le vouloir, vous pouvez la recréer en saisissant le texte ci-après :

Règle par défaut	Texte à saisir :
Aller au préréglage en fin de PTZ	Réaliser une action sur session manuelle PTZ arrêtée de toutes les caméras Passer immédiatement à la position prédéfinie par défaut sur le périphérique sur lequel l'événement s'est produit
Enregistrer sur signet	Réaliser une action sur Référence de signet demandée par toutes les caméras, tous les microphones, tous les haut-parleurs lance l'enregistrement trois secondes auparavant sur le périphérique sur lequel l'événement s'est produit. Réaliser une action 30 secondes immédiatement après l'arrêt de l'enregistrement

Règle par défaut	Texte à saisir :
Enregistrer sur mouvement	Réaliser une action sur Mouvement lancé par toutes les caméras lance l'enregistrement trois secondes avant sur le périphérique sur lequel l'événement s'est produit Réaliser une action d'arrêt sur Mouvement arrêté par les caméras arrête l'enregistrement trois secondes après
Enregistrer sur demande	Réaliser une action sur Demander le départ de l'enregistrement d'une source externe lance l'enregistrement immédiatement sur les périphériques à partir de métadonnées Réaliser une action d'arrêt sur Demander l'arrêt de l'enregistrement d'une source externe arrête l'enregistrement immédiatement
Activer le flux audio	Exécuter une action dans un intervalle de temps lance toujours les flux sur tous les microphones, tous les haut-parleurs Réaliser une action lorsque l'intervalle de temps termine immédiatement le flux
Activer le flux	Exécuter une action dans un intervalle de temps lance toujours les flux sur toutes les caméras Réaliser une action lorsque l'intervalle de temps termine immédiatement le flux
Activer le flux de métadonnées	Exécuter une action dans un intervalle de temps lance toujours les flux sur toutes les métadonnées Réaliser une action lorsque l'intervalle de temps termine immédiatement le flux
Afficher la notification de demande d'accès	Exécuter une action sur demande d'Accès (Catégories de Contrôle d'accès) à partir des Systèmes [+ unités] Afficher la notification de demande d'accès intégrée

À propos des règles de validation

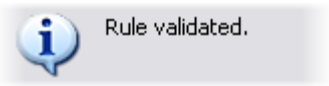
Vous pouvez valider le contenu d'une règle individuelle ou de toutes les règles en une seule fois. Lorsque vous créez une règle, l'assistant **Gérer la règle** veille à ce que tous les éléments de la règle aient un sens. Toutefois, lorsqu'une règle a existé pendant quelque temps, il est possible qu'un ou que plusieurs éléments de la règle aient pu être affectés par une autre configuration et il est possible que la règle ne fonctionne plus. Par exemple, si une règle est déclenchée par un profil de temps spécifique, la règle ne fonctionnera plus si le profil de temps en question a été effacé ou si vous ne disposez plus des permissions vous permettant d'y accéder. Il peut être difficile de se faire une vue d'ensemble de tels effets involontaires de configuration.

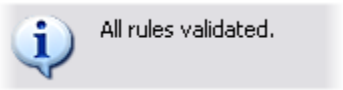
La validation des règles vous aide à suivre les règles concernées par une modification. La validation a lieu en se basant sur chaque règle et chaque règle est validée de manière isolée. Il n'est pas possible de valider les règles les unes par rapport aux autres (par exemple pour savoir si une règle est en conflit avec une autre), même lors de l'utilisation de la fonction **Valider toutes les règles**.

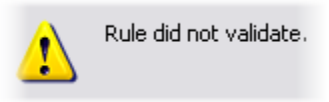
Notez qu'il n'est pas possible de valider si la configuration des conditions préalables en-dehors de la règle elle-même empêche la règle de fonctionner. Par exemple, une règle qui indique qu'un enregistrement doit avoir lieu lorsqu'un mouvement est détecté par une caméra précise valide OK si les éléments de la règle sont corrects et cela même si la détection du mouvement (qui est

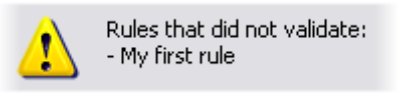
activée au niveau de la caméra, et non au travers des règles) n'a pas été activée pour la caméra concernée.

Vous pouvez valider une règle individuelle ou toutes les règles en même temps en faisant un clic droit sur la règle à valider et en sélectionnant **Valider la règle** ou **Valider toutes les règles.** Une boîte de dialogue vous indique si la ou les règles ont été bien validées. Si vous décidez de valider plus d'une règle et si une règle ou plusieurs règles ont échoué, la boîte de dialogue affiche les noms des règles concernées.









À propos de la complexité de règle

Votre nombre exact d'options dépend du type de règle que vous souhaitez créer et du nombre de périphériques à disposition sur votre système. Les règles offrent un degré élevé de flexibilité : vous pouvez associer un événement et des conditions de temps, spécifier plusieurs actions dans une seule règle et souvent créer des règles qui couvrent plusieurs ou tous les périphériques de votre système.

Vous pouvez rendre vos règles aussi simples ou aussi complexes que nécessaire. Par exemple, vous pouvez créer des règles très simples basées sur une durée :

Exemple	Explication
Règle très simple basée sur une durée	Les lundis entre 08h30 et 11h30 (condition de temps), les caméras 1 et 2 lancent l'enregistrement (action) au début de la période spécifiée et arrêtent l'enregistrement (arrêt d'action) lorsque la période spécifiée expire.
Règle très simple basée sur un événement	Lorsqu'un mouvement est détecté (condition d'événement) sur la caméra 1, elle lance immédiatement l'enregistrement (action) puis arrête l'enregistrement (arrêt d'action) après 10 secondes. Même si une règle basée sur événement est activée par un événement sur un périphérique, vous pouvez préciser que des actions doivent avoir lieu sur un ou plusieurs périphériques différents.
Règle impliquant plusieurs périphériques	Lorsqu'un mouvement est détecté (condition d'événement) sur la caméra 1, la caméra 2 doit immédiatement lancer l'enregistrement (action) puis la sirène raccordée à la sortie 3 doit sonner (action) immédiatement. Puis, après écoulement de 60 secondes, la caméra 2 doit arrêter l'enregistrement (arrêt d'action), et la sirène raccordée à la sortie 3 doit arrêter de sonner (arrêt d'action).
Règle combinant la durée, les événements et les périphériques	Lorsqu'un mouvement est détecté (condition d'événement) sur la caméra 1, que le jour de la semaine est samedi ou dimanche (condition de temps), la caméra 1 et la caméra 2 lancent immédiatement l'enregistrement (action), et une notification est envoyée au responsable de la sécurité (action). Puis, 5 secondes après la fin de détection du mouvement sur la caméra 1 ou 2, les 2 caméras arrêtent l'enregistrement (arrêt d'action).

Selon les besoins de votre entreprise, il convient souvent de créer plusieurs règles simples plutôt que de créer quelques règles complexes. Même si cela représente un nombre plus important de règles dans le système, cette façon de procéder constitue une façon simple de garder une bonne vue d'ensemble des actions engendrées par les règles. La simplicité des règles signifie également plus de flexibilité pour vous lorsqu'il s'agit de désactiver/activer des éléments individuels de la règle. Avec des règles simples, vous pouvez désactiver/activer des règles complètes le cas échéant.

Ajouter une règle

Lorsque vous créer des règles, vous êtes guidé par l'assistant **Gérer la règle** qui ne contient que les options pertinentes.

Il veille à ce qu'une règle ne contienne pas d'éléments manquants. En fonction du contenu de votre règle, il suggère automatiquement des actions d'arrêt appropriées (à savoir ce qui devrait se passer lorsqu'une règle n'est plus applicable), afin de veiller à ce que vous ne créiez pas accidentellement des règles sans fin.

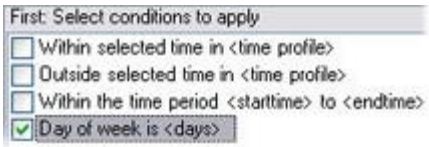
1. Faites un clic droit sur l'élément **Règles** > **Ajouter une règle**. Cela ouvrira l'assistant **Gestion des règles**. L'assistant vous guide à travers la spécification du contenu de votre règle.

2. Spécification d'un nom et d'une description de la nouvelle règle dans les champs **Nom** et **Description** respectivement.

3. Sélectionnez le type pertinent de condition de la règle : soit une règle qui effectue une ou plusieurs actions lorsqu'un événement particulier a lieu, soit une règle qui exécute plusieurs actions lorsqu'une période de temps précise est saisie.

4. Cliquez sur **Suivant** dans l'assistant pour passer à l'étape 2 de l'assistant. Dans la seconde étape de l'assistant, définissez les autres conditions de la règle.

5. Sélectionnez une ou plusieurs conditions, par exemple **Le jour de la semaine est <jour>** :

   Exemple seulement. Vos sélections peuvent varier.

   En fonction de vos sélections, modifiez la description de la règle dans la partie inférieure de la fenêtre de l'assistant.

   Exemple seulement. Vos sélections peuvent varier.

   Cliquez sur les éléments soulignés en **italique gras** pour préciser le contenu exact. Par exemple, le fait de cliquer sur le lien **jours** dans notre exemple, vous permet de sélectionner un ou plusieurs jours de la semaine lors desquels la règle est applicable.

6. Après avoir indiqué vos conditions exactes, cliquez sur **Suivant** pour passer à la prochaine étape de l'assistant et sélectionner les actions qui doivent être couvertes par la règle. En fonction du contenu et de la complexité de votre règle, vous devrez peut-être définir

d'autres étapes, telles que des événements et des actions d'arrêt. Par exemple, si une règle indique qu'un périphérique doit exécuter une action particulière durant un intervalle de temps (par exemple les jeudis entre 8h00 et 10h30), l'assistant peut vous demander de préciser ce qui doit se passer et quand l'intervalle de temps se termine.

7. Votre règle est activée par défaut après sa création si ses conditions sont satisfaites. Si vous ne voulez pas que votre règle soit activée directement, décochez la case **Activé**.
8. Cliquez sur **Terminer**.

Modifier, copier et renommer une règle

1. Dans le volet **Vue d'ensemble**, faites un clic droit sur la règle concernée.
2. Sélectionnez :

   Modifier règle ou **Copier règle** ou **Renommer règle.** L'assistant **Gérer la règle** s'ouvre.
3. Dans l'assistant, renommez et/ou modifiez la règle. Si vous avez sélectionné **Copier règle**, l'assistant s'ouvre, affichant une copie de la règle sélectionnée.
4. Cliquez sur **Terminer**.

Désactiver et activer une règle

Votre système applique une règle dès que les conditions de la règle s'appliquent ce qui signifie qu'elle est active. Si vous ne voulez pas qu'une règle soit active, vous pouvez la désactiver. Lorsqu'une règle est désactivée, le système n'applique pas la règle, même si les conditions s'appliquent. Vous pouvez facilement activer/désactiver la règle ultérieurement.

Désactiver une règle

1. Dans le volet **Vue d'ensemble**, sélectionnez la règle.
2. Décochez la case **Activé** dans le volet **Propriétés**.
3. Cliquez sur **Sauvegarder** dans la barre d'outils.
4. Une icône avec une croix rouge indique que la règle a été désactivée dans la liste des **Règles** :

Exemple : la croix sur l'icône indique que la troisième règle est désactivée

Activer une règle

Lorsque vous souhaitez réactiver la règle, sélectionnez la règle, cochez la case **Activer** et sauvegardez la configuration.

Profils de temps

À propos des profils de temps

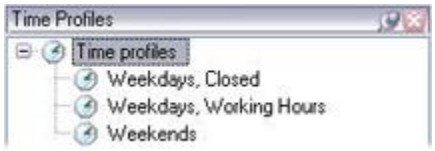
Les profils de temps sont des périodes de temps définies par l'administrateur. Vous pouvez utiliser les profils de temps lors de la création de règles, par exemple une règle spécifiant qu'une certaine action doit se dérouler dans une certaine période de temps.

En outre, les profils de temps sont attribués aux rôles en plus des profils Smart Client. Par défaut, il est attribué par défaut à tous les rôles le profil de temps **Toujours.** Cela signifie que les membres de rôles avec ce profil de temps par défaut n'ont aucune limite de temps sur leurs droits d'utilisateurs dans le système. Vous pouvez également assigner un profil de temps alternatif à un rôle.

Les profils de temps sont très souples : ils peuvent être basés sur une ou plusieurs périodes uniques, une ou plusieurs périodes récurrentes ou une combinaison de périodes uniques et récurrentes. De nombreux utilisateurs connaissent les concepts des périodes uniques et récurrentes de par les applications de calendrier, comme par exemple celle de Microsoft® Outlook.

Les profils de temps s'appliquent toujours à l'heure locale. Cela signifie que si votre système est doté de serveurs d'enregistrement dans différents fuseaux horaires, les actions (par ex. enregistrement des caméras) associées aux profils de temps sont exécutées dans chaque heure locale du serveur d'enregistrement. Exemple : Si vous avez un profil de temps couvrant la période allant de 8 h 30 à 9 h 30, toutes les actions associées à un serveur d'enregistrement à New York sont exécutées entre 8 h 30 et 9 h 30 heure de New York, tandis que les mêmes actions sur un serveur placé à Los Angeles ont lieu plus tard, lorsqu'il est entre 8 h 30 et 9 h 30 à Los Angeles.

Les profils de temps sont créés et gérés en développant **Règles et événements** > **Profils de temps**. Une liste de **profils de temps** s'ouvre :



Par exemple

Pour voir une alternative aux profils de temps, reportez-vous aux Profils de durée la journée (voir "À propos des profils de temps toute la journée" á la page 199).

Spécifier un profil de temps

1. Dans la liste des **profils de temps**, faites un clic droit dans **Profils de temps** > **Ajouter profil de temps** Cela ouvre la fenêtre **Profil de temps**.

2. Dans la fenêtre **Profil de temps**, saisissez un nom pour le nouveau profil de temps dans le champ **Nom**. Facultativement, saisissez une description du nouveau profil de temps dans le champ **Description**.

3. Dans le calendrier de la fenêtre **Profil de temps**, sélectionnez **Vue quotidienne, Vue hebdomadaire**, ou **Vue mensuelle**, puis faites un clic droit à l'intérieur du calendrier et sélectionnez **Ajouter une période unique** ou **Ajouter une période récurrente**.

4. Une fois que vous avez spécifié les périodes pour votre profil de temps, cliquez sur **OK** dans la fenêtre **Profil de temps**. Votre système ajoute le nouveau profil de temps dans la liste des **profils de temps**. Si à un stade ultérieur vous voulez modifier ou supprimer le profil de temps, vous pouvez également le faire à partir de la liste des **profils de temps**.

Ajouter une période unique

Lorsque vous sélectionnez **Ajouter une période unique**, la fenêtre **Sélectionner la période** s'affiche :

Le format de présentation de la date et de l'heure peut s'afficher différemment sur votre système

1. Dans la fenêtre **Sélectionner la période**, indiquez une **Heure de début** et une **Heure de fin**. Si la période doit couvrir des journées entières, cochez la case **Événement d'un jour**.
2. Cliquez sur **OK**.

Spécifier une période récurrente

Lorsque vous sélectionnez **Ajouter une période récurrente**, la fenêtre **Sélectionner la période récurrente** s'affiche :

Le format de présentation de la date et de l'heure peut s'afficher différemment sur votre système

1. Dans la fenêtre **Sélectionner la période**, indiquez la plage horaire, le modèle de périodicité et la plage de périodicité.
2. Cliquez sur **OK**.

Un profil de temps peut contenir plusieurs périodes. Si vous souhaitez que votre profil de temps contienne d'autres périodes, ajoutez des périodes uniques ou récurrentes.

Modifier un profil de temps

1. Dans la liste des **profils de temps** du volet **Vue d'ensemble**, faites un clic droit sur le profil de temps concerné, puis sélectionnez **Modifier le profil de temps**. Cela ouvre la fenêtre **Profil de temps**.
2. Modifiez le profil de temps en fonction de vos besoins. Après modification du profil de temps, cliquez sur **OK** dans la fenêtre **Profil de temps**. Vous revenez dans la liste des **profils de temps**.

Les mois peuvent défiler en cliquant sur les petits boutons Retour/Avance.

Remarque : Dans la fenêtre **Informations** profil de temps, vous pouvez modifier le profil de temps selon vos besoins. N'oubliez pas qu'un profil de temps peut contenir plusieurs périodes et que les périodes peuvent être récurrentes. Le petit aperçu mensuel dans le coin supérieur droit peut vous aider à obtenir un aperçu rapide des périodes couvertes par le profil, car les dates contenant des heures spécifiques sont en gras.

Dans cet exemple, les dates en gras indiquent que les périodes s'étendent sur plusieurs jours et qu'une durée récurrente a été précisée les lundis.

À propos des profils de temps toute la journée

Lorsque les caméras sont placées à l'extérieur, il est souvent nécessaire de diminuer la résolution des caméras, d'activer le noir et blanc ou de modifier d'autres paramètres lorsqu'il fait sombre ou lorsqu'il y a beaucoup de soleil. Le plus au nord ou le plus au sud par rapport à l'équateur se trouvent les caméras, plus les heures de lever et de coucher du soleil varient au cours de l'année. Ce qui fait qu'il est impossible d'utiliser des profils de temps fixes pour ajuster les paramètres de la caméra en fonction de la lumière.

Dans une telle situation, vous pouvez créer des profils de temps toute la journée en lieu et place afin de définir le lever et le coucher de soleil dans une zone géographique spécifique. Au travers des coordonnées GPS, le système calcule les heures de lever et de coucher du soleil et incorpore même l'heure d'été ou l'heure d'hiver. Ainsi, le profil de temps suit automatiquement les changements annuels de lever/coucher du soleil dans la zone choisie, faisant que le profil est actif uniquement lorsque nécessaire. Toutes les heures et toutes les dates se basent sur les paramètres de date et d'heure des serveurs de gestion. Vous pouvez également définir un décalage négatif ou positif (en minutes) pour l'heure de début (lever du soleil) et l'heure de fin (coucher du soleil). Le décalage pour l'heure de début et de fin peut être identique ou différent.

Vous pouvez utiliser les profils de temps toute la journée quand vous créez des règles, mais également des rôles.

Créer un profil de temps toute la journée

1. Développez le dossier **Règles et événements** > **Profils de temps**.
2. Dans la liste des **profils de temps**, faites un clic droit dans **Profils de temps** et sélectionnez **Ajouter profil de temps toute la journée**.

3. Dans la fenêtre **Profil de temps toute la journée**, soumettez les informations nécessaires. Pour gérer les périodes de transition entre le jour et la nuit, vous avez la possibilité de décaler l'activation et la désactivation du profil. L'heure et le nom des mois sont affichés dans la langue désignée conformément aux réglages régionaux/de langue de votre ordinateur.
4. Pour voir l'emplacement des coordonnées GPS saisies sur une carte, cliquez sur **Montrer la position dans le navigateur**. Cette action ouvre un navigateur dans lequel vous pouvez voir l'emplacement.
5. Cliquez sur **OK**.

Propriétés du profil de temps toute la journée

Réglez les paramètres suivants pour le profil de temps toute la journée :

Nom	Description
Nom	Le nom du profil.
Description	Une description du profil (facultatif).
Coordonnées GPS	Coordonnées GPS qui indiquent l'emplacement physique des caméras attribuées au profil.
Décalage lever du soleil	Nombre de minutes (+/-) en fonction desquelles l'activation du profil est décalée par le lever du soleil.
Décalage coucher du soleil	Nombre de minutes (+/-) en fonction desquelles la désactivation du profil est décalée par le coucher du soleil.
Fuseau horaire	Fuseau horaire qui indique l'emplacement physique des caméras.

Profils de notification

À propos des profils de notification

Vous pouvez utiliser les profils de notification pour configurer des notifications par e-mail prêtes à l'emploi, qui peuvent être automatiquement déclenchées par une règle, par exemple lorsqu'un événement particulier se produit. Vous pouvez inclure des photos et des clips vidéo AVI dans ces notifications par e-mail.

Le système ne prend pas en charge le format TLS (Transport Layer Security) et son prédécesseur SSL (Secure Socket Layer). Si l'expéditeur appartient à un serveur nécessitant des notifications par e-mail au format TLS ou SSL, cette fonction ne fonctionnera pas correctement. Vous devrez peut-être également désactiver tous les logiciels d'analyse de messagerie qui peuvent bloquer l'envoi des notifications par e-mail par l'application.

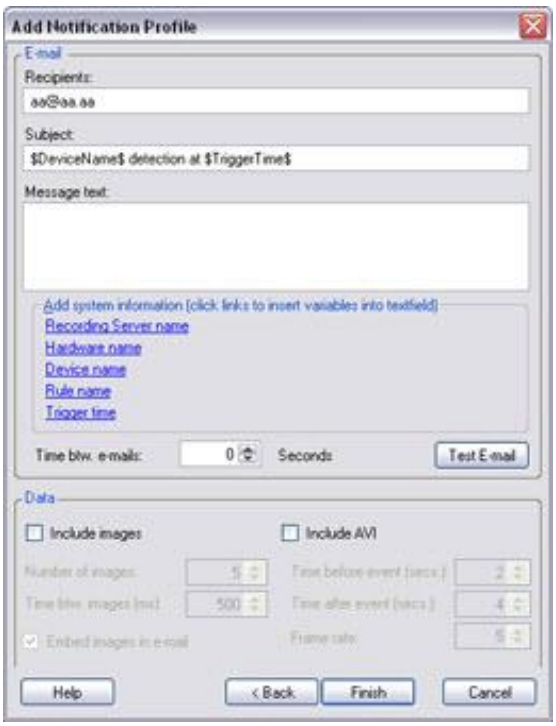
Conditions préalables

Avant de pouvoir créer des profils de notification, vous devez préciser les paramètres du serveur de messagerie SMTP sortant pour les notifications par e-mail.

Si vous souhaitez que les notifications par e-mail soient en mesure de contenir des clips vidéo au format AVI, vous devez également préciser les paramètres de compression à utiliser. Pour ce faire, allez dans **Outils** > **Options**. Cela ouvre la fenêtre **Options**. Précisez le **serveur de messagerie SMTP sortant** dans l'onglet **Serveur de messagerie** ainsi que les paramètres de compression dans l'onglet **Génération AVI**.

Ajouter des profils de notification

1. Développez **Règles et événements**, faites un clic droit sur **Profils de notification**> **Ajouter profil de notification**. Cela ouvre l'assistant **Ajouter profil de notification**.
2. Précisez le nom et une description. Cliquez sur **Suivant**.
3. Saisissez le destinataire, l'objet, le texte du message et la durée entre les messages :



4. Pour envoyer une notification par e-mail test aux destinataires indiqués, cliquez sur **Tester e-mail**.
5. Pour inclure des photos de pré-alarme, sélectionnez **Inclure images** et indiquez le nombre de photos, la durée entre les photos et l'intégration des photos dans le message ou non.
6. Pour inclure des clips vidéo AVI, sélectionnez **Inclure AVI** et indiquez la durée avant et après l'événement ainsi que la fluidité de l'image.
7. Cliquez sur **Terminer**.

Utiliser des règles pour déclencher des notifications par e-mail

Utilisez l'assistant **Gérer la règle** pour créer des règles L'assistant vous guide tout au long des étapes pertinentes. Vous spécifiez l'utilisation d'un profil de notification à l'étape où vous indiquez les actions de la règle.

Lorsque vous sélectionnez l'action **Envoyer notification à <profil>**, vous pouvez sélectionner le profil de notification correspondant et les caméras depuis lesquelles les enregistrements à inclure dans les notifications par e-mail du profil de notification doivent être issus :

Exemple seulement. Dans **Gérer la règle**, vous cliquez sur les liens pour effectuer vos sélections

N'oubliez pas que les enregistrements ne peuvent être inclus dans les notifications par e-mail du profil de notification à moins que quelque chose ne soit effectivement enregistré. Si vous souhaitez intégrer des photos ou des clips vidéos AVI dans les notifications par e-mail, vérifiez que la règle indique que l'enregistrement doit avoir lieu. L'exemple suivant provient d'une règle incluant à la fois l'action **Commencer l'enregistrement** et l'action **Envoyer la notification à** :

Profils de notification (propriétés)

Indiquer les propriétés suivantes pour les profils de notification :

Composant	Exigences
Nom	Entrez un nom descriptif pour le profil de notification. Le nom apparaît ensuite lorsque vous sélectionnez le profil de notification au cours du processus de création de règle.
Description (facultatif)	Saisissez une description du profil de notification. La description apparaît lorsque vous pointez votre curseur sur le profil de notification, dans la liste **Profils de notification** du volet Vue d'ensemble :
Destinataires	Entrez les adresses e-mail auxquelles les notifications par e-mail du profil de notification doivent être envoyées. Pour saisir plusieurs adresses e-mail, séparez les adresses par un point-virgule. Exemple : aa@aaaa.aa;bb@bbbb.bb;cc@cccc.cc
Objet	Entrez le texte que vous souhaitez faire apparaître dans le champ objet d'une notification par e-mail. Vous pouvez insérez des variables système, telles que le **nom du Périphérique**, dans le champ de texte message et objet. Pour insérer des variables, cliquez sur les liens de variables requises dans la case située sous le champ.

Composant	Exigences
Texte du message	Saisissez le texte que vous souhaitez faire apparaître dans le corps des notifications par e-mail. Outre le texte du message, le corps de chaque notification par e-mail contient automatiquement l'information suivante : • Ce qui a déclenché la notification par e-mail. • La source de toute image fixe ou clip vidéo AVI attaché(e)
Temps entre les e-mails	Spécifiez le temps minimum requis (en secondes) devant s'écouler entre chaque envoi de notification par e-mail. Exemples : • Si vous indiquez une valeur de **120**, 2 minutes minimum s'écoulent entre chaque envoi de notification par e-mail, même si le profil de notification est de nouveau déclenché par une règle avant la fin des 2 minutes. • Si vous indiquez une valeur de **0**, les notifications par e-mail sont envoyées à chaque déclenchement du profil de notification par une règle. Potentiellement, cela peut entraîner un très grand nombre d'envois de notifications par e-mail. Si vous utilisez la valeur **0**, vous devez ainsi soigneusement décider si vous souhaitez utiliser le profil de notification avec des règles susceptibles d'être déclenchées régulièrement.
Nombre d'images	Indiquez le nombre maximum d'images fixes que vous souhaitez inclure dans chaque notification par e-mail du profil de notification. Par défaut, ce nombre d'images est de cinq.
Temps entre les images (ms)	Spécifiez le nombre de millisecondes désiré entre les enregistrements présentés sur les images incluses. Exemple : Avec une valeur par défaut de 500 millisecondes, les images incluses affichent les enregistrements présentés espacées d'une demi-seconde.
Temps avant l'événement (sec.)	Ce paramètre est utilisé pour spécifier le début du fichier AVI. Par défaut, le fichier AVI contient les enregistrements débutés 2 secondes avant le déclenchement du profil de notification. Vous pouvez le remplacer par le nombre de secondes requis.
Temps après l'événement (sec.)	Ce paramètre est utilisé pour spécifier la fin du fichier AVI. Par défaut, le fichier AVI prend fin 4 secondes après le déclenchement du profil de notification. Vous pouvez le remplacer par le nombre de secondes requis.
Nombre d'images par seconde	Spécifiez le nombre d'images par seconde que vous souhaitez que le fichier AVI contienne. Par défaut, les images sont au nombre de cinq. Plus la fluidité d'images est élevée, plus la qualité d'image et la taille du fichier AVI sont importantes.
Insérer les images dans l'e-mail	Si sélectionné (par défaut), les images sont insérées dans le corps des notifications par e-mail. Dans le cas contraire, les images sont intégrées en pièces jointes aux notifications par e-mail.

Événements définis par l'utilisateur

À propos des évènements définis par l'utilisateur

Si l'événement nécessaire n'est pas sur la liste **Vue d'ensemble des événements**, vous pouvez créer vos propres événements définis par l'utilisateur. Utilisez de tels événements définis par l'utilisateur pour intégrer d'autres systèmes à votre système de surveillance.

Les événements définis par l'utilisateur vous permettent d'utiliser les données provenant d'un système de contrôle d'accès tiers sous forme d'événements dans le système. Les événements peuvent ensuite déclencher des actions. Ainsi, vous pouvez par exemple, commencer à enregistrer une vidéo à partir des caméras pertinentes lorsqu'une personne entre dans un bâtiment.

Vous pouvez également utiliser les événements définis par l'utilisateur dans le cas d'événements à déclenchement manuel tout en visionnant une vidéo en direct dans XProtect Smart Client ou automatiquement s'ils sont utilisés dans des règles. Par exemple, lorsqu'un événement défini par l'utilisateur 37 a lieu, la caméra PTZ 224 doit arrêter de patrouiller et aller sur la position prédéfinie 18.

Au travers des rôles, vous définissez lequel de vos utilisateurs peut déclencher les événements définis par l'utilisateur. Vous pouvez utiliser les événements définis par l'utilisateur de deux manières et en même temps le cas échéant :

Événements	Description
Pour fournir la possibilité de déclencher manuellement des événements dans XProtect Smart Client	Dans ce cas, les événements définis par l'utilisateur font qu'il est possible pour les utilisateurs finaux de déclencher manuellement des événements tout en visualisant une vidéo en direct dans XProtect Smart Client. Lorsqu'un événement défini par l'utilisateur survient parce qu'il est déclenché manuellement par un utilisateur XProtect Smart Client, une règle peut déclencher qu'une ou plusieurs action(s) doivent se produire sur le système.

Événements	Description
Pour fournir la possibilité de déclencher des événements au travers d'API	Dans ce cas, vous pouvez déclencher les événements définis par l'utilisateur depuis l'extérieur du système de surveillance. L'utilisation des événements définis par l'utilisateur de la manière décrite nécessite l'usage d'une API (Application Program Interface, un ensemble de blocs de construction pour la création ou la personnalisation d'applications logicielles) séparée lors du déclenchement de l'événement défini par l'utilisateur. L'authentification au travers d'Active Directory est nécessaire pour utiliser de cette manière les événements définis par l'utilisateur. Cela veille à ce que si les événements définis par l'utilisateur peuvent être déclenchés depuis l'extérieur du système de surveillance, seuls les utilisateurs autorisés peuvent le faire. Par ailleurs, les événements définis par l'utilisateur peuvent être associés, via l'API, à des métadonnées, définissant certains périphériques ou groupes de périphériques. Cette fonction est très utile lors de l'emploi d'événements définis par l'utilisateur pour déclencher des règles : vous évitez d'avoir une règle pour chaque périphérique qui finalement fait la même chose. Exemple : Une société utilise un contrôle de l'accès, avec 35 entrées, chacune dotée d'un périphérique de contrôle de l'accès. Lorsqu'un périphérique de contrôle de l'accès est activé, un événement défini par l'utilisateur est déclenché dans le système. Cet événement défini par l'utilisateur est utilisé dans une règle pour lancer l'enregistrement sur une caméra associée au périphérique activé de contrôle de l'accès. La caméra associée à une règle est définie dans les métadonnées. Ainsi, la société n'a pas besoin d'avoir 35 événements définis par l'utilisateur et 35 règles déclenchées par des événements définis par l'utilisateur. Un seul événement défini par l'utilisateur et une seule règle suffisent. Quand vous utilisez des événements définis par l'utilisateur de cette manière, il est possible que vous ne vouliez pas qu'ils soient toujours disponibles au déclenchement manuel dans XProtect Smart Client. Vous pouvez utiliser les rôles pour définir quels événements définis par l'utilisateur doivent être visibles dans XProtect Smart Client.

Quelle que soit la manière dont vous utilisez les événements définis par l'utilisateur, vous devez ajouter chacun de ces événements par le biais du Management Client.

si vous renommez un événement défini par l'utilisateur, les utilisateurs XProtect Smart Client déjà connectés doivent se déconnecter et se reconnecter avant que le changement de nom soit visible.

Veuillez également noter que si vous supprimez un événement défini par l'utilisateur, les règles dans lesquelles l'événement défini par l'utilisateur est utilisé sont affectées. De la même manière, un événement défini par l'utilisateur effacé disparaît de XProtect Smart Client seulement après déconnexion des utilisateurs XProtect Smart Client.

Ajouter un événement défini par l'utilisateur

1. Développez **Règles et événements** > **Événements définis par l'utilisateur**.

2. Dans le volet **Vue d'ensemble**, faites un clic droit sur **Événements** > **Ajouter un événement défini par l'utilisateur**.
3. Saisissez un nom pour le nouvel événement défini par l'utilisateur et cliquez sur **OK**. L'événement défini par l'utilisateur nouvellement ajouté apparaît désormais dans la liste du volet **Vue d'ensemble**.
4. L'utilisateur peut désormais déclencher l'événement défini par l'utilisateur manuellement dans XProtect Smart Client s'il possède les droits correspondants.

Renommer un événement défini par l'utilisateur

1. Développez **Règles et événements** > **Événements définis par l'utilisateur**.
2. Dans le volet **Vue d'ensemble**, sélectionnez l'événement défini par l'utilisateur.
3. Dans le volet **Propriétés**, remplacez le nom existant.
4. Dans la boîte à outils, cliquez sur **Enregistrer**.

Événements analytiques

À propos des événements analytiques

Les événements analytiques sont généralement des données reçues de la part de fournisseurs d'analyse de contenus vidéo (VCA) tiers externes.

L'utilisation d'événements analytiques comme base des alarmes est un processus à trois étapes :

- La première : activation de la fonction événements analytiques et configuration de sa sécurité. Utilisez une liste d'adresses autorisées pour contrôler les expéditeurs de données d'événements au système et le port d'écoute du serveur.
- La deuxième : création d'un événement analytique, éventuellement avec une description de l'événement, et test.
- La troisième : utilisation de l'événement analytique comme source de définition d'une alarme.

Vous pouvez configurer les événements analytiques dans la liste **Règles et événements** du volet **Navigation sur le site**.

Pour utiliser des événements basés VCA, un outil VCA tiers est nécessaire pour fournir les données au système. Le choix de l'outil VCA à utiliser vous revient, tant que les données fournies par l'outil respectent le format. Ce format est stipulé dans la section se rapportant aux événements analytiques Milestone : Manuel de du développeur. Contactez le fournisseur de votre système pour en savoir plus. Les outils VCA tiers sont développés par des partenaires indépendants proposant des solutions basées sur une plate-forme ouverte Milestone. Ces solutions peuvent avoir un impact sur les performances du système.

Ajouter et modifier un événement analytique

Ajouter un événement analytique

1. Développez **Règles et événements**, faites un clic droit sur **Événements analytiques**, puis sélectionnez **Ajouter nouveau**.
2. Dans la fenêtre **Propriétés**, saisissez un nom pour le nouveau profil de temps dans le champ **Nom**.
3. Saisissez un texte de description dans le champ **Description** le cas échéant.
4. Dans la boîte à outils, cliquez sur **Enregistrer**. Vous pouvez tester la validité de l'événement en cliquant sur **Événement test**. Vous pouvez à chaque instant corriger les erreurs signalées dans le test et effectuer le test autant de fois que vous le souhaitez et à n'importe quel moment du processus.

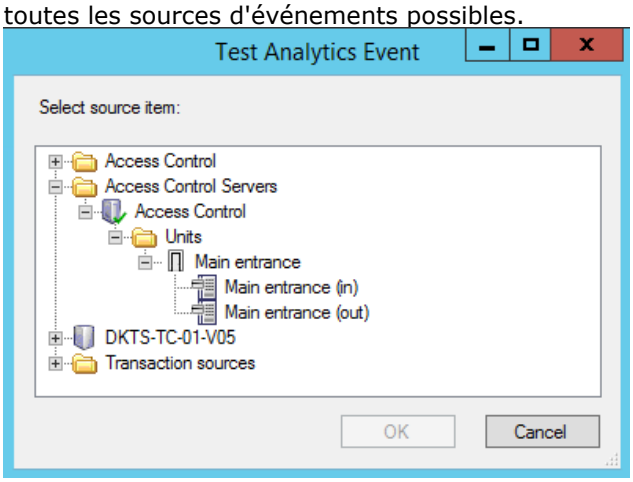
Modifier un événement analytique

1. Cliquez sur un événement analytique existant pour afficher la fenêtre **Propriétés** dans laquelle vous pouvez modifier les champs concernés.
2. Vous pouvez tester la validité de l'événement en cliquant sur **Événement test**. Vous pouvez à chaque instant corriger les erreurs signalées dans le test et effectuer le test autant de fois que vous le souhaitez et à n'importe quel moment du processus.

Tester un événement analytique

Après avoir créé un événement analytique, vous pouvez tester les exigences (voir "Événement analytique test (propriétés)" á la page 208), par exemple que la fonction événements analytiques a été activée dans Management Client.

1. Sélectionnez un événement analytique existant.
2. Dans les propriétés, cliquez sur le bouton **Évènement test**. Une fenêtre s'ouvre affichant toutes les sources d'événements possibles.



3. Sélectionnez la source de votre événement test, par exemple une caméra. La fenêtre se ferme et une nouvelle fenêtre s'ouvre affichant et passe par quatre différents stades qui doivent être respectés pour que l'événement analytique fonctionne.

Comme autre test, dans XProtect Smart Client vous pouvez vérifier si l'événement analytique a été envoyé au serveur d'événement. Pour ce faire, ouvrez XProtect Smart Client et affichez l'événement dans l'onglet **Gestionnaire des alarmes**.

Voir également

À propos des événements analytiques (á la page 206)

Événement analytique test (propriétés)

Lorsque vous testez les exigences d'un événement analytique, une fenêtre s'ouvre et vérifie quatre stades et fournit les descriptions des erreurs et les solutions possibles.

Condition	Description	Messages d'erreur et solutions
Changements sauvegardés	Si l'événement est nouveau, est-il sauvegardé ? Ou si le nom de l'événement a été modifié, ces modifications sont-elles enregistrées ?	**Sauvegarde des changements avant le teste de l'événement analytique** Solution/explication : Enregistrer les modifications.
Événements d'analyse activés	la fonction Évènement d'analyse est-elle activée ?	**Les événements analytiques n'ont pas été activés.** Solution/explication : activez la fonction Évènements d'analyse. Pour faire cela, cliquez sur **Outils** > **Options** > **Événements analytiques** et cochez la case **Activé**.
Adresse permise	L'adresse IP/le nom d'hôte de la machine qui envoie le ou les événement(s) est-il/elle autorisé(e) (indiqué(e) dans la liste d'adresses des événements d'analyse) ?	**Le nom d'hôte local doit être ajouté comme adresse autorisée pour le service d'événements d'analyse.** Solution/explication : Ajoutez votre machine à la liste d'adresse des événements analytiques des adresses IP ou noms d'hôtes autorisés. **Erreur lors de la résolution de l'hôte local.** Solution/explication : L'adresse IP ou le nom d'hôte de la machine est introuvable ou incorrect.
Envoi d'événement analytique	L'envoi d'un évènement test au serveur d'évènements a-t-il réussi ?	Voir le tableau ci-dessous.

Chaque étape porte la mention Échec : ✗ ou Réussite : ✓.

Messages d'erreur et solutions pour la condition **Envoi d'événement analytique** :

Serveur d'événements introuvable	impossible de trouver le serveur d'évènements sur la liste des services inscrits.
Erreur lors de la connexion au serveur d'événements	Impossible de se connecter au serveur d'événement sur le port défini. L'erreur est sûrement le résultat de problèmes de réseau ou de l'interruption du service du serveur d'événement.

Erreur lors de l'envoi de l'événement analytique	La connexion au serveur d'événement a été établie mais il est impossible d'envoyer l'événement. Probablement en raison d'un problème de réseau, un dépassement du délai par exemple.
Erreur lors de la réception de la réponse du serveur d'événements	L'événement a été envoyé au serveur d'événement mais aucune réponse n'a été reçue. L'erreur est sûrement le résultat d'un problème de réseau ou d'un port occupé. Reportez-vous au journal du serveur d'événements, généralement situé sous *ProgramData\Milestone\XProtect Event Server\logs*.
Événement analytique inconnu du serveur d'événements	Le service du serveur d'événements ne connaît pas cet événement. La raison la plus probable à cela est que l'événement ou des modifications apportées à l'événement n'ont pas été enregistrés.
Événement analytique reçu par le serveur d'événements	Le format de l'événement est incorrect.
Expéditeur non autorisé par le serveur d'événements	Votre machine ne se trouve probablement pas sur la liste des adresses IP ou noms d'hôtes autorisés.
Erreur interne dans le serveur d'évènements.	Erreur de serveur d'événements. Reportez-vous au journal du serveur d'événements, généralement situé sous *ProgramData\Milestone\XProtect Event Server\logs*.
Réponse du serveur d'évènements invalide	La réponse n'est pas valide. Le port est peut-être occupé ou il y a des problèmes réseau. Reportez-vous au journal du serveur d'événements, généralement situé sous *ProgramData\Milestone\XProtect Event Server\logs*.
Réponse inconnue du serveur d'événements	La réponse est valide mais incompréhensible. L'erreur est sûrement le résultat d'un problème de réseau ou d'un port occupé. Reportez-vous au journal du serveur d'événements, généralement situé sous *ProgramData\Milestone\XProtect Event Server\logs*.
Erreur imprévue	Veuillez contacter l'assistance Milestone pour obtenir de l'aide.

Modifier les paramètres des événements analytiques

Dans la barre d'outils, allez dans **Outils** > **Options** > **Événements analytiques** pour modifier les paramètres pertinents.

Événements génériques

À propos des évènements génériques

Important : cette fonction ne fonctionne pas si vous n'avez pas installé au préalable le serveur d'événements XProtect.

Les événements génériques vous permettent de déclencher des actions sur le serveur d'événements XProtect en envoyant des chaînes simples via le réseau IP à votre système.

Vous pouvez utiliser tout matériel ou logiciel qui peut envoyer des chaînes via TCP ou UDP pour déclencher des événements génériques. Votre système peut analyser des paquets de données TCP ou UDP reçus et déclencher automatiquement des événements génériques si les critères spécifiques sont satisfaits. De cette manière, vous pouvez intégrer votre système avec des sources externes, par exemple des sources de contrôle d'accès et des systèmes d'alarme. Le but est d'autoriser autant de sources externes que possible pour interagir avec le système.

Grâce au concept des sources de données, vous évitez d'avoir à adapter les outils tiers pour répondre aux normes de votre système. Les sources de données vous permettent de communiquer avec un matériel ou un logiciel particulier sur un port IP spécifique et d'affiner la manière dont le nombre d'octets qui arrivent sur ce port sont interprétés Chaque type d'événement générique s'associe à une source de données et créé un langage utilisé pour la communication avec une partie de matériel ou de logiciel précise.

Le fait de travailler avec des sources de données nécessite une connaissance générale de la mise en réseau IP, outre une connaissance spécifique du logiciel et du matériel à partir duquel vous souhaitez créer l'interface. Il existe plusieurs paramètres que vous pouvez utiliser et aucune solution prête à l'emploi pour savoir comment faire. En fait, votre système fournit les outils et non pas la solution. Au contraire des événements définis par l'utilisateur, les événements génériques n'ont pas d'authentification. Ainsi, ils sont plus faciles à déclencher, mais afin d'éviter de nuire à la sécurité, seuls les événements provenant de l'hôte local sont acceptés. Vous pouvez autoriser d'autres adresses IP clients depuis l'onglet **Événements génériques** du menu **Options**.

Ajouter un événement générique

Vous pouvez définir des événements génériques pour aider le video management software à reconnaître des chaînes spécifiques dans les paquets TCP ou UDP à partir d'un système externe. En fonction d'un événement générique, vous pouvez configurer Management Client pour déclencher des actions, par exemple démarrer un enregistrement ou des alarmes.

Conditions préalables : Vous avez des événements génériques activés et avez précisé les destinations sources autorisées. Pour en savoir plus, voir onglet Événements génériques (voir "Onglet Événements génériques (options)" á la page 277).

1. Déroulez **Règles et événements**.
2. Cliquez avec le bouton droit sur **Événements génériques** et sélectionnez **Ajouter un nouvel.**
3. Remplissez les informations et propriétés nécessaires. Pour en savoir plus, consultez la rubrique Propriétés de l'événement générique (voir "Événements génériques (propriétés)" á la page 211).
4. (facultatif) Pour valider que l'expression de la recherche est valide, saisissez une chaîne de recherche dans le champ **Contrôler si l'expression correspond à la chaîne de l'expression** correspondant aux paquets attendus :
   - **Correspondance** - la chaîne peut être validée par rapport à l'expression de la recherche.
   - **Aucune correspondance** - l'expression de la recherche est invalide. Modifiez-la et réessayez.

Dans XProtect Smart Client, vous pouvez vérifier si vos événements génériques ont été reçus par le serveur d'événement. Vous le faites dans la **Liste des alarmes** dans l'onglet **Gestionnaire des alarmes** en sélectionnant **Événements**.

Événements génériques (propriétés)

Composant	Exigences
Nom	Nom unique pour l'événement générique. Le nom doit être unique parmi tous les types d'événements, tels que les événements définis par l'utilisateur, les événements analytiques, etc.
Activé	Par défaut, les événements génériques sont activés. Supprimez la coche pour désactiver l'événement.
Expression	Expression que le système doit chercher lors de l'analyse de paquets de données. Vous pouvez vous servir des opérateurs suivants : • **( ) :** Utilisés pour garantir le traitement de termes associés en tant qu'unité logique. Ils peuvent être utilisés pour imposer un certain ordre de traitement au cours de l'analyse. **Exemple :** Les critères de recherche « (**Utilisateur001** OU **Porte053**) ET **Dimanche** » traitent les deux termes entre parenthèses en premier, puis le résultat est combiné à la dernière partie de la chaîne. Ainsi, le système cherche tout d'abord n'importe quel paquet contenant les termes **Utilisateur001** ou **Porte053**, puis il analyse les résultats pour voir quels paquets contiennent également le mot **Dimanche**. • **ET :** Avec un opérateur ET, vous indiquez que les termes des deux côtés de l'opérateur ET doivent être présents. **Exemple :** Les critères de recherche « **Utilisateur001** ET **Porte053** ET **Dimanche »** ne renvoient un résultat que si les termes **Utilisateur001**, **Porte053** et **Dimanche** sont inclus dans votre expression. Il ne suffit pas qu'un ou deux des termes soient présents. Plus vous combinez de termes avec ET, moins vous obtenez de résultats. • **OU :** Avec un opérateur OU, vous indiquez que l'un ou l'autre terme doit être présent. **Exemple :** Les critères de recherche « **Utilisateur001** OU **Porte053** OU **Dimanche »** renvoient tous les résultats contenant **Utilisateur001**, **Porte053** ou **Dimanche**. Plus vous combinez de termes avec OU, plus vous obtenez de résultats.

Type d'expression	Indique le degré de particularité du système lors de l'analyse des paquets de données reçus. Les options sont les suivantes : • **Rechercher :** Pour que l'événement ait lieu, le paquet de données reçu doit contenir le texte indiqué dans le champ **Expression :** bien qu'il puisse avoir également plus de contenu. **Exemple :** Si vous avez indiqué que le paquet reçu devait contenir les termes **Utilisateur001** et **Porte053**, l'événement est déclenché si le paquet reçu contient les termes **Utilisateur001** et **Porte053** et **Dimanche** car vos deux termes requis sont contenus dans le paquet reçu. • **Correspond :** Pour que l'événement ait lieu, le paquet de données reçu doit contenir exactement le texte indiqué dans le champ **Expression :** et rien d'autre. • **Expression standard :** Pour que l'événement ait lieu, le texte indiqué dans le champ **Expression :** doit identifier des modèles particuliers dans les paquets de données reçus. Si vous passez de **Rechercher :** ou **Correspond :** à une **Expression standard :**, le texte dans le champ **Expression :** est automatiquement traduit par une expression standard.
Priorité	La priorité doit être indiquée par un nombre compris entre 0 (priorité la plus faible) et 999999 (priorité la plus élevée). le même paquet de données peut être analysé pour différents événements. La possibilité d'attribuer une priorité à chaque événement vous permet de gérer l'événement qui doit être déclenché si un paquet reçu correspond aux critères pour plusieurs événements. Lorsque le système reçoit un paquet TCP et/ou UDP, l'analyse du paquet commence par l'analyse de l'événement à la priorité la plus élevée. Ainsi, lorsqu'un paquet correspond aux critères pour plusieurs événements, seul l'événement à la priorité la plus élevée est déclenché. Si un paquet correspond aux critères pour plusieurs événements avec une priorité identique, par ex. deux événements avec une priorité à 999, tous les événements avec cette priorité sont déclenchés.
Vérifier si l'expression correspond à la chaîne d'événement	Une chaîne d'événement à tester par rapport à l'expression saisie dans le champ **Expression :**.

Source de données d'un événement générique (propriétés)

Composant	Exigences
Source de données	Vous pouvez choisir entre deux sources de données par défaut et définir une source de données personnalisée. Votre choix dépend du type de votre programme tiers et/ou du type de matériel ou logiciel à partir duquel vous souhaitez établir une interface : **Compatible :** les propriétés par défaut sont activées, écho de tous les octets, TCP et UDP, Ipv4 uniquement, port 1234, aucun séparateur, hôte local uniquement, encodage de pages de codes actuel (ANSI). **International :** les propriétés par défaut sont activées, écho des statistiques uniquement, TCP uniquement, Ipv4+6, port 1235, <CR><LF> comme séparateur, hôte local uniquement, encodage UTF-8. (<CR><LF> = 13,10). [Source de données A] [Source de données B] etc.
Nouveau	Cliquez pour créer une nouvelle source de données.
Nom	Nom de la source de données.
Activé	Par défaut, les sources de données sont activées. Décochez la case pour désactiver la source de données.
Réinitialiser	Cliquez pour réinitialiser tous les paramètres de la source de données sélectionnée. Le nom saisi dans le champ **Nom** est conservé.
Port	Le numéro de port de la source de données.
Sélecteur type de protocole	Les protocoles que le système doit écouter et analyser en vue de détecter les événements génériques : **Tout :** TCP aussi bien que UDP. **TCP :** TCP uniquement. **UDP :** UDP uniquement. Les paquets TCP et UDP utilisés pour les événements génériques peuvent contenir des caractères spéciaux, tels que @, #, +, å, ~, et autres.
Sélecteur type IP	Types d'adresses IP à sélectionner : IPv4, IPv6 ou les deux.
Octets de séparation	Sélectionnez les octets séparateurs utilisés pour séparer les enregistrements d'événements génériques individuels. Le type de source de données **International** par défaut (consultez **Sources de données** plus haut) est **13,10**. (13,10 = <CR><IF>).

Composant	Exigences
Sélecteur type d'écho	Formats de retour d'écho disponibles : • **Statistiques d'écho :** Renvoie le format suivant : **[X],[Y],[Z],[Nom de l'événement générique]** **[X]** = numéro de demande. **[Y]** = nombre de caractères. **[Z]** = nombre de concordances avec un événement générique. **[Nom de l'événement générique]** = nom saisi dans le champ **Nom :** . • **Écho tous les octets :** Renvoie tous les octets. • **Pas d'écho :** Supprime tous les échos.
Sélecteur type d'encodage	Par défaut, la liste affiche uniquement les options les plus pertinentes. Cochez la case **Afficher tout** pour afficher tous les codages à disposition.
Afficher tout	Cf. le point précédent.
Adresses IPv4 externes autorisées	Spécifiez les adresses IP avec lesquelles le serveur de gestion doit pouvoir communiquer afin de gérer les événements externes. Vous pouvez également utiliser cette fonction pour exclure les adresses IP dont vous ne souhaitez pas recevoir de données.
Adresses IPv6 externes autorisées	Spécifiez les adresses IP avec lesquelles le serveur de gestion doit pouvoir communiquer afin de gérer les événements externes. Vous pouvez également utiliser cette fonction pour exclure les adresses IP dont vous ne souhaitez pas recevoir de données.

Astuce : Les plages peuvent être précisées dans chacune des quatre positions telles que **100, 105, 110-120**. Par exemple, toutes les adresses sur le réseau 10.10 peuvent être autorisées par **10.10.[0-254].[0-254]** ou par **10.10.255.255**.

Sécurité

Rôles

À propos des rôles

Les rôles déterminent les périphériques auxquels les utilisateurs peuvent accéder. Les rôles déterminent également les droits et assurent la sécurité au sein du système de gestion vidéo. Vous devez tout d'abord ajouter des rôles, plus ajouter des utilisateurs et des groupes et enfin, ajouter un profil Smart Client et un profil Management Client ainsi que d'autres profils par défaut appartenant à chaque rôle. Les rôles que vous pouvez créer dans le système disposent de leurs propres groupes de vues dans XProtect Smart Client, dans lesquels leurs vues sont créées et stockées.

Le système s'accompagne d'un rôle prédéfini que vous ne pouvez pas supprimer : le rôle d'**Administrateurs**. Les utilisateurs et groupes ayant le rôle **Administrateurs** bénéficient d'un accès total et illimité à l'intégralité du système. C'est pourquoi vous ne pouvez pas spécifier les paramètres du rôle pour le rôle **Administrateurs**. Le rôle **Administrateurs** est doté du profil Smart Client par défaut et des profils de verrouillage des preuves par défaut et n'a pas de profil de temps.

Les utilisateurs ayant des droits d'administrateur de l'ordinateur local sur l'ordinateur qui exécute le serveur de gestion ont automatiquement des droits d'administrateur sur le serveur de gestion. Seuls les utilisateurs à qui vous faites confiance en tant qu'administrateurs de votre système doivent avoir des droits d'administrateur de l'ordinateur local sur l'ordinateur qui exécute le serveur de gestion. Vous ne pouvez pas désactiver cette fonction. Vous ajoutez des utilisateurs et groupes au rôle **Administrateurs** tout comme vous le feriez pour tout autre rôle. Voir Assigner et supprimer des utilisateurs et groupes aux/des rôles (á la page 218).

Outre le rôle **Administrateurs**, vous pouvez ajouter autant de rôles que nécessaire en fonction de vos besoins. Vous pourriez, par exemple, avoir des rôles différents pour les utilisateurs de XProtect Smart Client en fonction des caméras auxquelles vous souhaitez qu'ils puissent accéder ou d'autres restrictions d'ordre similaire. Pour configurer les rôles dans votre système, développez le menu **Sécurité** > **Rôles**.

À propos des droits d'un rôle

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

Lorsque vous créez un rôle dans votre système, vous pouvez lui donner un nombre de droits vis-à-vis des composants ou fonctions du système auxquels le rôle en question peut accéder ou qu'il peut utiliser. Vous pouvez par exemple créer des rôles qui disposent uniquement des droits relatifs aux fonctions de XProtect Smart Client ou d'autres clients d'affichage Milestone, avec les droits nécessaires pour ne voir que certaines caméras. Si vous créez de tels rôles, ces rôles ne doivent pas avoir de droits d'accès et d'utilisation du Management Client, mais avoir uniquement accès à une partie ou à l'intégralité des fonctions disponibles dans XProtect Smart Client ou dans d'autres clients. Pour adresser ce problème, vous souhaiterez peut-être configurer un rôle disposant de certains des droits d'administrateur les plus courants, comme, par exemple, les droits d'ajout et de suppression de caméras, de serveurs et autres fonctions similaires.

Vous pouvez créer des rôles qui disposent d'une partie ou de l'intégralité des droits d'un administrateur système. Par exemple, ceci peut s'avérer pertinent si votre organisation souhaite faire la distinction entre les personnes pouvant gérer un sous-ensemble du système et les personnes qui peuvent gérer l'ensemble du système. Cette fonction vous permet de fournir des permissions différentiées aux administrateurs de façon à ce qu'ils puissent accéder à une large gamme de fonctions système, les modifier ou encore les changer, comme, par exemple, le droit de modifier les paramètres des serveurs ou caméras de votre système. Ces permissions sont spécifiées sur l'onglet Sécurité globale (voir "Onglet Sécurité globale (rôles)" á la page 221). Au minimum, pour permettre à l'administrateur du système différencié de lancer le Management Client, vous devez accorder des permissions Lire à ce rôle sur le serveur de gestion.

Vous pouvez également refléter ces restrictions dans l'interface utilisateur du Management Client pour chaque rôle en associant le rôle à un profil Management Client supprimant les fonctions système correspondantes de l'interface utilisateur. Voir À propos des profils Management Client (á la page 169) pour de plus amples informations.

Pour doter un rôle de tels droits d'administrateur différenciés, la personne détentrice du rôle d'administrateur complet par défaut doit installer le rôle dans **Sécurité** > **Rôles > Onglet info > Ajouter nouveau**. Lorsque vous configurez le nouveau rôle, vous pouvez ensuite associer le rôle à vos propres profils comme vous le feriez pour tout autre rôle dans le système, ou utiliser les profils par défaut du système. Pour de plus amples informations, voir Ajouter et gérer un rôle (á la page 217).

Une vois que vous avez spécifiez les profils que vous souhaitez associer au rôle, allez dans l'onglet **Sécurité globale** pour spécifier les droits du rôle.

Les droits que vous pouvez configurer pour un rôle sont différents d'un produit à l'autre. Vous ne pouvez accorder tous les droits disponibles à un rôle que dans XProtect Corporate.

À propos des utilisateurs

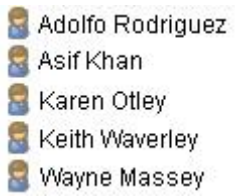
Le terme **utilisateurs** fait principalement référence aux utilisateurs en mesure de se connecter au système de surveillance par le biais des clients. Vous pouvez configurer ces utilisateurs des deux manières suivantes :

- En tant qu'**utilisateurs de base**, authentifiés par une combinaison nom d'utilisateur/mot de passe.
- En tant qu'**utilisateurs Windows**, authentifiés à partir de leurs identifiants de connexion Windows.

Utilisateurs Windows

Vous pouvez ajouter des utilisateurs Windows en utilisant Active Directory. Active Directory (AD) est un service d'annuaire mis en œuvre par Microsoft pour les réseaux avec domaine Windows. Il est inclus dans la plupart des systèmes d'exploitation Windows Server. Il identifie les ressources sur un réseau afin que les utilisateurs ou applications puissent y accéder. L'Active Directory utilise les concepts d'utilisateurs et de groupes.

Les utilisateurs sont des objets de l'Active Directory représentant des individus avec un compte utilisateur. Exemple :



Les groupes sont des objets de l'Active Directory contenant plusieurs utilisateurs. Dans cet exemple, le Groupe d'administration compte trois utilisateurs :

Les groupes peuvent contenir un nombre illimité d'utilisateurs. En ajoutant un groupe au système, vous ajoutez tous ses membres en même temps. Une fois que vous avez ajouté le groupe au système, toute modification effectuée ultérieurement sur le groupe dans l'Active Directory, lorsque vous ajoutez de nouveaux membres ou supprimez d'anciens membres ultérieurement par exemple, sera immédiatement reflétée dans le système. Notez qu'un utilisateur peut être un membre appartenant à plusieurs groupes en même temps.

Vous pouvez utiliser Active Directory pour ajouter au système des informations existantes sur les utilisateurs et groupes et en tirer des avantages :

- Les utilisateurs et groupes sont spécifiés centralement dans Active Directory. Vous n'avez donc pas à créer des comptes utilisateur à partir de rien.
- Vous n'avez pas besoin de configurer l'authentification des utilisateurs du système car Active Directory prend l'authentification en charge.

Avant que vous puissiez ajouter des utilisateurs et groupes par le biais du service Active Directory, vous devez disposer d'un serveur doté d'Active Directory installé sur votre réseau.

Utilisateurs de base

Si votre système ne dispose pas d'un accès à Active Directory, créez un utilisateur basique (voir "À propos des utilisateurs basiques" á la page 248). Pour obtenir des informations sur la configuration des utilisateurs basiques, voir Créer un utilisateur basique (voir "Créer des utilisateurs de base" á la page 248).

Ajouter et gérer un rôle

1. Développez **Sécurité**, et cliquez avec le bouton droit sur **Rôles**.
2. Sélectionnez **Ajouter un rôle**. La boîte de dialogue **Ajouter rôle** s'ouvre.
3. Saisissez un nom et une description du nouveau rôle et cliquez sur **OK**.
4. Le nouveau rôle est ajouté à la liste **Rôles**. Par défaut, un nouveau rôle n'est associé à aucun utilisateur/groupe, mais est associé à divers profils par défaut.
5. Pour choisir des profils Smart Client et Management Client différents, des profils de verrouillage des preuves ou des profils de temps, cliquez sur les menus déroulants.
6. Vous pouvez maintenant assigner les utilisateurs/groupes au rôle, et spécifier à quelles fonctions du système ils peuvent accéder.

Voir également Assigner et supprimer des utilisateurs et groupes aux/des rôles (á la page 218) et Paramètres des rôles (á la page 219).

Copier, renommer ou supprimer un rôle

Copier un rôle

Si vous avez un rôle avec des paramètres et/ou droits complexes et qu'il vous faut un rôle similaire ou quasi similaire, il peut être plus simple de copier le rôle déjà existant et d'apporter de petites modifications à la copie plutôt que de créer un nouveau rôle à partir de zéro.

1. Développez le menu **Sécurité**, cliquez sur **Rôles,** faites un clic droit sur le rôle pertinent et sélectionnez **Copier Rôle**.
2. Dans la boîte de dialogue qui s'ouvre, donnez au rôle copié un nouveau nom spécifique ainsi qu'une description.
3. Cliquez sur **OK**.

Renommer un rôle

Si vous renommez un rôle, cela ne modifie pas le nom du groupe de vues basé sur le rôle.

1. Développez **Sécurité**, et cliquez avec le bouton droit sur **Rôles**.

2. Faites un clic droit sur le rôle requis et sélectionnez **Renommer Rôle**
3. Dans la boîte de dialogue qui s'ouvre, modifiez le nom du rôle.
4. Cliquez sur **OK**.

Supprimer un rôle

1. Développez **Sécurité**, et cliquez sur **Rôles**.
2. Cliquez avec le bouton droit sur le rôle indésirable, puis sélectionnez **Supprimer**.
3. Cliquez sur **Oui**.

Important : Si vous supprimez un rôle, vous ne supprimez pas automatiquement le groupe de vues basé sur le rôle.

Assigner et supprimer des utilisateurs et groupes aux/des rôles

Pour assigner ou supprimer des utilisateurs Windows ou groupes ou des utilisateurs de base à/d'un rôle :

1. Développez **Sécurité**, et cliquez avec le bouton droit sur **Rôles**. Ensuite, sélectionnez le rôle requis dans le volet **Vue d'ensemble** :
2. Dans le **panneau Propriétés**, sélectionnez l'onglet **Utilisateurs et Groupes** en bas.
3. Cliquez sur **Ajouter**, sélectionnez **Utilisateur Windows** ou **Utilisateur de base**.

Assigner des utilisateurs Windows et groupes à un rôle

1. Sélectionner **utilisateur Windows**. Cela ouvre la boîte de dialogue **Sélectionner des utilisateurs, ordinateurs et groupes** :
2. Vérifiez que le type d'objet requis est spécifié. Si, par exemple, il vous faut ajouter un ordinateur, cliquez sur **Types d'objet** et indiquez **Ordinateur**. Vérifiez également que le domaine requis figure dans le champ **À partir de cet emplacement**. Dans le cas contraire, cliquez sur le bouton **Emplacements** afin de rechercher le domaine requis.
3. Dans la case **Entrer les noms d'objet à sélectionner**, saisissez les noms des utilisateurs, initiales, ou autres types d'identifiant pertinents que l'Active Directory peut reconnaître. Utilisez la fonction **Vérifier les noms** pour vérifier qu'Active Directory reconnaît bien les noms ou initiales que vous avez saisis. Autrement, utilisez la fonction **« Avancé... »** pour rechercher des utilisateurs et des groupes.
4. Cliquez sur **OK**. Les utilisateurs/ groupes sélectionnés sont maintenant ajoutés à la liste des utilisateurs de l'onglet **Utilisateurs et Groupes** que vous avez assignés au rôle sélectionné. Vous pouvez ajouter plus d'utilisateurs et de groupes en saisissant plusieurs noms séparés par un point-virgule (**;**).

Assigner des utilisateurs de base à un rôle

1. Sélectionner un **utilisateur basique**. Cela ouvre la boîte de dialogue **Sélectionner des utilisateurs de base à ajouter au rôle** :
2. Sélectionnez le(s) utilisateur(s) basique(s) que vous souhaitez assigner à ce rôle.

3. Facultatif : Cliquez sur **Nouveau** pour créer une nouvelle source de données.
4. Cliquez sur **OK**. Les utilisateurs basiques sélectionnés sont maintenant ajoutés à la liste des utilisateurs basiques de l'onglet **Utilisateurs et Groupes** qui ont été assignés au rôle sélectionné.

Supprimer des utilisateurs et groupes d'un rôle

1. Dans l'onglet **Utilisateurs et Groupes**, sélectionnez l'utilisateur ou le groupe que vous souhaitez supprimer et cliquez sur le bouton **Supprimer** en bas de l'onglet. Vous pouvez sélectionner plusieurs utilisateurs ou groupes, ou une combinaison de groupes et d'utilisateurs individuels, le cas échéant.
2. Confirmez que vous souhaitez supprimer le ou les utilisateur(s) et/ou groupe(s). Cliquez sur **Oui**.

Un utilisateur peut également avoir des rôles au travers d'appartenances à des groupes. Auquel cas, vous ne pouvez supprimer l'utilisateur individuel du rôle. Par ailleurs, les membres de groupes peuvent également avoir des rôles en tant qu'individus. Pour voir les rôles que les utilisateurs, groupes, ou membres individuels d'un groupe ont, utilisez la fonction **Afficher les rôles effectifs**.

Afficher les rôles effectifs

Grâce à la fonction Rôles effectifs, vous pouvez afficher tous les rôles d'un utilisateur ou groupe sélectionné. Ceci peut s'avérer pratique si vous utilisez des groupes et qu'il s'agit du leur moyen de voir à quels rôles un utilisateur spécifique est affilié.

1. Ouvrez la fenêtre **Rôles effectifs** en développant **Sécurité**, puis faites un clic droit sur **Rôles et sélectionnez Rôles effectifs**.
2. Si vous voulez en savoir plus sur un utilisateur basique, tapez le nom dans le champ **Nom d'utilisateur**. Cliquez sur **Réactualiser** pour afficher les rôles de l'utilisateur.
3. Si vous utilisez des utilisateurs ou des groupes Windows dans Active Directory, cliquez sur le bouton parcourir "...". Sélectionnez le type d'objet, entrez le nom et cliquez sur **OK**. Les rôles d'utilisateur s'affichent automatiquement.

Paramètres des rôles

Onglet Info (rôles)

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

Dans l'onglet **Info** d'un rôle, vous pouvez configurer les éléments suivants :

Nom	Description
Nom	Saisissez un nom pour le rôle.
Description	Saisissez une description pour le rôle.

Nom	Description
Profil Management Client	Sélectionnez un profil Management Client pour l'associer au rôle. Vous ne pouvez pas appliquer ceci au rôle d'**Administrateurs** par défaut. Nécessite une autorisation pour gérer la sécurité du serveur de gestion.
Profil Smart Client	Sélectionnez un profil Smart Client pour l'associer au rôle. Nécessite une autorisation pour gérer la sécurité du serveur de gestion.
Profil de temps par défaut	Sélectionnez un profil de temps par défaut pour l'associer au rôle. Vous ne pouvez pas appliquer ceci au rôle d'**Administrateurs** par défaut.
Profils de verrouillage des preuves	Sélectionnez un profil de verrouillage des preuves pour l'associer au rôle.
Connexion Smart Client au sein du profil de temps	Sélectionnez un profil de temps pour lequel l'utilisateur XProtect Smart Client associé à ce rôle est autorisé à se connecter. Si l'utilisateur XProtect Smart Client est connecté lorsque la période prend fin, il ou elle est alors déconnecté automatiquement. Vous ne pouvez pas appliquer ceci au rôle d'**Administrateurs** par défaut.
Autorisation de connexion requise	Cochez la case pour associer l'autorisation de connexion au rôle. Cela signifie que, lorsque l'utilisateur se connecte, XProtect Smart Client ou le Management Client demande une deuxième autorisation, généralement par un superutilisateur ou responsable. Pour permettre aux administrateurs d'autoriser des utilisateurs, configurez le droit **Autoriser utilisateurs** du serveur de gestion dans l'onglet **Sécurité globale**. Vous ne pouvez pas appliquer ceci au rôle d'**Administrateurs** par défaut.
Rendre les utilisateurs anonymes au cours des sessions PTZ	Cochez la case pour masquer les noms des utilisateurs associés à ce rôle lorsqu'ils contrôlent des sessions PTZ.

Onglet Utilisateur et Groupes (rôles)

Dans l'onglet **Utilisateurs et groupes**, vous assignez des utilisateurs et des groupes à des rôles (voir "Assigner et supprimer des utilisateurs et groupes aux/des rôles" á la page 218). Vous pouvez assigner des utilisateurs et groupes Windows ou des utilisateurs basiques (voir "À propos des utilisateurs" á la page 216).

Nom	Description
Nom	Affiche le nom de l'utilisateur ou du groupe assigné à ce rôle.

Nom	Description
Description	Affiche la description que vous avez saisie lors de la création de l'utilisateur basique.

Onglet Sécurité globale (rôles)

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

Dans l'onglet **Sécurité globale**, vous pouvez configurer les droits globaux des rôles. Pour chaque composant disponible dans votre système, décidez d'**Autoriser** ou de **Refuser** aux utilisateurs affectés au rôle les droits d'accès et d'utilisation de différentes parties du composant pertinent.

Les paramètres de sécurité globaux s'appliquent uniquement au site actuel.

Vous pouvez associer un utilisateur à plus d'un rôle. Si vous sélectionnez **Refuser** pour un paramètre de sécurité pour un rôle et **Autoriser** pour un autre, le **Refus** de permission prime sur l'**Autorisation** de permission.

L'onglet **Sécurité globale** est disponible dans XProtect Corporate et XProtect Expert, mais l'onglet vous donne la possibilité de modifier plus de fonctions dans XProtect Corporate que dans XProtect Expert. En effet, vous pouvez configurer des droits d'administrateur différenciés dans XProtect Corporate, tandis que ces droits ne sont pas disponibles dans XProtect Expert. Cependant, vous pouvez configurer des droits globaux pour un rôle utilisant XProtect Smart Client dans les deux produits XProtect.

Dans ce qui suit, les descriptions présentent ce qui se produit au niveau de chaque droit individuel pour les différents composants du système si vous sélectionnez **Autoriser** pour le rôle pertinent. Si vous utilisez XProtect Expert, vous pouvez voir quels sont les paramètres qui ne vous sont pas disponibles sous chaque composant du système.

Pour chaque composant ou fonction du système, l'administrateur système complet peut utiliser les cases **Autoriser** ou **Refuser** pour configurer les permissions de sécurité du rôle. Chaque permission de sécurité établie s'applique à l'ensemble du composant ou de la fonction du système. Ainsi, par exemple, si vous cochez la case **Refuser** pour les **Caméras**, toutes les caméras ajoutées sur le système sont indisponibles pour ce rôle. À l'inverse, si vous cochez la case **Autoriser** à la place, le rôle peut voir toutes les caméras ajoutées sur le système. Suite à la sélection d'**Autoriser** ou **Refuser** sur vos caméras, les paramètres des caméras sur l'onglet **Périphérique** héritent alors des sélections que vous avez effectuées dans l'onglet **Sécurité globale** de façon à ce que toutes les caméras soient disponibles ou indisponibles pour le rôle en question.

Si vous souhaitez configurer des permissions de sécurité pour chaque caméra ou similaire, vous ne pouvez configurer ces permissions individuelles dans l'onglet du composant ou de la fonction correspondant que si vous avez désactivé tous les paramètres globaux pour le composant ou la fonction du système dans l'onglet **Sécurité globale**.

Les descriptions ci-dessous s'appliquent également aux droits que vous pouvez configurer par l'intermédiaire des SDK MIP.

Si vous passez d'une licence de base XProtect Corporate à une licence XProtect Expert, vous ne pouvez y parvenir que si vous n'avez pas configuré de droits de sécurité du rôle pour la fonction qui n'est pas disponible dans XProtect Expert. Ainsi, pour effectuer un tel transfert, assurez-vous de supprimer tous les droits de sécurité qui sont disponibles uniquement sur XProtect Corporate.

Serveur de gestion

Droit de sécurité	Description	XProtect Expert
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
Lire	Active le droit d'accéder à un large éventail de fonctionnalités, y compris : • Se connecter avec le Management Client. • Liste des tâches actuelles • Journaux des serveurs. Active également l'accès aux fonctionnalités suivantes : • Services de connexion à distance • Profils Smart Client • Profils Management Client • Matrix • Profils de temps • Serveurs enregistrés et Enregistrement de service API • Serveurs Enterprise.	Non disponible
Modifier	Active le droit de modifier les données dans un large éventail de fonctionnalités, y compris : • Options • Gestion des licences. Permet également aux utilisateurs de créer, de supprimer et de modifier les fonctionnalités suivantes : • Services de connexion à distance • Groupes de périphériques • Matrix • Profils de temps • Profils de notification • Serveurs enregistrés • Serveurs Enterprise. Active le droit de configurer des plages IP locales lors de la configuration du réseau sur le serveur d'enregistrement.	Non disponible
Moniteur système	Active le droit de consulter les données du moniteur système.	

Droit de sécurité	Description	XProtect Expert
État API	Active le droit d'exécuter des demandes concernant l'état API situé sur le serveur d'enregistrement. Cela signifie que le rôle pour lequel ce droit est activé dispose d'un accès suffisant pour lire l'état des éléments situés sur le serveur d'enregistrement.	
Hiérarchie des sites fédérés	Active le droit d'ajouter ou de détacher le site actuel à d'autres sites dans une hiérarchie des sites fédérés. Si vous autorisez uniquement l'accès à un site enfant, l'utilisateur peut toujours le connecter au site parent.	Non disponible
Sauvegarde de configuration	Active le droit de création de sauvegardes de la configuration du système à l'aide de la fonction de sauvegarde/restauration du système.	Non disponible
Autoriser des utilisateurs	Active le droit d'autorisation d'utilisateurs lorsqu'une seconde authentification leur est demandée dans XProtect Smart Client ou Management Client. Vous déterminez si un rôle nécessite une autorisation de connexion dans l'onglet **Info**.	
Gérer la sécurité	Active le droit de gestion des permissions pour le Management Server. Permet également aux utilisateurs de créer, de supprimer et de modifier les fonctionnalités suivantes : • Rôles • Utilisateurs de base • Profils Smart Client • Profils Management Client.	Non disponible

Serveurs d'enregistrement

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
Modifier	Active le droit de modification des propriétés sur les serveurs d'enregistrement, sauf pour les paramètres de configuration du réseau qui nécessite un droit **Modifier** sur le serveur de gestion.

Supprimer	Active le droit de suppression des serveurs d'enregistrement. Pour ce faire, vous devez également octroyer les permissions de suppression d'utilisateurs sur : • les groupes de sécurité matérielle si vous avez ajouté du matériel au serveur d'enregistrement. Si un des dispositifs situés sur le serveur d'enregistrement contient des preuves verrouillées, vous pouvez uniquement supprimer le serveur d'enregistrement s'il est hors ligne.
Gérer le matériel	Active le droit d'ajouter du matériel sur les serveurs enregistrés.
Gérer le stockage	Active le droit d'administration des conteneurs de stockage sur le serveur d'enregistrement, c'est-à-dire le droit de créer, de supprimer, de déplacer et de vider des conteneurs de stockage.
Autoriser le serveur d'enregistrement	Active le droit d'autorisation de nouveaux serveurs d'enregistrement.
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour des serveurs d'enregistrement.

Serveurs de redondance

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
Lire	Active le droit d'accéder aux et de consulter les serveurs de basculement dans le Management Client.
Modifier	Active le droit de créer, mettre à jour, supprimer, déplacer et activer/désactiver les serveurs de redondance dans le Management Client.
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour les serveurs de secours.

Serveurs portabless

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
Lire	Active le droit d'accéder aux et de consulter les serveurs portablesserveurs portables dans le Management Client.
Modifier	Active le droit de modifier et supprimer les serveurs portablesserveurs portables dans le Management Client.
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour les serveurs portablesserveurs portables.
Créer	Active le droit d'ajouter des serveurs portables sur le système.

Matériel

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
Modifier	Active le droit de modification des propriétés du matériel.
Supprimer	Active le droit de suppression de matériel. Si un des dispositifs matériels contient des preuves verrouillées, vous pouvez uniquement supprimer le matériel lorsque le serveur d'enregistrement est hors ligne.
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour le matériel.

Caméras

Droit de sécurité	Description	XProtect Expert
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
Lire	Active le droit de visualisation des caméras dans les clients et dans le Management Client.	
Modifier	Active le droit de modification des propriétés pour les caméras dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver une caméra.	Non disponible
Voir en direct	Active le droit de consultation de vidéos en direct à partir des caméras dans les clients et dans le Management Client.	
Lecture	Active le droit de lecture de vidéos enregistrées à partir des caméras dans tous les clients.	
Rappeler les enregistrements à distance	Active le droit de rappeler les enregistrements des clients depuis les caméras se trouvant dans des sites distants ou sur le stockage externe des caméras.	
Lire les séquences	Active le droit de lecture des informations séquentielles liées à l'explorateur de séquence dans les clients, par exemple.	
Recherche avancée	Active le droit d'utilisation de la fonction de recherche avancée dans les clients.	
Export	Active le droit d'exporter des enregistrements à partir des clients.	
Créer des signets	Active le droit de création de signet dans des vidéos enregistrées et en direct dans les clients.	
Lire des signets	Active le droit de recherche et de lecture des détails des signets dans les clients.	

Droit de sécurité	Description	XProtect Expert
Modifier des signets	Active le droit de modification des signets dans les clients.	
Supprimer des signets	Active le droit de suppression de signets dans les clients.	
Création et extension du verrouillage des preuves	Active le droit de création et d'extension du verrouillage des preuves dans les clients.	Non disponible
Lire les preuves verrouillées	Active le droit de recherche et de lecture de preuves verrouillées dans les clients.	Non disponible
Suppression et réduction du verrouillage des preuves	Active le droit de suppression ou de réduction du verrouillage des preuves dans les clients.	Non disponible
Démarrer l'enregistrement manuel	Active le droit de démarrer l'enregistrement manuel de la vidéo dans les clients.	
Arrêter l'enregistrement manuel	Active le droit d'arrêter l'enregistrement manuel de la vidéo dans les clients.	
Commandes AUX	Active le droit d'utiliser des commandes auxiliaires (AUX) sur la caméra à partir des clients. Les **commandes AUX** permettent aux utilisateurs de contrôler, par exemple, les essuie-glaces d'une caméra connectée via un encodeur vidéo. Les périphériques associés à la caméra, connectés via des connexions auxiliaires, sont contrôlés depuis le client.	
PTZ manuel	Active le droit d'utilisation des fonctions PTZ sur les caméras PTZ dans les clients et dans le Management Client.	
Activer des positions prédéfinies PTZ ou des profils de patrouille	Active le droit de déplacer des caméras PTZ vers des positions prédéfinies, de démarrer et arrêter des profils de patrouille et de mettre des patrouilles en pause dans les clients et dans le Management Client. Pour autoriser ce rôle à utiliser d'autres fonctions PTZ sur la caméra, activez le droit **PTZ manuel**.	
Gérer les positions prédéfinies PTZ ou les profils de patrouille	Active le droit d'ajouter, de modifier et d'effacer les positions et les profils de patrouille sur les caméras PTZ, dans les clients et dans le Management Client. Pour autoriser ce rôle à utiliser d'autres fonctions PTZ sur la caméra, activez le droit **PTZ manuel**.	
Verrouiller/Déverrouiller des positions prédéfinies PTZ	Active le droit de bloquer et débloquer les positions PTZ prédéfinies dans le Management Client. Ceci empêche ou autorise d'autres utilisateurs à changer les positions prédéfinies dans les clients et dans le Management Client.	Non disponible

Droit de sécurité	Description	XProtect Expert
Réserver des sessions PTZ	Active le droit de paramétrer les caméras PTZ en mode de session réservée dans les clients et dans le Management Client. Dans une session PTZ réservée, d'autres utilisateurs dotés d'une priorité PTZ supplémentaire ne peuvent pas prendre le contrôle. Pour autoriser ce rôle à utiliser d'autres fonctions PTZ sur la caméra, activez le droit **PTZ manuel**.	Non disponible
Libérer les sessions PTZ	Active le droit de libérer les sessions PTZ d'autres utilisateurs du Management Client. Vous pouvez toujours libérer vos propres sessions PTZ, même sans cette permission.	Non disponible
Supprimer des enregistrements	Active le droit de suppression des enregistrements vidéo stockés à partir du système via le Management Client.	Non disponible
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client.	Non disponible

Microphones

Droit de sécurité	Description	XProtect Expert
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
Lire	Active le droit de visualisation des microphones dans les clients et dans le Management Client.	
Modifier	Active le droit de modification des propriétés pour les microphones dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver des microphones.	Non disponible
Écouter	Active le droit d'écoute d'audio en direct à partir des microphones dans les clients et dans le Management Client.	
Lecture	Active le droit de lecture d'audio enregistré à partir des microphones dans les clients.	
Rappeler les enregistrements à distance	Active le droit de rappeler les enregistrements des clients depuis les microphones se trouvant dans des sites distants ou sur le stockage externe des caméras.	
Lire les séquences	Active le droit de lecture des informations séquentielles liées à l'explorateur de séquence dans les clients, par exemple.	
Export	Active le droit d'exporter des enregistrements à partir des clients.	
Créer des signets	Active le droit de création de signets dans les clients.	

Droit de sécurité	Description	XProtect Expert
Lire des signets	Active le droit de recherche et de lecture des détails des signets dans les clients.	
Modifier des signets	Active le droit de modification des signets dans les clients.	
Supprimer des signets	Active le droit de suppression de signets dans les clients.	
Création et extension du verrouillage des preuves	Active le droit de création ou d'extension du verrouillage des preuves dans les clients.	Non disponible
Lire les preuves verrouillées	Active le droit de recherche et de lecture des détails des preuves verrouillées dans les clients.	Non disponible
Suppression et réduction du verrouillage des preuves	Active le droit de suppression ou de réduction du verrouillage des preuves dans les clients.	Non disponible
Démarrer l'enregistrement manuel	Active le droit de démarrer l'enregistrement manuel de l'audio dans les clients.	
Arrêter l'enregistrement manuel	Active le droit d'arrêter l'enregistrement manuel de l'audio dans les clients.	
Supprimer des enregistrements	Active le droit de suppression des enregistrements stockés à partir du système.	Non disponible
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour les microphones.	Non disponible

Haut-parleurs

Droit de sécurité	Description	XProtect Expert
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
Lire	Active le droit de visualisation des haut-parleurs dans les clients et dans le Management Client.	
Modifier	Active le droit de modification des propriétés pour les haut-parleurs dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver des haut-parleurs.	Non disponible
Écouter	Active le droit d'écoute d'audio en direct à partir des haut-parleurs dans les clients et dans le Management Client.	
Parole	Active le droit de parler dans les haut-parleurs au sein des clients.	

Droit de sécurité	Description	XProtect Expert
Lecture	Active le droit de lecture d'audio enregistré à partir des haut-parleurs dans les clients.	
Rappeler les enregistrements à distance	Active le droit de rappeler les enregistrements des clients depuis les haut-parleurs se trouvant dans des sites distants ou sur le stockage externe des caméras.	
Lire les séquences	Active le droit d'utilisation de la fonctionnalité Séquences tout en parcourant l'audio enregistré à partir des haut-parleurs dans les clients.	
Export	Active le droit d'export d'audio enregistré à partir des haut-parleurs dans les clients.	
Créer des signets	Active le droit de création de signets dans les clients.	
Lire des signets	Active le droit de recherche et de lecture des détails des signets dans les clients.	
Modifier des signets	Active le droit de modification des signets dans les clients.	
Supprimer des signets	Active le droit de suppression de signets dans les clients.	
Création et extension du verrouillage des preuves	Active le droit de création ou d'extension du verrouillage des preuves sur l'audio enregistré dans les clients.	Non disponible
Lire les preuves verrouillées	Active le droit de consultation du verrouillage des preuves sur l'audio enregistré dans les clients.	Non disponible
Suppression et réduction du verrouillage des preuves	Active le droit de suppression ou de réduction du verrouillage des preuves sur l'audio enregistré dans les clients.	Non disponible
Démarrer l'enregistrement manuel	Active le droit de démarrer l'enregistrement manuel de l'audio dans les clients.	
Arrêter l'enregistrement manuel	Active le droit d'arrêter l'enregistrement manuel de l'audio dans les clients.	
Supprimer des enregistrements	Active le droit de suppression des enregistrements stockés à partir du système.	Non disponible
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour les haut-parleurs.	Non disponible

Métadonnées

Droit de sécurité	Description	XProtect Expert
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	

Droit de sécurité	Description	XProtect Expert
Lire	Active le droit de réception de métadonnées dans les clients.	
Modifier	Active le droit de modification des propriétés pour les métadonnées dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver des périphériques de métadonnées.	Non disponible
En direct	Active le droit de réception de métadonnées en direct à partir des caméras dans les clients.	
Lecture	Active le droit de lecture de données enregistrées à partir des périphériques de métadonnées dans les clients.	
Rappeler les enregistrements à distance	Active le droit de rappeler les enregistrements des clients depuis les périphériques de métadonnées se trouvant dans des sites distants ou sur le stockage externe des caméras.	
Lire les séquences	Active le droit de lecture des informations séquentielles liées à l'explorateur de séquence dans les clients, par exemple.	
Export	Active le droit d'exporter des enregistrements dans les clients.	
Création et extension du verrouillage des preuves	Active le droit de création du verrouillage des preuves dans les clients.	Non disponible
Lire les preuves verrouillées	Active le droit de consultation du verrouillage des preuves dans les clients.	Non disponible
Suppression et réduction du verrouillage des preuves	Active le droit de suppression ou de réduction du verrouillage des preuves dans les clients.	Non disponible
Démarrer l'enregistrement manuel	Active le droit de démarrer l'enregistrement manuel des métadonnées dans les clients.	
Arrêter l'enregistrement manuel	Active le droit d'arrêter l'enregistrement manuel des métadonnées dans les clients.	
Supprimer des enregistrements	Active le droit de suppression des enregistrements stockés à partir du système.	Non disponible
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour les métadonnées.	Non disponible

Entrées

Droit de sécurité	Description	XProtect Expert
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	Non disponible
Lire	Active le droit de visualisation des périphériques de saisie dans les clients et dans le Management Client.	
Modifier	Active le droit de modification des propriétés pour les périphériques d'entrée dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver un périphérique d'entrée.	Non disponible
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour les périphériques de saisie.	Non disponible

Sortie

Droit de sécurité	Description	XProtect Expert
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
Lire	Active le droit de visualisation des périphériques de sortie dans les clients.	
Modifier	Active le droit de modification des propriétés pour les périphériques de sortie dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver un périphérique de sortie.	Non disponible
Activer	Active le droit d'activation de sorties dans les clients.	
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour les périphériques de sortie.	Non disponible

Smart Wall

Droit de sécurité	Description	XProtect Expert
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
Lire	Active le droit de visualisation des Smart Walls dans les clients.	
Modifier	Active le droit de modification des propriétés pour les Smart Wall dans le Management Client.	Non disponible
Supprimer	Active le droit de suppression des Smart Walls existants dans le Management Client.	Non disponible

Droit de sécurité	Description	XProtect Expert
Opérer	Active le droit d'activer et modifier les Smart Walls, par exemple pour modifier et activer des préréglages ou affecter des caméras à des vues dans les clients et dans le Management Client.	
Créer Smart Wall	Active le droit de création de nouveaux Smart Walls dans le Management Client.	Non disponible
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour le Smart Wall.	Non disponible
Lecture	Active le droit de lecture de données enregistrées à partir des Smart Walls dans les clients.	

Groupes de vues

Droit de sécurité	Description	XProtect Expert
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
Lire	Active le droit de visualisation des groupes de vues dans les clients et dans le Management Client. Les groupes de vues sont créés dans le Management Client.	
Modifier	Active le droit de modification des propriétés pour les groupes de vues dans le Management Client.	Non disponible
Supprimer	Active le droit de suppression des groupes de vues dans le Management Client.	
Opérer	Active le droit d'utilisation de groupes de vues dans XProtect Smart Client. Autrement dit, la création de sous-groupes et de vues.	
Créer un groupe de vues	Active le droit de création des groupes de vues dans le Management Client.	Non disponible
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour les groupes de vues.	Non disponible

Événements définis par l'utilisateur

Droit de sécurité	Description	XProtect Expert
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
Lire	Active le droit d'afficher des événements définis par les utilisateurs dans les clients.	

Droit de sécurité	Description	XProtect Expert
Modifier	Active le droit de modification des propriétés pour les événements définis par les utilisateurs dans le Management Client.	Non disponible
Supprimer	Active le droit de visualiser des événements définis par les utilisateurs dans le Management Client.	Non disponible
Déclencher	Active le droit de déclencher des événements définis par les utilisateurs dans les clients.	
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour les événements définis par les utilisateurs dans le Management Client.	Non disponible
Créer un événement défini par l'utilisateur	Active le droit de création de nouveaux événements définis par les utilisateurs dans le Management Client.	Non disponible

Événements génériques

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
Lire	Active le droit de visualisation des événements génériques dans les clients et dans le Management Client.
Modifier	Active le droit de modifier des propriétés pour les événements génériques dans le Management Client.
Supprimer	Active le droit de visualiser des événements génériques dans le Management Client.
Gérer la sécurité	Active le droit de gérer les permissions de sécurité des événements génériques dans le Management Client.
Créer	Active le droit de créer de nouveaux événements génériques dans le Management Client.

Événements analytiques

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
Lire	Active le droit de visualiser des événements analytiques dans le Management Client.
Modifier	Active le droit de modifier des propriétés pour les événements analytiques dans le Management Client.

Droit de sécurité	Description
Supprimer	Active le droit de visualiser des événements analytiques dans le Management Client.
Créer	Active le droit de créer de nouveaux événements analytiques dans le Management Client.
Gérer la sécurité	Active le droit de gérer les permissions de sécurité des événements analytiques dans le Management Client.

Matrix

Droit de sécurité	Description	XProtect Expert
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	Non disponible
Lire	Active le droit de sélectionner et d'envoyer une vidéo au destinataire Matrix à partir des clients.	
Modifier	Active le droit de modification des propriétés pour les Matrix dans le Management Client.	Non disponible
Supprimer	Active le droit de suppression des Matrix existants dans le Management Client.	Non disponible
Créer Matrix	Active le droit de création de nouveaux Matrix dans le Management Client.	Non disponible
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour tous les Matrix.	Non disponible

Règles

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
Lire	Active le droit de visualiser des règles existantes dans le Management Client.
Modifier	Active le droit de modification des propriétés pour les règles et de définition du comportement des règles dans le Management Client. Il requiert également que l'utilisateur dispose de permissions de lecture sur tous les périphériques affectés par la règle.
Supprimer	Active le droit de suppression de règles dans le Management Client. Il requiert également que l'utilisateur dispose de permissions de lecture sur tous les périphériques affectés par la règle.

Droit de sécurité	Description
Créer règle	Active le droit de création de nouvelles règles dans le Management Client. Il requiert également que l'utilisateur dispose de permissions de lecture sur tous les périphériques affectés par la règle.
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour toutes les règles.

Sites

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
Lire	Active le droit de visualiser d'autres sites dans le Management Client. Les sites connectés sont connectés par le biais de Milestone Federated Architecture. Pour modifier les propriétés vous devez avoir des permissions de modification sur le serveur de gestion de chaque site.
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour tous les sites.

Alarmes

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
Lire	Active le droit de visualiser les définitions d'alarmes, les sons d'alarmes et les paramètres des données d'alarmes dans le Management Client. L'onglet **Serveur d'événements** de la fenêtre de dialogue **Options** n'apparaît que lorsque vous choisissez d'activer cette fonction.
Modifier	Active le droit de modifier les propriétés des définitions d'alarmes, des sons d'alarmes et des paramètres des données d'alarmes dans le Management Client.
Supprimer	Active le droit de supprimer des définitions d'alarmes dans le Management Client.
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour les alarmes.
Créer	Active le droit de créer de nouvelles définitions d'alarmes dans le Management Client.

Contrôle d'accès

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
Lire	Active le droit de visualisation des propriétés pour les systèmes de contrôle d'accès dans le Management Client.
Modifier	Active le droit de modifier des propriétés pour les systèmes de contrôle d'accès dans le Management Client.
Supprimer	Active le droit de supprimer des systèmes de contrôle d'accès dans le Management Client.
Créer	Active le droit de créer de nouveaux systèmes de contrôle d'accès dans le Management Client.
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour tous les systèmes de contrôle d'accès.

Moniteurs système

Droit de sécurité	Description
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
Lire	Active le droit de visualiser les moniteurs système dans XProtectSmart Client.
Modifier	Active le droit de modifier les propriétés des moniteurs système dans le Management Client.
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour tous les moniteurs système.

Sources de transaction

Droit de sécurité	Description
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
Lire	Active le droit de visualisation des propriétés pour les sources de transactions dans le Management Client.
Modifier	Active le droit de modification des propriétés pour les sources de transactions dans le Management Client.
Supprimer	Active le droit de supprimer des sources de transactions dans le Management Client.
Créer	Active le droit de créer de nouvelles sources de transactions dans le Management Client.

Droit de sécurité	Description
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour toutes les sources de transactions dans le Management Client.

Définitions de transactions

Droit de sécurité	Description
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
Lire	Active le droit de visualisation des propriétés des définitions de transactions dans le Management Client.
Modifier	Active le droit de modification des propriétés des définitions de transactions dans le Management Client.
Supprimer	Active le droit de suppression des définitions de transactions dans le Management Client.
Créer	Active le droit de créer de nouvelles définitions de transactions dans le Management Client.
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour toutes les définitions de transactions dans le Management Client.

Onglet Périphériques (rôles)

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

L'onglet **Périphérique** vous permet de spécifier quelles fonctions les utilisateurs/groupes avec le rôle sélectionné peuvent utiliser pour chaque périphérique (une caméra, par exemple) ou groupe de périphériques dans XProtect Smart Client.

N'oubliez pas de répéter cette procédure pour chaque périphérique. Vous pouvez également sélectionner un groupe de périphériques, et spécifier les droits du rôle pour tous les périphériques du groupe en même temps.

Vous avez toujours la possibilité de sélectionner ou de supprimer lesdites cases à cocher remplies d'un carré, cependant notez que votre choix s'applique dans ce cas à **tous** les périphériques d'un groupe de périphériques. Autre alternative, sélectionnez les périphériques individuels dans le groupe de périphériques afin de vérifier exactement à quel périphérique le droit pertinent s'applique.

Droits d'utilisation des caméras

Spécifiez les droits suivants pour les caméras :

Nom	Description
Lire	La ou les caméra(s) sélectionnée(s) seront visibles dans les clients.

Nom	Description
Voir en direct	Permet de visionner les vidéos de la ou des caméra(s) sélectionnée(s) en direct dans les clients. Pour XProtect Smart Client cette fonction exige également que le rôle ait reçu le droit de visualiser l'onglet **En direct** des clients. Le droit est attribué dans le cadre des droits sur les applications. Spécifiez le profil de temps ou conservez la valeur par défaut.
Lecture > Dans le profil de temps :	Permet la lecture des vidéos enregistrées de la ou des caméra(s) sélectionnée(s) en direct dans les clients. Spécifiez le profil de temps ou conservez la valeur par défaut.
Lecture > Limiter la lecture à	Permet la lecture des vidéos enregistrées de la ou des caméra(s) sélectionnée(s) en direct dans les clients. Spécifiez une limite de lecture ou n'appliquez aucune restriction.
Lire les séquences	Permet de lire des informations séquentielles liées à l'explorateur de séquence dans les clients, par exemple.
Recherche avancée	Permet à l'utilisateur d'utiliser la fonction de recherche avancée dans les clients.
Export	Permet à l'utilisateur d'exporter des enregistrements à partir des clients.
Démarrer l'enregistrement manuel	Permet de démarrer l'enregistrement manuel des vidéos de la ou des caméra(s) sélectionnée(s) en direct dans les clients.
Arrêter l'enregistrement manuel	Permet d'arrêter l'enregistrement manuel des vidéos de la ou des caméra(s) sélectionnée(s) en direct dans les clients.
Lire des signets	Permet de recherches et de lire des détails des signets dans les clients.
Modifier des signets	Permet de modifier des signets dans les clients.
Créer des signets	Permet d'ajouter des signets dans les clients.
Supprimer des signets	Permet de supprimer des signets dans les clients.
Commandes AUX	Permet d'utiliser les commandes auxiliaires à partir des clients.
Création et extension du verrouillage des preuves	Permet à l'utilisateur du client de : • Ajouter la caméra à un ou plusieurs verrouillages de preuves nouveaux ou existants. • Étendre la durée d'expiration pour les preuves verrouillées existantes. • Étendre l'intervalle protégé pour les preuves verrouillées existantes. Exige que les droits d'utilisateur associés à tous les périphériques soient inclus dans le verrouillage des preuves.

Nom	Description
Suppression et réduction du verrouillage des preuves	Permet à l'utilisateur du client de : • Supprimer la caméra des verrouillages de preuves existants. • Voir les preuves verrouillées existantes. • Réduire la durée d'expiration pour les preuves verrouillées existantes. • Réduire l'intervalle protégé pour les preuves verrouillées existantes. Exige que les droits d'utilisateur associés à tous les périphériques soient inclus dans le verrouillage des preuves.
Lire les preuves verrouillées	Permet à l'utilisateur du client de rechercher et de lire les détails des preuves verrouillées.

Droits d'utilisation des microphones

Spécifiez les droits suivants pour les microphones :

Nom	Description
Lire	Le ou les microphone(s) sélectionné(s) seront visibles dans les clients.
En direct > Écouter	Permet d'écouter l'audio en direct du ou des microphone(s) sélectionné(s) en direct dans les clients. Pour XProtect Smart Client cette fonction exige également que le rôle ait reçu le droit de visualiser l'onglet **En direct** des clients. Le droit est attribué dans le cadre des droits sur les applications. Spécifiez le profil de temps ou conservez la valeur par défaut.
Lecture > Dans le profil de temps :	Permet la lecture de l'audio enregistrées du ou des microphone(s) sélectionné(s) en direct dans les clients. Spécifiez le profil de temps ou conservez la valeur par défaut.
Lecture > Limiter la lecture à	Permet la lecture de l'audio enregistrées du ou des microphone(s) sélectionné(s) en direct dans les clients. Spécifiez une limite de lecture ou n'appliquez aucune restriction.
Lire les séquences	Permet de lire des informations séquentielles liées à l'explorateur de séquence dans les clients, par exemple.
Export	Permet à l'utilisateur d'exporter des enregistrements à partir des clients.
Démarrer l'enregistrement manuel	Permet de démarrer l'enregistrement manuel de l'audio du ou des microphone(s) sélectionné(s) en direct dans les clients.
Arrêter l'enregistrement manuel	Permet d'arrêter l'enregistrement manuel de l'audio du ou des microphone(s) sélectionné(s) en direct dans les clients.
Lire des signets	Permet de recherches et de lire des détails des signets dans les clients.
Modifier des signets	Permet de modifier des signets dans les clients.

Nom	Description
Créer des signets	Permet d'ajouter des signets dans les clients.
Supprimer des signets	Permet de supprimer des signets dans les clients.
Création et extension du verrouillage des preuves	Permet à l'utilisateur du client de : • Ajouter le microphone à un ou plusieurs verrouillages de preuves nouveaux ou existants. • Étendre la durée d'expiration pour les preuves verrouillées existantes. • Étendre l'intervalle protégé pour les preuves verrouillées existantes. Exige que les droits d'utilisateur associés à tous les périphériques soient inclus dans le verrouillage des preuves.
Suppression et réduction du verrouillage des preuves	Permet à l'utilisateur du client de : • Supprimer le microphone des verrouillages de preuves existants. • Voir les preuves verrouillées existantes. • Réduire la durée d'expiration pour les preuves verrouillées existantes. • Réduire l'intervalle protégé pour les preuves verrouillées existantes. Exige que les droits d'utilisateur associés à tous les périphériques soient inclus dans le verrouillage des preuves.
Lire les preuves verrouillées	Permet à l'utilisateur du client de rechercher et de lire les détails des preuves verrouillées.

Droits d'utilisation des haut-parleurs

Spécifiez les droits suivants pour les haut-parleurs :

Nom	Description
Lire	Le ou les haut-parleur(s) sélectionné(s) seront visibles dans les clients.
En direct > Écouter	Permet d'écouter l'audio en direct du ou des haut-parleur(s) sélectionné(s) en direct dans les clients. Pour XProtect Smart Client cette fonction exige également que le rôle ait reçu le droit de visualiser l'onglet **En direct** des clients. Le droit est attribué dans le cadre des droits sur les applications. Spécifiez le profil de temps ou conservez la valeur par défaut.
Lecture > Dans le profil de temps :	Permet la lecture de l'audio enregistrées du ou des haut-parleur(s) sélectionné(s) en direct dans les clients. Spécifiez le profil de temps ou conservez la valeur par défaut.

Nom	Description
Lecture > Limiter la lecture à	Permet la lecture de l'audio enregistrées du ou des haut-parleur(s) sélectionné(s) en direct dans les clients. Spécifiez une limite de lecture ou n'appliquez aucune restriction.
Lire les séquences	Permet de lire des informations séquentielles liées à l'explorateur de séquence dans les clients, par exemple.
Export	Permet à l'utilisateur d'exporter des enregistrements à partir des clients.
Démarrer l'enregistrement manuel	Permet de démarrer l'enregistrement manuel de l'audio du ou des haut-parleur(s) sélectionné(s) en direct dans les clients.
Arrêter l'enregistrement manuel	Permet d'arrêter l'enregistrement manuel de l'audio du ou des haut-parleur(s) sélectionné(s) en direct dans les clients.
Lire des signets	Permet de recherches et de lire des détails des signets dans les clients.
Modifier des signets	Permet de modifier des signets dans les clients.
Créer des signets	Permet d'ajouter des signets dans les clients.
Supprimer des signets	Permet de supprimer des signets dans les clients.
Création et extension du verrouillage des preuves	Permet à l'utilisateur du client de : • Ajouter le haut-parleur à un ou plusieurs verrouillages de preuves nouveaux ou existants. • Étendre la durée d'expiration pour les preuves verrouillées existantes. • Étendre l'intervalle protégé pour les preuves verrouillées existantes. Exige que les droits d'utilisateur associés à tous les périphériques soient inclus dans le verrouillage des preuves.
Suppression et réduction du verrouillage des preuves	Permet à l'utilisateur du client de : • Supprimer le haut-parleur des verrouillages de preuves existants. • Voir les preuves verrouillées existantes. • Réduire la durée d'expiration pour les preuves verrouillées existantes. • Réduire l'intervalle protégé pour les preuves verrouillées existantes. Exige que les droits d'utilisateur associés à tous les périphériques soient inclus dans le verrouillage des preuves.
Lire les preuves verrouillées	Permet à l'utilisateur du client de rechercher et de lire les détails des preuves verrouillées.

Droits relatifs aux métadonnées

Spécifiez les droits suivants pour les périphériques à métadonnées :

Nom	Description
Lire	Active le droit de visualisation des périphériques à métadonnées et de récupération des données à partir de ces derniers dans les clients.
Modifier	Active le droit de modification des propriétés pour les métadonnées. Il permet également aux utilisateurs d'activer ou de désactiver les périphériques à métadonnées dans le Management Client et par le biais du MIP SDK.
Voir en direct	Active le droit de visualisation de métadonnées à partir des caméras dans les clients. Pour XProtect Smart Client cette fonction exige également que le rôle ait reçu le droit de visualiser l'onglet **En direct** des clients. Le droit est attribué dans le cadre des droits sur les applications.
Lecture	Active le droit de lecture de données enregistrées à partir des périphériques de métadonnées dans les clients.
Lire les séquences	Active le droit d'utilisation de la fonctionnalité Séquences tout en parcourant les données enregistrées à partir des périphériques à métadonnées dans les clients.
Export	Active le droit d'export d'audio enregistré à partir des périphériques à métadonnées dans les clients.
Création et extension du verrouillage des preuves	Active le droit de création et d'extension du verrouillage des preuves sur les métadonnées dans les clients.
Lire les preuves verrouillées	Active le droit de consultation du verrouillage des preuves sur les métadonnées dans les clients.
Suppression et réduction du verrouillage des preuves	Active le droit de suppression ou de réduction du verrouillage des preuves sur les métadonnées dans les clients.
Démarrer l'enregistrement manuel	Active le droit de démarrer l'enregistrement manuel des métadonnées dans les clients.
Arrêter l'enregistrement manuel	Active le droit d'arrêter l'enregistrement manuel des métadonnées dans les clients.

Droits d'utilisation des entrées

Spécifiez les droits suivants pour les périphériques d'entrée :

Nom	Description
Lire	La ou les entrée(s) sélectionnée(s) seront visibles dans les clients ainsi que dans XProtect Central, un produit complémentaire fournissant une vision complète des états et des alarmes du système de surveillance.

Droits d'utilisation des sorties

Spécifiez les droits suivants pour les périphériques de sortie :

Nom	Description
Lire	La ou les sortie(s) sélectionnée(s) seront visibles dans les clients. Si visible, la sortie pourra être sélectionnée dans une liste dans les clients.
Activer	La ou les sortie(s) sélectionnée(s) peuvent être activées à partir du Management Client et des clients. Spécifiez le profil de temps ou conservez la valeur par défaut.

Onglet PTZ (rôles)

Les droits relatifs aux caméras Pan/Tilt/Zoom (PTZ) peuvent être configurés dans l'onglet **PTZ**. Vous pouvez spécifier les fonctions que les utilisateurs/groupes peuvent utiliser dans les clients. Vous pouvez sélectionner des caméras PTZ individuelles ou des groupes de périphériques contenant des caméras PTZ

Spécifiez les droits suivants pour les périphériques PTZ :

Nom	Description
PTZ manuel	Détermine si le rôle sélectionné peut utiliser des fonctions PTZ et mettre une patrouille en pause sur la caméra sélectionnée. Spécifiez un profil de temps, sélectionnez **Toujours**, ou laissez la valeur par défaut, qui suit le profil de temps par défaut définie dans l'onglet **Info** pour ce rôle.
Activer des positions prédéfinies PTZ ou des profils de patrouille	Détermine si le rôle sélectionné peut déplacer la caméra sélectionnée vers des positions prédéfinies, démarrer et arrêter des profils de patrouille et mettre des patrouilles en pause. Spécifiez un profil de temps, sélectionnez **Toujours**, ou laissez la valeur par défaut, qui suit le profil de temps par défaut définie dans l'onglet **Info** pour ce rôle. Pour autoriser ce rôle à utiliser d'autres fonctions PTZ sur la caméra, activez le droit **PTZ manuel**.
Priorité PTZ	Détermine la priorité des caméras PTZ. Lorsque plusieurs utilisateurs sur un système de surveillance veulent contrôler la même caméra PTZ en même temps, des conflits peuvent survenir. Vous pouvez éviter une telle situation en spécifiant une priorité d'utilisation de la ou des caméra(s) PTZ par des utilisateurs/groupes ayant le rôle sélectionné. Spécifiez une valeur de priorité comprise entre 1 et 32 000, où 1 désigne la priorité la plus faible. La priorité par défaut est 3 000. Le rôle disposant du numéro de priorité le plus élevé est celui qui peut contrôler la ou les caméra(s) PTZ.

Nom	Description
Gérer les positions prédéfinies PTZ ou les profils de patrouille	Détermine le droit d'ajouter, de modifier et d'effacer les positions et les profils de patrouille sur la caméra sélectionnée, dans Management Client et XProtect Smart Client. Pour autoriser ce rôle à utiliser d'autres fonctions PTZ sur la caméra, activez le droit **PTZ manuel**.
Verrouiller/Déverrouiller des positions prédéfinies PTZ	Détermine si le rôle peut verrouiller et déverrouiller des positions prédéfinies pour la caméra sélectionnée.
Réserver des sessions PTZ	Détermine le droit de mettre la caméra sélectionnée en mode session PTZ réservée. Dans une session PTZ réservée, d'autres utilisateurs ou sessions de patrouille dotés d'une priorité PTZ supplémentaire ne peuvent pas prendre le contrôle. Pour autoriser ce rôle à utiliser d'autres fonctions PTZ sur la caméra, activez le droit **PTZ manuel**.
Libérer les sessions PTZ	Détermine si le rôle sélectionné peut libérer les sessions PTZ d'autres utilisateurs du Management Client. Vous pouvez toujours libérer vos propres sessions PTZ, même sans cette permission.

Onglet Audio (rôles)

Pertinent uniquement vous utilisez des haut-parleurs sur votre système. Spécifiez les droits suivants pour les haut-parleurs :

Nom	Description
Parole	Détermine si les utilisateurs doivent être autorisé à parler par le biais du ou des haut-parleur(s) sélectionné(s). Spécifiez le profil de temps ou conservez la valeur par défaut.
Priorité de parole	Lorsque plusieurs utilisateurs de clients souhaitent parler en même temps par l'intermédiaire du même haut-parleur, des conflits peuvent survenir. Pour résoudre ce problème, spécifier une priorité d'utilisation d'un ou plusieurs haut-parleurs par des utilisateurs/groupes ayant le rôle sélectionné. Indiquez une priorité comprise entre **Très faible** et **Très haute**. Le rôle doté de la priorité la plus élevée est autorisé à utiliser le haut-parleur avant les autres rôles. Si deux utilisateurs avec le même rôle souhaitent parler en même temps, la règle du premier arrivé premier servi s'applique.

Onglet Enregistrements à distance (rôles)

Indiquez les paramètres suivants relatifs aux enregistrements à distance :

Nom	Description
Rappeler les enregistrements à distance	Active le droit de rappeler les enregistrements des clients depuis les caméras, microphones, haut-parleurs et périphériques de métadonnées se trouvant dans des sites distants ou sur le stockage externe des caméras.

Onglet Smart Wall (rôles)

Grâce aux rôles, vous pouvez accorder à vos utilisateurs de clients des droits d'utilisation relatifs à Smart Wall pour la fonction Smart Wall :

Nom	Description
Lire	Autorise les utilisateurs à afficher le Smart Wall sélectionné dans les clients.
Modifier	Autorise les utilisateurs à modifier le Smart Wall sélectionné dans le Management Client.
Supprimer	Autorise les utilisateurs à supprimer le Smart Wall sélectionné dans le Management Client.
Opérer	Autorise les utilisateurs à appliquer des dispositions sur le Smart Wall sélectionné dans le client et à activer le préréglage sélectionné.
Lecture	Autorise les utilisateurs à lire les données enregistrées à partir du Smart Wall sélectionné dans les clients.

Onglet Événement externe (rôles)

Spécifiez les droits suivants relatifs aux événements externes :

Nom	Description
Lire	Autorise les utilisateurs à chercher et consulter les événements système externes sélectionnés dans les clients et dans le Management Client.
Modifier	Autorise les utilisateurs à modifier l'événement système externe sélectionné dans le Management Client.
Supprimer	Autorise les utilisateurs à supprimer l'événement système externe sélectionné dans le Management Client.
Déclencher	Autorise les utilisateurs à déclencher l'événement système externe sélectionné dans les clients.

Onglet Groupe de vues (rôles)

Dans l'onglet Groupe de vues, vous pouvez spécifier quels groupes les utilisateurs et groupes d'utilisateurs dotés du rôle sélectionné sont autorisés à utiliser dans le client.

Spécifiez les droits suivants pour les groupes de vues :

Nom	Description
Lire	Active le droit de visualisation des groupes de vues dans les clients et dans le Management Client. Les groupes de vues sont créées dans le Management Client.
Modifier	Active le droit de modification des propriétés pour les groupes de vues dans le Management Client.
Supprimer	Active le droit de suppression des groupes de vues dans le Management Client.
Opérer	Active le droit d'utilisation de groupes de vues dans XProtect Smart Client. Autrement dit, la création de sous-groupes et de vues.

Onglet Serveurs (rôles)

La spécification des droits d'un rôle dans l'onglet **Serveurs** n'est appropriée que si vous avez des serveurs XProtect Enterprise intégrés dans votre système ou que votre système fonctionne dans une configuration Milestone Federated Architecture.

Nom	Description
Serveurs Enterprise	Compte utilisateur donnant accès au serveur Enterprise sélectionné. L'utilisateur doit être configuré sur le serveur Enterprise.
Sites	Active le droit de visualiser le site sélectionné dans le Management Client. Les sites connectés sont connectés par le biais de Milestone Federated Architecture. Pour modifier les propriétés vous devez avoir des permissions de modification sur le serveur de gestion de chaque site.

Voir À propos des serveurs XProtect Enterprise (á la page 411) ou À propos de Milestone Federated Architecture (á la page 286) pour de plus amples informations.

Onglet Matrix (rôles)

Si vous avez configuré des destinataires Matrix sur votre système, vous pouvez configurer des droits de rôle Matrix. À partir d'un client, vous pouvez envoyer la vidéo aux destinataires Matrix. Sélectionnez les utilisateurs qui peuvent la recevoir sur l'onglet Matrix.

Sont disponibles les droits suivants :

Nom	Description
Lire	Déterminez si les utilisateurs et groupes dotés du rôle sélectionné peuvent sélectionner et envoyer des vidéos au destinataire Matrix à partir des clients.

Onglet alarmes (rôles)

Si vous utilisez des alarmes dans votre configuration système afin d'offrir une vue d'ensemble et un meilleur contrôle de votre installation (incluant tout autre serveur XProtect), vous pouvez utiliser l'onglet **Alarmes** pour spécifier les droits d'alarme dont devraient disposer les utilisateurs/groupes dotés du rôle sélectionné, pour définir la façon de traiter les alarmes dans les clients, par exemple.

Spécifiez les droits suivants pour les alarmes :

Nom	Description
Gestion	Active le droit de gérer les alarmes, pour, par exemple, modifier les priorités des alarmes et réaffecter des alarmes à d'autres utilisateurs, acquitter les alarmes et modifier l'état de plusieurs alarmes en même temps, pour les faire passer de **Nouveau** à **Assigné**, par exemple.
Vue	Active le droit d'afficher les alarmes et d'imprimer les rapports d'alarme.
Désactiver alarmes	Active le droit de désactiver les alarmes.
Recevoir des notifications	Active le droit de recevoir des notifications à propos des alarmes dans les clients.

Onglet Contrôle d'accès (rôles)

Lorsque vous ajoutez ou modifiez des utilisateurs de base, des utilisateurs Windows ou des groupes, vous pouvez indiquer des paramètres de contrôle d'accès :

Nom	Description
Utiliser le contrôle d'accès	Permet à l'utilisateur d'utiliser les fonctions relatives au contrôle d'accès dans les clients.
Voir la liste des détenteurs de cartes	Permet à l'utilisateur de voir la liste des détenteurs de cartes sur l'onglet **Contrôle d'accès** dans les clients.

Onglet LPR (rôles)

Si votre système fonctionne sous XProtect LPR, spécifiez les droits suivants pour les utilisateurs :

Nom	Description
Utiliser LPR	Permet à l'utilisateur d'utiliser n'importe quelles fonctions relatives à LPR dans les clients.

Nom	Description
Gérer les listes de correspondance de plaques d'immatriculation	Active le droit d'ajouter, importer, modifier, exporter et supprimer les listes de correspondance de plaques d'immatriculation dans le Management Client.
Lire les listes de correspondance de plaques d'immatriculation	Active le droit d'afficher les listes de correspondance de plaques d'immatriculation.

Onglet MIP (rôles)

Au travers du kit de développement logiciel d'intégration MIP (SDK), un vendeur tiers peut développer des modules d'extension personnalisés pour votre système, par exemple, l'intégration à des systèmes de contrôle de l'accès externes ou semblables.

Les paramètres à modifier pour votre module d'extension dépendent du module d'extension en question. Vous trouverez les paramètres personnalisés des modules d'extension dans l'onglet **MIP**.

Utilisateurs de base

À propos des utilisateurs basiques

Lorsque vous ajoutez un utilisateur de base sur votre système, vous créez un compte d'utilisateur de système de surveillance dédié avec une authentification par nom d'utilisateur de base et mot de passe pour l'utilisateur individuel. Contrairement à l'utilisateur Windows, ajouté avec Active Directory.

Lorsque vous travaillez avec des utilisateurs basiques, il est important de comprendre la différence entre un utilisateur basique et un utilisateur Windows.

- Les utilisateurs basiques sont soumis à une authentification alliant un nom d'utilisateur et un mot de passe et sont spécifiques à un système. Même si les utilisateurs de base ont le même nom d'utilisateur et mot de passe, un utilisateur de base créé sur l'un des sites fédérés n'a pas accès à un autre site fédéré.
- Les utilisateurs Windows sont authentifiés à partir de leurs identifiants de connexion Windows et sont spécifiques à un ordinateur.

Créer des utilisateurs de base

Pour créer un utilisateur de base sur votre système :

1. Développez **Sécurité** > **Utilisateurs de base**.
2. Dans le volet des utilisateurs de base, faites un clic droit et sélectionnez **Créer un utilisateur de base**.
3. Indiquez un nom d'utilisateur et un mot de passe et répétez-les pour être sûr de les avoir indiqués correctement.
4. Cliquez sur **OK** pour créer l'utilisateur de base.

Tableau de bord système

À propos du tableau de bord système

Le tableau de bord système vous offre des fonctions de surveillance de votre système et de ses composants.

Vous pouvez accéder aux fonctions suivantes :

Nom	Description
Moniteur système	Surveillez l'état de vos serveurs et caméras selon des paramètres définis par vos soins.
Seuils du moniteur système	Définissez des valeurs seuils pour les paramètres surveillés sur le serveur et surveillez les tuiles utilisées dans le moniteur système.
Protection de preuves	Obtenez une vue d'ensemble de toutes les données protégées dans le système.
Tâche actuelle	Pour obtenir un aperçu des tâches en cours sur un serveur d'enregistrement sélectionné.
Rapports de configuration	Pour décider des éléments à inclure dans vos rapports de configuration système avant leur impression.

À propos du moniteur système

Le moniteur système vous offre une vue d'ensemble visuelle et rapide de l'état actuel des serveurs et caméras de votre système par le biais de tuiles colorées représentant le matériel du système. Par défaut, le système affiche des tuiles représentant tous les **Serveurs d'enregistrement**, **Tous les serveurs** et **Toutes les caméras**.

La couleur des tuiles :

Couleur des tuiles	Description
Vert	État **normal**. Tout fonctionne normalement.
Jaune	État d'**avertissement**. Un ou plusieurs paramètres de surveillance se trouvent au-dessus de la valeur de seuil (voir "À propos des seuils du moniteur système" á la page *252*) pour l'état **Normal**.
Rouge	État **critique**. Un ou plusieurs paramètres de surveillance se trouvent au-dessus de la valeur de seuil pour l'état **Normal** et l'état d'**Avertissement**.

Vous pouvez personnaliser les tuiles des serveurs et des caméras si vous souhaitez afficher plus ou moins de tuiles sur le tableau de bord. Par exemple, vous pouvez configurer des tuiles afin de représenter un serveur unique, une caméra individuelle, un groupe de caméras ou un groupe de serveurs. Vous pouvez également supprimer une tuile si vous ne souhaitez pas l'utiliser ou modifier ses paramètres de surveillance. Les paramètres de surveillance sont, par exemple, l'usage du processeur ou la mémoire disponible pour un serveur. Si vous supprimez ces paramètres de la tuile du serveur, la tuile ne surveille pas ces paramètres sur la tuile correspondante. Cliquez sur

Personnaliser dans le coin supérieur droit de l'onglet pour ouvrir la fenêtre Personnaliser le tableau de bord. Voir Personnaliser le tableau de bord (á la page 250) pour plus d'informations.

Les tuiles changent d'état et donc de couleur en fonction des valeurs de seuil définies dans les Seuils du moniteur système. Bien que le système définisse des valeurs de seuil par défaut, vous pouvez décider par vous-même de la valeur de seuil pour chacun des trois états. Pour configurer ou modifier les valeurs de seuil, vous pouvez utiliser des **Seuils du moniteur système**. Voir À propos des seuils du moniteur système (á la page 252).

Si une tuile change de couleur et si vous souhaitez savoir quel serveur/paramètre a entraîné son changement de couleur, il vous suffit de cliquer sur la tuile. Une vue d'ensemble s'ouvre alors en bas de l'écran et présenter les couleurs rouge, jaune ou verte pour chaque paramètre de surveillance que vous avez activé pour votre tuile. Cliquez sur le bouton **Détails** pour obtenir des informations plus détaillées au sujet des raisons du changement d'état.

Si vous voyez un indicateur d'avertissement sur une tuile, il se peut qu'un collecteur de données pour l'un de vos serveurs ou caméras surveillés ne fonctionne pas. Si vous placez votre souris au-dessus de la tuile, le système vous indique à quel moment la dernière collecte de données a eu lieu pour la tuile en question.

Personnaliser le tableau de bord

Ajouter une nouvelle tuile de caméra ou de serveur

1. Dans la fenêtre Moniteur système, cliquez sur **Personnaliser**.
2. Dans la fenêtre **Personnaliser le tableau de bord** qui s'ouvre, , cliquez sur **Nouveau** sous **Tuiles de serveur** ou **Tuiles de caméras**.
3. Dans la fenêtre **Nouvelle tuile de serveur/Nouvelle tuile de caméra**, sélectionnez les caméras ou les serveurs à surveiller.
4. Dans **Paramètres de surveillance**, cochez ou décochez les cases correspondant aux paramètres à ajouter ou supprimer à partir de la tuile pertinente.
5. Cliquez sur **OK.** La nouvelle tuile de serveur ou de caméra est maintenant ajoutée aux tuiles affichées sur votre tableau de bord.

Modifier les propriétés des moniteurs

1. Dans la fenêtre du tableau de bord du Moniteur système, cliquez sur **Personnaliser**.
2. Dans la fenêtre **Personnaliser le tableau de bord** qui s'ouvre, , cliquez sur **Modifier** sous **Tuiles de serveur** ou **Tuiles de caméras**.
3. Dans la fenêtre **Modifier la tuile du serveur** ou **Modifier la tuile de la caméra**, sélectionnez le composant du serveur ou les caméras que vous souhaitez modifier.
4. Dans la case **Paramètres de surveillance**, cochez ou décochez les cases correspondant aux paramètres de surveillance à ajouter ou supprimer à partir de la tuile pertinente.
5. Cliquez sur **OK**. Les paramètres de surveillance ainsi modifiés font maintenant partie de la tuile correspondante ou en ont disparu.

Vous pouvez activer et désactiver des données d'historique sur le système à votre guise. Si vous désactivez ces données, vous ne pourrez pas afficher les graphiques de comportement de système précédant. Si vous voulez réduire la charge sur la base des données du serveur SQL ou sur la bande passante, vous pouvez réduire l'intervalle d'échantillonnage des données d'historique. Si vous réduisez l'intervalle d'échantillonnage des données d'historique, les graphiques contiendront moins de détails.

À propos des détails du moniteur système

Si vous cliquez sur un serveur ou une tuile de caméras, vous pouvez consulter l'état de chaque paramètre de surveillance sélectionné sous le tableau de bord.

Exemple : Les paramètres de surveillance FPS en direct d'une caméra a atteint l'état d'Avertissement.

Le champ **État** affiche l'état de la caméra. Par exemple, un avertissement apparaît en rouge si la connexion avec le périphérique est rompue. L'icône comprend une astuce avec une brève description du problème à l'origine de l'avertissement.

Le champ **Espace utilisé** présente des données d'autres serveurs d'enregistrement sur lesquels ce périphérique a des enregistrements, si le périphérique était précédemment situé sur d'autres serveurs d'enregistrement, par exemple.

Si vous cliquez sur le bouton **Détails** correspondant à la caméra/au serveur concerné, vous pouvez consulter des informations système et créer des rapports au sujet de :

Composant	Description
Serveur de gestion	Présente des données provenant du serveur de gestion sélectionné
Serveur(s) d'enregistrement	Présente des données provenant du serveur d'enregistrement sélectionné. Vous pouvez les afficher en fonction du : • Disque • Stockage • Réseau • Caméra
Serveurs d'enregistrement de redondance	Présente des données provenant du serveur d'enregistrement de redondance sélectionné.
Serveurs supplémentaires	Affiche les données sur le serveur de journaux, les serveurs d'événements et bien plus encore.
Caméras	Affiche les données de toute caméra de n'importe quel groupe au sein de votre configuration.

Chacun de ces éléments est un espace sur lequel vous pouvez cliquer et que vous pouvez agrandir. Lorsque vous cliquez dans cet espace, vous obtenez des données dynamiques pertinentes au sujet de ce serveur ou de cette caméra.

La barre **Caméras** contient une liste des groupes de caméras sélectionnables. Une fois qu'un groupe est sélectionné, choisissez une caméra spécifique et affichez ses données dynamiques. Tous les serveurs affichent des informations sur l'utilisation CPU et la mémoire disponibles. Les serveurs d'enregistrement affichent également des informations sur l'état de connexion. Vous pouvez trouver dans chaque vue le lien **Historique**. Cliquez sur ce lien pour afficher les données et les rapports historiques (pour afficher des rapports sur une caméra, cliquez sur le nom de la caméra). Pour chaque rapport historique, vous pouvez visualiser les données des 24 dernières heures, 7 jours ou 30 jours. Pour enregistrer et / ou imprimer des rapports, cliquez sur l'icône **Envoyer vers un PDF**. Utilisez les icônes < et Accueil pour naviguer dans le moniteur système.

Vous ne pouvez créer des rapports historiques qu'avec des données provenant du serveur d'enregistrement sur lequel le périphérique se trouve actuellement.

Important : Si vous accédez aux détails du moniteur système à partir d'un système d'exploitation serveur, il est possible qu'un message sur la **Configuration de sécurité améliorée d'Internet Explorer** apparaisse. Suivez les instructions dans le message pour ajouter la page du **Moniteur système** à la **Zone des sites de confiance** avant de continuer.

À propos des seuils du moniteur système

Les seuils du moniteur système vous permettent de configurer et d'ajuster les seuils généraux à partir desquels les tuiles du moniteur système devraient indiquer par un signal visuel que votre matériel change d'état, lors que l'usage du processeur d'un serveur passe d'un état normal (vert) à un état d'avertissement (jaune) par exemple.

Le système est configuré avec des valeurs de seuil par défaut. Vous pouvez donc commencer à surveiller le matériel de votre système dès que votre système est configuré. Vous pouvez modifier ces valeurs si vous le souhaitez (voir "Définir les seuils du moniteur système" á la page 253). Par défaut, le système est configuré de façon à afficher les valeurs de seuil pour toutes les unités d'un matériel particulier, comme, par exemple, toutes les caméras ou tous les serveurs. Vous pouvez également configurer des valeurs de seuil pour des serveurs et caméras individuels ou pour une partie de ceux-ci. Par exemple, il est conseillé d'établir des valeurs de seuil pour des serveurs ou caméras individuels si certaines caméras doivent être autorisées à utiliser un **FPS en direct** ou un **FPS d'enregistrement** plus élevé que les autres caméras.

Vous pouvez configurer les valeurs de seuil pour des serveurs, des caméras, des disques et des espaces de stockage. Si vous souhaitez modifier les valeurs de seuil, vous pouvez utiliser le curseur de contrôle des seuils. Le curseur de contrôle des seuils vous permet d'accroître ou de réduire les valeurs de seuil en faisant glisser les poignées séparant les différents états vers le haut ou le bas. Le curseur de contrôle des seuils est divisé en différentes couleurs similaires à celles affichées sur les tuiles de serveurs ou de caméras de votre Moniteur système (voir "À propos du moniteur système" á la page 249).

Pour vous assurer de ne pas observer d'état**Critique** ou **Avertissement** dans les cas où l'usage ou la charge du matériel de votre système atteint une valeur de seuil élevée pendant une seconde ou une période similaire, utilisez l'**Intervalle de calcul**. L'**Intervalle de calcul** répartit l'effet de changements brefs ou fréquents de l'état d'un matériel du système. Dans la pratique, cela signifie que l'**Intervalle de calcul** nivelle les effets des changements du matériel au fil de temps, de sorte que vous ne receviez pas d'alerte à chaque fois qu'un seuil est dépassé.

Par exemple, vous pouvez fixer l'**Intervalle de calcul** sur une (1) minute, pour vous assurer de ne recevoir d'alertes que lorsque la valeur moyenne de la minute entière dépasse le seuil. L'avantage de ce système est que vous évitez de recevoir des alertes au sujet de changements fréquents et potentiellement non pertinents pour ne recevoir que les alertes reflétant des problèmes récurrents au niveau de l'usage du processeur ou de la mémoire, par exemple.

Seuils de serveur

Seuil	Description	Unité
Mémoire	Les seuils correspondant à la mémoire RAM utilisée sur les serveurs que vous surveillez.	MB
Usage du processeur	Les seuils correspondant à l'usage du processeur sur les serveurs que vous surveillez.	%

Seuils de caméras

Seuil	Description	Unité
Espace utilisé	Les seuils correspondant à l'espace utilisé par les caméras que vous surveillez.	Go
FPS d'enregistrement	Les seuils pour le FPS des caméras en cours d'utilisation lorsque le système enregistre des vidéos sur les caméras que vous surveillez.	%
FPS en direct	Les seuils pour le FPS des caméras en cours d'utilisation lorsque des vidéos en direct sont diffusées sur les caméras que vous surveillez.	%

Seuils de disques

Seuil	Description	Unité
Espace libre	Les seuils correspondant à l'espace disponible sur les disques que vous surveillez.	Go

Seuils de stockage

Seuil	Description	Unité
Durée de rétention	Le seuil présentant une prédiction du moment ou votre stockage ne disposera plus d'espace libre. L'état indiqué est basé sur la configuration de votre système et est mis à jour deux fois par jour.	Jours

Vous pouvez également configurer des règles (voir "À propos des règles" á la page 190) afin d'effectuer des actions spécifiques ou d'activer des alarmes (voir "À propos des alarmes" á la page 261) lorsqu'un seuil passe d'un état à un autre.

Définir les seuils du moniteur système

1. Cochez la case **Activer** du matériel pertinent du système si vous ne l'avez pas encore fait
2. Faites glisser le curseur de contrôle des seuils vers le haut ou le bas afin d'accroître ou de réduire la valeur du seuil. Il y a deux curseurs disponibles pour chaque périphérique du système présenté dans le contrôle des seuils, qui séparent les niveaux **Normal**, **Avertissement** et **Critique**.

3. Une fois que vous avez réglé les différents niveaux de seuils, sélectionnez **Fichier** > **Sauvegarder** dans le menu.

Un exemple de réglage d'un curseur de contrôle des seuils. Faites glisser les curseurs vers le haut et le bas pour accroître ou réduire l'un ou l'autre des trois niveaux de seuils. La couleur rouge indique que vous avez atteint un état Critique, le jaune est un état d'Avertissement indiquant que vous êtes proche de l'état Critique et la couleur verte indique que le système est dans son état normal et se trouve dans la plage des valeurs de seuil sélectionnées.

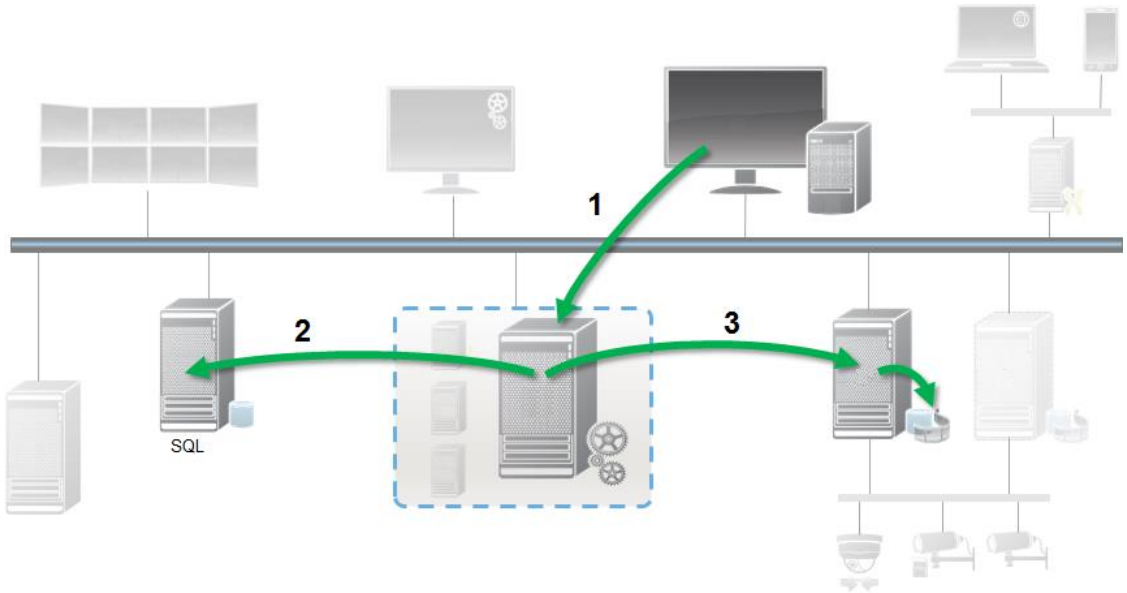
À propos de la protection des preuves

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

Avec la fonctionnalité de protection des preuves, les opérateurs du client peuvent protéger des séquences vidéo, y compris l'audio et d'autres données, contre toute suppression, si nécessaire, par exemple, lorsqu'une enquête ou un procès est en cours. Pour plus d'informations sur la façon de verrouiller des preuves, référez-vous à la documentation XProtect Smart Client.

Lorsque les données sont protégées, elles ne peuvent pas être supprimées, ni automatiquement par le système après le temps de rétention par défaut du système ou dans d'autres situations, ni manuellement par les utilisateurs du client. Le système ou un utilisateur ne peut pas supprimer les données tant qu'un utilisateur disposant des droits d'utilisateur suffisants ne déverrouille pas la protection de la preuve.

Organigramme pour la protection des preuves :



1. L'utilisateur crée une protection des preuves dans XProtect Smart Client. Des informations sont envoyées au serveur de gestion.
2. Le serveur de gestion stocke les informations au sujet de la protection des preuves sur le serveur SQL.
3. Le serveur de gestion informe le serveur d'enregistrement qu'il faut stocker et protéger les enregistrements protégés dans la base de données.

Lorsque l'opérateur crée une protection des preuves, les données protégées restent dans l'espace de stockage des enregistrements dans lequel elles ont été enregistrées et sont déplacées vers des disques d'archivage en même temps que les données non protégées, mais les données protégées :

- Se conforment à la durée de rétention configurée pour la protection des preuves. Potentiellement indéfiniment.
- Conservent la qualité d'origine des enregistrements, même si la réduction a été configurée pour les données non protégées.

Lorsqu'un opérateur crée des protections, la taille minimum d'une séquence est la durée choisie par la base de données pour diviser les fichiers enregistrés. Par défaut, cette durée est fixée à une heure. Vous pouvez modifier ce paramètre, mais vous devrez alors personnaliser le fichier RecorderConfig.xml sur le serveur d'enregistrement. Si une petite séquence s'étend sur deux périodes d'une heure, le système verrouille les enregistrements des deux périodes.

Dans le journal d'activité du Management Client, vous pouvez voir à quel moment un utilisateur crée, modifie ou supprime des protections des preuves.

Lorsqu'un disque est à court d'espace libre, cela n'affecte aucunement les données protégées. Ce sont alors les données non protégées les plus anciennes qui sont supprimées. S'il n'y a plus de données non protégées à supprimer, le système s'arrête d'enregistrer. Vous pouvez créer des règles et des alarmes déclenchées par des événements disque plein, de façon à en être informé automatiquement.

À l'exception des cas où plus de données sont stockées sur une longue période et ont un impact potentiel sur l'espace de stockage du disque, la fonction de protection des preuves en elle-même n'influe pas sur la performance du système.

Si vous déplacez du matériel (voir "À propos du déplacement de matériel" á la page 107) vers un autre serveur d'enregistrement :

- Les enregistrements protégés par la protection des preuves restent sur l'ancien serveur d'enregistrement conformément à la durée de rétention fixée pour la protection des preuves lors de sa création.
- L'utilisateur XProtect Smart Client peut continuer à protéger les données à l'aide de la protection des preuves sur les enregistrements effectués sur une caméra avant qu'elle n'ait été déplacée vers un autre serveur d'enregistrement. Ceci est vrai même si vous déplacez la caméra plusieurs fois et si les enregistrements sont stockés sur de multiples serveurs d'enregistrement.

Par défaut, tous les opérateurs ont un profil de protection des données par défaut qui leur est assigné, mais ne disposent pas des droits d'accès de l'utilisateur à cette fonction. Pour indiquer les droits d'accès à la protection des preuves d'un rôle, voir l'onglet Périphériques (voir "Onglet Périphériques (rôles)" á la page 237) pour les paramètres de rôle. Pour indiquer le profil de la protection des preuves d'un rôle, voir l'onglet Info (voir "Onglet Info (rôles)" á la page 219) pour les paramètres de rôle.

Dans le Management Client, vous pouvez modifier les propriétés du profil de protection des preuves par défaut et créer des profils de protection de preuves supplémentaires et les affecter aux rôles à la place.

Protection des preuves sous **Tableau de bord du système** affiche un aperçu de toutes les données protégées sur le système de surveillance actuel :

- la date de début et de fin pour les données protégées

- l'utilisateur qui a protégé la preuve
- le moment où la preuve n'est plus protégée
- l'endroit où les données sont stockées
- la taille de chaque preuve protégée

Toutes les informations affichées dans **Protection des preuves** sont des captures d'écran. Appuyez sur F5 pour actualiser.

À propos des tâches actuelles

Le nœud **Tâches actuelles** affiche un aperçu des tâches sous un serveur d'enregistrement sélectionné, leur heure de début, l'heure de fin estimée et la progression. Toutes les informations affichées dans les **tâches actuelles** sont des captures d'écran. Vous pouvez les rafraîchir en cliquant sur le bouton **Actualiser** en bas à droite du volet **Propriétés**.

À propos des rapports de configuration

Lors de la création de rapports de configuration au format PDF, vous pouvez inclure n'importe quel élément de votre système dans le rapport. Vous pouvez par exemple y inclure des licences, la configuration d'un périphérique, la configuration des alarmes et bien plus encore. Vous pouvez également personnaliser votre mise en page et votre police et inclure une page de couverture personnalisée.

Créer un rapport de configuration

1. Développez le **Tableau de bord système**, puis cliquez sur **Rapports de configuration**. Cela génère la page de configuration du rapport.
2. Sélectionnez les éléments que vous souhaitez inclure à votre rapport.
3. **Facultatif** : Cliquez sur **Page de couverture** afin de personnaliser votre première page. Dans la fenêtre qui s'affiche, complétez les informations requises. Sélectionnez la **Page de couverture** comme un élément à inclure dans votre rapport, sinon la première page que vous personnalisez ne sera pas intégrée à votre rapport.
4. Cliquez sur **Formatage** afin de personnaliser votre police, mise en page et les marges. Dans la fenêtre qui s'affiche, sélectionnez les paramètres désirés.
5. Une fois que vous êtes prêt à exporter, cliquez sur **Exporter**, sélectionnez un nom et sauvegardez l'emplacement de votre rapport.

Configurer les détails du rapport

Les éléments suivants sont accessibles lors de la configuration des rapports :

Nom	Description
Sélectionner tout	Sélectionne tous les éléments de la liste.
Effacer tout	Efface tous les éléments de la liste.
Page de Couverture	Pour personnaliser la page de couverture du rapport.

Nom	Description
Formatage	Pour formater le rapport.
Export	Pour sélectionner un emplacement d'enregistrement du rapport et créer un fichier PDF.

Journaux des serveurs

À propos des journaux

Vous pouvez visualiser et exporter le contenu des différents journaux associés au système. L'objectif des journaux est de documenter l'activité, les événements, les actions et les erreurs dans le système, pour une analyse ou une documentation ultérieure.

Les journaux ont différentes fins :

Nom	Description
Journal système	Journalise les informations associées au système.
Journal d'audit	Journalise l'activité des utilisateurs.
Journal de règles	Journalise les règles dans lesquelles les utilisateurs ont spécifié l'action Créer une entrée au journal.

Votre système compte plusieurs paramètres par défaut associés aux différents journaux. Pour modifier les paramètres, reportez-vous à l'onglet Journaux des serveurs (voir "Onglet Journaux de serveurs (options)" á la page 271) sous Options.

Vous pouvez afficher les journaux dans un certain nombre de langues différentes et exporter les journaux sous forme de fichiers texte (.txt) délimités par des balises.

Si un journal contient plusieurs pages d'informations, vous pouvez parcourir les pages du journal en cliquant sur les boutons situés dans le coin inférieur droit du volet du journal :

Dans le coin inférieur gauche, passez à une date et une heure spécifique du journal :

Rechercher des journaux

Pour rechercher un journal, utilisez les **Critères de recherche** situés dans la partie supérieure du volet du journal :

1. Précisez vos critères de recherche dans les listes.
2. Cliquez sur le bouton **Actualiser** pour que la page du journal reflète vos critères de recherche. Pour supprimer vos critères de recherche, et revenir à l'affichage de l'ensemble du contenu du journal, cliquez sur le bouton **Supprimer**.

Vous pouvez double cliquer sur n'importe quelle ligne pour obtenir tous les détails présentés dans une fenêtre **Détails du journal**. Vous pouvez ainsi lire également les entrées du journal qui contiennent plus de texte pouvant être affiché sur une seule ligne.

Exporter les journaux

Vous pouvez exporter les journaux sous forme de fichiers texte (.txt) délimités par des balises. Vous pouvez personnaliser le contenu du journal en spécifiant quel journal, quels éléments du journal, et quelle plage horaire à inclure dans l'exportation. Par exemple, vous pouvez indiquer que seules les entrées du journal associées à une erreur du Journal système entre le 2 janvier 2016 08:00:00 et le 4 janvier 2016 07:59:59 doivent être incluses dans votre exportation.

Pour exporter un journal :

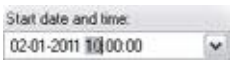
1. Dans le champ **Nom de fichier** de la fenêtre **Exporter le journal**, indiquez un nom pour le fichier du journal exporté.

   Par défaut, les fichiers de journaux exportés sont sauvegardés dans votre dossier **Mes Documents**. Vous pouvez toutefois spécifier un autre emplacement en cliquant sur le bouton de navigation à côté du champ.

2. Tout critère que vous avez sélectionné afin de cibler le contenu du journal exporté est listé dans le champ **Filtres**. Vous ne pouvez pas modifier ce champ. Si vous devez modifier vos critères, fermez la fenêtre et répétez les étapes 1 et 2.

3. Indiquez la durée que vous voulez que l'exportation couvre. Spécifiez les champs **Date et heure de début** et **Date et heure de fin** respectivement. Vous pouvez sélectionner la date en cliquant sur la flèche :

   Pour indiquer une heure exacte, écrasez les éléments de l'heure requis (heures:minutes:secondes) en inscrivant les valeurs requises. Dans cet exemple, l'élément des heures est écrasé :

4. Cliquez sur **Exporter** pour exporter le contenu du journal.

Modifier la langue d'un journal

1. Dans la partie inférieure du volet du journal, dans le champ déroulant **Afficher le journal dans la liste**, sélectionnez la langue souhaitée.

2. Le journal s'affiche dans la langue sélectionnée. À la prochaine ouverture, le journal sera de nouveau configuré dans la langue par défaut.

Journal système (propriétés)

Chaque ligne dans un journal représente une entrée de journal. Une entrée de journal contient un certain nombre de champs d'informations :

Nom	Description
Niveau	Affiche une icône indiquant le niveau de l'entrée du journal : - indique une information - indique un avertissement - indique une erreur 'vierge' - indique une entrée non définie.
Heure UTC	Horodaté en temps universel coordonné (UTC)
Heure locale	Horodaté en heure locale du serveur de votre système.
ID	Numéro d'identification de l'incident journalisé.
Type de source	Type d'équipement sur lequel l'incident journalisé est intervenu, par exemple, serveur ou périphérique.
Nom de la source	Serveur de gestion, nom du serveur d'enregistrement ou du périphérique sur lequel l'incident journalisé est intervenu.
Type d'événement	Type d'événement correspondant à l'incident journalisé.
Description	Affiche une description de l'incident journalisé.

Journal d'audit (propriétés)

Chaque ligne dans un journal représente une entrée de journal. Une entrée de journal contient un certain nombre de champs d'informations :

Nom	Description
Niveau	Affiche une icône indiquant le niveau de l'entrée du journal : - indique une information - indique un avertissement - indique une erreur 'vierge' - indique une entrée non définie.
Heure UTC	Horodaté en temps universel coordonné (UTC)
Heure locale	Horodaté en heure locale du serveur de votre système.
ID	Numéro d'identification de l'incident journalisé.
Utilisateur	Nom de l'utilisateur distant ayant causé l'incident journalisé.
Emplacement de l'utilisateur	Adresse IP ou nom d'hôte de l'ordinateur utilisé par l'utilisateur distant ayant causé l'incident journalisé.
Autorisation	Informations indiquant si l'action de l'utilisateur distant était autorisée ou non.

Nom	Description
Catégorie	Type d'incident journalisé.
Type de ressource	Type d'équipement sur lequel l'incident journalisé est intervenu, par exemple, serveur ou périphérique.
Nom de la ressource	Serveur de gestion, ou nom du serveur d'enregistrement ou du périphérique sur lequel l'incident journalisé est intervenu.
Hôte ressource	Nom du serveur d'enregistrement qui héberge un périphérique ou un emplacement de stockage sur lequel l'incident journalisé est intervenu. Nom du serveur de gestion qui héberge le serveur d'enregistrement ou le serveur de gestion sur lequel l'incident journalisé est intervenu.
Description	Affiche une description de l'incident journalisé.

Journal de règles (propriétés)

Chaque ligne dans un journal représente une entrée de journal. Une entrée de journal contient un certain nombre de champs d'informations :

Nom	Description
Niveau	Affiche une icône indiquant le niveau de l'entrée du journal : - indique une information - indique un avertissement - indique une erreur 'vierge' - indique une entrée non définie.
Heure UTC	Horodaté en temps universel coordonné (UTC)
Heure locale	Horodaté en heure locale du serveur de votre système.
ID	Numéro d'identification de l'incident journalisé.
Nom du service	Nom du service sur lequel l'incident journalisé est intervenu.
Nom de la règle	Nom de la règle qui déclenche la journalisation de l'entrée.
Type de source	Type d'équipement sur lequel l'incident journalisé est intervenu, par exemple, serveur ou périphérique.
Nom de la source	Serveur de gestion, nom du serveur d'enregistrement ou du périphérique sur lequel l'incident journalisé est intervenu.
Type d'événement	Type d'événement correspondant à l'incident journalisé.
Type de générateur	Type d'équipement sur lequel l'incident journalisé a été déclenché. Les entrées du journal sont définies par l'administrateur et se rapportent aux incidents intervenus dans votre système.
Nom du générateur	Nom de l'équipement sur lequel l'incident journalisé a été généré.
Description	Affiche une description de l'incident journalisé.

Alarmes

À propos de la configuration des alarmes

La configuration des alarmes comprend les éléments suivants :

- La configuration dynamique de la gestion des alarmes basée sur un rôle spécifique
- Une vue d'ensemble technique centrale de tous les composants : serveurs, caméras et unités externes
- La configuration de la journalisation centralisée de toutes les alarmes entrantes et des informations du système
- La prise en charge des modules d'extension, permettant ainsi l'intégration personnalisée d'autres systèmes, par exemple des systèmes de contrôle d'accès externe ou des systèmes basés sur VCA.

En règle générale, les alarmes sont contrôlées par la visibilité de l'objet déclenchant l'alarme. Cela signifie que quatre aspects potentiels peuvent jouer un rôle en matière d'alarmes et de la personne pouvant les contrôler/gérer et dans quelle mesure :

Nom	Description
Visibilité de la source/périphérique	Si le périphérique qui génère l'alarme n'est pas configuré pour être visible dans un rôle d'utilisateur, l'utilisateur ne peut pas voir l'alarme dans la liste des alarmes dans XProtect Smart Client.
Le droit de déclencher des événements définis par l'utilisateur	Ce droit détermine si le rôle de l'utilisateur peut déclencher les événements sélectionnés définis par l'utilisateur dans XProtect Smart Client.
Modules d'extension externes	Si des modules d'extension externes sont configurés dans votre système, ils peuvent contrôler les droits des utilisateurs relatifs à la gestion des alarmes.
Droits généraux des rôles	Déterminent si l'utilisateur peut uniquement voir les alarmes, ou également les gérer. Ce qu'un utilisateur d'**alarmes** peut faire avec les alarmes dépend du rôle de l'utilisateur et des paramètres configurés pour ce rôle en particulier.

L'onglet **Serveur d'événements** dans **Options**, vous permet de spécifier les paramètres des alarmes, des événements et des journaux.

À propos des alarmes

Important : cette fonction ne fonctionne pas si vous n'avez pas installé au préalable le serveur d'événements XProtect.

Basée sur les fonctions gérées par un serveur d'événements, la fonction des alarmes centralise la visualisation, le contrôle et le dimensionnement des alarmes dans un nombre illimité d'installations (y compris tous les autres systèmes XProtect) au sein d'une même entreprise. Vous pouvez configurer cette fonction afin qu'elle génère des alarmes en fonction des éléments suivants :

- **Événements internes liés au système**

  Par exemple, mouvement, réponse ou non-réponse d'un serveur, anomalie d'archivage, manque d'espace sur un volume de stockage, etc.

- **Événements externes intégrés**

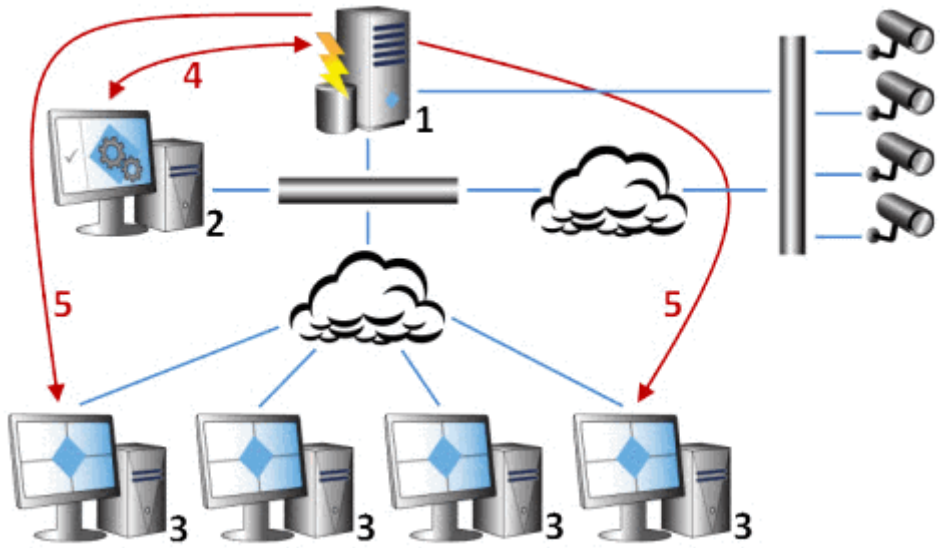
  Ce groupe peut être composé de plusieurs types d'événements externes :

  - **Événements analytiques**

    Généralement, les données reçues de la part de fournisseurs d'analyses de contenus vidéo (VCA) tiers externes.

  - **Événements du module d'extension MIP**

    Au travers du kit de développement logiciel MIP (SDK), un vendeur tiers peut développer des modules d'extension personnalisés (par exemple, l'intégration à des systèmes de contrôle de l'accès externes ou d'autres services semblables) pour votre système.



Légende :

1. Système de surveillance
2. Management Client
3. XProtect Smart Client
4. Configuration de l'alarme
5. Flux des données de l'alarme

Les alarmes sont gérées et déléguées dans la liste d'alarmes sous XProtect Smart Client. Vous pouvez également intégrer des alarmes à l'aide de la fonctionnalité de plan de XProtect Smart Client.

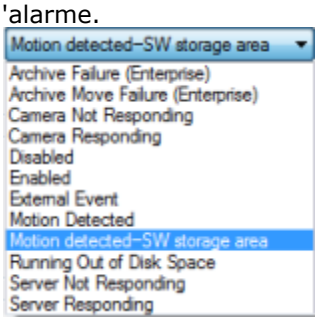
Définitions des alarmes

Lorsque vous système enregistre un événement, vous pouvez le configurer afin de générer une alarme dans XProtect Smart Client. Vous devez définir les alarmes avant de les utiliser et elles sont définies à partir des événements enregistrés sur les serveurs de votre système. Vous pouvez également utiliser des événements définis par l'utilisateur pour déclencher des alarmes et utiliser le même événement pour déclencher plusieurs alarmes différentes.

Ajout d'une alarme

Pour définir une alarme, vous devez créer une définition d'alarme, dans laquelle vous spécifiez, par exemple, ce qui déclenche l'alarme, des instructions quant aux actions que l'opérateur devrait prendre, ce qui peut arrêter l'alarme et à quel moment. Pour obtenir des informations détaillées au sujet des paramètres, voir Définitions des alarmes (propriétés) (voir "Définitions d'alarmes (Propriétés)" á la page 264).

1. Dans le **volet Navigation du site**, agrandissez **Alarmes** et faites un clic droit sur **Définitions d'alarme**.
2. Sélectionnez **Ajouter nouveau**.
3. Remplissez ces propriétés :
   - **Nom** : Saisissez un nom pour la définition d'alarme. Le nom de la définition d'alarme apparaît dès que la définition d'alarme est répertoriée.
   - **Instructions** : Vous pouvez rédiger des instructions pour l'opérateur recevant l'alarme.
   - **Déclenchement de l'événement** : Utilisez les menus déroulants pour sélectionner un type d'événement et un message d'événement à utiliser lors du déclenchement de l'alarme.

     Une liste d'événements déclencheurs pouvant être sélectionnés. L'événement en surbrillance est créé et personnalisé à l'aide d'événements analytiques.
   - **Sources** : Sélectionnez les caméras et/ou autres dispositifs qui devraient être à l'origine de l'événement afin de déclencher l'alarme. Vos options dépendent du type d'événements que vous avez sélectionné.
   - **Profil de temps** : Si vous souhaitez que l'alarme soit activée au cours d'un intervalle de temps spécifique, sélectionnez le bouton radio puis un profil de temps dans le menu déroulant.
   - **Basé sur l'événement :** Si vous souhaitez que l'alarme soit activée par un événement, sélectionnez le bouton radio et spécifiez l'événement qui déclenchera l'alarme. Vous devez également spécifier l'événement qui arrêtera l'alarme.
4. Dans le menu déroulant **Limite de temps**, spécifiez une limite de temps pour les mesures que l'opérateur devrait prendre.

5. Dans le menu déroulant **Événements déclenchés**, indiquez quel événement devrait être déclenché une fois la limite de temps écoulée.

6. Spécifiez des paramètres supplémentaires, tels que les caméras associées et le propriétaire de l'alarme initiale, par exemple.

Définitions d'alarmes (Propriétés)

Le tableau décrit les paramètres que vous pouvez effectuer lorsque vous créez une définition d'alarme

Paramètres de définition d'alarme :

Nom	Description
Activer	Par défaut, la définition de l'alarme est activée. Pour la désactiver, décochez la case.
Nom	Les noms d'alarme ne sont pas nécessairement uniques, mais utiliser des noms et des descriptions d'alarme uniques peut s'avérer avantageux dans de nombreuses situations.
Instructions	Saisissez un texte descriptif au sujet de l'alarme et expliquez comment résoudre le problème ayant causé l'alarme. Le texte apparaît dans XProtect Smart Client lorsque l'utilisateur s'occupe de l'alarme.
Événement déclencheur	Sélectionnez le message d'événement à utiliser en cas de déclenchement de l'alarme. Choisissez dans les deux menus déroulants : • Le premier menu déroulant : Sélectionnez le type d'événement, comme un événement analytique ou des événements système, par exemple. • Le second menu déroulant : Sélectionnez le message d'événement spécifique à utiliser. Les messages disponibles dépendent du type d'événement sélectionné par vos soins dans le premier menu déroulant.
Sources	Spécifie les sources dont proviennent les événements. En dehors des caméras ou autres périphériques, les sources peuvent également être des sources définies par des modules d'extension, telles que VCA et MIP, par exemple. Les options dépendent du type d'événements que vous avez sélectionné.

Déclencheur d'alarme :

Nom	Description
Profil de temps	Sélectionnez le bouton radio **Profil de temps** pour sélectionner l'intervalle de temps au cours duquel la définition d'alarme est active. Seuls les profils de temps que vous avez définis dans le nœud **Règles et événements** figurent dans la liste. Si aucun profil de temps n'est défini, seule l'option **Toujours** est disponible.

Nom	Description
Basée sur l'événement	Si vous souhaitez que l'alarme soit basée sur un événement, sélectionnez ce bouton radio. Une fois sélectionné, choisissez l'événement de démarrage et d'arrêt Vous pouvez sélectionner des événements matériels définis sur les caméras, serveurs vidéo et entrées (voir "Vue d'ensemble des événements" á la page *184*). Vous pouvez également utiliser les définitions d'événement globales/manuelles (voir "À propos des évènements définis par l'utilisateur" á la page *204*).

Action requise de la part de l'opérateur :

Nom	Description
Limite de temps	Sélectionnez une limite de temps relative au moment où une action de l'opérateur est nécessaire. La valeur par défaut est 1 minute. La limite de temps n'est pas active tant que vous n'avez pas attaché d'événement dans le menu déroulant **Événements déclenchés**.
Événements déclenchés	Sélectionnez l'événement à déclencher lorsque la limite de temps est dépassée.

Paramètres supplémentaires :

Nom	Description
Caméras associées	Sélectionnez jusqu'à 15 caméras à inclure dans la définition des alarmes même si ces caméras ne sont pas directement responsables du déclenchement de l'alarme. Cela peut être utile, par exemple, si vous avez sélectionné un message d'événement externe (tel que l'ouverture d'une porte) comme élément déclencheur de l'alarme. En définissant une ou plusieurs caméras à proximité de la porte, vous pouvez associer les enregistrements de l'incident par les caméras à l'alarme.
Plans associés	Assignez un plan à l'alarme lorsqu'elle apparaît dans la liste **Gestionnaire d'alarme** de XProtect Smart Client.
Propriétaire de l'alarme initiale	Sélection d'un utilisateur par défaut responsable de l'alarme.
Priorité initiale de l'alarme	Sélectionnez une priorité (**Haute**, **Moyenne**, **Basse** ou aucune) pour l'alarme. Utilisez ces priorités dans XProtect Smart Client pour définir l'importance d'une alarme.
Catégorie de l'alarme initiale	Sélectionnez une catégorie pour l'alarme, par exemple **Fausse alarme** ou **Investigation requise**.
Événements déclenchés par l'alarme	Définissez un événement que l'alarme peut déclencher dans XProtect Smart Client.
Alarme de fermeture automatique	Si vous souhaitez qu'un événement particulier arrête automatiquement l'alarme, cochez cette case. Les événements ne peuvent pas tous déclencher des alarmes. Décochez la case pour désactiver le lancement de la nouvelle alarme.

Voir également

Ajout d'une alarme (á la page 263)

Paramètres des données de l'alarme

Lorsque vous configurez les paramètres des données d'alarme, indiquez les propriétés suivantes :

Onglet niveaux de données d'alarme

Priorités

Nom	Description
Niveau	Ajoutez de nouvelles priorités avec des chiffres de niveau de votre choix ou utilisez/modifiez les niveaux de priorité par défaut (chiffres 1, 2 or 3). Ces niveaux de priorité servent à configurer les **paramètres de priorités initiaux de** l'alarme.
Nom	Saisissez un nom pour l'entité. Vous pouvez en créer autant que vous le souhaitez.
Son	Sélectionnez le son à associer à l'alarme. Utilisez un son si les sons par défaut ou ajoutez-en plus dans **Paramètres de son**.

États

Nom	Description
Niveau	Vous pouvez, en plus des niveaux d'état par défaut (numéros **1**, **4**, **9** et **11** , qui ne peuvent être ni modifiés ni réutilisés), ajouter des numéros de niveaux de votre choix. Ces niveaux d'états ne sont visibles que dans la *Liste des alarmes* du XProtect Smart Client.

Catégories

Nom	Description
Niveau	Ajoutez de nouvelles catégories avec les numéros de niveau de votre choix. Ces niveaux de catégorie servent à configurer les **paramètres de priorités initiaux de** l'alarme.
Nom	Saisissez un nom pour l'entité. Vous pouvez en créer autant que vous le souhaitez.

Onglet Configuration de la liste d'alarme

Nom	Description
Colonnes disponibles	Dans les colonnes disponibles, utilisez > pour sélectionner les colonnes à mettre à la disposition de la *liste d'alarme* du XProtect Smart Client. Utilisez < pour effacer la sélection. Une fois que vous avez terminé, les **Colonnes sélectionnées** doivent comporter les éléments à intégrer.

Onglet Raisons de la fermeture

Nom	Description
Activer	Toutes les alarmes doivent se voir attribuer une raison de fermeture avant de les fermer.
Raison	Ajoutez des raisons de fermeture pour que l'utilisateur puisse choisir entre plusieurs lors de la fermeture des alarmes. Par exemple *Problème résolu* ou *Fausse alarme*. Vous pouvez en créer autant que vous le souhaitez.

Paramètres sons

Lorsque vous configurez des paramètres de son, indiquez les propriétés suivantes :

Nom	Description
Sons	Sélectionnez le son à associer à l'alarme. La liste de son intègre un certain nombre de sons Windows par défaut. Vous ne pouvez pas les modifier. Cependant, vous pouvez ajouter de nouveau son (au format .wav) si et seulement s'ils sont encodés via Pulse Code Modulation (PCM). Même si les sons par défaut sont des fichiers sons standards Windows, les paramètres locaux de Windows peuvent générer des sons différents en fonction des machines. Certains utilisateurs peuvent également avoir supprimé un ou plusieurs de ces fichiers sons et sont donc par conséquent dans l'incapacité de les jouer. Afin de garantir que le son sera le même partout, nous vous recommandons d'importer et d'utiliser vos propres fichiers .wav encodés avec PCM.
Ajouter	Ajouter des sons. Naviguez dans les sons pour télécharger un ou plusieurs fichiers .wav.
Supprimer	Supprimer un son sélectionné dans la liste des sons ajoutés manuellement. Les sons par défaut ne peuvent être supprimés.
Test	Tester le son. Sélectionnez le son dans la liste. Le son est diffusé une fois.

À propos de la configuration des alarmes à l'aide des esclaves Enterprise

Pertinent uniquement si vous exécutez XProtect Corporate.

Identifiant et mot de passe

Si votre configuration de surveillance inclut un ou plusieurs esclaves XProtect Enterprise et que vous souhaitez inclure un ou plusieurs de ces derniers dans la configuration de vos alarmes, il est important que l'identifiant et le mot de passe de connexion spécifiés lors de l'ajout de l'esclave soient les mêmes que ceux utilisés dans XProtect Central complémentaire dans le serveur XProtect

Enterprise. Dans le cas contraire, le serveur sera incapable de se connecter au XProtect Central complémentaire dans XProtect Enterprise et de collecter les informations de statut.

Mettre à jour les informations de numéro de port

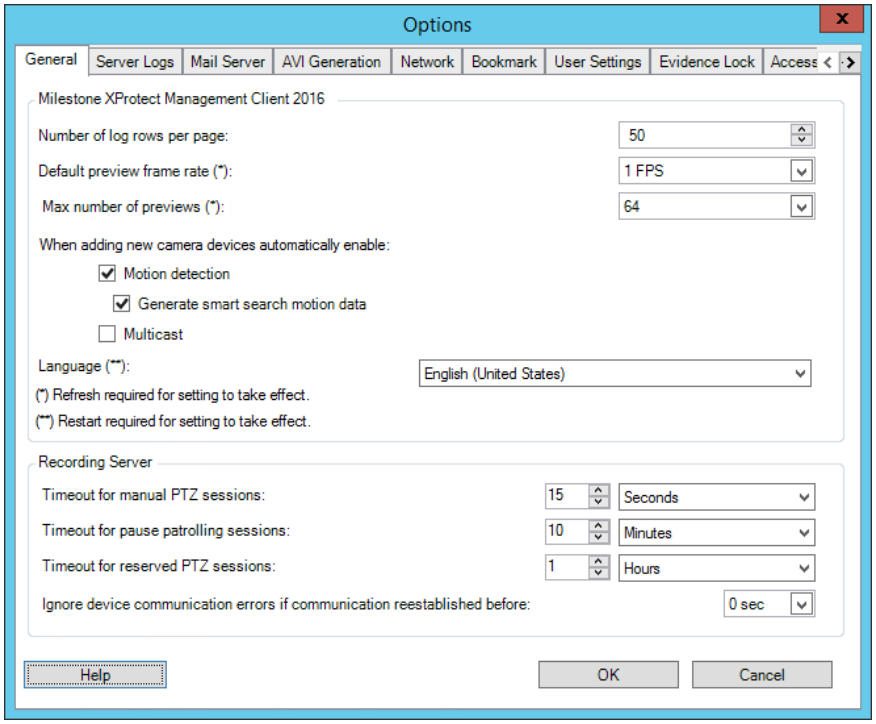
Si vous avez modifié les paramètres du numéro de port dans le XProtect Central complémentaire dans le serveur XProtect Enterprise, vous devez actualiser les informations du numéro de port dans le fichier XML contenant les configurations pour le serveur d'événements. Cela est effectué directement dans le fichier de configuration concerné.

Boîte de dialogue Options

Dans la boîte de dialogue **Options**, vous pouvez spécifier un certain nombre de paramètres en relation avec l'aspect général et la fonctionnalité du système.

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

Pour accéder à la boîte de dialogue, sélectionnez **Outils** > **Options**.



La boîte de dialogue **Options** comporte les onglets suivants :

- Onglet Général (voir "Onglet Général (options)" á la page 269)
- Onglet Journaux de serveurs (voir "Onglet Journaux de serveurs (options)" á la page 271)
- Onglet Serveur de messagerie (voir "Onglet Serveur de messagerie (options)" á la page 272)
- Onglet Génération AVI (voir "Onglet Génération AVI (options)" á la page 273)
- Onglet Réseau (voir "Onglet Réseau (options)" á la page 273)

- Onglet Signet (voir "Onglet Signet (options)" á la page 274)
- Onglet Paramètres utilisateur (voir "Onglet Paramètres utilisateur (options)" á la page 274)
- Onglet Protection des preuves (voir "Onglet Protection des preuves (options)" á la page 274)
- Onglet Paramètres de contrôle d'accès (voir "Onglet Paramètres de contrôle d'accès (options)" á la page 275)
- Onglet Événements analytiques (voir "Onglet Événements analytiques (options)" á la page 275)
- Onglet Serveur d'événements (voir "Onglet Serveur d'événements (options)" á la page 276)
- Onglet Événements génériques (voir "Onglet Événements génériques (options)" á la page 277)

Onglet Général (options)

Dans l'onglet Général, vous pouvez préciser les paramètres d'ordre général pour le Management Client et le serveur d'enregistrement.

Management Client

Nom	Description
Nombre de lignes de journal par page	Sélectionnez le nombre de lignes pouvant être contenues dans une page de journal. La valeur par défaut est 50 lignes. Si un journal contient plus de lignes, les lignes supplémentaires seront affichées sur la page suivante.
Fluidité des images d'aperçu par défaut	Sélectionnez le nombre d'images par seconde pour l'affichage des images miniatures des caméras dans le volet **Aperçu**. Par défaut, le nombre d'images est de 1 par seconde. Sélectionnez **Action** > **Rafraîchir** dans le menu pour confirmer la modification. Notez qu'une fluidité d'image élevée combinée à un grand nombre d'images miniatures dans le volet **Aperçu** ralentit l'ordinateur qui exécute le Management Client. Vous pouvez limiter le nombre d'images miniatures avec le paramètre **Nombre max. d'aperçus**.
Nombre max. d'aperçus	Sélectionnez le nombre maximum d'images miniatures affichées dans le volet **Aperçu**. Par défaut, le nombre d'images miniatures est de 64. Sélectionnez **Action** > **Rafraîchir** dans le menu pour confirmer la modification. Notez qu'une grande quantité d'images miniatures combinée à une fluidité d'images élevée peut ralentir le système. Vous pouvez limiter la fréquence d'images utilisée pour les images miniatures avec le paramètre **Fluidité par défaut des images d'aperçu**.

Nom	Description
Lors de l'ajout de nouveaux périphériques de type caméra, activer automatiquement : **Détection du mouvement**	Cochez la case pour activer la détection de mouvement pour les nouvelles caméras lorsque vous les ajoutez au système à l'aide de l'assistant **Ajouter du matériel**. Ce paramètre n'influence pas les paramètres de détection du mouvement des caméras existantes. Vous activez et désactivez la détection du mouvement pour une caméra dans l'onglet **Mouvement** pour le périphérique de type caméra.
Lors de l'ajout de nouveaux périphériques de type caméra, activer automatiquement : **Générer des données de mouvement pour la recherche intelligente**	La génération de données de mouvement pour la recherche intelligente exige que la détection du mouvement soit activée pour la caméra. Cochez la case pour activer la génération de données de recherche intelligente sur les nouvelles caméras lorsque vous les ajoutez au système à l'aide de l'assistant **Ajouter du matériel**. Ce paramètre n'influence pas les paramètres de détection du mouvement des caméras existantes. Vous activez et désactivez la génération de données de recherche intelligente pour une caméra dans l'onglet **Mouvement** pour le périphérique de type caméra.
Lors de l'ajout de nouveaux périphériques de type caméra, activer automatiquement : **Multicast**	Cochez la case pour activer la diffusion multiflux pour les nouvelles caméras lorsque vous les ajoutez au système à l'aide de l'assistant **Ajouter du matériel**. Ce paramètre n'influence pas les paramètres de diffusion multiflux des caméras existantes. Vous activez et désactivez le multicast en direct pour une caméra dans l'onglet **Client** pour le périphérique de type caméra.
Langue	Sélectionnez la langue du Management Client. Redémarrez le Management Client pour activer la nouvelle langue.

Serveur d'enregistrement

Nom	Description
Période d'inactivité pour les sessions PTZ manuelles	Les utilisateurs du client dotés des droits d'utilisateurs nécessaires peuvent interrompre manuellement la patrouille des caméras PTZ. Sélectionnez la durée qui doit s'écouler avant que le programme de patrouille habituel reprenne suite à une interruption manuelle. Ce paramètre s'applique à toutes les caméras PTZ de votre système. Le paramètre par défaut est de 15 secondes. Si vous souhaitez appliquer des délais individuels aux caméras, spécifiez ceux-ci dans l'onglet **Préréglages** de la caméra.

Nom	Description
Période d'inactivité pour la mise en pause des sessions PTZ	Les utilisateurs du client disposant d'une priorité PTZ suffisante peuvent mettre des patrouilles en pause sur les caméras PTZ. Sélectionnez la durée qui doit s'écouler avant que le programme de patrouille habituel reprenne suite à une pause. Ce paramètre s'applique à toutes les caméras PTZ de votre système. La limite de temps par défaut est de 10 minutes. Si vous souhaitez appliquer des délais individuels aux caméras, spécifiez ceux-ci dans l'onglet **Préréglages** de la caméra.
Période d'inactivité pour les sessions PTZ réservées	Réglez la période d'inactivité par défaut pour les sessions PTZ réservées. Lorsqu'un utilisateur exécute une session PTZ réservée, la caméra PTZ ne peut pas être utilisée par d'autres personnes tant qu'elle n'est pas libérée manuellement ou que la période d'inactivité n'a pas pris fin. Le paramètre par défaut est de 1 heure. Si vous souhaitez appliquer des délais individuels aux caméras, spécifiez ceux-ci dans l'onglet **Préréglages** de la caméra.
Ignorer les erreurs de communication avec le périphérique si la communication est rétablie avant	Sélectionnez la durée de présence d'une erreur de communication avant que le système ne l'inscrive au journal comme étant une erreur et ne déclenche l'événement **Erreur de communication** .

Onglet Journaux de serveurs (options)

Dans l'onglet **Journaux de serveurs**, vous pouvez spécifier les paramètres pour les journaux des serveurs de gestion du système.

Reportez-vous également à la section À propos des journaux (á la page 257) pour plus d'informations.

Nom	Description
Journaux	Sélectionnez le journal que vous souhaitez configurer : • Journal système • Journal d'audit • Journal de règles

Nom	Description
Paramètres	Désactivez/activez les journaux et indiquez la durée de conservation et le nombre maximum de lignes pour chaque journal. Pour les journaux **Système**, indiquez le niveau des messages que vous souhaitez consigner : • Tous les messages - y compris les messages indéfinis • Informations, avertissements et erreurs • Avertissements et erreurs • Erreurs (paramètre par défaut) Pour les journaux **Audit**, activez le protocole des accès utilisateur si vous souhaitez que le système consigne toutes les actions des utilisateurs dans XProtect Smart Client. Il s'agit par exemple des exportations, de l'activation des sorties, du visionnage de caméras en direct ou en mode lecture. Précisez : • la durée d'une séquence de lecture. Cela signifie qu'à condition que l'utilisateur procède à la lecture pendant cette période, le système ne génère qu'une entrée du journal. Lors d'une lecture en dehors de la période, le système crée une nouvelle entrée du journal. • le nombre d'enregistrements (images) qu'un utilisateur a vu avant que le système ne crée une entrée au journal.

Onglet Serveur de messagerie (options)

L'onglet **Serveur de messagerie** vous permet de préciser les paramètres du serveur de messagerie SMTP sortant de votre système.
Voir également À propos des profils de notification (á la page 200).

Nom	Description
Adresse e-mail de l'expéditeur	Saisissez l'adresse e-mail à afficher en tant qu'expéditeur des notifications par e-mail pour tous les profils de notifications. Exemple : expéditeur@entreprise.org.
Nom du serveur (SMTP) de messagerie sortant	Saisissez le nom du serveur de messagerie SMTP procédant à l'envoi des notifications par e-mail. Exemple : serveurmessagerie.entreprise.org.
Connexion au serveur requise	Indiquez un identifiant et mot de passe pour les utilisateurs qui se connectent au serveur de messagerie.

Onglet Génération AVI (options)

L'onglet **Génération AVI** vous permet de spécifier les paramètres de compression pour la génération de fichiers de clip vidéo AVI. La spécification de ces paramètres est requise si vous désirez inclure des fichiers AVI dans les notifications par e-mail envoyées par les profils de notification déclenchés par les règles.

Reportez-vous également à la section Utiliser des règles pour déclencher les notifications par e-mail (voir "Utiliser des règles pour déclencher des notifications par e-mail" á la page 202).

Nom	Description
Logiciel de compression	Sélectionnez le codec (technologie de compression/décompression) à appliquer. Pour disposer de plusieurs codecs sur la liste, installez-les sur le serveur de gestion. Toutes les caméras ne prennent pas tous les codecs en charge.
Qualité de compression	(N'est pas disponible pour tous les codecs). À l'aide du curseur, sélectionnez le niveau de compression (**0**-**100**) que le codec doit exécuter. **0** signifie aucune compression, entraînant généralement une haute qualité d'image et une taille de fichier importante. **100** signifie compression maximum, entraînant généralement une faible qualité d'image et une petite taille de fichier. Si le curseur n'est pas accessible, la qualité de compression est intégralement déterminée par le codec sélectionné.
Image-clé toutes les	(N'est pas disponible pour tous les codecs). Si vous souhaitez utiliser les images-clés, cochez la case et spécifiez le nombre requis d'images entre les images-clés. Une image-clé est une seule image stockée à intervalles définis. L'image-clé contient l'intégralité de la vue de la caméra, alors que les images suivantes ne contiennent que les pixels qui changent. Cela permet de réduire considérablement la taille des fichiers. Si la case à cocher n'est pas accessible, ou non sélectionnée, chaque image contient l'intégralité de la vue de la caméra.
Débit	(N'est pas disponible pour tous les codecs). Si vous souhaitez utiliser un débit spécifique, cochez la case et spécifiez le nombre de kilooctets par seconde requis. Le débit indique la taille du fichier AVI joint. Si la case à cocher n'est pas accessible, ou non sélectionnée, le débit est déterminé par le codec sélectionné.

Onglet Réseau (options)

L'onglet **Réseau** vous permet de préciser les adresses IP des clients locaux si les clients doivent se connecter au serveur d'enregistrement via Internet. Le système de surveillance les reconnaît comme venant du réseau local.

Vous pouvez également préciser la version IP du système : IPv4 ou IPv6. La valeur par défaut est IPv4.

Onglet Signet (options)

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

L'onglet **Signets** vous permet de préciser les paramètres des signets, leur ID et leur fonction dans XProtect Smart Client.

Nom	Description
Préfixe d'ID de signet	Indiquez un préfixe pour tous les signets crées par les utilisateurs de XProtect Smart Client.
Durée du signet par défaut	Indiquez le début et la fin par défaut d'un signet défini dans XProtect Smart Client. Ce paramètre doit être aligné avec : • La règle du signet par défaut, voir Règle enregistrement par défaut du signet. • La période pré-enregistrement pour chaque caméra, voir Gérer les pré-enregistrements (voir "Gérer la mise en mémoire-tampon préalable" á la page 134).

Pour indiquer les droits de signet d'un rôle, reportez-vous à la section Droits du périphérique (voir "Onglet Périphériques (rôles)" á la page 237).

Onglet Paramètres utilisateur (options)

L'onglet **Paramètres utilisateur** vous permet de préciser les paramètres de préférence, par exemple le fait d'afficher un message lorsque l'enregistrement à distance est activé.

Onglet Customer dashboard (Tableau de bord client)

Dans l'onglet **Customer dashboard**, vous pouvez activer ou désactiver le tableau de bord Milestone Customer Dashboard.

Le tableau de bord client est un service de surveillance en ligne qui fournit une représentation graphique de l'état actuel de votre système, y compris d'éventuels problèmes techniques, comme les défaillances de la caméra, aux administrateurs système ou à d'autres personnes qui ont eu accès aux informations sur l'installation de votre système.

Vous pouvez cocher ou décocher la case pour modifier les paramètres du tableau de bord client.

Onglet Protection des preuves (options)

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

Dans l'onglet **Protection des preuves** vous définissez et modifiez les profils de protection des preuves et la durée que vos utilisateurs du client peuvent choisir pour conserver les données protégées.

Nom	Description
Profiles de protection des preuves	Une liste de profils de protection des preuves définis. Vous pouvez ajouter et supprimer des profils de protection des preuves existants. Vous ne pouvez pas supprimer le profil de protection des preuves par défaut, mais vous pouvez modifier ses options de durée et son nom.
Options de durée	La durée que les utilisateurs du client peuvent choisir pour la protection des preuves. Les options de durée disponibles sont : heure(s), jour(s), semaine(s), mois(s), année(s), indéterminés ou définis par l'utilisateur.

Pour indiquer les droits d'accès à la protection des preuves d'un rôle, voir l'onglet Périphériques (voir "Onglet Périphériques (rôles)" á la page 237) pour les paramètres de rôle.

Onglet Paramètres de contrôle d'accès (options)

L'utilisation de XProtect Access nécessite l'achat d'une licence de base qui vous permet d'accéder à cette fonction.

Définissez les paramètres de contrôle d’accès suivants :

Nom	Description
Afficher le volet des propriétés de développement	Si elles sont sélectionnées, les informations de développeur supplémentaire apparaissent pour **Contrôle d'accès > Paramètres généraux**. Ce paramètre est uniquement destiné aux développeurs d'intégrations de systèmes de contrôle d'accès.
Conserver les événements de contrôle d’accès pendant	Indiquez le nombre de jours durant lesquels vous souhaitez que le système garde les événements de contrôle d'accès visibles dans XProtect Smart Client. Par défaut, ce laps de temps est de 30 jours. Le paramètre s'applique uniquement aux événements futurs. Il n'a aucun effet sur les événements déjà stockés dans la base de données. Une valeur de 0 indique que le système ne stocke aucun événement.

Onglet Événements analytiques (options)

L'onglet **Événements analytiques** vous permet d'activer et de spécifier la fonction d'événements analytiques.

Nom	Description
Activer	Spécifiez si vous souhaitez utiliser les événements analytiques. Par défaut, la fonction est désactivée.

Nom	Description
Port	Indiquez le port utilisé par cette fonction. Port par défaut : 9090. Veillez à ce que les fournisseurs de l'outil VCA concernés utilisent également ce numéro de port. Si vous modifiez le numéro de port, rappelez-vous d'également modifier le numéro de port des fournisseurs.
Toutes les adresses du réseau ou Adresses réseau spécifiée	Indiquez si l'autorisation porte sur les événements de toutes les adresses IP/noms d'hôtes ou seulement sur les événements des adresses IP/noms d'hôte spécifiés dans la **liste des adresses** (voir ci-dessous).
Liste des adresses	Saisissez une liste des adresses IP/noms d'hôte de confiance. La liste filtre les données entrantes de sorte que seuls les événements de certaines adresses IP/ noms d'hôtes soient autorisées. Vous pouvez utiliser les deux formats d'adresse pour le système de nom de domaine (DNS), IPv4 et IPv6. Vous pouvez ajouter les adresses à la liste manuellement, en entrant chaque adresse IP ou nom d'hôte ou en important une liste externe d'adresses. • **Saisie manuelle :** Saisissez l'adresse IP/le nom d'hôte dans la liste d'adresses. Répétez l'opération pour chaque adresse désirée. • **Importer :** Cliquez sur le bouton **Importer** pour parcourir la liste d'adresses externe. La liste externe doit être au format .txt et chaque adresse IP ou nom d'hôte doit se trouver sur une ligne séparée.

Onglet Serveur d'événements (options)

L'onglet **Serveur d'événements** vous permet de spécifier les paramètres des alarmes, des événements et des journaux.

Nom	Description
Désactiver les alarmes pendant	Sélectionnez le nombre de jours pendant lesquels garder les alarmes désactivées. Les alarmes désactivées ont un statut **Fermé**, **Ignoré** et **Rejeté**.

Nom	Description
Activer toutes les autres alarmes pendant	Sélectionnez le nombre de jours pendant lesquels conserver toutes les autres alarmes que celles se trouvant dans l'état **Fermé**, **Ignoré** et **Rejeté**. **Important :** des horodateurs sont toujours associés aux alarmes. Si l'alarme est déclenchée par une caméra, l'horodateur dispose d'une image de l'heure de la caméra. Les informations sur l'alarme elle-même sont stockées sur le serveur d'événements, alors que les enregistrements vidéo correspondant à l'image attachée sont sauvegardés sur le serveur du système de surveillance concerné. Pour voir les images de vos alarmes, conservez les enregistrements vidéo pendant une durée au moins égale à celle pendant laquelle vous souhaitez conserver les alarmes sur le serveur d'événements.
Activer les événements pendant	Indiquez le nombre de jours pendant lesquels conserver les événements.
Activer les journaux pendant	Indiquez le nombre de jours pendant lesquels conserver le journal des alarmes. Vous pouvez définir un nombre allant jusqu'à 99999 jours, en fonction de l'espace disponible sur le serveur. Vous pouvez utiliser la valeur 0 pour conserver les alarmes désactivées pendant une durée infinie, en fonction de l'espace disponible sur le serveur.
Communication du serveur de journaux	Cochez la case si vous souhaitez enregistrer un journal distinct de communication du serveur en plus du journal ordinaire, pendant le nombre de jours indiqué.

Onglet Événements génériques (options)

L'onglet **Évènements génériques** vous permet de spécifier les paramètres associés aux sources de données et aux évènements génériques.

Pour de plus amples informations sur la façon dont configurer les événements génériques, reportez-vous à la section À propos des événements génériques (voir "À propos des évènements génériques" á la page 209).

Nom	Description
Source de données	Vous pouvez choisir entre deux sources de données par défaut et définir une source de données personnalisée. Votre choix dépend du type de votre programme tiers et/ou du type de matériel ou logiciel à partir duquel vous souhaitez établir une interface : **Compatible :** les propriétés par défaut sont activées, écho de tous les octets, TCP et UDP, Ipv4 uniquement, port 1234, aucun séparateur, hôte local uniquement, encodage de pages de codes actuel (ANSI). **International :** les propriétés par défaut sont activées, écho des statistiques uniquement, TCP uniquement, Ipv4+6, port 1235, <CR><LF> comme séparateur, hôte local uniquement, encodage UTF-8. (<CR><LF> = 13,10). [Source de données A] [Source de données B] etc.
Nouveau	Cliquez pour définir une nouvelle source de données.
Nom	Nom de la source de données.
Activé	Par défaut, les sources de données sont activées. Décochez la case pour désactiver la source de données.
Réinitialiser	Cliquez pour réinitialiser tous les paramètres de la source de données sélectionnée. Le nom saisi dans le champ **Nom** est conservé.
Port	Le numéro de port de la source de données.
Sélecteur type de protocole	Les protocoles que le système doit écouter et analyser en vue de détecter les événements génériques : **Tout :** TCP aussi bien que UDP. **TCP :** TCP uniquement. **UDP :** UDP uniquement. Les paquets TCP et UDP utilisés pour les événements génériques peuvent contenir des caractères spéciaux, tels que @, #, +, å, ~, et autres.
Sélecteur type IP	Types d'adresses IP à sélectionner : IPv4, IPv6 ou les deux.
Octets de séparation	Sélectionnez les octets séparateurs utilisés pour séparer les enregistrements d'événements génériques individuels. Le type de source de données **International** par défaut (consultez **Sources de données** plus haut) est **13,10**. (13,10 = <CR><IF>).

Nom	Description
Sélecteur type d'écho	Formats de retour d'écho disponibles : • **Statistiques d'écho :** Renvoie le format suivant : **[X],[Y],[Z],[Nom de l'événement générique]** **[X]** = numéro de demande. **[Y]** = nombre de caractères. **[Z]** = nombre de concordances avec un événement générique. **[Nom de l'événement générique]** = nom saisi dans le champ **Nom :** . • **Écho tous les octets :** Renvoie tous les octets. • **Pas d'écho :** Supprime tous les échos.
Sélecteur type d'encodage	Par défaut, la liste affiche uniquement les options les plus pertinentes. Cochez la case **Afficher tout** pour afficher tous les codages à disposition.
Adresses IPv4 externes autorisées	Spécifiez les adresses IP avec lesquelles le serveur de gestion doit pouvoir communiquer afin de gérer les événements externes. Vous pouvez également utiliser cette fonction pour exclure les adresses IP dont vous ne souhaitez pas recevoir de données.
Adresses IPv6 externes autorisées	Spécifiez les adresses IP avec lesquelles le serveur de gestion doit pouvoir communiquer afin de gérer les événements externes. Vous pouvez également utiliser cette fonction pour exclure les adresses IP dont vous ne souhaitez pas recevoir de données.

Configuration des fonctions

Serveurs de gestion de redondance

À propos des serveurs de gestion multiples (grappes)

Le logiciel du serveur de gestion peut être installé sur de multiples serveurs au sein d'une grappe de serveurs. Ceci permet de garantir un temps d'arrêt limité du système. Si un serveur dans une grappe devient indisponible, un autre serveur de cette grappe prend automatiquement le relais du serveur défaillant et continue d'exécuter le serveur de gestion. Le processus automatique de basculement entre le service du serveur et un autre serveur de la grappe ne prend que quelques instants (jusqu'à 30 secondes).

Il n'est possible d'avoir qu'un seul serveur de gestion actif par configuration de surveillance, mais d'autres serveurs de gestion peuvent être configurés pour prendre le relais en cas de défaillance.

Le nombre de redondances permis est limité à deux pour toute période de six heures. En cas de dépassement de ce seuil, le service de regroupement ne démarre pas automatiquement les services Management Server. Le nombre de redondances permises peut être modifié pour mieux correspondre à vos besoins. Reportez-vous à la page d'accueil de Microsoft® http://technet.microsoft.com/en-us/library/cc787861%28WS.10%29.aspx pour de plus amples informations.

Conditions préalables au regroupement

- Deux serveurs ou plus installés dans une grappe :

  - Pour les grappes sous Microsoft Windows 2008®, reportez-vous à la section Grappes de redondance http://technet.microsoft.com/en-us/library/cc732488(WS.10).aspx.

- **Soit** une base de données SQL externe installée **en dehors** de la grappe de serveurs **soit** un service SQL **interne** (en grappe) au sein de la grappe de serveurs (la création d'un service SQL interne nécessite l'utilisation de SQL Server Standard ou d'une version ultérieure capable de fonctionner en tant que serveur SQL en grappe).

- Un serveur Microsoft® Windows® (édition Enterprise ou Data Center).

Installation dans une grappe

Les descriptions et illustrations présentées peuvent être différentes de ce que vous voyez à l'écran.

Installation et modification de l'adresse URL :

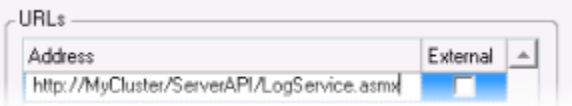
1. Installez le serveur de gestion et tous ses composants secondaires sur le premier serveur de la grappe.

   Le serveur de gestion doit être installé avec un utilisateur spécifique, et non en tant que **service de réseau**. Pour ce faire, vous devez utiliser l'option d'installation **Personnalisée.** De plus, l'utilisateur spécifique doit avoir accès au disque de réseau partagé et à un mot de passe sans expiration de préférence.

2. Après avoir installé le serveur de gestion et le Management Client sur le premier serveur de la grappe, ouvrez le Management Client, puis, à partir du menu **Outils**, sélectionnez **Services enregistrés**.

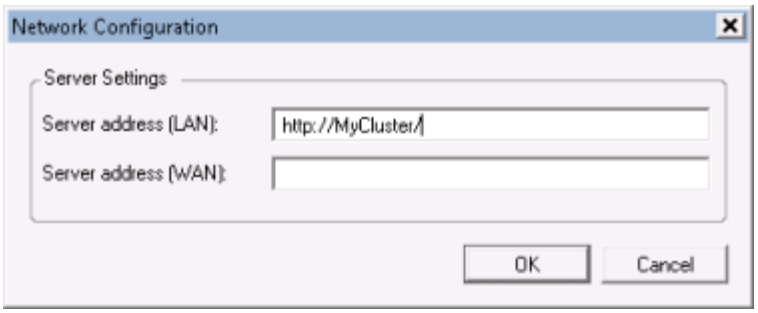
   a) Dans la fenêtre **Ajouter/supprimer des services enregistrés**, sélectionnez **Service de journal** dans la liste, puis cliquez sur **Modifier**.

   b) Dans la fenêtre **Modifier le service enregistré**, remplacez l'adresse URL du service de journal par l'adresse URL de la grappe.



   c) Répétez les étapes a et b pour tous les services listés dans la fenêtre **Ajouter/supprimer des services enregistrés**. Cliquez sur **Réseau**.

   d) Dans la fenêtre **Configuration réseau**, remplacez l'adresse URL du serveur par l'adresse URL de la grappe. (Cette étape s'applique uniquement au premier serveur de la grappe.) Cliquez sur **OK**.



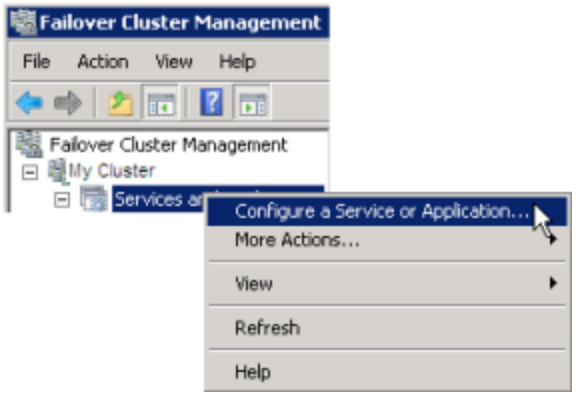
3. Dans la fenêtre **Ajouter/supprimer des services enregistrés**, cliquez sur **Réseau...** Quittez le Management Client.

4. Arrêtez le service Management Server ainsi qu'IIS. Obtenez de plus amples informations sur la façon d'arrêter l'IIS sur la page d'accueil de Microsoft® http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx.

5. Répétez les étapes 1-4 pour tous les serveurs suivants de la grappe, en les orientant cette fois-ci vers la base de données SQL. Cependant, pour le **dernier** serveur de la grappe sur lequel vous installez le serveur de gestion, n'arrêtez pas le service Management Server.

Ensuite, afin qu'il puisse prendre effet, le service Management Server doit être configuré en tant que service générique dans la grappe de redondance :

1. Sur le dernier serveur sur lequel vous avez installé le serveur de gestion, allez dans **Démarrer** > **Outils d'administration**, ouvrez le module de **Gestion de la grappe de redondance** de Windows. Dans la fenêtre **Gestion de la grappe de redondance**, agrandissez votre grappe, cliquez sur **Services et applications** à l'aide du bouton droit de votre souris et sélectionnez **Configurer un service ou une application**.



2. Dans la boîte de dialogue **Haute disponibilité**, cliquez sur **Suivant**, sélectionnez **Service générique** et cliquez sur **Suivant**. Ne spécifiez rien sur la troisième page de la boîte de dialogue et cliquez sur **Suivant**.

3. Sélectionnez le service **Milestone XProtect Management Server**, cliquez sur **Suivant**. Spécifiez le nom (nom de l'hôte de la grappe), que les clients utilisent pour accéder au service, cliquez sur **Suivant.**

4. Aucun espace de stockage n'est requis pour ce service ; cliquez sur **Suivant**. Aucun paramètre de registre ne doit être répliqué ; cliquez sur **Suivant.** Vérifiez que le service regroupé est configuré selon vos besoins, cliquez sur **Suivant.** Le serveur de gestion est maintenant configuré en tant que service général de la grappe de redondance. Cliquez sur **Terminer**.

5. Dans la configuration de la grappe, le serveur d'événements et le collecteur de données doivent être configurés comme service dépendant du serveur de gestion pour que le serveur d'événements s'arrête lorsque le serveur de gestion s'arrêtera.

6. Pour ajouter le service **Milestone XProtect Event Server** en tant que ressource pour le service **Milestone XProtect Management Server Cluster**, cliquez sur le service de grappe à l'aide du bouton droit de votre souris et cliquez sur **Ajouter une ressource**> **4 - Service générique** et sélectionnez **Serveur d'événements Milestone XProtect.**

Mise à jour dans une grappe

Assurez-vous d'avoir une copie de sauvegarde de la base de données avant de mettre la grappe à niveau.

1. Arrêtez les services Management Server sur tous les serveurs de gestion de la grappe.

2. Désinstallez le serveur de gestion sur tous les serveurs de la grappe.

3. Utilisez la procédure d'installation de serveurs de gestion multiples dans une grappe, comme décrite pour l'installation dans une grappe, voir Installation dans une grappe (á la page 280).

Important : Lors de l'installation, assurez-vous de réutiliser la base de données de configuration SQL existante (qui passe automatiquement de l'ancienne version de la base de données existante à la nouvelle version).

Services de connexion à distance

À propos des services de connexion à distance

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

La fonction Services de connexion à distance bénéficie de la technologie de connexion de la caméra Axis One-click, développée par Axis Communications. Elle active le système pour récupérer des vidéos (et audio) des caméras extérieures où les pare-feu et / ou une configuration de réseaux de routeurs empêche toute tentative de connexion à ces caméras. La communication réelle a lieu par les serveurs de tunnel sécurisés (serveurs ST). Les serveurs ST utilisent un VPN. Seuls les périphériques détenant une clé valide fonctionnent avec un VPN. Ceci offre un tunnel de sécurité où les réseaux publics peuvent échanger des données en toute sécurité.

Les services de connexion à distance vous permettent de :

- Modifier les données de connexion au sein du service de répartition d'axis
- Ajouter, modifier et retirer les serveurs ST
- Enregistrer/désenregistrer et modifier les caméras Axis One-click.
- Atteindre le matériel relatif à la caméra Axis One-Click.

Avant de pouvoir bénéficier de la connexion à la caméra Axis One-click, commencez par installer un environnement approprié avec un serveur ST. Pour travailler avec les environnements de serveurs de tunnel sécurisé (serveur ST) et des caméras Axis One-click, veuillez contacter au préalable votre fournisseur de système pour obtenir le nom d'utilisateur et le mot de passe exigés pour les services de répartition Axis.

Installer un environnement STS pour une connexion à la caméra One-click

Conditions préalables :

- Créez un compte auprès d'Axis pour obtenir le nom d'utilisateur et le mot de passe requis pour les services de répartition d'Axis.
- Assurez-vous que votre/vos caméra(s) prennent en charge Axis Video Hosting System. Allez sur le site web d'Axis pour voir les périphériques pris en charge http://axis-avhs.com/supported-devices/.
- Si nécessaire, actualisez vos caméras Axis avec le nouveau firmware. Allez sur le site web d'Axis pour télécharger le firmware http://www.axis.com/techsup/firmware.php.

1. Sur la page d'accueil de chaque caméra, allez sur **Configuration de base**, **TCP/IP**, et sélectionnez **Activer AVHS** et **Toujours**.

2. À partir de la page web de téléchargement de votre serveur de gestion (contrôlée par le Download Manager, installez le **composant de connexion Axis One-Click** pour créer un cadre de tunnel sécurisé pour Axis

Ajouter/Modifier des STS

1. Procédez comme suit :

a) Pour ajouter un serveur ST, cliquez sur le nœud principal **Serveurs de tunnel sécurisé Axis** avec le bouton droit de votre souris et sélectionnez **Ajouter serveur de tunnel sécurisé Axis**.

b) Pour modifier un serveur ST, cliquez dessus avec le bouton droit de votre souris et sélectionnez **Modifier serveur de tunnel sécurisé Axis**.

2. Dans la fenêtre qui apparaît, remplissez les informations pertinentes.
3. Si vous avez choisi d'utiliser des certificats lorsque vous avez installé le **composant de connexion Axis One-Click**, cochez la case **Utiliser les certificats** et utilisez exactement le même nom d'utilisateur et le même mot de passe que pour le **composant de connexion Axis One-Click**.
4. Cliquez sur **OK**.

Enregistrer une nouvelle caméra Axis One-click

1. Pour enregistrer une caméra sous un serveur ST, cliquez dessus avec le bouton droit de votre souris et sélectionnez **Enregistrer caméra Axis One-click**.
2. Dans la fenêtre qui apparaît, remplissez les informations pertinentes.
3. Cliquez sur **OK**.
4. La caméra apparaît alors sous le serveur ST pertinent.

La caméra peut avoir les codes couleur suivants :

Couleur	Description
Rouge	État initial. Enregistrée, mais pas connectée au serveur ST.
Jaune	Enregistrée. Connectée au serveur ST, mais pas ajoutée en tant que matériel.
Vert	Ajoutée en tant que matériel. Peut être connectée au serveur ST ou non.

Lorsque vous ajoutez une nouvelle caméra, son état est toujours vert. L'état de connexion est reflété par l'option **Périphériques** sur **Serveurs d'enregistrement** dans le volet **Vue d'ensemble**. Dans le volet **Vue d'ensemble**, vous pouvez regrouper vos caméras pour pouvoir les examiner plus facilement. Si vous choisissez de ne **pas** enregistrer votre caméra sur le service de répartition Axis à ce moment-là, vous pouvez le faire par la suite à l'aide du menu apparaissant lorsque vous cliquez sur le bouton droit de la souris, en sélectionnant **Modifier caméra Axis One-click**.

Propriétés de connexion à la caméra Axis One-Click

Nom	Description
Mot de passe caméra	Saisir/modifier Fourni avec votre caméra à l'achat. Pour plus d'informations, consulter le manuel de votre caméra ou rendez-vous sur le site web d'Axis http://www.axis.com.
Utilisateur caméra :	Voir les détails concernant le **Mot de passe caméra.**
Description	Saisir/modifier une description pour la caméra.
Adresse externe	Saisir/modifier l'adresse http du serveur ST auquel la/les caméra(s) se connectent.
Adresse interne	Saisir/modifier l'adresse http du serveur ST auquel le serveur d'enregistrement se connecte.
Nom	Modifiez le nom de l'élément si nécessaire.
Clé d'identification du propriétaire	Voir **Mot de passe caméra.**
Mots de passe (pour Dispatch Server)	Saisir le mot de passe : Doit être identique à celui fourni par le fournisseur de votre système.
Mots de passe (pour le serveur ST)	Saisir le mot de passe : Doit être identique à celui saisi lors de la création de **Connection Component Axis One-Click**.
Enregistrement/Dé-recensement sur le service de répartition Axis	Indiquez si vous souhaitez enregistrer votre caméra Axis avec le service de répartition Axis. Peut être effectué au moment de la création ou à une date ultérieure.
Numéro de série	Numéro de série du matériel tel que spécifié par le fabricant. Le numéro de série est souvent, mais pas toujours, identique à l'adresse MAC.
Utiliser les certificats	Cochez la case si vous avez décidé d'utiliser des certificats lors de l'installation du serveur ST.
Nom d'utilisateur (pour Dispatch Server)	Saisissez un nom d'utilisateur. Le nom d'utilisateur doit être identique à celui fourni par le fournisseur de votre système.
Nom d'utilisateur (pour le serveur ST)	Saisissez/modifiez un nom d'utilisateur. Doit être identique à celui saisi lors de la création de **Connection Component Axis One-Click**.

Milestone Federated Architecture

À propos de la sélection de Milestone Interconnect ou Milestone Federated Architecture

Dans un système Advanced VMS à distribution physique où les utilisateurs d'un site central doivent pouvoir accéder à la vidéo directement sur le site distant, vous pouvez choisir entre Milestone Interconnect™ et Milestone Federated Architecture™.

Milestone recommande Milestone Federated Architecture lorsque :

- La connexion réseau entre les sites centralisés et fédérés est stable
- Le réseau utilise le même domaine.
- Il y a peu de sites, mais ils sont grands.
- La bande passante est suffisante pour l'usage requis.

Milestone recommande Milestone Interconnect lorsque :

- La connexion réseau entre les sites centraux et distants est instable.
- Vous ou votre organisation souhaitez utiliser un autre produit XProtect sur les sites distants.
- Le réseau utilise différents domaines ou groupes de travail.
- Il y a beaucoup de sites de petite envergure.

À propos de Milestone Federated Architecture

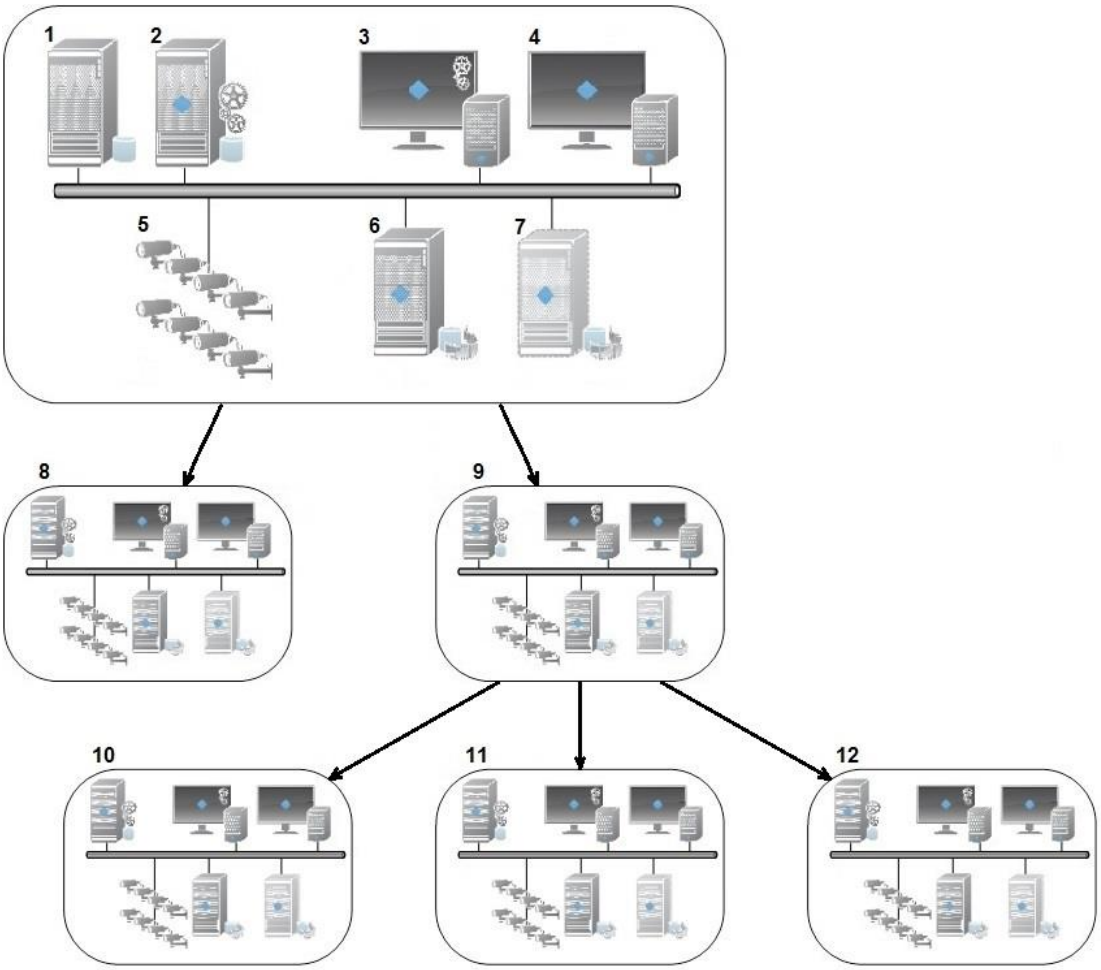
XProtect Expert ne peuvent fédérés qu'en tant que sites enfants.

Milestone Federated Architecture relie de multiples systèmes standard individuels pour créer une hiérarchie de sites fédérés, composée de sites parents/enfants. Les utilisateurs du client dotés de droits suffisants bénéficient d'un accès transparent aux vidéos, fichiers audio et autres ressources via les sites individuels. Les administrateurs peuvent gérer de façon centrale l'ensemble de sites de la hiérarchie fédérée, en fonction des droits d'administrateur pour les sites individuels.

Les utilisateurs basiques ne sont pas pris en charge dans les systèmes Milestone Federated Architecture, vous devrez ajouter des utilisateurs en tant qu'utilisateurs de Windows via le service Active Directory.

Important : À partir du Management Client 2016, vous pouvez gérer centralement les sites fédérés fonctionnant sous des versions antérieures du produit après avoir appliqué le correctif sur les serveurs (voir "Appliquer des correctifs aux serveurs sur les versions plus anciennes" á la page 291). Les versions prises en charge sont XProtect Corporate 2013 et XProtect Expert 2013 ou toute autre version plus récente.

Milestone Federated Architecture est configuré avec un seul site central (site supérieur) et un nombre illimité de sites fédérés (voir "Configurer votre système pour exécuter des sites fédérés" á la page 289). Lorsque vous êtes connecté à un site, vous pouvez accéder à des informations concernant tous ses sites enfants et les sites enfants de ses sites enfants. Le lien entre deux sites est établi lorsque vous demandez le lien à partir du site parent (voir "Ajouter un site à la hiérarchie" á la page 292). Un site enfant ne peut être relié qu'à un seul site parent. Si vous n'êtes pas l'administrateur du site enfant lorsque vous l'ajoutez à la hiérarchie des sites fédérés, la demande doit être acceptée par l'administrateur du site enfant.



Voici les composants d'une configuration Milestone Federated Architecture :

1. Serveur SQL
2. Serveur de gestion
3. Management Client
4. XProtect Smart Client
5. Caméras
6. Serveur d'enregistrement
7. Serveur d'enregistrement de redondance
8. à 12. Sites fédérés

Synchronisation de la hiérarchie

Un site parent contient une liste mise à jour de tous les sites enfants qui y sont attachés à présent, ainsi que de tous les sites enfants des sites enfants, etc. La hiérarchie des sites fédérés inclut une synchronisation programmée entre les sites, ainsi qu'une synchronisation déclenchée par la direction à chaque fois qu'un site est ajouté ou supprimé. La synchronisation de la hiérarchie par le système a lieu niveau par niveau. Chaque niveau transmet et retourne des messages jusqu'à ce qu'il atteigne le serveur demandant les informations. Le système envoie moins de 1 Mo à chaque fois. En fonction du nombre de niveaux, les modifications apportées à une hiérarchie peuvent mettre du temps à apparaître dans le Management Client. Vous ne pouvez pas planifier vos propres synchronisations.

Trafic des données

Le système envoie des communications ou des données de configuration lorsqu'un utilisateur ou un administrateur consulte des vidéos enregistrées ou en direct, ou qu'il configure un site. La quantité de données dépend de la quantité et du contenu visualisé ou configuré.

Milestone Federated Architecture avec d'autres produits

- Si le site central utilise XProtect Smart Wall, vous pouvez également utiliser les fonctions XProtect Smart Wall dans la hiérarchie des sites fédérés. Voir Configurer XProtect Smart Walls (voir "Configurer les Smart Wall" á la page 306) pour découvrir comment configurer un XProtect Smart Wall.
- Si le site central utilise XProtect Access et si un utilisateur XProtect Smart Client se connecte à un site dans une hiérarchie de sites fédérés, les notifications de demande d'accès envoyées par les sites fédérés apparaissent également dans XProtect Smart Client.
- Vous ne pouvez ajouter des systèmes XProtect Expert 2013 (ou des versions plus récentes) à la hiérarchie des sites fédérés qu'en tant que sites enfants, et non en tant que sites parents.
- Pour intégrer des serveurs XProtect Enterprise versions 6.0 et ultérieures dans votre système, voir À propos des serveurs XProtect Enterprise (á la page 411).
- Milestone Federated Architecture ne nécessite aucune licence supplémentaire.
- Pour plus d'informations sur les applications et les avantages de ce système, consultez le livre blanc concernant la technologie Milestone Milestone Federated Architecture sur le site web de Milestone.

Établir une hiérarchie de sites fédérés

Avant de commencer à bâtir la hiérarchie dans le Management Client, Milestone vous recommande de planifier les liaisons entre vos sites.

Vous installez et configurez chaque site au sein d'une hiérarchie fédérée comme un système autonome normal avec des standards en termes de composants système, paramètres, règles, programmations, administrateurs, utilisateurs et droits d'utilisateurs. Si vous avez déjà installé et configuré les sites et qu'il ne vous reste plus qu'à les combiner au sein d'une hiérarchie de sites fédérés, vos systèmes sont prêts à être configurés.

Une fois les sites individuels installés, vous devez les configurer afin qu'ils fonctionnent en tant que sites fédérés (voir "Configurer votre système pour exécuter des sites fédérés" á la page 289).

Pour commencer la hiérarchie, vous pouvez vous connecter au site que vous souhaitez utiliser en tant que site central et ajouter (voir "Ajouter un site à la hiérarchie" á la page 292) le premier site fédéré. Lorsque le lien est établi, les deux sites créent automatiquement une hiérarchie de sites

fédérés dans le volet **Hiérarchie des sites fédérés** du Management Client et vous pouvez y ajouter d'autres sites pour développer la hiérarchie fédérée.

Lorsque vous avez créé la hiérarchie, les utilisateurs et administrateurs peuvent se connecter à un site pour y accéder et accéder à tout site fédéré dont il dispose. L'accès aux sites fédérés dépend des droits de l'utilisateur.

Vous pouvez ajouter un nombre illimité de sites à une hiérarchie fédérée. En outre, vous pouvez lier un site fonctionnant sur une version plus ancienne du produit à une version plus récente et vice versa. Les numéros de version apparaissent automatiquement et ne peuvent pas être supprimés. Le site auquel vous êtes connecté est toujours en haut du volet de la **Hiérarchie des sites fédérés** et s'appelle le site d'origine.

Exemples de sites fédéré dans le Management Client.
À gauche : Connecté au site supérieur.
À droite : Connecté à l'un des sites enfants. Dans cet exemple, le serveur Paris, qui est ainsi le site d'origine.

Icônes d'état dans Milestone Federated Architecture

Les icônes représentent les états possibles d'un site :

Description	Icône
Le site supérieur de l'ensemble de la hiérarchie est opérationnel.	
Le site supérieur de l'ensemble de la hiérarchie est encore opérationnel, mais un ou plusieurs problèmes nécessitent votre attention. Affiché par-dessus l'icône du site supérieur.	
Le site est opérationnel.	
Le site est en attente d'acceptation dans la hiérarchie.	
Le site est attaché mais n'est pas encore opérationnel.	

Configurer votre système pour exécuter des sites fédérés

Afin de préparer votre système pour Milestone Federated Architecture, vous devez effectuer certains choix lors de l'installation du serveur de gestion. Selon la façon dont votre infrastructure informatique est configurée, choisissez parmi les trois alternatives suivantes :

Alternative 1 : Connecter des Sites d'un même Domaine (ayant un utilisateur de Domaine Commun)

Avant d'installer le serveur de gestion, vous devez créer un utilisateur de domaine commun et configurer cet utilisateur en tant qu'administrateur sur tous les serveurs associés à la hiérarchie de sites fédérés.

Installation Personnalisée

1. Commencez l'installation du produit sur le serveur devant être utilisé comme serveur de gestion et sélectionnez **Personnalisé**.
2. Sélectionnez afin d'installer le service Management Server en utilisant un compte utilisateur. Le compte utilisateur sélectionné doit être l'administrateur sur l'ensemble des serveurs de gestion. Vous devez utiliser le même compte utilisateur lorsque vous installez les autres serveurs de gestion dans la hiérarchie des sites fédérés.
3. Terminez l'installation. Répétez les étapes 1 à 3 afin d'installer tout autre système que vous souhaitez ajouter à la hiérarchie des sites fédérés.
4. Si votre hiérarchie des sites fédérés contient des sites avec différentes versions de XProtect Advanced VMS, continuez en appliquant des correctifs sur les versions plus anciennes des sites fédérés (voir "Appliquer des correctifs aux serveurs sur les versions plus anciennes" á la page 291). Si tous les sites fonctionnent à partir de la même version, continuez à Ajouter un site à la hiérarchie (á la page 292)

Installation à serveur unique ou distribuée - configurer le service réseau sur tous les serveurs :

1. Commencez l'installation du produit sur le premier serveur à utiliser en tant que serveur de gestion et sélectionnez **Serveur unique** ou **Distribué**. Ceci installe le serveur de gestion en utilisant un compte de service réseau. Répétez cette étape pour tous les sites de votre hiérarchie de sites fédérés.
2. Connectez-vous au site que vous souhaitez utiliser en tant que site central dans la hiérarchie de sites fédérés.
3. Dans le Management Client, développez **Sécurité** > **Rôles** > **Administrateurs.**
4. Dans l'onglet **Utilisateurs et groupes**, cliques sur **Ajouter** et sélectionnez **Utilisateur Windows**.
5. Dans la fenêtre de dialogue, sélectionnez **Ordinateurs** en tant que type d'objet, saisissez le nom du serveur du site fédéré et cliquez sur **OK** pour ajouter le serveur au rôle d'**Administrateur** du site central. Répétez cette étape jusqu'à ce que tous les sites fédérés soient ajoutés de cette façon puis quittez l'application.
6. Connectez-vous à chaque site fédéré et ajoutez les serveurs suivants au rôle d'**Administrateur**, comme indiqué ci-dessus :
   - Le serveur du site parent.
   - Les serveurs du site enfant que vous souhaitez connecter directement à ce site fédéré.
7. Si votre hiérarchie des sites fédérés contient des sites avec différentes versions de XProtect Advanced VMS, continuez en appliquant des correctifs sur les versions plus anciennes des sites fédérés (voir "Appliquer des correctifs aux serveurs sur les versions plus anciennes" á la page 291). Si tous les sites fonctionnent à partir de la même version, continuez à Ajouter un site à la hiérarchie (á la page 292)

Alternative 2 : Connecter des sites de différents domaines

Afin de pouvoir vous connecter aux sites sur l'ensemble des domaines, assurez-vous que ces domaines se font mutuellement confiance. Configurez les domaines de façon à ce qu'ils se fassent mutuellement confiance dans la configuration du domaine de Microsoft Windows. Lorsque vous avez établi une relation de confiance entre les différents domaines de chaque site de la hiérarchie des sites fédérés, procédez comme indiqué au paragraphe Alternative 1. Pour plus d'informations sur la façon de configurer les domaines fiables, voir le site web de Microsoft http://technet.microsoft.com/en-us/library/cc961481.aspx.

Milestone recommande Milestone Interconnect pour la création de systèmes à sites multiples avec plusieurs domaines.

Alternative 3 : Connecter des sites dans un ou plusieurs groupe(s) de travail

Lorsque vous connectez des sites à l'intérieur de groupes de travail, le même compte d'administrateur doit être présent sur tous les serveurs que vous souhaitez connecter à la hiérarchie des sites fédérés. Vous devez définir le compte d'administrateur avant d'installer le système.

1. Connectez-vous à **Windows** en utilisant un compte administrateur commun.
2. Commencez à installer le produit et cliquez sur **Personnaliser**
3. Sélectionnez pour installer le service Management Server en utilisant le compte administrateur commun.
4. Terminez l'installation. Répétez les étapes 1 à 4 pour installer tous les autres systèmes que vous souhaitez connecter. Vous devez installer tous ces systèmes en utilisant le compte administrateur commun.
5. Si votre hiérarchie des sites fédérés est composée de sites sur différentes versions de XProtect Advanced VMS, continuez en appliquant des correctifs sur les versions plus anciennes des sites fédérés (voir "Appliquer des correctifs aux serveurs sur les versions plus anciennes" á la page 291). Si tous les sites fonctionnent à partir de la même version, continuez à Ajouter un site à la hiérarchie (á la page 292)

Milestone recommande Milestone Interconnect pour la création de systèmes à sites multiples connectés lorsque les sites ne font pas partie d'un domaine.

Vous ne pouvez pas mélanger domaine(s) et groupe(s) de travail. Cela signifie que vous ne pouvez pas connecter les sites d'un domaine aux sites d'un groupe de travail et vice versa.

Appliquer des correctifs aux serveurs sur les versions plus anciennes

Pour ajouter et gérer des sites fonctionnant sur des versions plus anciennes du produit, vous devez remplacer certains fichiers dans le dossier serveur de gestion des serveurs exécutant les versions plus anciennes. Les fichiers des correctifs sont inclus dans l'installation de XProtect Corporate 2016 R2. Le chemin par défaut menant aux fichiers des correctifs est :

```
...\Program Files\Milestone\XProtect Management Client\[dossier de l'ancienne version]\ServerPatch
```

Le tableau fait le lien entre les versions du produit prises en charge et les dossiers correspondants. Il se peut que votre système comporte des versions plus récentes :

Produit	Version du logiciel	Dossier de la version plus ancienne
XProtect Corporate 2013	6.0a	MC601
XProtect Corporate 2013 R2	6.1a	MC611
XProtect Corporate 2014	7.0a	MC701
XProtect Corporate 2014 SP1	7.0b	MC702
XProtect Corporate 2014 SP2	7.0c	MC703
XProtect Corporate 2014 SP3	7.0d	MC704

Préalable : Avant d'entamer l'application du correctif, vous devez connaître les versions du logiciel utilisées par les sites.

Suivez les étapes ci-dessous pour appliquer le correctif aux versions plus anciennes :

1. Connectez-vous à l'ordinateur sur lequel le Management Client 2016 R2 est installé.
2. Ouvrez un explorateur de fichiers et copiez les fichiers du dossier :

   ...\Program Files\Milestone\XProtect Management Client\[dossier de l'ancienne version]\ServerPatch

   vers un emplacement auquel vous pouvez accéder à partir des serveurs exécutant les versions plus anciennes.

   Le chemin menant au correctif des serveurs est peut-être différent dans votre système.
3. Connectez-vous au serveur de gestion de la version plus ancienne de XProtect Corporate.
4. Ouvrez un explorateur de fichiers et naviguez jusqu'au dossier : ....\Program Files\Milestone\XProtect Management Server\IIS\ManagementServer\bin.
5. Remplacez les fichiers du dossier par les fichiers du correctif.
6. Procédez de même à partir de l'étape 2 pour les autres sites fonctionnant sous des versions plus anciennes.

   Vous êtes prêt à configurer la hiérarchie des sites fédérés dans le Management Client, reportez-vous à Ajouter un site à la hiérarchie (á la page 292)

Les fichiers d'aide du Management Client sont les fichiers installés à l'origine avec le produit, car ils ne nécessitent pas de correctif.

Ajouter un site à la hiérarchie

Lorsque vous agrandissez le système, vous pouvez ajouter des sites à votre site supérieur et à ses sites enfants dans la mesure où le système est configuré correctement.

1. Sélectionnez le volet **Hiérarchie des sites fédérés**.

2. Sélectionnez le site auquel vous souhaitez ajouter un site enfant, faites un clic droit et cliquez sur **Ajouter un site à la hiérarchie**.
3. Saisissez l'URL du site requis dans la fenêtre **Ajouter un site à la hiérarchie** et cliquez sur **OK**.
4. Le site parent envoie une demande de liaison au site enfant et, après quelques temps, un lieu entre les deux sites est ajouté dans le volet **Hiérarchie des sites fédérés**.
5. Si vous pouvez établir le lien vers le site enfant sans avoir à obtenir l'acceptation de l'administrateur du site enfant, passez à l'étape 7.

   Sinon, le site enfant est accompagné de l'icône d'attente d'autorisation  jusqu'à ce que l'administrateur du site enfant autorise la demande.
6. Assurez-vous que l'administrateur du site enfant autorise la demande de lien à partir du site enfant (voir "Accepter les ajouts à la hiérarchie" á la page 293).
7. Le nouveau lien parent/enfant est établi et le panneau **Hiérarchie des sites fédérés** est mis à jour avec l'icône  pour le nouveau site enfant.

Accepter les ajouts à la hiérarchie

Lorsqu'un site enfant a reçu une demande de liaison d'un site parent potentiel et que l'administrateur ne disposait pas de droits d'administrateur pour le site enfant, elle porte l'icône en attente d'acceptation  .

Pour accepter une demande de liaison :

1. Connectez-vous au site.
2. Dans le volet **Hiérarchie des sites fédérés**, cliquez avec le bouton droit sur le site et cliquez sur **Accepter l'inclusion dans la hiérarchie**.

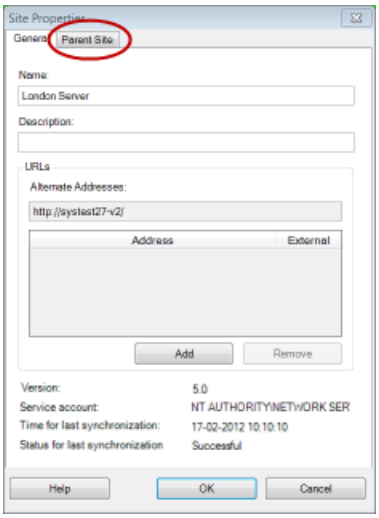
   Si le site exécute une version XProtect Expert, effectuez un clic droit sur e site dans le volet **Navigation du site**.
3. Cliquez sur **Oui**.
4. Le nouveau lien parent/enfant est établi et le panneau **Hiérarchie des sites fédérés** est mis à jour avec l'icône de site normal  pour le site sélectionné.

   Les modifications que vous apportez aux sites enfants à partir du site parent peuvent mettre du temps à se voir reflétée dans le panneau **Hiérarchie des sites fédérés**.

Définir les propriétés du site

Vous pouvez voir et, le cas échéant, modifier les propriétés de votre site d'accueil et de ses enfants.

1. Dans le client d'administration, dans le panneau **Hiérarchie des sites fédérés**, sélectionnez le site concerné, double cliquez, et sélectionnez **Propriétés.**



2. Le cas échéant, modifiez ce qui suit :

   Onglet **Général** (á la page 295)

   Onglet **Site Parent** (á la page 296) **(accessible sur les sites enfants seulement)**

Pour des questions de synchronisation, toute modification apportée à un enfant distant peut mettre du temps à se voir reflété dans le panneau **Navigation du Site**.

Mettre à jour les renseignements sur le site

Cette section n'est pertinente que si vous utilisez XProtect Advanced VMS 2014 ou une version plus récente.

Vous pouvez lire les informations relatives au site lorsque vous arrêtez votre souris sur le nom du site dans le volet **Hiérarchie des sites fédérés**. Pour mettre à jour les informations relatives au site :

1. Connectez-vous au site.
2. Cliquez sur le volet **Navigation sur le site** et sélectionnez **Informations sur le site**.
3. Cliquez sur **Modifier** et ajoutez les informations pertinentes dans chaque catégorie.

Actualiser la hiérarchie des sites

À intervalles réguliers, le système procède automatiquement à une synchronisation de la hiérarchie et inspecte tous les niveaux de votre configuration parent/enfant. Vous pouvez la rafraîchir manuellement si vous souhaitez voir les changements apparaître instantanément dans la hiérarchie, et ne voulez pas attendre la prochaine synchronisation automatique.

Vous devez être connecté à un site pour procéder à un rafraîchissement manuel. Seules les modifications sauvegardées par ce site depuis la dernière synchronisation sont affichées lors d'un rafraîchissement. Autrement dit, les modifications apportées plus bas dans la hiérarchie ne seront pas forcément reflétés par le rafraîchissement manuel, si les modifications n'ont pas encore atteint le site.

1. Connectez-vous au site pertinent.
2. Cliquez avec le bouton droit sur le site d'accueil supérieur dans le volet Hiérarchie des sites fédérés et cliquez sur **Rafraîchir la hiérarchie des sites.**

   Ceci prendra quelques secondes.

Connexion à d'autres sites de la hiérarchie

Vous pouvez vous connecter à d'autres sites et les gérer. Le site auquel vous êtes connecté est votre site d'origine.

1. Dans le volet **Hiérarchie des sites fédérés**, cliquez avec le bouton droit sur le site auquel vous souhaitez vous connecter.
2. Cliquez sur **Se connecter au site**.

   Le Management Client de ce site s'ouvre.
3. Saisissez les informations de connexion et cliquez sur **OK**.
4. Une fois la connexion effectuée, vous êtes prêt à procéder à vos tâches administratives sur ce site.

Détacher un site de la hiérarchie

Lorsque vous détachez un site de son site parent, le lien entre les sites est aboli. Vous pouvez détacher des sites à partir du site central, du site en lui-même ou de son site parent.

1. Dans le volet **Hiérarchie des sites fédérés**, cliquez avec le bouton droit sur le site et cliquez **Détacher le site de la hiérarchie**.
2. Cliquez sur **Oui** pour mettre à jour le volet **Hiérarchie des sites fédérés**.

   Si le site détaché a des sites enfants, il devient le nouveau site supérieur pour cette branche de la hiérarchie et l'icône de site normal  se transforme en une icône de site supérieur  .
3. Cliquez sur **OK**.

Les modifications apportées à la hiérarchie sont reflétées après une actualisation manuelle ou une synchronisation automatique.

Propriétés des sites fédérés

Onglet Général

Vous pouvez modifier certaines informations liées au site auquel vous êtes actuellement connecté.

Nom	Description
Nom	Saisissez le nom du site.
Description	Saisissez une description du site.

Nom	Description
URL	Utilisez la liste pour ajouter et supprimer des URL pour ce site et indiquez si elles sont externes ou non. Les adresses externes peuvent être contactées en dehors du réseau local.
Version	Le numéro de version du serveur de gestion du site.
Compte service	Le compte service sous lequel fonctionne le serveur de gestion.
Temps de la dernière synchronisation	Date et heure de la dernière synchronisation de la hiérarchie.
État de la dernière synchronisation	L'état de la dernière synchronisation de la hiérarchie. Cela peut être soit **Réussi**, soit **Échoué**.

Onglet Site parent

Cet onglet présente des informations non modifiables concernant le site parent du site auquel vous êtes actuellement connecté. L'onglet n'est pas visible si votre site n'a aucun site parent.

Nom	Description
Nom	Affiche le nom du site parent.
Description	Affiche une description du site parent (facultatif).
URL	Répertorie les URL pour le site parent et indique si elles sont externes ou non. Les adresses externes peuvent être contactées en dehors du réseau local.
Version	Le numéro de version du serveur de gestion du site.
Compte service	Le compte service sous lequel fonctionne le serveur de gestion.
Temps de la dernière synchronisation	Date et heure de la dernière synchronisation de la hiérarchie.
État de la dernière synchronisation	L'état de la dernière synchronisation de la hiérarchie. Cela peut être soit **Réussi**, soit **Échoué**.

Milestone Interconnect

À propos de la sélection de Milestone Interconnect ou Milestone Federated Architecture

Dans un système Advanced VMS à distribution physique où les utilisateurs d'un site central doivent pouvoir accéder à la vidéo directement sur le site distant, vous pouvez choisir entre Milestone Interconnect™ et Milestone Federated Architecture™.

Milestone recommande Milestone Federated Architecture lorsque :

- La connexion réseau entre les sites centralisés et fédérés est stable

- Le réseau utilise le même domaine.
- Il y a peu de sites, mais ils sont grands.
- La bande passante est suffisante pour l'usage requis.

Milestone recommande Milestone Interconnect lorsque :

- La connexion réseau entre les sites centraux et distants est instable.
- Vous ou votre organisation souhaitez utiliser un autre produit XProtect sur les sites distants.
- Le réseau utilise différents domaines ou groupes de travail.
- Il y a beaucoup de sites de petite envergure.

Milestone Interconnect et les licences

Pour exécuter Milestone Interconnect, vous avez besoin de licences de caméra Milestone Interconnect sur votre site central pour voir les vidéos des périphériques sur les sites distants. N'oubliez pas que seul XProtect Corporate peut servir de site central.

L'état de vos licences de caméra Milestone Interconnect s'affiche sur la page **Renseignements sur la licence** sur le site central.

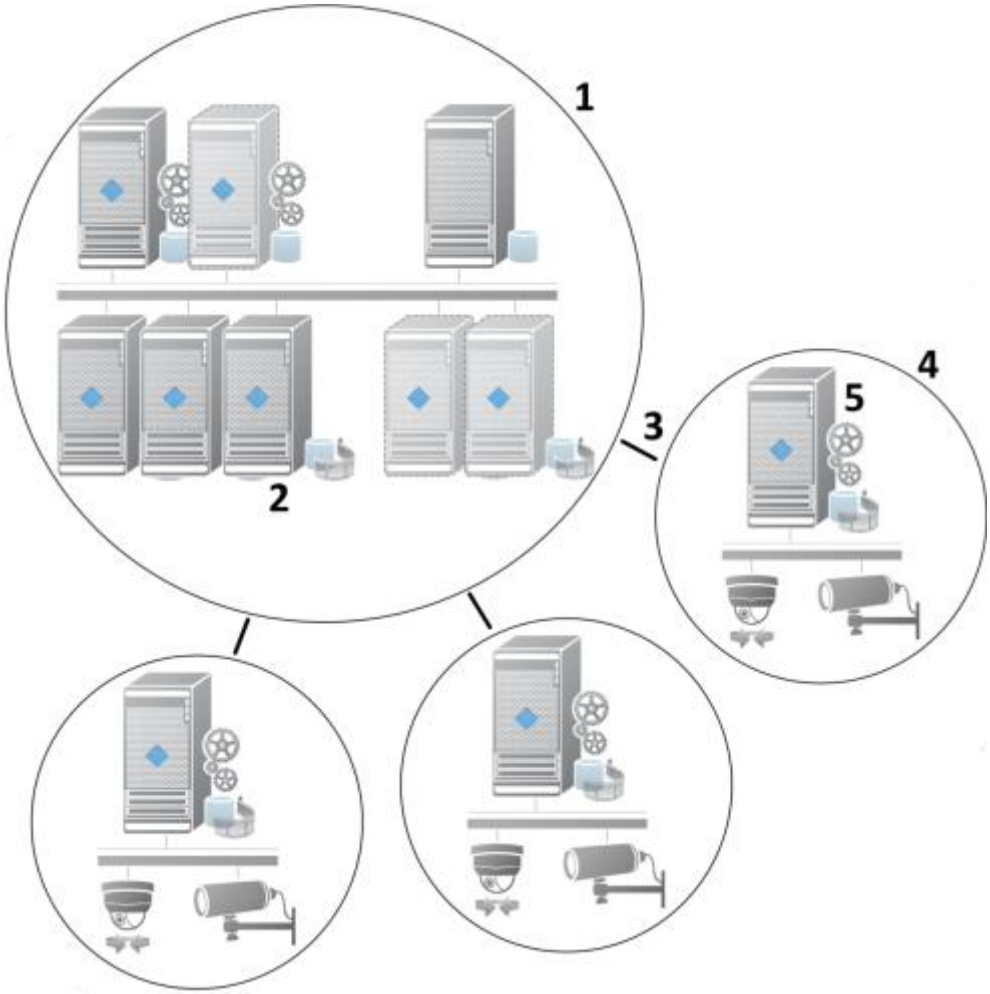
À propos de Milestone Interconnect

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

Milestone Interconnect™ vous permet d'intégrer un nombre d'installations XProtect ou Milestone Husky™ NVR plus petites, géographiquement fragmentées et distantes avec un seul site central XProtect Corporate. Vous pouvez installer ces sites plus petits, appelés sites distants, sur des unités mobiles, par exemple des bateaux, des bus ou des trains. Cela signifie que ces sites n'ont pas besoin d'être connectés en permanence à un réseau.

Depuis XProtect 2016 R3, il n’est plus possible d’ajouter les systèmes XProtect Essential en tant que sites distants.

L'illustration suivante vous montre comment configurer Milestone Interconnect sur votre système :



1. Site Milestone Interconnect XProtect Corporate central
2. Les pilotes Milestone Interconnect (établissant la connexion entre les serveurs d'enregistrement des sites centraux et le site distant et devant être sélectionnés dans la liste de pilotes lorsque l'on ajoute des systèmes distants par le biais de l'assistant **Ajouter un matériel**).
3. Connexion Milestone Interconnect
4. Site distant Milestone Interconnect (le site distant complet avec installation du système, utilisateurs, caméras, etc.)
5. Système à distance Milestone Interconnect (l'installation technique sur le site distant)

Ajoutez des sites distants au site central à l'aide de l'assistant **Ajouter du matériel** sur le site central (voir "Ajouter un site distant à votre site Milestone Interconnect central" á la page 300).

Chaque site distant fonctionne indépendamment et peut effectuer n'importe quelle tâche de surveillance normale. Selon les connexions réseau et les droits d'utilisateur (voir "Attribuer des droits d'utilisateur" á la page 301) appropriés, Milestone Interconnect offre une fonction de lecture en direct à partir des caméras des sites distants et de lecture des enregistrements des sites distants sur le site central.

Le site central ne peut seulement voir et accéder aux périphériques auxquels le compte d'utilisateur spécifié a accès (lors de l'ajout du site distant). Ceci permet aux administrateurs de systèmes locaux de contrôler les périphériques devant être mis à la disposition du site central et de ses utilisateurs.

Sur le site central, vous pouvez afficher l'état du système pour les caméras interconnectées, mais pas directement l'état du site distant. Pour contrôler le site distant, vous pouvez utiliser les événements du site distant pour déclencher des alarmes ou d'autres notifications sur le site central (voir "Configurer votre site central pour répondre aux événements des sites distants" á la page 303).

Il vous permet également de transférer les enregistrements des sites distants vers le site central en fonction d'événements, de règles/calendriers, ou de demandes manuelles des utilisateurs XProtect Smart Client.

Seuls les systèmes XProtect Corporate peuvent fonctionner en tant que sites centraux. Tous les autres produits peuvent servir de sites distants, y compris XProtect Corporate. La prise en charge diffère d'une configuration à une autre, de la version considérée, du nombre de caméras et de la façon dont les périphériques et les événements provenant du site distant sont traités (le cas échéant) par le site central. Pour de plus amples détails sur la façon dont des produits XProtect spécifiques communiquent dans une configuration Milestone Interconnect, rendez-vous sur le site web http://www.milestonesys.com/our-products/milestone-interconnect/ Milestone Interconnect.

À propos des configurations Milestone Interconnect

Il existe trois façons d'exécuter Milestone Interconnect. La façon dont vous exécutez votre configuration dépend de votre connexion au réseau, de la manière dont vous revoyez les enregistrements et du fait que vous rappeliez ou non des enregistrements à distance et de l'ampleur de ces activités.

La section suivante décrit les trois configurations les plus probables.

Lecture directe à partir des sites distants (bonne connexion réseau) :

La configuration la plus simple. Le site central est toujours en ligne et connecté à ses sites distants et les utilisateurs du site central lisent les enregistrements à distance directement à partir des sites distants. Pour ce faire, ils doivent utiliser l'option de **lecture des enregistrements à partir d'un système à distance** (voir "**Activer la lecture directe à partir de la caméra du site distant**" á la page 302).

Rappel des séquences d'enregistrement à distance sélectionnées basé sur des règles ou sur XProtect Smart Client à partir des sites distants (connexions au réseau limitées périodiquement) :

Utilisé lorsque des séquences d'enregistrement sélectionnées (provenant de sites distants) doivent être stockées au niveau central pour garantir leur indépendance vis-à-vis des sites distants. Cette indépendance est cruciale en cas de panne de réseau ou de restrictions affectant le réseau. Vous pouvez configurer les paramètres de rappel d'enregistrements à distance sur l'onglet **Rappel à distance** (voir "**Onglet Rappel à distance**" á la page 114).

Le rappel des enregistrements à distance peut être déclenché à partir du XProtect Smart Client en cas de besoin. Il est également possible de configurer une règle. Dans certains scénarios, les sites distants sont en ligne. Dans d'autres cas, ils sont hors ligne la plupart du temps. Ce paramètre dépend bien souvent du secteur d'activité. Dans certains secteurs, le site central est généralement en ligne et connecté à ses sites distants en permanence (par exemple, un QG commercial (site central) et plusieurs magasins (sites distants)). Dans d'autres secteurs, tels que les transports, les sites distants sont mobiles (il peut s'agir, par exemple, de bus, de trains, de bateaux, etc.) et ne peuvent établir une connexion au réseau que de façon aléatoire. En cas d'échec de connexion au réseau au cours d'un rappel d'enregistrements à distance déjà entamé, la tâche se poursuit lorsque l'occasion se présente à nouveau.

Si le système détecte un rappel automatique ou une demande de rappel à partir du XProtect Smart Client en dehors de l'intervalle de temps que vous avez spécifié dans l'onglet **Rappel à distance**, il

est accepté, mais n'est pas commencé avant d'avoir atteint l'intervalle de temps sélectionné. Les nouvelles demandes de rappel d'enregistrements à distance seront mises en attente et ne débuteront que lorsque l'intervalle de temps autorisé aura pris fin. Vous pouvez visualiser les tâches de rappel d'enregistrement à distance en instance à partir du **Tableau de bord système** -> **Tâches actuelles**.

Après un échec de connexion, les enregistrements à distance manquants sont rappelés par défaut à partir des sites distants

Utilise des sites distants comme un serveur d'enregistrement utilise le stockage externe sur une caméra. Généralement, les sites distants sont en ligne et connectés à leur site central, et lui diffusent un flux en direct que le site central enregistre. En cas de défaillance du réseau pour quelque raison que ce soit, le site central ne peut pas accéder à certaines séquences d'enregistrement. Cependant, une fois que le réseau est rétabli, le site central rappelle automatiquement les enregistrements à distance couvrant la période d'arrêt de la connexion. Ceci nécessite l'utilisation de l'option **Rappeler les enregistrements à distance automatiquement lorsque la connexion est rétablie** (voir "**Rappeler les enregistrements à distance de la caméra du site distant**" á la page 302) sur l'onglet **Enregistrement** de la caméra.

Vous pouvez recourir à un mélange des solutions ci-dessus afin de répondre aux besoins spécifiques à votre organisation.

Ajouter un site distant à votre site Milestone Interconnect central

Ajoutez des sites distants au site central à l'aide de l'assistant **Ajouter du matériel.**

Conditions préalables :

- Nombre suffisant de licences (voir "Milestone Interconnect et les licences" á la page 297) de caméra Milestone Interconnect.
- Un autre système configuré et fonctionnel compatible XProtect, Milestone Husky NVR ou Milestone Arcus comprenant un compte d'utilisateur (utilisateur basique, utilisateur Windows local ou utilisateur Windows Active Directory) doté de droits pour les périphériques auquel le système central XProtect Corporate peut accéder.
- Connexion réseau entre le site central XProtect Corporate et le site distant avec un accès ou un port redirigeant vers les ports utilisés sur les sites distants.

Pour ajouter un site distant :

1. Sur le site central, agrandissez **Serveurs** et sélectionnez **Serveurs d'enregistrement**.
2. Dans le volet de vue d'ensemble, agrandissez le serveur d'enregistrement en question et faites un clic droit.
3. Sélectionnez **Ajouter su matériel** pour lancer l'assistant d'installation.
4. Sur la première page, sélectionnez **Analyse des plages d'adresses** ou **Manuel** et cliquez sur **Suivant**.
5. Précisez les noms d'utilisateur et mots de passe. Le compte d'utilisateur doit être prédéfini sur le système à distance. Vous pouvez ajouter autant de noms d'utilisateurs et de mots de passe que nécessaire en appuyant sur le bouton **Ajouter**. Lorsque vous avez fini, cliquez sur **Suivant**.
6. Sélectionnez les pilotes à utiliser lors de votre analyse. Dans ce cas, choisissez l'un des pilotes Milestone. Cliquez sur **Suivant**.

7. Précisez l'adresse IP et les numéros de port que vous souhaitez analyser. Le port par défaut est 80. Cliquez sur **Suivant**.

   Attendez que votre système détecte les sites distants. L'indicateur d'état présente le processus de détection. Si un site est détecté, un message de **Réussite** apparaît dans la colonne **État**. Si vous n'arrivez pas à ajouter un système, vous pouvez cliquer sur le message d'erreur **Échec** pour découvrir pourquoi la détection a échoué.

8. Choisissez d'activer ou de désactiver les systèmes correctement détectés. Cliquez sur **Suivant**.

9. Attendez que votre système détecte un matériel et recueille les informations spécifiques au périphérique. Cliquez sur **Suivant**.

10. Choisissez d'activer ou de désactiver les périphériques et matériel correctement détectés. Cliquez sur **Suivant**.

11. Sélectionner un groupe par défaut. Cliquez sur **Terminer**.

12. Une fois l'installation terminée, vous pouvez voir le système et ses périphériques dans le volet **Vue d'ensemble**.

    Selon les droits d'utilisateur de l'utilisateur sélectionné sur le site distant, le site central a accès à toutes les caméras et fonctions ou à une partie de celles-ci.

Attribuer des droits d'utilisateur

On configure les droits d'utilisateur pour une caméra interconnectée de la même manière que pour d'autres caméras, en créant un rôle et en attribuant un accès à des fonctions.

1. Dans le volet **Navigation du Site** du site central, développez l'onglet **Sécurité** et sélectionnez **Rôles**.

2. Dans le volet Vue d'ensemble, cliquez sur le rôle administrateur intégré avec le bouton droit de votre souris et sélectionnez **Ajouter un rôle** (voir "**Ajouter et gérer un rôle**" á la page 217).

3. Donnez un nom au rôle et configurez les paramétrages sur l'onglet **Périphérique** (voir "**Onglet Périphériques (rôles)**" á la page 237) et **Enregistrement à distance** (voir "**Onglet Enregistrements à distance (rôles)**" á la page 244).

Mise à jour du matériel du site distant

Si la configuration a été modifiée sur un site distant, par exemple si des caméras ou événements ont été ajoutés, il vous faudra mettre à jour la configuration du site central pour qu'elle corresponde à celle du site distant.

1. Sur le site central, agrandissez **Serveurs** et sélectionnez **Serveurs d'enregistrement**.

2. Dans le volet Vue d'ensemble, agrandissez le serveur d'enregistrement requis et sélectionnez le système à distance concerné. Cliquez dessus à l'aide du bouton droit de votre souris.

3. Sélectionnez **Mettre le matériel à jour**. Cela ouvre la boîte de dialogue **Mise à niveau du matériel**.

4. La boîte de dialogue présente tous les changements (périphériques supprimés, mis à jour et ajoutés) dans le système à distance depuis la création ou le dernier rafraîchissement de

votre configuration Milestone Interconnect. Cliquez sur **Confirmer** pour mettre votre site central à jour avec ces changements.

Établir une connexion à distance entre le bureau et un système à distance

Préalable : Les connexions distantes du bureau à l'ordinateur que vous souhaitez faire fonctionner à distance doivent être installées et activées.

Cette fonction n'est pas prise en charge par le matériel fonctionnant avec Milestone Arcus.

1. Sur le site central, agrandissez **Serveurs** et sélectionnez **Serveurs d'enregistrement**.
2. Dans le volet Vue d'ensemble, agrandissez le serveur d'enregistrement requis et sélectionnez le système à distance concerné.
3. Dans le volet Propriétés, sélectionnez l'onglet **Info**.
4. Dans la zone **Administration à distance**, saisissez le nom d'utilisateur Windows et le mot de passe appropriés.
5. Une fois que vous avez sauvegardé le nom d'utilisateur et le mot de passe, cliquez sur **Connexion** pour établir une connexion à distance sur le bureau.
6. Dans la boîte à outils, cliquez sur **Enregistrer**.

Activer la lecture directe à partir de la caméra du site distant

Si votre site central est toujours en ligne et connecté à ses sites distants, vous pouvez configurer votre système pour que les utilisateurs effectuent la lecture des enregistrements directement sur les sites distants. Voir également <À propos des configurations Milestone Interconnect possibles (voir "À propos des configurations Milestone Interconnect" á la page 299).

1. Sur le site central, agrandissez **Serveurs** et sélectionnez **Serveurs d'enregistrement**.
2. Dans le volet Vue d'ensemble, agrandissez le serveur d'enregistrement requis et sélectionnez le système à distance concerné. Sélectionnez la caméra interconnectée pertinente.
3. Dans le volet Propriétés, sélectionnez l'onglet **Enregistrer**, puis sélectionnez l'option **Lire les enregistrements à partir du système à distance**.
4. Dans la boîte à outils, cliquez sur **Enregistrer**.

Dans une configuration Milestone Interconnect, le site central ignore le masquage de confidentialité défini dans un site distant. Si vous souhaitez utiliser le même masquage de confidentialité, vous devez le redéfinir sur le site central.

Rappeler les enregistrements à distance de la caméra du site distant

Si votre site central **n'est pas** connecté en permanence à ses sites distants, vous pouvez configurer votre système pour sauvegarder les enregistrements de manière centralisée et vous pouvez configurer le rappel des enregistrements à distance lorsque la connexion du réseau est

optimale. Voir également À propos des configurations Milestone Interconnect possibles (voir "À propos des configurations Milestone Interconnect" á la page 299).

Pour permettre aux utilisateurs de récupérer des enregistrements, vous devez activer l'autorisation pour le rôle pertinent (voir "Onglet Enregistrements à distance (rôles)" á la page 244).

Pour configurer votre système :

1. Sur le site central, agrandissez **Serveurs** et sélectionnez **Serveurs d'enregistrement**.
2. Dans le volet Vue d'ensemble, agrandissez le serveur d'enregistrement requis et sélectionnez le système à distance concerné. Sélectionnez serveur à distance pertinent.
3. Dans le volet des Propriétés, sélectionnez l'onglet **Récupération à distance** et mettez à jour les paramètres (voir "Onglet Rappel à distance" á la page 114).

En cas de défaillance du réseau pour quelque raison que ce soit, le site central ne peut pas accéder à certaines séquences d'enregistrement. Vous pouvez configurer votre système pour que le site central récupère automatiquement les enregistrements à distance pour couvrir la période d'arrêt une fois que le réseau est rétabli.

1. Sur le site central, agrandissez **Serveurs** et sélectionnez **Serveurs d'enregistrement**.
2. Dans le volet Vue d'ensemble, agrandissez le serveur d'enregistrement requis et sélectionnez le système à distance concerné. Sélectionnez la caméra pertinente.
3. Dans le volet Propriétés, sélectionnez l'onglet **Enregistrer**, puis sélectionnez l'option **Rappeler automatiquement les enregistrements à distance lorsque la connexion est rétablie** (voir "**À propos de l'enregistrement à distance**" á la page 137).
4. Dans la boîte à outils, cliquez sur **Enregistrer**.

Autrement, vous pouvez utiliser des règles ou commencer à rappeler des enregistrements à distance à partir du XProtect Smart Client en fonction de vos besoins.

Dans une configuration Milestone Interconnect, le site central ignore le masquage de confidentialité défini dans un site distant. Si vous souhaitez utiliser le même masquage de confidentialité, vous devez le redéfinir sur le site central.

Configurer votre site central pour répondre aux événements des sites distants

Vous pouvez utiliser les événements définis sur les sites distants pour déclencher des règles et des alarmes sur votre site central et ainsi répondre immédiatement aux événements des sites distants. Les sites distants doivent être connectés et en ligne. Le nombre et type d'événements dépendent des événements configurés et prédéfinis dans les sites distants.

La liste des événements pris en charge est disponible sur le site web http://www.milestonesys.com/our-products/milestone-interconnect/milestone-interconnect-compatibility Milestone.

Vous ne pouvez pas supprimer les événements prédéfinis.

Conditions préalables :

- Si vous voulez utiliser des événements manuels ou définis par l'utilisateur sur les sites distants en tant qu'événements à déclenchement, vous devez d'abord les créer sur les sites distants.

- Assurez-vous d'avoir une liste à jour des événements des sites distants (voir "Mise à jour du matériel du site distant" á la page 301).

Ajouter un événement manuel ou défini par l'utilisateur sur le site distant

1. Sur le site central, agrandissez **Serveurs** et sélectionnez **Serveurs d'enregistrement**.
2. Dans le volet Vue d'ensemble, sélectionnez le serveur distant en question et l'onglet **Événements**.
3. La liste contient les événements prédéfinis. Cliquez sur **Ajouter** pour inclure les événements manuels ou définis par l'utilisateur sur le site distant dans la liste.

Utiliser un événement sur un site distant pour déclencher une alarme sur le site central :

1. Sur le site central, agrandissez **Alarmes** et sélectionnez **Définitions d'alarmes**.
2. Dans le volet Vue d'ensemble, faites un clic droit sur **Définitions d'alarmes** et cliquez sur **Ajouter nouveau.**
3. Saisissez les valeurs nécessaires.
4. Dans le champ **Événement à déclenchement**, vous pouvez sélectionner les événements prédéfinis ou définis par l'utilisateur.
5. Dans le champ **Sources,** sélectionnez le serveur à distance représentant le site distant dont vous voulez les alarmes.
6. Enregistrez la configuration une fois terminé.

Utiliser un événement sur un site distant pour déclencher une action basée sur des règles sur le site central :

1. Sur le site central, développez **Règles et événements** et sélectionnez **Règles**.
2. Dans le volet Vue d'ensemble, faites un clic droit sur **Règles** et cliquez sur **Ajouter un règle.**
3. Dans l'assistant, sélectionnez **Réaliser une action lors de l'événement <event>.**
4. Dans la zone **Modifier la description de la règle**, cliquez sur **événement** et sélectionnez les événements prédéfinis ou définis par l'utilisateur. Cliquez sur **OK**.
5. Cliquez sur p**ériphériques/serveur d'enregistrement/serveur de gestion** et sélectionnez le serveur à distance représentant le site distant sur lequel vous voulez que le site central réalise une action. Cliquez sur **OK**.
6. Cliquez sur **Suivant** pour passer à la page suivante de l'assistant.
7. Sélectionnez les conditions que vous voulez appliquer pour cette règle. Si vous ne sélectionnez aucune condition, la règle s'applique toujours. Cliquez sur **Suivant**.
8. Sélectionnez une action et précisez les détails dans la zone **Modifier la description de la règle.** Cliquez sur **Suivant**.
9. Sélectionnez un critère d'arrêt si nécessaire. Cliquez sur **Suivant**.

10. Sélectionnez une action d'arrêt si nécessaire. Cliquez sur **Terminer**.

XProtect Smart Wall

À propos de XProtect Smart Wall

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits (voir "Graphique de comparaison des produits" á la page 23) pour de plus amples informations.

XProtect Smart Wall est un produit de mur vidéo de pointe qui fournit une excellente perception de la situation dans les grands centres de surveillance et aide les opérateurs de surveillance à se concentrer sur ce qui est important en assurant une plus grande efficacité et des délais de réponse plus courts.

XProtect Smart Wall permet un changement rapide de la vidéo en direct affichée sur le mur vidéo pour répondre à des scénarios et à des besoins de sécurité spécifiques. Une façon de changer ce qui est affiché sur le mur vidéo est d'utiliser les préréglages de Smart Wall. L'administrateur de surveillance définit les préréglages Smart Wall dans le Management Client pour l'optimisation de la couverture de surveillance pour différents scénarios de surveillance récurrents. Les préréglages Smart Wall s'appliquent pour l'intégralité du mur vidéo ou des parties du mur vidéo et déterminent quelles caméras sont affichées et la disposition du contenu sur les écrans du mur vidéo.

Avec les préréglages Smart Wall, les changements d'affichage peuvent être déclenchés automatiquement par des règles. Les changements d'affichage peuvent également être déclenchés manuellement par les opérateurs de surveillance utilisant XProtect Smart Client en déposant les vues et les caméras sur la représentation logique du mur vidéo dans XProtect Smart Client ou en sélectionnant les différents préréglages de Smart Wall définis par l'administrateur de surveillance.

Consultez la documentation XProtect Smart Client pour plus d'informations sur la façon d'utiliser les fonctions XProtect Smart Wall dans XProtect Smart Client.

Licences XProtect Smart Wall

XProtect Smart Wall nécessite les licences de mur vidéo suivantes :

- Une **licence de base** pour XProtect Smart Wall qui couvre un nombre infini de moniteurs affichant des vidéos sur un mur vidéo.

Une licence de base pour XProtect Smart Wall est comprise dans la licence de base pour XProtect Corporate. Si vous avez XProtect Expert vous pouvez acheter séparément une licence de base pour XProtect Smart Wall.

Configurer les Smart Wall

Une configuration de Smart Wall consiste à définir le Smart Wall, en ajoutant des moniteurs et en définissant la disposition de l'écran et le cas échéant des préréglages Smart Wall et en spécifiant la disposition et le contenu des différents moniteurs.

Vous n'avez pas besoin de définir des préréglages Smart Wall, si vous voulez uniquement afficher les caméras et les points de vue XProtect Smart Client que vos utilisateurs XProtect Smart Client peuvent manuellement activer sur le mur vidéo.

Si vous souhaitez utiliser des règles pour changer automatiquement ce qui est affiché sur le mur vidéo et/ou si vous avez généralement des scénarios de surveillance pour lesquels vous souhaitez afficher le même contenu sur le mur vidéo chaque fois que le scénario se produit, vous devez définir les préréglages Smart Wall.

La configuration de Smart Wall est très flexible. Vous pouvez inclure tous les moniteurs sur le mur vidéo dans un Smart Wall ou regrouper les moniteurs et configurer un Smart Wall pour chaque groupe. Les préréglages Smart Wall peuvent changer la disposition et le contenu de tous les moniteurs dans un Smart Wall ou seulement quelques-uns des moniteurs. Les moniteurs peuvent faire partie de plusieurs préréglages Smart Wall et Smart Walls. Créez autant de préréglages Smart Wall et Smart Walls que vous avez besoin pour optimiser la couverture de vos scénarios de surveillance classiques.

a. Définir le Smart Wall

1. Développez **Client**, et sélectionnez **Smart Wall**.
2. Dans le volet **Vue d'ensemble**, faites un clic droit sur **Smart Walls** et sélectionnez **Ajouter Smart Wall**.
3. Indiquez les paramètres relatifs au Smart Wall.
4. Dans les paramètres **Propriétés générales des éléments de la vue** , définissez si vous souhaitez obtenir des informations d'état du système et les barres de titre qui apparaissent au-dessus des articles de disposition des caméras.
5. Cliquez sur **OK**.

b. Ajouter un moniteur et définissez la disposition du moniteur

1. Cliquez avec le bouton droit de la souris sur le Smart Wall et sélectionnez **Ajouter un moniteur**.
2. Configurez les dimensions du moniteur de sorte qu'il ressemble à l'un des moniteurs physiques sur le mur vidéo.
3. Utilisez les paramètres de comportement prédéfinis **Présélection vide** et **Élément prédéfinis vide** pour définir ce qui est affiché sur un moniteur avec une disposition prédéfinie vide ou des éléments prédéfinis vides dans un préréglage lorsqu'un nouveau préréglage de Smart Wall est déclenché automatiquement ou sélectionné manuellement dans XProtect < SC >. Vous pouvez utiliser les préréglages vides et les éléments prédéfinis vides pour le contenu qui n'est pas contrôlé par le préréglage de Smart Wall.
4. Utilisez le paramètre **Insertion d'éléments** pour définir ce qui doit se passer quand un utilisateur XProtect Smart Client déplace une caméra sur un élément de disposition dans le préréglage Smart Wall. Sélectionnez **Indépendant** pour remplacer la caméra déjà placée dans l'élément prédéfini avec la nouvelle caméra ou **Lié** pour pousser le contenu des articles de disposition de gauche à droite depuis l'endroit où vous avez inséré la nouvelle caméra.

5. Ajoutez autant de moniteurs que vous pouvez sur le mur vidéo physique.
6. Sélectionnez le Smart Wall et sur l'onglet **disposition** cliquez sur **Modifier** pour positionner les différents moniteurs de sorte que leur position ressemble au montage des écrans physiques sur le mur vidéo.
7. Cliquez sur **OK**. La même disposition est utilisée dans XProtect Smart Client.

c. Ajouter des préréglages Smart Wall (éventuellement)

1. Sélectionnez le Smart Wall et de l'onglet **Préréglages** cliquez sur **Ajouter**.
2. Saisissez un nom et une description, puis cliquez sur **OK.**
3. Cliquez sur **Activer** pour afficher le préréglage Smart Wall sur le mur vidéo.
4. Créez autant de préréglages Smart Wall que vous avez besoin.

d. Ajouter une présentation et des caméras aux moniteurs (nécessite une présélection de Smart Wall)

1. Sélectionnez un des moniteurs que vous avez créé et à partir de l'onglet **Préréglages** , sélectionnez un préréglage dans la liste pour configurer ce que vous souhaitez que le moniteur sélectionné affiche lorsqu'il est utilisé avec le préréglage Smart Wall sélectionné.
2. Cliquez sur **Modifier**.
3. Cliquez sur le bouton de disposition pour sélectionner la disposition à utiliser avec votre moniteur, puis cliquez sur **OK**.

4. Faites glisser les caméras à partir des onglets **Groupes de périphériques**, **Serveurs d'enregistrement** ou **Hiérarchie des sites fédérés** sur les différents éléments de disposition. Les caméras sur l'onglet **Hiérarchie des sites fédérés** sont accessibles dans une configuration Milestone Federated Architecture. Vous pouvez laisser les éléments de disposition vierges pour qu'ils soient disponibles pour d'autres contenus non contrôlés par le préréglage Smart Wall.
5. Si le moniteur a déjà une disposition pour le préréglage sélectionné, vous pouvez cliquer sur **Effacer** pour définir une nouvelle disposition ou exclure le moniteur de la présélection Smart Wall, de sorte que le moniteur soit disponible pour tout autre contenu qui n'est pas contrôlé par le préréglage Smart Wall.
6. Cliquez sur **OK**.
7. Répétez les étapes, jusqu'à ce que vous ayez ajouté une disposition et des caméras sur les moniteurs que vous souhaitez inclure dans le préréglage Smart Wall.

Configurer des droits d'utilisateur pour XProtect Smart Wall

Vous pouvez contrôler les tâches que les utilisateurs de XProtect Smart Client peuvent effectuer dans XProtect Smart Wall en spécifiant des droits d'utilisateurs pour les rôles. Les droits d'utilisateurs s'appliquent à tous les utilisateurs assignés à ce rôle. Pour de plus amples informations, veuillez vous reporter à Rôles avec propriétés des droits Smart Wall (voir "Onglet Smart Wall (rôles)" á la page 245).

Les sélections relatives aux droits d'utilisateurs **Lire**, **Modifier** et **Supprimer** sont toujours appliquées. Pour les droits d'utilisateur **Opérer** et **Lecture**, vous pouvez également accorder les droits d'utilisateur pour une période spécifique en sélectionnant un profil de temps. Par exemple, cette option est utile si vous souhaitez autoriser un utilisateur à modifier le contenu affiché sur un Smart Wall, mais uniquement au cours de ses heures de travail normales.

Afin de configurer des droits d'utilisateur pour un rôle, procédez comme suit :

1. Dans le volet Navigation du site, développez **Sécurité** et sélectionnez **Rôles**.
2. Dans le volet **Rôles**, sélectionnez un rôle ou créez un nouveau rôle en effectuant un clic droit sur le volet et en sélectionnant **Ajouter le rôle**.
3. Dans la partie supérieure du volet **Paramètres des rôles**, sélectionnez le Smart Wall.
4. Dans la partie inférieure du volet Paramètres des rôles, cliquez sur l'onglet **Smart Wall** puis sélectionnez les droits d'utilisateurs à assigner.
   - **Lire** - Voir des Smart Walls dans les applications du client
   - **Modifier** - Modifier des Smart Walls dans les applications du client
   - **Supprimer** - Supprimer des Smart Walls dans les applications du client
   - **Opérer** - Appliquer des dispositions sur le moniteur sélectionné dans les applications du client et activer des préréglages
   - **Lecture** - Passer en revue et gérer des vidéos en direct et enregistrées

   Remarque : Si vous ne sélectionnez pas la permission **Lecture**, les utilisateurs peuvent voir le contenu affiché sur le mur vidéo mais ne peuvent pas le modifier. Si un utilisateur apporte une modification, le système se déconnecte automatiquement de l'état partagé et le contenu du mur vidéo n'est pas affecté. Pour revenir à la vue partagée, cliquez sur **Reconnecter le moniteur Smart Wall**.
5. Facultatif : Afin d'accorder les droits d'utilisateur **Opérer** ou **Lecture** pour une durée spécifique, cochez la case puis sélectionnez le profil de temps.

À propos de l'utilisation de règles avec des préréglages Smart Wall

En combinant les règles et les présélections Smart Wall, vous pouvez contrôler ce qui est affiché sur votre mur vidéo de la même manière que le système utilise des règles pour contrôler le comportement des caméras et autres. Par exemple, une règle peut déclencher votre mur vidéo pour afficher un certain préréglage Smart Wall pendant un certain jour. Vous pouvez même utiliser des règles pour contrôler quels sont les moniteurs individuels dans un écran du mur vidéo. Voir Ajouter une règle (á la page 195) pour plus d'informations sur la façon de créer des règles.

Exemple d'une règle déclenchant un préréglage Smart Wall.

Propriétés Smart Wall

Onglet Info (Propriétés du Smart Wall)

Dans l'onglet **Info** pour un Smart Wall, vous pouvez ajouter et modifier Smart Walls.

Nom	Description
Nom	Le nom du Smart Wall. S'affiche dans le XProtect Smart Client sous forme de nom du groupe de vues de Smart Wall.
Description	Une description du Smart Wall. Cette description est utilisée uniquement dans le cadre du Management Client.
Texte d'état	Si ce paramètre est sélectionné, les informations sur d'état de la caméra s'affichent sur les éléments de disposition des caméras sur le mur vidéo.
Pas de barre de titre	Si elle est sélectionnée, tous les éléments de disposition Smart Wall n'ont aucune barre de titre sur le mur vidéo.
Barre de titre	Si elle est sélectionnée, tous les éléments de disposition Smart Wall ont des barres de titre sur le mur vidéo.
Barre de titre avec indicateur En direct	Lorsqu'elle est sélectionnée, les barres de titre de tous les éléments de disposition Smart Wall présentent des indicateurs de mouvement et en direct sur le mur vidéo.

Onglet Positions prédéfinies (Propriétés du Smart Wall)

Dans l'onglet **Paramètres prédéfinis** pour un Smart Wall, vous pouvez ajouter et modifier les préréglages Smart Wall.

Nom	Description
Ajouter nouveau	Cliquez pour ajouter un préréglage à votre installation XProtect Smart Wall. Définissez un nom et une description pour le nouveau préréglage Smart Wall.
Modifier	Modifiez le nom et/ou la description d'un préréglage Smart Wall.
Supprimer	Supprimer un préréglage Smart Wall.
Activer	Cliquez pour afficher le préréglage Smart Wall sur le mur vidéo. Vous devez créer des règles avec le préréglage Smart Wall avant que le système ne puisse automatiquement déclencher l'affichage du préréglage Smart Wall. Voir aussi À propos de l'utilisation des règles avec des préréglages Smart Wall (voir "À propos de l'utilisation de règles avec des préréglages Smart Wall" á la page *308*).

Onglet Disposition (Propriétés du Smart Wall)

Sous l'onglet **disposition** pour un Smart Wall, vous placez les moniteurs dans votre Smart Wall si leurs positions ressemblent au montage des écrans physiques sur le mur vidéo. La disposition est également utilisée dans le XProtect Smart Client.

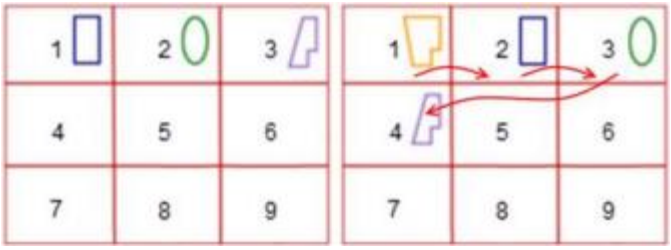
Nom	Description
Modifier	Cliquez pour ajuster le positionnement des moniteurs.
Déplacement	Pour déplacer un moniteur vers une nouvelle position, sélectionnez le moniteur pertinent, puis faites-le glisser à la position désirée, ou cliquez sur les boutons flèches pour déplacer le moniteur dans la direction sélectionnée.
Boutons de zoom	Cliquez sur les boutons de zoom avant/arrière de l'aperçu de disposition Smart Wall pour vous assurer de positionner les moniteurs correctement.
Nom	Le nom du moniteur. Le nom s'affiche dans XProtect Smart Client.
Taille	La taille de l'écran physique sur le mur vidéo.
Proportions	Le rapport hauteur/largeur de l'écran physique sur le mur vidéo.

Propriétés du moniteur

Onglet Info (propriétés du moniteur)

Dans l'onglet **Infos** pour un moniteur dans un préréglage Smart Wall, vous pouvez ajouter des moniteurs et modifier les paramètres des moniteurs.

Nom	Description
Nom	Le nom du moniteur. Le nom s'affiche dans XProtect Smart Client.
Description	Une description de chaque moniteur. Cette description est utilisée uniquement dans le cadre du Management Client.
Taille	La taille de l'écran physique sur le mur vidéo.
Proportions	Le rapport hauteur/largeur de l'écran physique sur le mur vidéo.
Préréglage vide	Définit ce qui doit être affiché sur un moniteur avec une disposition prédéfinie vide quand un nouveau préréglage Smart Wall est déclenché ou sélectionné dans XProtect Smart Client. Sélectionnez **Conserver** pour garder le contenu actuel de l'écran. Sélectionnez **Effacer** pour effacer tout le contenu si rien ne s'affiche sur le moniteur.

Nom	Description
Élément de préréglage vide	Définit ce qui doit être affiché dans une disposition prédéfinie vide quand un nouveau préréglage Smart Wall est déclenché ou sélectionné dans XProtect Smart Client. Sélectionnez **Conserver** pour garder le contenu actuel dans l'élément de disposition. Sélectionnez **Effacer** pour effacer le contenu afin que rien ne s'affiche dans l'élément de disposition.
Insertion d'éléments	Définit la façon dont les caméras sont insérées dans la disposition du moniteur lorsqu'il est affiché dans XProtect Smart Client. En sélectionnant **Indépendant**, seul le contenu de la disposition des éléments concernés change, le reste du contenu de la disposition reste le même. En sélectionnant **Lié**, les contenus des éléments de disposition sont poussés de gauche à droite. Si, par exemple, une caméra est insérée en position 1, la caméra précédente de la position 1 est poussée à la position 2, la caméra précédente de la position 2 est poussée à la position 3, et ainsi de suite comme illustré dans cet exemple.  Avant l'insertion d'une nouvelle caméra et après.

Onglet Positions prédéfinies (propriétés du moniteur)

Dans l'onglet **Paramètres prédéfinis** pour un moniteur dans un préréglage Smart Wall, vous pouvez modifier la disposition et le contenu de l'écran dans le préréglage Smart Wall sélectionné.

Nom	Description
Préposition	Une liste de préréglages Smart Wall pour la Smart Wall sélection.

Nom	Description
Modifier	Cliquez sur **Modifier** pour modifier la disposition et le contenu de l'écran sélectionné. Double-cliquez sur une caméra pour supprimer une seule caméra. Cliquez sur **Effacer** pour définir une nouvelle disposition ou exclure le moniteur dans le préréglage Smart Wall afin que le moniteur soit disponible pour tout autre contenu qui n'est pas contrôlé par le préréglage Smart Wall. Cliquez sur  pour sélectionner la disposition que vous souhaitez utiliser avec votre moniteur dans le préréglage sélectionné, et cliquez sur **OK**. Faites glisser les caméras à partir des **Groupes de périphériques**, **Serveurs d'enregistrement** ou **Sites fédérés** sur les différents éléments de disposition. Vous pouvez laisser les éléments de disposition vides, afin qu'ils soient disponibles pour d'autres contenus non contrôlés par le préréglage Smart Wall.

Module de contrôle d’accès XProtect

À propos de l'intégration du contrôle de l’accès

L'utilisation de XProtect Access nécessite l'achat d'une licence de base qui vous permet d'accéder à cette fonction au sein de votre système XProtect. Vous avez également besoin d'une licence de porte à contrôle d’accès pour chaque porte que vous souhaitez contrôler.

Vous pouvez utiliser XProtect Access avec les systèmes de contrôle d'accès des fournisseurs lorsqu'il existe un module d’extension spécifique au fournisseur pour XProtect Access.

La fonction d'intégration du contrôle d'accès contient une nouvelle fonctionnalité qui facilite l'intégration des systèmes de contrôle d'accès des clients avec XProtect. Vous obtenez ainsi :

- Une interface utilisateur commune destinée aux opérateurs pour de multiples systèmes de contrôle d'accès dans XProtect Smart Client.
- Une intégration plus rapide et plus puissante des systèmes de contrôle d'accès.
- Plus de fonctions pour l'opérateur (voir ci-dessous).

Dans XProtect Smart Client, l'opérateur obtient :

- La surveillance en direct des événements et des points d'accès.
- Un passage autorisé par un opérateur pour les demandes d'accès.
- L'intégration du plan.
- Des définitions d'alarmes pour les événements de contrôle d’accès.

- Une enquête sur les événements et les points d'accès.
- Une vue d'ensemble centralisée et un contrôle de l'état des portes.
- Des informations sur les détenteurs de carte et la gestion de ces derniers.

Le **Journal d'activité** enregistre toutes les commandes effectuées par chaque utilisateur dans le système de contrôle d'accès à partir de XProtect Smart Client.

Hormis la licence de base XProtect Access, vous devez installer un module d'extension d'intégration spécifique au fabricant sur le serveur d'événements avant de pouvoir débuter une intégration (voir "Configurer un système de contrôle d'accès intégré" á la page 313).

Licences XProtect Access

XProtect Access nécessite les licences de contrôle d'accès suivantes :

- Une **licence de base** pour XProtect Access, qui couvre un nombre illimité de serveurs Access.
- Une **licence de contrôle d'accès pour une porte** pour chaque porte que vous souhaitez intégrer et contrôler dans XProtect Access. **Deux** licences de contrôle d'accès pour une porte sont comprises dans la licence de base XProtect Access. Toutes les licences de contrôle d'accès pour une porte sont installées automatiquement lorsque vous installez votre produit XProtect Access. Cependant, les licences de porte installées sont désactivées par défaut et vous devez donc activer les portes que vous souhaitez utiliser. Vous ne pouvez activer qu'un nombre de portes identique au nombre de licences de porte que vous possédez.

Exemple : Vous possédez 5 licences de contrôle d'accès pour une porte et vous avez ajouté 10 portes. Une fois que vous avez ajouté 5 portes, vous ne pouvez plus en sélectionner d'autres. Vous devez supprimer certaines de vos portes avant de pouvoir en ajouter d'autres.

Pour obtenir plus d'informations à propos de l'état de vos licences de contrôle d'accès pour une porte, veuillez agrandir le nœud **Contrôle d'accès**.

Pour acheter des licences de base ou de porte XProtect Access supplémentaires, veuillez contacter votre fournisseur.

Configurer un système de contrôle d'accès intégré

Cette rubrique présente les étapes de la création fructueuse d'une configuration et d'un système de contrôle d'accès intégré.

Conditions préalables :

- Vous avez acheté les licences XProtect Access requises.
- Vous avez installé le module d'extension d'intégration spécifique à votre système de contrôle d'accès sur le serveur d'événements.

1. Ajouter le système de contrôle d'accès intégré à votre système XProtect Voir Assistant pour l'intégration de systèmes de contrôle d'accès (á la page 314). L'assistant vous guide à travers les étapes les plus élémentaires.
2. Spécifiez des propriétés supplémentaires pour l'intégration du système de contrôle d'accès, en particulier les événements de contrôle d'accès peuvent exiger que vous mappiez des

événements du système de contrôle d'accès avec des catégories d'événements que XProtect reconnaît. Voir Propriétés du contrôle de l’accès (á la page 315).

3. Vous devez créer un rôle avec la permission d'utiliser les fonctionnalités de contrôle d'accès dans XProtect Smart Client. Voir l'onglet Contrôle d’accès (voir "Onglet Contrôle d'accès (rôles)" á la page 247).

4. Vous devez également associer ce rôle à un profil Smart Client. Voir Propriétés du profil Smart Client (á la page 168).

5. Le système prévoit une règle par défaut qui permet aux notifications de demande d'accès d'apparaitre à l'écran XProtect Smart Client en cas de refus d'accès. Vous pouvez ajouter et modifier les notifications de demande d'accès, voir Notifications de demande d'accès (propriétés) (voir "Onglet Notification de demande d'accès (Contrôle d'accès)" á la page 318).

6. Vous pouvez créer des règles supplémentaires en fonction des actions et des événements du système de contrôle d'accès. Voir À propos des actions et de l'arrêt des actions (voir "À propos des actions et des actions d'arrêt" á la page 175) et Aperçu des événements (voir "Vue d'ensemble des événements" á la page 184).

7. Si nécessaire, modifiez les paramètres généraux de contrôle d'accès dans **Options** > **Paramètres de contrôle d’accès**. Voir Onglet Paramètres de contrôle d'accès (voir "Onglet Paramètres de contrôle d'accès (options)" á la page 275).

Assistant pour l'intégration de systèmes de contrôle d'accès

L'assistant **Intégration du système de contrôle d'accès** sert à configurer l'intégration initiale d'un système de contrôle d'accès étape par étape. Utilisez l'assistant pour effectuer les tâches de configuration les plus basiques. Vous pouvez effectuer des opérations de configuration plus détaillées par la suite.

Avant de démarrer l'assistant d'intégration du contrôle d'accès, assurez-vous de bien avoir installé le module d’extension d'intégration sur le serveur d'événements.

Certains champs à remplir et leurs valeurs par défaut proviennent du module d’extension d'intégration. L'apparence de l'assistant est donc susceptible de changer en fonction du système de contrôle d'accès auquel vous vous intégrez.

Pour démarrer l'assistant, sélectionnez **Contrôle d’accès** dans l'arborescence à nœuds, cliquez avec le bouton droit puis cliquez sur **Créer nouveau**.

Créer l'intégration du système de contrôle d'accès

Saisissez le nom et spécifiez les détails de connexion pour le système de contrôle d'accès que vous souhaitez ajouter. Les paramètres que vous devez spécifier dépendent du type de système, mais il s'agit généralement de l'adresse du réseau du serveur du système de contrôle d'accès et d'un nom d'utilisateur et mot de passe pour l'administrateur du contrôle d'accès.

Le système de gestion vidéo utiliser le nom d'utilisateur et le mot de passe spécifiés pour vous connecter au système de contrôle d'accès afin d'en récupérer la configuration complète.

Le module d’extension d'intégration peut également définir des paramètres secondaires qui n'apparaissent pas dans la liste de l'assistant, mais vous pouvez modifier ces paramètres dans **Paramètres généraux** après avoir configuré l'intégration. Les valeurs par défaut des paramètres sont fournies avec le module d’extension ou avec le système XProtect.

Connexion au système de contrôle d'accès

Une fois le module d’extension intégré avec succès, un résumé de la configuration du système de contrôle d'accès récupérée apparaît. Examinez la liste pour vous assurer que tous les éléments ont bien été intégrés avant de passer à l'étape suivante de l'assistant.

Caméras associées

Mappage des points d'accès du système de contrôle d'accès avec les caméras du système XProtect pour afficher les vidéos correspondant aux événements des portes ;

Vous pouvez associer plusieurs caméras à un seul point d'accès. L'utilisateur XProtect Smart Client est alors capable de voir les vidéos de toutes les caméras lors des enquêtes au sujet d'événements, par exemple.

L'utilisateur XProtect Smart Client est également capable d'ajouter une des caméras lorsqu'il configure les éléments de vue **Access Monitor**.

Les portes sous licence sont activées par défaut. Décochez la case pour désactiver une porte et libérer une licence de porte à contrôle d’accès.

Résumé final

Votre intégration du système de contrôle d'accès a été créée avec succès dans XProtect avec les paramètres par défaut hérités du module d'intégration. Les utilisateurs du client doivent se connecter à XProtect Smart Client pour voir et utiliser le nouveau système de contrôle d'accès.

Vous pouvez raffiner la configuration en fonction des besoins.

Propriétés du contrôle de l’accès

Onglet Paramètres Généraux (Contrôle d’accès)

Nom	Description
Activer	Les systèmes sont activés par défaut, ce qui signifie qu'ils sont visibles dans le XProtect Smart Client pour les utilisateurs bénéficiant de droits suffisants et que le système XProtect reçoit les événements de contrôle d’accès. Vous pouvez désactiver un système, par exemple au cours de la maintenance, afin d'éviter de créer des alarmes inutilement.
Nom	Le nom du système de contrôle d'accès intégré tel qu'il apparaît dans l'application d'administration ainsi que dans les clients. Vous pouvez remplacer le nom actuel par un nouveau.
Description	Présente une description de l'intégration du contrôle d'accès. Cette option est facultative.
Module d'extension d'intégration	Affiche le type de système de contrôle d'accès sélectionné au cours de l'intégration initiale.
Rafraîchissement de la dernière configuration	Affiche la date et heure du dernier moment où la configuration a été importée à partir du système de contrôle d'accès.

Nom	Description
Rafraîchir la configuration	Cliquez sur le bouton lorsque vous devez refléter les modifications de configuration effectuées sur le système de contrôle d'accès sur XProtect, par exemple lorsque vous avez ajouté ou supprimé une porte. Un résumé des modifications de la configuration effectuées dans le système de contrôle d'accès apparaît. Passez la liste en revue pour vous assurer que votre système de contrôle d'accès est reflété correctement avant d'appliquer la nouvelle configuration.
Connexion de l'opérateur nécessaire	Permet une connexion supplémentaire pour les utilisateurs du client, si le système de contrôle d'accès prend en charge les droits des utilisateurs différenciés. Cette option n'est visible que si le plug-in d'intégration prend en charge les droits des utilisateurs différenciés.

Le nom et le contenu des champs suivants sont importés à partir du module d'extension d'intégration. Vous trouverez ci-dessous des exemples de certains champs typiques :

Nom	Description
Adresse	Saisissez l'adresse du serveur hébergeant le système de contrôle d'accès intégré.
Port	Spécifiez le numéro de port sur le serveur auquel le système de contrôle d'accès est connecté.
Nom d'utilisateur	Saisissez le nom de l'utilisateur, comme défini dans le système de contrôle d'accès, qui doit être l'administrateur du système intégré dans XProtect.
Mot de passe	Spécifiez le mot de passe pour l'utilisateur.

Onglet Portes et caméras associées (Contrôle d'accès)

Cet onglet fournit un mappage entre les points d'accès des portes et les caméras, microphones ou haut-parleurs. L'association des caméras a lieu dans le cadre de l'assistant d'intégration, mais vous pouvez modifier la configuration à tout moment. Le mappage aux microphones et haut-parleurs se fait de façon implicite par le biais du microphone ou haut-parleur associé sur la caméra.

Nom	Description
Portes	Affiche la liste des points d'accès des portes disponibles définis dans le système de contrôle d'accès, groupés par porte. Pour naviguer plus facilement jusqu'aux portes pertinentes, vous pouvez filtrer les portes dans votre système de contrôle d'accès à l'aide de la liste déroulante située en haut. **Activé** : Les portes sous licence sont activées par défaut. Vous pouvez désactiver une porte pour libérer une licence. **Licence** : Indique si une porte est sous licence ou si la licence a expiré. Le champ est vide lorsque la porte est désactivée. **Supprimer** : Cliquez sur **Supprimer** pour supprimer une caméra d'un point d'accès. Si vous supprimez toutes les caméras, la case correspondant aux caméras sera automatiquement décochée.
Caméras	Affiche la liste des caméras configurées dans le système XProtect. Sélectionnez une caméra dans la liste et faites-la glisser et tomber sur le point d'accès pertinent pour associer le point d'accès à la caméra.

Onglet Événements de contrôle d’accès (Contrôle d'accès)

Les catégories d'événements vous permettent de grouper des événements. La configuration des catégories d'événements affecte le comportement du contrôle d’accès dans le système XProtect et vous permet par exemple de définir une alarme de façon à ce qu'elle déclenche une seule alarme pour de multiples types d'événements.

Nom	Description
Événement de contrôle de l’accès	Affiche la liste des événements de contrôle d’accès importés à partir du système de contrôle d'accès. Le module d’extension d'intégration contrôle l'activation et la désactivation par défaut des événements. Vous pouvez désactiver ou activer des événements à tout moment après l'intégration. Lorsqu'un événement est activé, il est stocké dans la base de données d'événements de XProtect et est disponible à des fins de filtrage sur le XProtect Smart Client.
Type de source	Indique l'unité de contrôle d'accès qui peut déclencher l'événement de contrôle d'accès.

Nom	Description
Catégorie d'événement	Assigne aucune, une ou plusieurs catégories d'événements aux événements de contrôle d'accès. Le système cartographie automatiquement les catégories d'événements pertinentes aux événements au cours de leur intégration. Cela permet d'activer une configuration par défaut dans le système XProtect. Vous pouvez modifier le mappage à tout moment. Les catégories d'événements intégrées sont : • Accès refusé • Accès accordé • Demande d'accès • Alarme • Erreur • Avertissement Les événements et catégories d'événements définis par le module d'extension d'intégration apparaissent également, mais vous pouvez aussi définir vos propres catégories d'événements, voir **Catégories définies par l'utilisateur**. **Important** : Si vous modifiez les catégories d'événements dans un système Corporate, veillez à ce que les règles de contrôle d'accès existantes fonctionnent toujours.
Catégories définies par l'utilisateur	Vous permet de créer, de modifier ou de supprimer des catégories d'événements définies par l'utilisateur. Vous pouvez créer des catégories d'événements lorsque les catégories intégrées ne répondent pas à vos exigences, par exemple, en lien avec la définition d'événements déclencheurs pour les actions de contrôle d'accès. Les catégories sont globales pour tous les systèmes d'intégration ajoutés au système XProtect. Elles permettent de configurer un système de traitement sur l'ensemble des systèmes, par exemple sur les définitions d'alarmes. Si vous supprimez une catégorie d'événement définie par l'utilisateur, un avertissement s'affiche si la catégorie en question est utilisée par toute intégration. Si vous la supprimez tout de même, toutes les configurations effectuées avec cette catégorie, par exemple les actions de contrôle d'accès, ne fonctionnent plus.

Onglet Notification de demande d'accès (Contrôle d'accès)

Vous pouvez spécifier les notifications de demande d'accès qui apparaissent sur l'écran XProtect Smart Client quand un événement donné se produit.

Nom	Description
Nom	Entrez un nom pour la notification de demande d'accès.

Nom	Description
Ajouter une notification de demande d'accès	Cliquez pour ajouter et définir des notifications de demande d'accès. Pour supprimer une notification, cliquez sur **X** sur la droite. Si un XProtect Smart Client se connecte à un site parent dans une hiérarchie Milestone Federated Architecture, les notifications de demande d'accès envoyées par les sites enfant apparaissent également dans XProtect Smart Client.
Détails de la notification de demande d'accès	Spécifiez les caméras, microphones ou haut-parleurs apparaissant dans les notifications de demande d'accès lorsqu'un événement donné se produit. Spécifier également le son qui avertira l'utilisateur de l'arrivée d'une notification.
Ajouter une commande	Sélectionner les commandes qui devraient être disponibles sous forme de boutons dans les fenêtres de dialogue de notification de demande d'accès dans XProtect Smart Client. Commandes de demande d'accès connexes : • Active toutes les commandes associées aux opérations de demande d'accès disponibles sur l'unité source. Par exemple **Ouvrir la porte**. Toutes les commandes connexes : • Active toutes les commandes sur l'unité source. Commande de contrôle de l’accès : • Activer une commande de contrôle d'accès sélectionnée. Commande du système : • Active une commande prédéfinie dans le système XProtect. Pour supprimer une commande, cliquez sur **X** sur la droite.

Onglet Titulaire d'une carte (Contrôle d’accès)

Utilisez l'onglet **Titulaires de cartes**pour consulter les informations sur les titulaires de carte dans le système de contrôle d'accès.

Nom	Description
Rechercher détenteur de carte	Saisissez les premiers caractères du nom du détenteur de carte que vous recherchez et il apparaîtra dans la liste, s'il existe.
Nom	Affiche les noms des détenteurs de cartes récupérés à partir du système de contrôle d'accès.

Nom	Description
Type	Affiche le type de détenteur de carte, par exemple : • Employé • Garde • Invité

Si votre système de contrôle d'accès prend en charge l'ajout/suppression de photos dans le système XProtect, vous pouvez ajouter des photos aux titulaires de carte. Ce qui est utile si votre système de contrôle d'accès ne comporte pas de photos des titulaires de carte.

Nom	Description
Sélectionner une image	Spécifiez le chemin d'accès à un fichier contenant une photographie du détenteur de carte. Ce bouton n'est pas visible si le système de contrôle d'accès gère les images. Les formats de fichiers autorisés sont .bmp, .png et .jpg. Les images sont redimensionnées afin de maximiser la vue. Milestone vous recommande d'utiliser une image quadratique.
Supprimer une image	Cliquez pour supprimer l'image. Si le système de contrôle d'accès avait une image, cette image est représentée après la suppression.

XProtect LPR

Aperçu du système LPR

À propos de XProtect LPR

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits pour de plus amples informations.

XProtect LPR propose une fonction d'analyse du contenu et de reconnaissance des plaques d''immatriculation de véhicules basée sur la vidéo (VCA) en interaction avec votre système de surveillance et votre XProtect Smart Client.

Pour lire les caractères d'une plaque, XProtect LPR utilise une fonction de reconnaissance optique de caractères sur des images, à l'aide de paramètres de caméra spécialisés.

Vous pouvez associer LPR (la reconnaissance de plaque) à d'autres fonctions de surveillance telles que l'enregistrement et l'activation de sorties en fonction d'événements.

Exemples d'événements dans XProtect LPR :

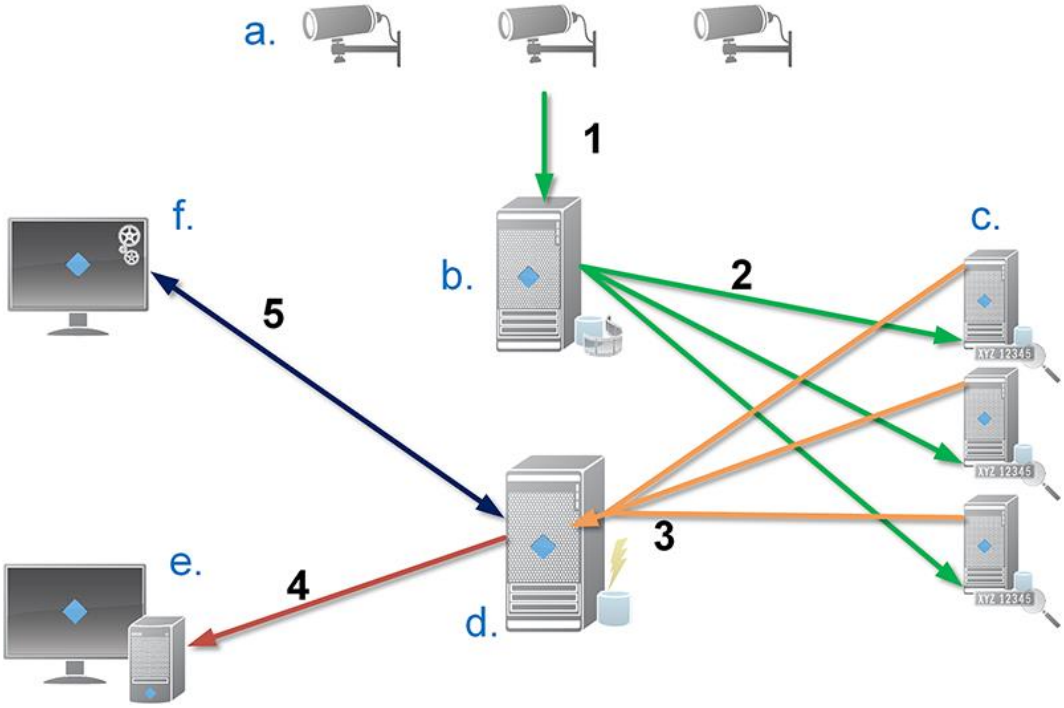
- Déclencher des enregistrements d'une qualité particulière dans le système de surveillance.
- Activer des alarmes.

- Faire la correspondance avec des éléments des listes de correspondance positive/négative des plaques d'immatriculation.
- Ouvrir des barrières.
- Allumer la lumière.
- Transmission de type push de la vidéo d'incidents sur les écrans d'ordinateurs de certains membres du personnel de sécurité.
- Envoyer des SMS sur téléphone mobile.

Avec un événement, vous pouvez activer des alarmes dans XProtect Smart Client.

Architecture du système LPR

Flux des données de base :



1. Les caméras LPR (a) envoient la vidéo au serveur d'enregistrement (b).
2. Le serveur d'enregistrement envoie la vidéo aux serveurs LPR (c) afin de reconnaître les plaques d'immatriculation en les comparant avec les caractéristiques des plaques d'immatriculation dans les modules de pays installés.
3. Les serveurs LPR envoient des reconnaissances au serveur d'événements (d) afin de les faire correspondre aux listes de correspondance des plaques d'immatriculation.
4. Le serveur d'événements envoie des événements et des alarmes à XProtect Smart Client (e) lorsqu'il trouve une correspondance.
5. L'administrateur système gère l'ensemble de la configuration LPR, comme, par exemple, la configuration d'événements, d'alarmes et de listes provenant de Management Client (f).

Serveur LPR : Le serveur LPR traite la vidéo LPR enregistrée par votre système de surveillance. Il analyse la vidéo et envoie des informations au serveur d'événements, qui les utilise pour déclencher les événements et alarmes définies. Milestone vous recommande d'installer le serveur LPR sur un ordinateur spécialement affecté à cette fin.

Caméra LPR : La caméra LPR capture la vidéo comme toute autre caméra, mais certaines caméras sont dédiées à la fonction LPR. Plus votre caméra est adaptée à cette application et plus vous obtiendrez de reconnaissances fructueuses.

Module de pays : Un module de pays est une série de règles définissant les plaques d'immatriculation d'un certain type et d'une certaine forme comme appartenant à un certain pays ou une certaine région. Il définit les éléments spécifiques aux plaques et aux caractères, tels que leur couleur, leur hauteur, leur espacement et autres caractéristiques similaires, qui sont utilisés au cours du processus de reconnaissance.

Liste de correspondance des plaques d'immatriculation : Une liste de correspondance de plaques d'immatriculation est une liste définie par l'utilisateur et créée par vos soins. Les listes de correspondance de plaques d'immatriculation sont des collections de plaques d'immatriculation que vous souhaitez voir traitées de façon spéciale par votre système. Une fois que vous avez spécifié une liste, vous pouvez configurer des événements afin de reconnaître les plaques d'immatriculation sur ces listes et, ainsi, de déclencher des événements et des alarmes.

Compatibilité

XProtect LPR 2016 est compatible avec la version 2014 SP3 ou une version ultérieure de :

- XProtect Corporate
- XProtect Expert
- Milestone Husky™ M30
- Milestone Husky™ M50.

XProtect LPR 2016 est compatible avec Milestone Husky M30 et Milestone Husky M50, mais ces produits ne prennent pas en charge toutes les fonctionnalités de XProtect LPR 2016 à présent.

Configuration système minimum

Pour obtenir de plus amples informations sur la configuration système minimale des divers éléments de votre système, allez sur le site web http://www.milestonesys.com/SystemRequirements de Milestone.

Milestone vous recommande d'installer le serveur LPR sur un ordinateur spécialement affecté à cette fin.

Licences LPR

XProtect LPR requiert les licences LPR suivantes :

- Une **licence de base** pour XProtect LPR, qui couvre un nombre illimité de serveurs LPR.
- Une **licence de périphérique LPR** par caméra LPR que vous souhaitez utiliser dans XProtect LPR.
- Une **licence de module de pays LPR** pour chaque pays, état ou région dont vous avez besoin dans votre solution XProtect LPR. **Cinq** licences LPR de module de pays sont incluses dans la licence de base XProtect LPR. Tous les modules de pays sont installés automatiquement lorsque vous installez votre produit XProtect LPR. Cependant, les modules installés sont désactivés par défaut et vous devez activer les modules (voir "Onglet Modules de pays" á la page 348) que vous souhaitez utiliser. Vous ne pouvez

activer qu'un nombre de modules de pays identique au nombre de licences de modules de pays que vous possédez.

Exemple : Vous avez cinq licences LPR de module de pays et vous avez installé 10 modules de pays. Une fois que vous avez sélectionné cinq modules de pays, vous ne pouvez plus en sélectionner d'autres. Vous devez effacer certaines de vos sélections avant de pouvoir sélectionner d'autres modules.

Pour obtenir plus d'informations au sujet de l'état actuel de vos licences, consultez Voir les informations relatives au serveur LPR (voir "Consulter les informations relatives au serveur LPR" á la page 337).

Pour acheter d'autres licences LPR ou modules de pays, veuillez contacter votre fournisseur.

À propos de la préparation des caméras pour LPR

LPR est différent de tous les autres types de vidéosurveillance. Normalement, vous choisissez des caméras en fonction de leur capacité à fournir les meilleures images possibles pour une visualisation par l'œil humain. Lorsque vous choisissez des caméras pour la fonction LPR, seule la zone dans laquelle vous vous attendez à détecter des plaques d'immatriculation est importante. Plus l'image que vous capturez dans cette petite zone est claire et cohérente, plus le taux de reconnaissance obtenu est élevé.

Cette rubrique vous aide à préparer les caméras pour la reconnaissance de plaques et vous présente également des théories importantes qu'il convient de comprendre au sujet des caméras et des objectifs afin d'obtenir des images d'une qualité optimale.

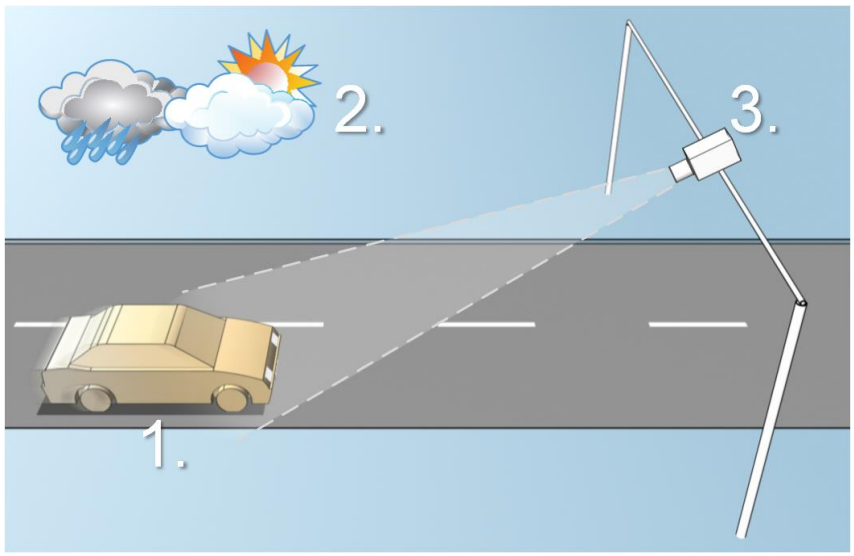


Illustration d'une solution LPR

Facteurs influençant votre configuration du LPR

1. Véhicule

- Vitesse
- Taille et position de la plaque

2. Environnement physique

- Conditions d'éclairage
- Conditions météorologiques

3. Caméra

- Exposition
- Champ de vision
- Vitesse d'Obturateur
- Résolution
- Positionnement

Il est important de prendre ces facteurs en compte car ils ont une influence prépondérante sur le succès de la reconnaissance des plaques d'immatriculation. Vous devez installer les caméras et configurer XProtect LPR d'une façon adaptée à chaque environnement spécifique. Ne vous attendez pas à ce que le produit fonctionne avec succès sans configuration. Une caméra utilisée pour la LPR présente une utilisation du processeur environ cinq fois supérieure à celle d'une caméra ordinaire. Si une caméra n'est pas configurée correctement, le niveau de reconnaissances fructueuses s'en trouvera affecté, tout comme la performance de l'unité centrale.

Veuillez lire les sections suivantes pour en savoir plus sur les facteurs qui influent sur votre solution LPR :

Positionnement de la caméra (á la page 324)

Angles de la caméra (á la page 325)

Recommandations en matière de largeur de plaques (á la page 326)

Résolution d'image (á la page 327)

Comprendre les expositions des caméras (á la page 329)

Environnement physique (á la page 332)

Objectif et vitesse d'obturation (á la page 334)

Contraste (á la page 335)

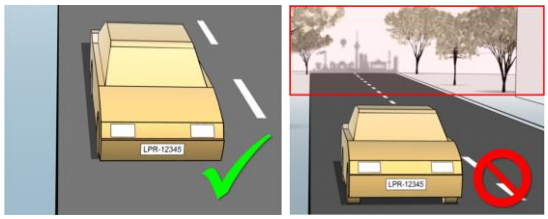
Fonctions non désirées des caméras (á la page 335)

Positionnement de la caméra

Lorsque vous installez des caméras à des fins de LPR, il est important d'avoir une vue claire et directe de la zone d'intérêt, de façon à ce que les plaques puissent être détectées de façon cohérente. Ceci garantit une performance optimale et un faible risque de fausse détection :

- La zone doit couvrir **uniquement** la portion de l'image où la plaque d'immatriculation est visible, lorsque le véhicule traverse l'image.
- Évitez les situations où des objets tels que des piliers, des barrières, des palissades ou des portails, bloquent le champ de vision de la caméra.
- Évitez les situations contenant des objets non pertinents en mouvement, tels que des personnes, des arbres ou encore du trafic routier

Si trop d'éléments non pertinents sont inclus, ils interfèrent avec le processus de détection et le serveur LPR utilise les ressources de l'unité centrale pour analyser des éléments non pertinents au lieu d'analyser les plaques d'immatriculation.

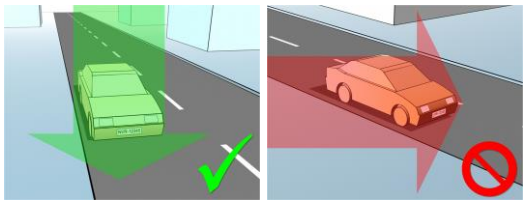


L'image de gauche présente une installation correcte, sans interférence dans le champ de vision. L'image de droite présente un montage incorrect. La caméra est installée trop bas et il y a trop de « bruit de fond » dans la vue.

Pour vous aider à obtenir une vue claire et non troublée, vous pouvez :

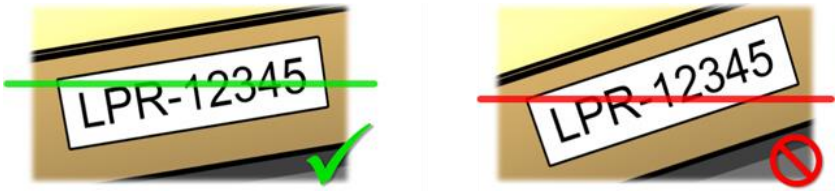
- Installer la caméra aussi près que possible de la zone d'intérêt.
- Changer l'angle de vue de votre caméra.
- Zoomer. Si vous zoomez, utilisez toujours le zoom optique de la caméra.

Installez la caméra de telle sort que la plaque d'immatriculation apparaisse à partir du haut de l'image (ou du bas si les véhicules s'éloignent de la caméra) au lieu de la faire apparaître à droite ou à gauche de l'image. Ainsi vous vous assurez que le processus de reconnaissance d'une plaque d'immatriculation ne commence que lorsque la plaque entière est en vue :

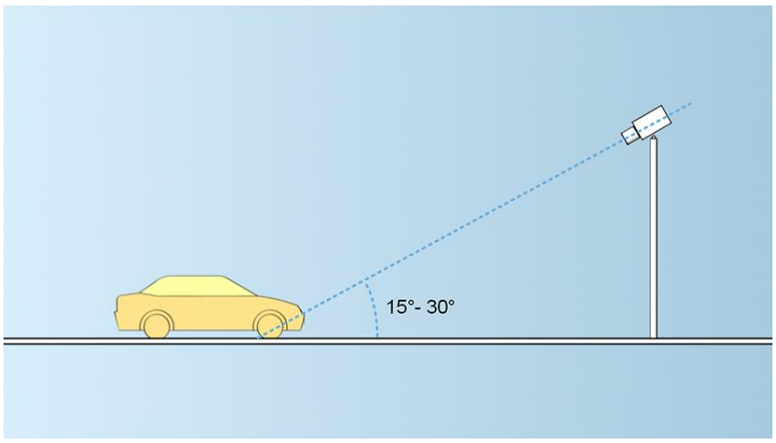


Angles de la caméra

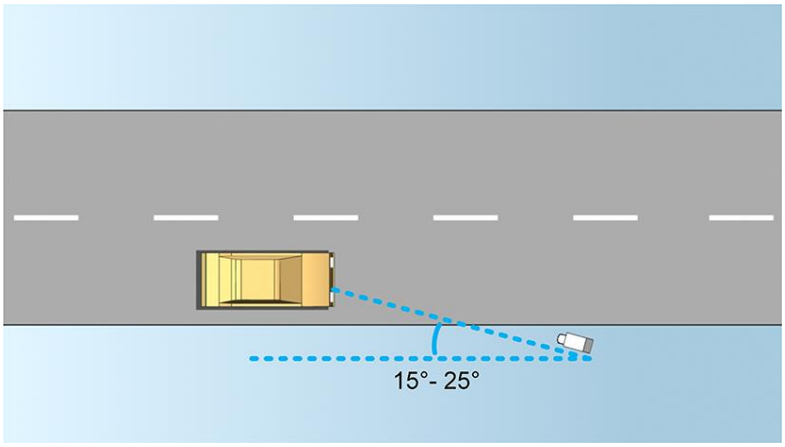
- **Règle de la ligne unique :** Installez la caméra de façon à pouvoir dessiner une ligne horizontale traversant à la fois le bord gauche et le bord droite de la plaque d'immatriculation dans les images capturées. Veuillez vous reporter aux illustrations ci-dessous pour connaître les angles de reconnaissance corrects et incorrects.



- **Angle vertical :** L'angle de vision vertical recommandé d'une caméra utilisée pour la LPR est compris entre 15° et 30°.

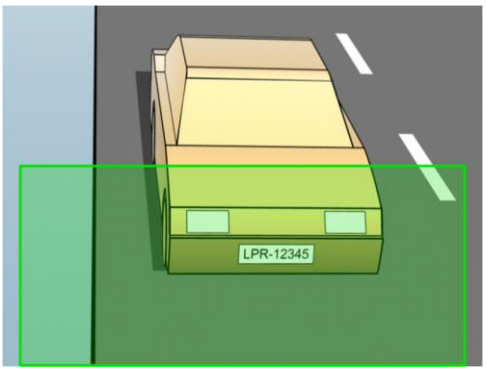


- **Angle horizontal :** L'angle de vision horizontal maximal recommandé d'une caméra utilisée pour la LPR est compris entre 15° et 25°.



Recommandations en matière de largeur de plaques

Installez la caméra de façon à ce que l'instantané idéal de la plaque d'immatriculation soit capturé lorsque la plaque d'immatriculation se trouve au centre ou dans la moitié inférieure de l'image :



Prenez un instantané et assurez-vous que les exigences de largeur de trait et de largeur de plaque décrites ci-dessous sont bien respectées. Utilisez un éditeur graphique standard pour mesurer la quantité de pixels. Lorsque vous entamer le processus consistant à atteindre la largeur de plaque minimale, commencez par une faible résolution sur la caméra, puis augmentez graduellement la résolution jusqu'à obtention de la largeur de plaque requise.

Largeur de trait

Le terme *pixels par trait* est utilisé pour définir une exigence minimum pour les polices censées être reconnues. L'illustration suivante présente ce que l'on entend par *trait* :

Comme l'épaisseur des traits dépend du pays et du style de plaque, les mesures telles que pixels/cm ou pixels/pouces ne sont pas utilisées.

La résolution offrant la meilleure performance en termes de LPR doit être d'au moins 2,7 pixels/trait.

Largeur de plaque

Type de plaque	Largeur de plaque	Configuration	Largeur de plaque minimale (pixels)
Plaques américaines sur une seule ligne	• largeur de plaque de 12 pouces • largeur de trait d'environ ¼ pouce	véhicules à l'arrêt ; pas de désentrelacement	130
		véhicules en mouvement ; entrelacés	215
Plaques européennes sur une seule ligne	• largeur de plaque de 52 cm • largeur de trait d'environ 1 cm	véhicules à l'arrêt ; pas de désentrelacement	170
		véhicules en mouvement ; entrelacés	280

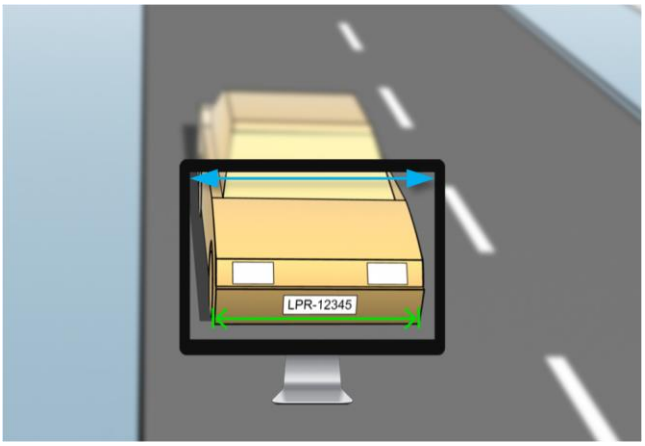
Si les véhicules sont en mouvement au moment de l'enregistrement et qu'une caméra entrelacée est utilisée, seule une moitié de l'image peut être utilisée (uniquement les lignes paires) pour la reconnaissance, contrairement à une caméra configurée pour les véhicules à l'arrêt sans entrelacement. Cela signifie que les exigences en termes de résolution sont quasiment deux fois plus élevées.

Résolution d'image

La qualité de l’image et la résolution sont des facteurs importants pour une reconnaissance fructueuse des plaques d'immatriculation. D'un autre côté, si la résolution de la vidéo est trop élevée, le processeur est susceptible d'être surchargé et risque de sauter des plaques ou

d'effectuer des détections erronées. Plus faible est le niveau sur lequel vous réglez la résolution acceptable, meilleurs seront la performance du processus et le taux de détection obtenu.

Dans cet exemple, nous vous expliquons comment procéder à un simple calcul de la qualité de l'image et trouver une résolution adaptée pour la reconnaissance de plaques. Le calcul est basé sur la largeur d'une voiture.



Exemple d'une capture pour laquelle nous souhaitons calculer une résolution adaptée.

Nous estimons que la largeur horizontale est de 200 cm/78 pouces, car nous partons du principe que la largeur d'une voiture standard est de 177 cm/70 pouces et nos rajoutons ~10 % d'espace supplémentaire. Vous pouvez également procéder à une mesure physique de la zone qui vous intéresse si vous avez besoin d'en connaître la largeur exacte.

La résolution recommandée de l'épaisseur de trait est de 2,7 pixels/trait et l'épaisseur de trait physique est de 1 cm pour une plaque européenne et de 0,27 pouce pour une plaque américaine. Ces informations nous permettent d'arriver au calcul suivant :

Calcul pour les plaques européennes en cm :

200 x 2,7 ÷ 1 = 540 pixels

Résolution recommandée = VGA (640x480)

Calcul pour les plaques américaines en pouces :

78 x 2,7 ÷ 0,27 = 780 pixels

Résolution recommandée = SVGA (800x600)

Comme les plaques américaines utilisent une police à traits étroits, il faut adopter une résolution plus élevée que celle requise pour les plaques européennes.

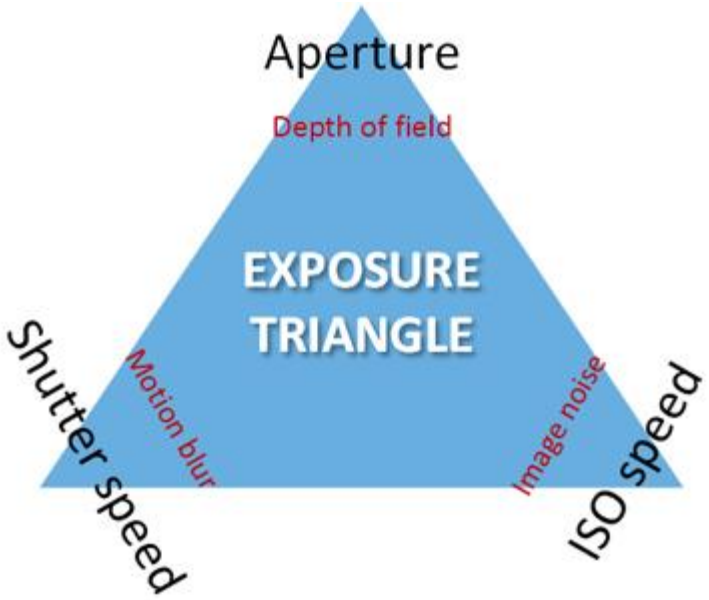
Résolutions vidéo fréquemment employées

Nom	Pixels (L×H)
QCIF	176×120
CIF	352×240
2CIF	704×240
VGA	640×480

Nom	Pixels (L×H)
4CIF	704×480
D1	720×576
SVGA	800×600
XGA	1024×768
720p	1280×1024

Comprendre les expositions des caméras

L'exposition de la caméra détermine le niveau de luminosité et la netteté d'une image lors de sa capture. Celle-ci dépend de trois paramètres des caméras : l'ouverture, la vitesse d'obturation et la sensibilité ISO. Pour vous aider à configurer la caméra correctement pour la solution LPR, il convient de comprendre la façon dont ils fonctionnent et agissent ensemble.



Le triangle d'exposition

Vous pouvez utiliser différentes combinaisons des trois paramètres pour parvenir à la même exposition. La clé consiste à savoir quels compromis il convient d'adopter, car chaque paramètre influence également les autres paramètres de l'image :

Paramètre des caméras	Contrôle...	Affecte...
Ouverture (Diaphragme)	L'ouverture réglable qui limite la quantité de lumière entrant dans la caméra	Profondeur de champ
Vitesse d'Obturateur	La durée de l'exposition	Flou de mouvement

Paramètre des caméras	Contrôle...	Affecte...
Sensibilité ISO	La sensibilité du capteur de la caméra pour une quantité donnée de lumière	Bruit de l'image

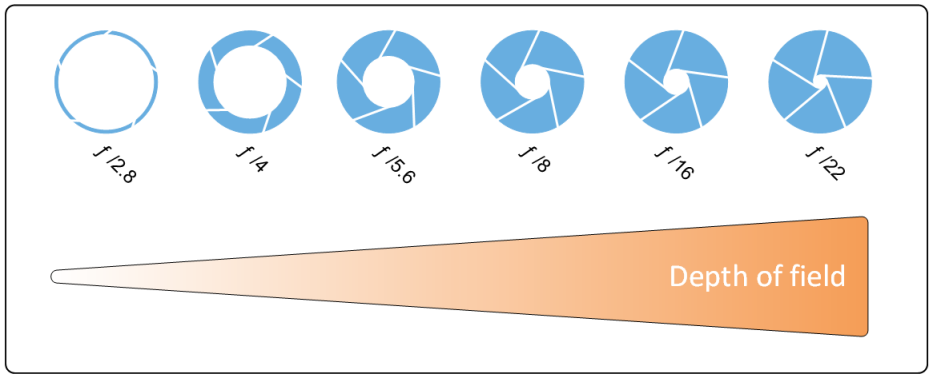
Les sections suivantes décrivent comment spécifier chaque paramètre, ce à quoi il ressemble et la façon dont un mode d'exposition donné affecte cette combinaison :

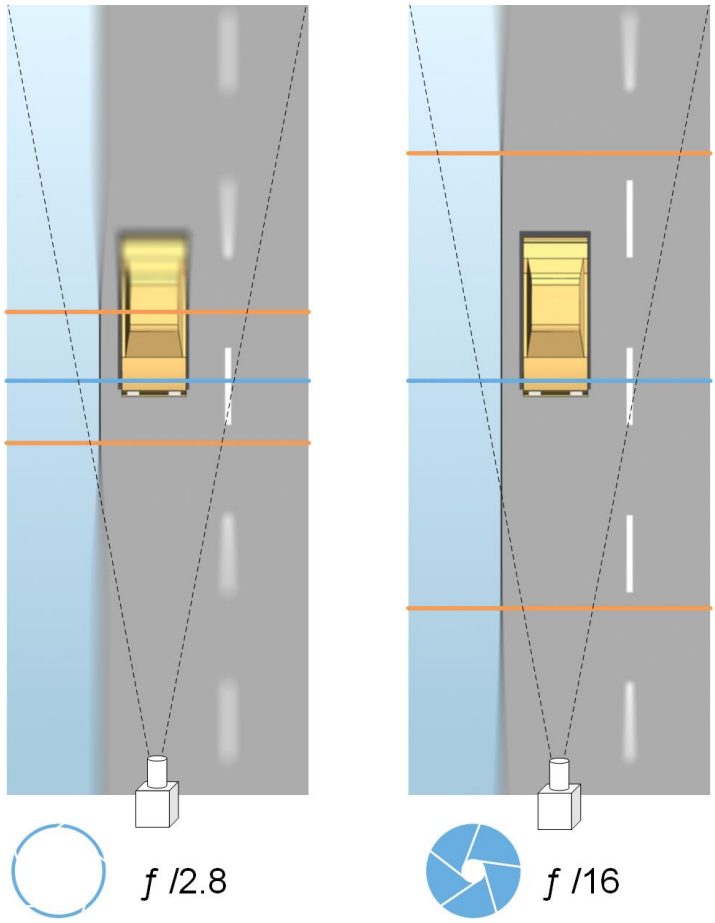
Paramètres d'ouverture

Le paramètre d'ouverture contrôle la quantité de lumière entrant dans votre caméra par le biais de l'objectif. Il est spécifié en termes de valeur d'ouverture (f-stop), qui peut parfois sembler contraire à la logique, car la superficie d'ouverture augmente lorsque la valeur d'ouverture (f-stop) diminue.

Valeur f-stop faible/grande ouverture = faible profondeur de champ

Valeur f-stop élevée/petite ouverture = grande profondeur de champ





L'exemple illustre la façon dont la profondeur de champ est affectée par la valeur f-stop. La ligne bleue indique le point de focalisation.

Une valeur f-stop élevée permet de focaliser l'image sur la plaque d'immatriculation sur une plus longue distance. De bonnes conditions de luminosité sont importantes pour obtenir une exposition suffisante. Si les conditions d'éclairage sont insuffisantes, la durée d'exposition doit être plus longue mais ceci augmente le risque d'obtention d'images floues.

Une valeur f-stop faible réduit la zone de focalisation et donc la zone utilisée pour la reconnaissance, mais elle est adaptée à des conditions de faible luminosité. S'il est possible de s'assurer que les véhicules traversent la zone de focalisation à faible vitesse, une valeur f-stop faible est adaptée et peut offrir une reconnaissance cohérente des plaques.

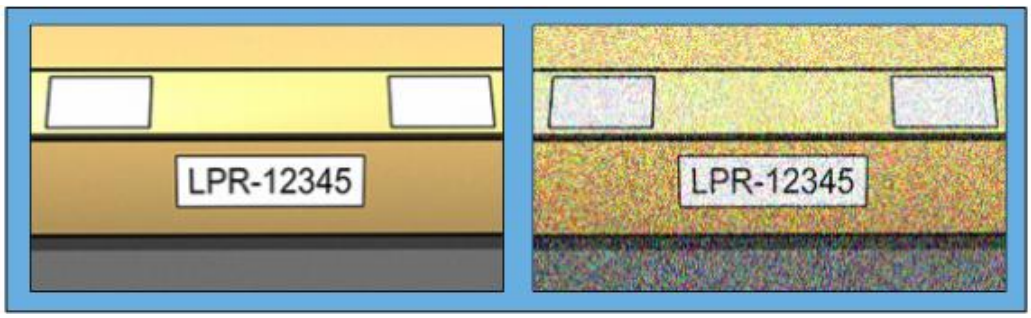
Vitesse d'Obturateur

L'obturateur d'une caméra détermine à quel moment le capteur de la caméra s'ouvre ou se ferme pour absorber la lumière entrant dans l'objectif de la caméra. La vitesse d'obturation se rapporte à la durée au cours de laquelle l'obturateur reste ouvert et la lumière peut entrer dans la caméra. La vitesse d'obturation et la durée d'exposition se rapportent au même concept et une vitesse d'obturation plus rapide correspond à une durée d'exposition plus faible.

Le flou de mouvement est indésirable pour la reconnaissance de plaques d'immatriculation et la surveillance. Bien souvent, les véhicules sont en mouvement lors de la détection des plaques d'immatriculation. C'est pourquoi une vitesse d'obturation correcte est un facteur important. La règle d'or consiste à conserver une vitesse d'obturation suffisamment élevée pour éviter un flou de mouvement mais suffisamment faible pour que les images ne souffrent pas d'une sous-exposition en fonction des conditions de luminosité et d'ouverture.

Sensibilité ISO

La sensibilité ISO détermine le niveau de sensibilité de la caméra vis-à-vis de la lumière entrante. Tout comme la vitesse d'obturation, elle est corrélée à l'augmentation ou la réduction de l'exposition avec un facteur de 1:1. Cependant, contrairement à l'ouverture et à la vitesse d'obturation, une sensibilité ISO inférieure est en général désirable, car les sensibilités ISO supérieures ont tendance à beaucoup accroître le bruit de l'image. Par conséquent, les augmentations de la sensibilité ISO à partir de sa valeur minimale n'ont généralement lieu que lorsqu'il est impossible d'obtenir la qualité d'image désirée en modifiant uniquement les paramètres d'ouverture et de vitesse d'obturation.



Exemple d'images avec des sensibilités ISO faibles et élevées. La sensibilité ISO élevée sur l'image de droite a un impact négatif sur le niveau de bruit de l'image.

Les sensibilités ISO communément employées sont 100, 200, 400 et 800, bien que de nombreuses caméras autorisent également l'utilisation de valeurs plus faibles ou plus élevées. Avec les caméras numériques mono-objectif reflex, une gamme de 50 à 800 (voire plus) est souvent acceptable.

Environnement physique

Lorsque vous installez et utilisez des caméras pour la reconnaissance de plaques (LPR), veuillez prendre note des facteurs suivants liés à l'environnement physique :

- **Trop de lumière :** Trop de lumière dans l'environnement peut conduire à une surexposition ou à des traces.
    - La **surexposition** correspond à ce qui se produit lorsque des images sont exposées à trop de lumière : elle entraîne un effet brûlé et une apparence trop blanche. Pour éviter toute surexposition, Milestone vous recommande d'utiliser une caméra dotée d'une plage dynamique élevée et/ou d'utiliser un objectif à diaphragme automatique. Le **diaphragme** est l'ouverture réglable. C'est pour cela que le diaphragme a un effet significatif sur l'exposition des images.

  - **Une trace** est un effet conduisant à la présence de lignes verticales claires indésirables dans les images. Cet effet est souvent causé par de petites imperfections sur les imageurs à dispositif à couplage de charge (CCD) des caméras. Les imageurs CCD sont les capteurs utilisés pour créer les images numériques.

Image d'une plaque d'immatriculation présentant des traces du fait d'une surexposition

- **Trop peu de lumière :** Trop peu de lumière dans l'environnement ou trop peu d'éclairage externe peut conduire à une sous-exposition.
  - La **sous-exposition** correspond à ce qui se produit lorsque des images sont exposées à trop peu de lumière : elle entraîne une image sombre quasiment sans contraste (á la page 335). Lorsque le gain automatique (voir "Fonctions non désirées des caméras" á la page 335) ne peut pas être désactivé ou lorsque vous ne pouvez pas configurer une durée maximale autorisée d'obturation (voir "Objectif et vitesse d'obturation" á la page 334) pour capturer les véhicules en mouvement, trop peu de lumière conduit tout d'abord à un brouillage dû au gain et à un flou de mouvement dans les images, et finalement à une sous-exposition. Pour éviter toute sous-exposition, utilisez un éclairage externe suffisant et/ou utilisez une caméra suffisamment sensible dans des environnements faiblement éclairés sans recourir au gain.
- **Infrarouges :** Un autre moyen permettant de surmonter des conditions d'éclairage difficiles consiste à utiliser un éclairage infrarouge artificiel combiné à une caméra infrarouge dotée d'un filtre passe-infrarouge. Les plaques d'immatriculation rétroréfléchissantes sont particulièrement adaptées à une utilisation avec la lumière infrarouge.
  - La **rétroréflectivité** est obtenue en recouvrant les surfaces d'un matériau réfléchissant spécial qui renvoie une grande proportion de la lumière d'une source lumineuse directement dans la direction dont elle provient. Les objets rétroréfléchissants semblent être beaucoup plus brillants que d'autres objets. Autrement dit, la nuit, ils peuvent être vus clairement à une distance considérable. La rétroréflectivité est fréquemment utilisée sur les panneaux de circulation ainsi que pour différents types de plaques d'immatriculation.
- **Conditions météorologiques :** Les caméras requièrent parfois une configuration spécifique, en cas de neige ou de soleil éblouissant, par exemple.
- **Condition de la plaque :** Certains véhicules ont des plaques d'immatriculation endommagées ou très sales. Parfois, il s'agit de dommages délibérés visant à éviter toute reconnaissance.

Objectif et vitesse d'obturation

Lors de la configuration des vitesses d'obturation et objectifs des caméras pour la LPR, veuillez noter les éléments suivants :

- **Mise au point :** Assurez-vous toujours que la plaque d'immatriculation soit bien nette.
- **Diaphragme automatique :** Si vous utilisez un objectif à diaphragme automatique, réglez toujours la mise au point de façon à ce que l'ouverture soit aussi grande que possible. Afin d'agrandir l'ouverture, vous pouvez utiliser des filtres à densité neutre (ND) ou, si la caméra prend en charge la configuration manuelle de la durée d'obturation, vous pouvez régler la durée d'obturation sur une durée très courte.
  - Les filtres à **Densité neutre** (ND) ou filtres gris réduisent tout simplement la quantité de lumière entrant dans une caméra. Ils fonctionnent comme des « lunettes de soleil » pour la caméra. Les filtres ND affectent l'exposition des images (voir "Comprendre les expositions des caméras" á la page 329)
- **Infrarouges :** Si vous utilisez une source de lumière infrarouge, la mise au point est susceptible de changer lorsque vous passez de la lumière visible à la lumière infrarouge et vice versa. Vous pouvez éviter ce changement de mise au point en utilisant un objectif à compensation infrarouge ou encore un filtre passe-infrarouge. Veuillez noter qu'en cas d'utilisation d'un filtre passe-infrarouge, une source de lumière infrarouge est requise, même en plein jour.
- **Vitesse des véhicules :** Lorsque les véhicules se déplacent, la durée d'obturation des caméras doit être suffisamment courte pour éviter une image floue en raison des mouvements. Une formule de calcul de la durée d'obturation maximale adaptée est :
  - **Vitesse du véhicule en km/h :** Durée d'obturation en secondes = 1 seconde / (11 x vitesse maximum du véhicule en kilomètres par heure)
  - **Vitesse du véhicule en mph :** Durée d'obturation en secondes = 1 seconde / (18 x vitesse maximum du véhicule en milles par heure)

  où / signifie « divisé par » et x signifie « multiplié par ».

Le tableau suivant fournit des recommandations quant aux vitesses d'obturation des caméras recommandées pour différentes vitesses de véhicules :

Durée d'obturation en secondes	Vitesse max. du véhicule en kilomètres par heure	Vitesse max. du véhicule en milles par heure
1/50	4	2
1/100	9	5
1/200	18	11
1/250	22	13
1/500	45	27
1/750	68	41
1/1000	90	55
1/1500	136	83
1/2000	181	111

1/3000	272	166
1/4000	363	222

Contraste

Lorsque vous déterminez le contraste approprié pour votre caméra de reconnaissance des plaques d'immatriculation (LPR), pensez à la différence de valeur de gris (lorsque les images sont converties au format 8 bits en nuances de gris) entre les caractères de la plaque d'immatriculation et la couleur d'arrière-plan de la plaque d'immatriculation.

Contraste approprié

Contraste acceptable ; il est encore possible de reconnaître la plaque

Les pixels d'une image de 8 bits en nuances en gris peuvent avoir des valeurs de couleur allant de 0 à 255, où une valeur de 0 en nuances de gris est un noir absolu et 255 est un blanc absolu. Lorsque vous convertissez votre image entrante en image de 8 bits en nuances de gris, la différence de valeur de pixel minimum entre un pixel du texte et un pixel de l'arrière-plan doit être d'au moins 15.

Veuillez noter qu'en raison du bruit de l'image (voir "Fonctions non désirées des caméras" á la page 335), du recours à la compression (voir "Fonctions non désirées des caméras" á la page 335), des conditions de luminosité et d'autres facteurs similaires, il peut être difficile de différencier les couleurs des caractères et de l'arrière-plan d'une plaque d'immatriculation.

Fonctions non désirées des caméras

Lors de la configuration des caméras pour la LPR, veuillez noter les éléments suivants :

- **Réglage automatique du gain :** L'un des types d'interférences d'image les plus communément causés par des caméras est ce que l'on appelle le bruit de gain.
  - Le **gain** est la façon dont une caméra capture l'image d'une scène et distribue la lumière au sein de l'image. Si la lumière n'est pas distribuée de façon optimale sur l'image, il en résulte un bruit de gain.

    Le contrôle du gain requiert l'application d'algorithmes complexes et de nombreuses caméras sont dotées de fonctions de réglage automatique du gain. Malheureusement, de telles fonctions sont rarement utiles dans le cadre d'une connexion avec un système LPR. Milestone vous recommande de configurer votre fonction de gain automatique sur le réglage le plus bas possible. Vous pouvez également désactiver la fonction de gain automatique.

    Image de plaque d'immatriculation avec bruit de gain

Dans un environnement sombre, vous pouvez éviter le bruit de gain en installant suffisamment de sources de lumière externes.

- **Amélioration automatique :** Certaines caméras utilisent des algorithmes d'amélioration des contours, des bords ou du contraste pour créer des images plus esthétiques pour l'œil humain. De tels algorithmes peuvent interférer avec les algorithmes utilisés dans le cadre du processus LPR. Dans la mesure du possible, Milestone vous recommande de désactiver les algorithmes d'amélioration des contours, des bords et du contraste.

- **Compression automatique :** Des taux de compression élevés peuvent avoir une influence négative sur la qualité des images de plaques d'immatriculation. Lorsqu'un taux de compression élevé est utilisé, il est nécessaire d'utiliser une résolution supérieure (voir "Recommandations en matière de largeur de plaques" á la page 326) pour obtenir une performance optimale du système LPR. En cas d'utilisation d'une faible compression JPEG, l'impact négatif sur la reconnaissance de plaques est très faible, tant que les images sont sauvegardées avec un niveau de qualité JPEG de 80 % ou plus, et que les images ont une résolution, un contraste et une mise au point normaux, ainsi qu'un faible niveau de bruit.

Gauche : Image d'une plaque d'immatriculation avec un niveau de qualité JPEG de 80 % (autrement dit, une faible compression) ; acceptable

Droite : Image d'une plaque d'immatriculation avec un niveau de qualité JPEG de 50 % (autrement dit, une compression élevée) ; inacceptable

Installation du système de reconnaissance de plaque (LPR)

Installer XProtect LPR

Pour exécuter XProtect LPR, vous devez installer :

- Au moins un serveur LPR.
- Le module d'extension LPR sur tous les ordinateurs exécutant le Management Client et le serveur d'événements.
- Assurez-vous que l'utilisateur sélectionné pour l'exécution du service LPR Server peut accéder au serveur de gestion.

Milestone recommande de ne pas installer le serveur LPR sur le même ordinateur que votre serveur de gestion ou vos serveurs d'enregistrement.

Pour commencer l'installation :

1. Allez sur la page de téléchargement du site web http://www.milestonesys.com/downloads de Milestone.
2. Téléchargez les deux programmes d'installation :

- Le programme d'installation du *module d'extension Milestone XProtect LPR* sur tous les ordinateurs exécutant Management Client et le serveur d'événements.
- Le programme d'installation du *Serveur Milestone XProtect LPR* sur tous les ordinateurs affectés à cette fin. Vous pouvez également créer des serveurs virtuels pour la LPR sur un ordinateur.

3. Tout d'abord, exécutez tous les programmes d'installation du *module d'extension Milestone XProtect LPR.*
4. Ensuite, exécutez le ou les programmes d'installation *Milestone XProtect LPR Server*.

   Au cours de l'installation, spécifiez l'adresse IP ou le nom d'hôte du serveur de gestion pour les produits XProtect Advanced VMS ou le serveur d'images pour les produits XProtect Professional VMS, y compris le nom d'utilisateur du domaine et le mot de passe d'un compte d'utilisateur disposant de droits d'administrateur sur le système de surveillance.
5. Lancez le Management Client.

   Dans le **Panneau Navigation du Site**, votre Management Client affiche automatiquement la liste des serveurs LPR installés dans la liste de **Serveurs LPR**.
6. Assurez-vous de disposer des licences nécessaires (voir "Licences LPR" á la page 322).
7. Tous les modules de pays sont installés automatiquement lorsque vous installez votre produit XProtect LPR. Cependant, les modules installés sont désactivés par défaut et vous devez activer les modules (voir "Onglet Modules de pays" á la page 348) que vous souhaitez utiliser. Vous ne pouvez activer qu'un nombre de modules de pays identique au nombre de licences de modules de pays que vous possédez.

Vous ne pouvez pas ajouter de serveurs LPR à partir du Management Client.

Si vous avez besoin d'installer plus de serveurs LPR après l'installation initiale, exécutez le programme d'installation *Milestone XProtect LPR Server* sur ces serveurs.

Mise à niveau du XProtect LPR

Pour mettre à jour le XProtect LPR, vous devez suivre les mêmes étapes que pour l'installation (voir "Installer XProtect LPR" á la page 336).

Si vous passez de la version XProtect LPR 1.0 à la version XProtect LPR 2016, certains paramètres de reconnaissance ne sont pas compatibles avec ceux de la configuration précédente. Pour appliquer les nouveaux paramètres, vous devez sauvegarder votre configuration. Les paramètres qui vous permettaient précédemment de retourner, pivoter et inverser les couleurs de la vidéo ont été supprimés. Si vous avez cependant encore besoin de ces fonctions, vous devez modifier les paramètres sur les caméras en elles-mêmes.

Configuration LPR

Consulter les informations relatives au serveur LPR

Pour vérifier l'état de vos serveurs LPR :

1. Dans le **Panneau Navigation du Site**, développez **Serveurs** et sélectionnez **Serveurs LPR**. Allez au panneau Vue d'ensemble

La fenêtre **informations relatives au serveur LPR** s'ouvre sur un résumé de l'état du serveur :

- Nom
- Nom de l'hôte
- État

2. Sélectionnez le serveur LPR pertinent et passez en revue tous les détails pour ce serveur (voir "Propriétés des informations du serveur LPR" á la page 338).

Propriétés des informations du serveur LPR

Champ	Description
Nom	Ici, vous pouvez également modifier le nom du serveur LPR.
Nom de l'hôte	Affiche le nom de l'hôte du serveur LPR. La première partie du nom du serveur LPR est constituée du nom de l'ordinateur hôte de votre installation de serveur LPR. Exemple : *MONHOTE.nomdedomaine.pays*.
État	Affiche l'état du serveur LPR. Si le serveur vient juste d'être ajouté, l'état est : • *Aucune caméra LPR configurée*. Si le système fonctionne sans problèmes, l'état est : • *Toutes les caméras LPR fonctionnent*. Autrement, le système renvoie : • *Le service ne répond pas.* • *Pas de connexion au système de surveillance.* • *Le service n'est pas en cours d'exécution.* • *Le serveur d'événements n'est pas connecté.* • *Erreur inconnue.* • *X caméras LPR sur Y fonctionnent.*
Durée de fonctionnement du service	Affiche la durée de fonctionnement depuis le dernier arrêt du serveur LPR et la mise en marche du service du serveur LPR.
Utilisation du processeur de l'ordinateur	Affiche l'utilisation actuelle du processeur sur l'ensemble de l'ordinateur avec le ou les serveurs LPR installés.
Mémoire disponible	Affiche la quantité de mémoire disponible sur le serveur LPR.
Plaques d'immatriculation reconnues	Affiche le nombre de plaques d'immatriculation que le serveur LPR a reconnues dans cette session.
Caméras LPR	Affiche une liste des caméras LPR activées qui fonctionnent sur le serveur LPR, ainsi que leur état.

Champ	Description
Caméras LPR disponibles	En fonction de votre licence, ce nombre indique le nombre de caméras LPR supplémentaires que vous êtes en droit d'ajouter et d'utiliser sur l'ensemble de vos serveurs LPR.
Modules de pays disponibles.	En fonction de votre licence, ce nombre indique le nombre de modules de pays supplémentaires que vous êtes en droit d'utiliser sur l'ensemble de vos serveurs LPR. Il présente également les numéros des modules de pays déjà utilisés.

Configuration des caméras pour LPR

Prérequis dans le Management Client

Une fois que les caméras sont montées et ajoutées sur le Management Client, réglez chaque paramètre des caméras de façon à ce qu'il corresponde aux exigences du LPR. Vous ajustez les paramètres des caméras dans les onglets propriétés de chaque caméra.

Pour les caméras pertinentes, Milestone recommande de :

- Régler le codec vidéo sur JPEG.

  Veuillez noter que, si vous utilisez le codec H.264 ou H.265, seules les images-clés sont prises en charge. Celles-ci surviennent généralement à un taux d'une image par seconde, ce qui est insuffisant pour LPR. Pour les fluidités d'image plus élevées, utilisez toujours un codec JPEG.

- Spécifiez une fluidité d'image de quatre images par seconde.
- Évitez la compression afin d'obtenir une meilleure qualité d'image.
- Si possible, spécifiez une résolution inférieure à un mégapixel.
- Si possible, conservez la netteté automatique à un faible niveau.

Pour en savoir plus sur les éléments fondamentaux de LPR, familiarisez-vous avec les informations contenues dans À propos de la préparation des caméras pour la LPR (voir "À propos de la préparation des caméras pour LPR" á la page 323).

À propos des instantanés

Le système utilise des instantanés pour optimiser la configuration automatiquement et pour visualiser l'effet des paramètres de reconnaissance dès qu'ils sont appliqués.

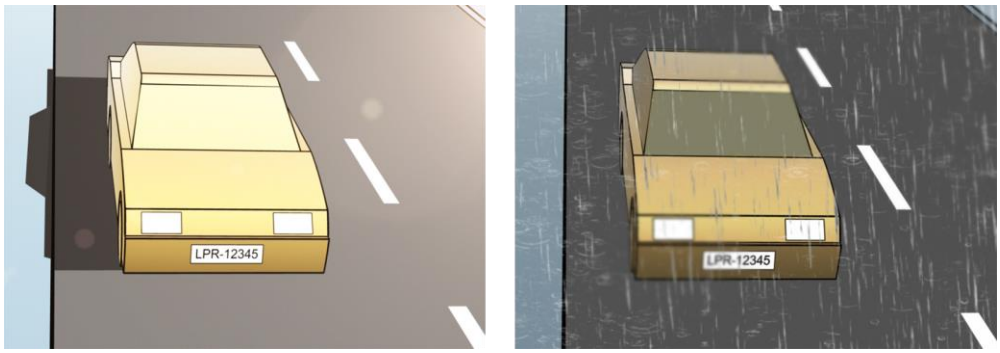
Vous devez fournir au moins un instantané valide afin de terminer la configuration initiale d'une caméra.

Pour avoir une idée de la configuration à obtenir, capturez des instantanés de véhicules dans l'environnement physique réel et les conditions dans lesquels vous souhaitez pouvoir reconnaître les plaques d'immatriculation.

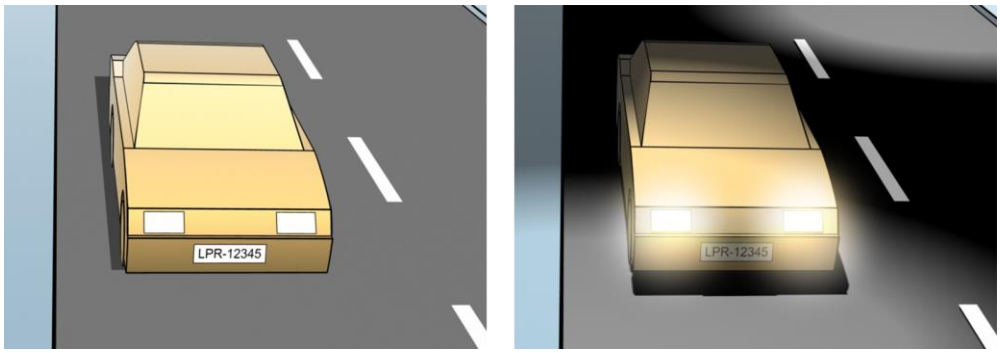
La liste ci-dessous illustre des exemples de situations que vous devriez prendre en compte lors de la capture et de la sélection d'instantanés. Elles ne seront pas forcément toutes applicables à votre environnement.

Milestone vous recommande de sélectionner au moins 5 à 10 instantanés représentant des conditions typiques en matière de :

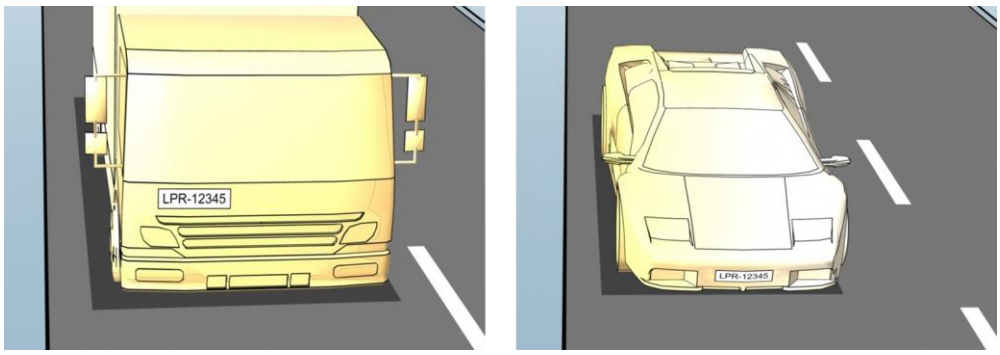
- **Météo ; par exemple, la lumière du soleil et la pluie**



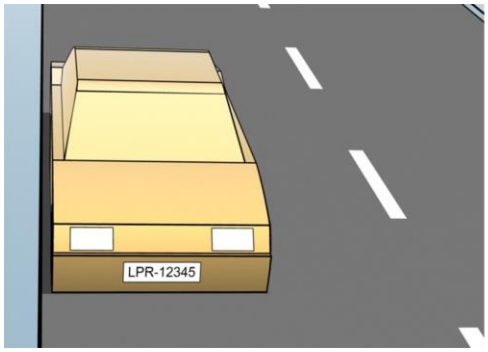
- **Lumière ; par exemple, la luminosité en journée et de nuit**

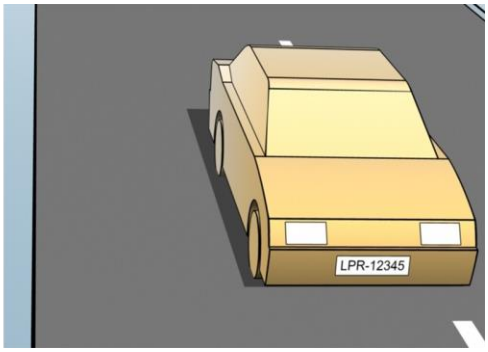


- **Types de véhicules ; pour définir le haut et le bas de la zone de reconnaissance**

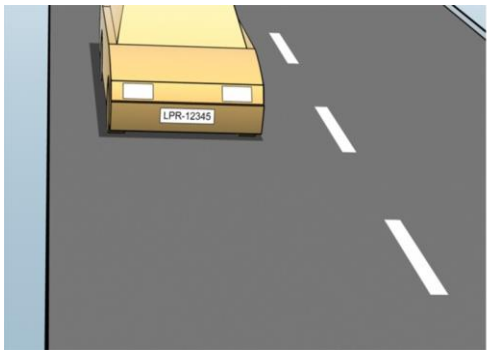


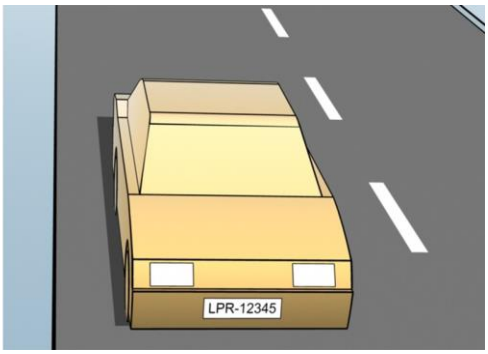
- **Position dans la file ; pour définir la gauche et la droite de la zone de reconnaissance**





- **Distance par rapport à la voiture ; pour définir la zone où le système LPR analyse les plaques d'immatriculation**





Ajouter une caméra LPR

Pour configurer les caméras à des fins de reconnaissance de plaques, vous devez tout d'abord exécuter l'assistant d'installation **Ajouter une caméra LPR**. L'assistant vous aide à procéder aux principales étapes de la configuration et optimise automatiquement la configuration.

Pour exécuter l'assistant :

1. Dans le **Panneau Navigation du Site**, développez **Serveurs**, développez **Serveurs LPR**, et sélectionnez **Caméra LPR**.
2. Allez au panneau Vue d'ensemble Cliquez avec le bouton droit sur **Caméra LPR**.
3. Dans le menu qui s'affiche, sélectionnez **Ajouter une caméra LPR** et suivez les instructions de l'assistant d'installation :
   - Sélectionnez la caméra que vous souhaitez configurer pour la LPR.
   - Sélectionnez les modules de pays que vous souhaitez utiliser avec votre caméra LPR (voir "Onglet Modules de pays" á la page 348).
   - Sélectionnez les instantanés à utiliser pour valider la configuration (voir "À propos des instantanés" á la page 339).

- Validez les résultats de l'analyse des instantanés (voir "Valider la configuration" á la page 349).
- Sélectionnez les listes de correspondance des plaques d'immatriculation à utiliser (voir "À propos des listes de correspondance de plaques d'immatriculation" á la page 350). Choisissez la sélection par défaut si vous n'avez pas encore créé de liste.

4. Sur la dernière page, cliquez sur **Fermer**.

   La caméra LPR apparaît dans le Management Client et, en fonction de vos sélections, le système optimise les paramètres de reconnaissance pour la caméra (voir "Onglet Paramètres de reconnaissance" á la page 343).

5. Sélectionnez la caméra que vous avez ajoutée et passez ses paramètres en revue. Il n'est nécessaire de modifier la configuration que si le système ne reconnaît pas les plaques d'immatriculation aussi bien qu'escompté.

6. Dans l'onglet **Paramètres de reconnaissance**, cliquez sur Valider la configuration (á la page 349).

Modifier des paramètres pour votre caméra LPR

Le système a automatiquement optimisé la configuration de votre caméra LPR lorsque vous avez ajouté la caméra LPR à l'aide de l'assistant d'installation **Ajouter une caméra LPR**. Si vous souhaitez apporter des modifications à la configuration initiale, vous pouvez :

- Modifier le nom du serveur ou changer de serveur (voir "Onglet Infos" á la page 342).
- Ajuster et valider les paramètres de reconnaissance (voir "Onglet Paramètres de reconnaissance" á la page 343).
- Ajouter plus de listes de correspondance de plaques d'immatriculation (voir "Onglet Listes de correspondance" á la page 347).
- Activer des modules de pays supplémentaires (voir "Onglet Modules de pays" á la page 348).

Onglet Infos

Cet onglet fournit des informations au sujet de la caméra sélectionnée :

Nom	Description
Activer	Par défaut, les caméras LPR sont activées après la configuration initiale. Désactivez toute caméra qui n'est pas utilisée en lien avec le système de reconnaissance de plaque. La désactivation d'une caméra LPR ne l'empêche pas de procéder à un enregistrement normal dans le système de surveillance.
Caméra	Affiche le nom de la caméra sélectionnée tel qu'il apparaît dans le XProtect Management Client et dans les clients.
Description	Utilisez ce champ pour saisir une description (facultatif).

Nom	Description
Changer de serveur	Cliquez pour changer de serveur LPR. Il est parfois sensé de changer le serveur LPR si vous avez besoin d'équilibrer la charge. Par exemple, si la charge du processeur est trop élevée sur un serveur LPR, Milestone vous recommande de déplacer une ou plusieurs caméras LPR vers un autre serveur LPR.

Onglet Paramètres de reconnaissance

Les paramètres de reconnaissance sont configurés automatiquement et optimisés par le système au cours de la configuration initiale de votre caméra LPR, principalement sur la base des instantanés que vous avez fournis.

Boutons d'action

Utilisez ces boutons pour mettre à jour et valider vos paramètres après la configuration initiale.

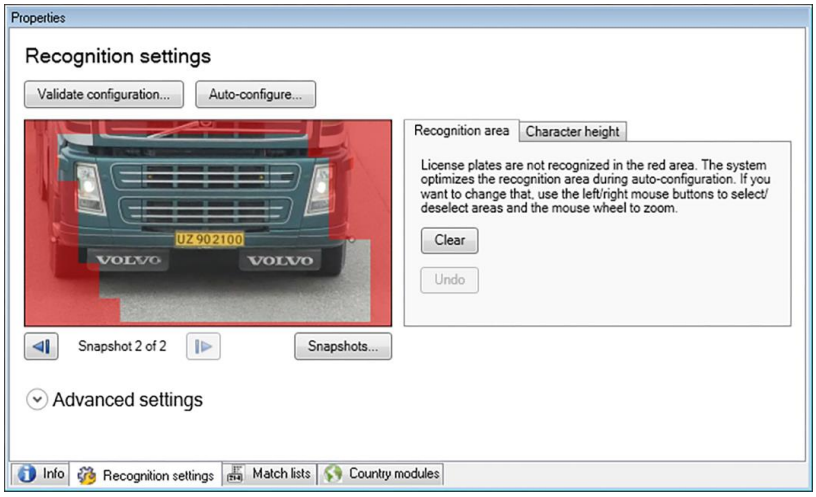
Nom	Description
Cliché	Ajoutez ou supprimez des instantanés (voir "Sélectionner des instantanés" á la page *349*).
Valider la configuration	Vérifiez que les plaques d'immatriculation sont reconnues comme escompté (voir "Valider la configuration" á la page *349*).
Auto-configuration	Rejetez les modifications manuelles et optimisez les paramètres (voir "Auto-configuration" á la page *350*).

Zone de reconnaissance

Le système optimise la zone de reconnaissance au cours de la configuration automatique, mais vous pouvez la modifier manuellement.

Pour garantir la meilleure performance possible et un faible risque de fausse détection, Milestone vous recommande de toujours sélectionner une zone de reconnaissance clairement définie et bien taillée. La zone doit couvrir **uniquement** la portion de l'image où la plaque d'immatriculation est visible, lorsque le véhicule traverse l'image. Évitez les situations contenant des objets non pertinents en mouvement, tels que des personnes, des arbres ou encore du trafic routier dans la zone de reconnaissance (voir "Positionnement de la caméra" á la page 324).

Les plaques d'immatriculation ne sont pas reconnues dans la zone rouge.



Lorsque vous spécifiez une zone de reconnaissance, vous disposez des options suivantes :

Nom	Description
Effacer	Cliquez pour effacer toutes les cases cochées de façon à ce qu'aucune zone ne soit utilisée pour la reconnaissance de plaque. Sélectionnez de nouvelles zones.
Annuler	Cliquez pour revenir à votre dernière configuration sauvegardée de la zone de reconnaissance.

Lorsque vous avez modifié les paramètres de votre caméra LPR, validez votre configuration (voir "Valider la configuration" á la page 349) pour voir si le système reconnaît bien les plaques d'immatriculation comme escompté.

Hauteur des caractères

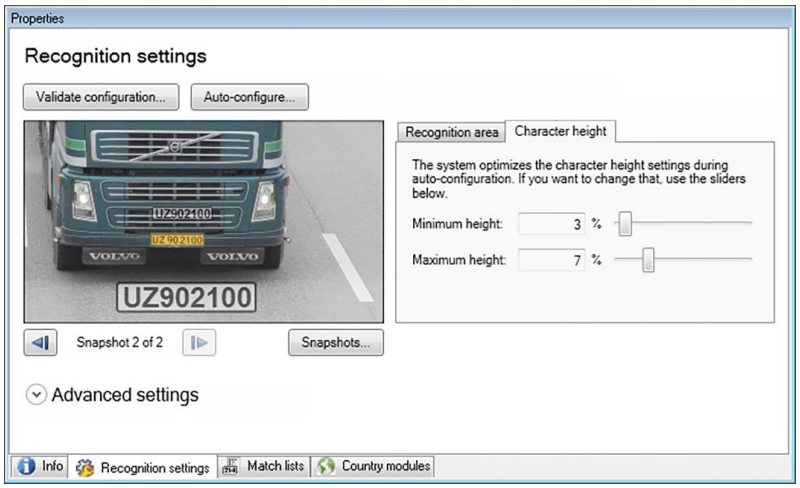
Le système optimise la hauteur des caractères au cours de la configuration automatique, mais vous pouvez la modifier manuellement.

Vous pouvez définir la hauteur minimum et maximum des caractères de la plaque d'immatriculation (sous forme de pourcentage). Sélectionnez des hauteurs de caractères aussi proches que possible de la hauteur des caractères de la véritable plaque d'immatriculation.

Ces paramètres relatifs aux caractères influencent le processus de reconnaissance car ils déterminent partiellement la durée de reconnaissance. En règle générale, plus la différence entre la hauteur minimum et la hauteur maximum des caractères est élevée et :

- Plus le processus LPR est complexe.
- Plus la charge du processeur est élevée.

- Plus vous devez attendre avant de recevoir les résultats.



La couche superposée sur l'instantané affiche le paramètre de hauteur de caractère défini actuellement. La couche superposée grandit ou rétrécit proportionnellement aux paramètres de hauteur de caractère présentés sur la droite. Pour une comparaison plus aisée, vous pouvez déplacer la couche superposée sur la véritable plaque d'immatriculation de l'instantané. Si nécessaire, utilisez la molette de la souris pour zoomer.

Nom	Description
Hauteur minimum	Utilisez les curseurs pour régler la hauteur minimum des caractères à inclure dans un processus de reconnaissance. Le système n'entamera pas le processus de reconnaissance sur les plaques d'immatriculation contenant des caractères d'une hauteur inférieure à la valeur spécifiée.
Hauteur maximum	Utilisez les curseurs pour régler la hauteur maximum des caractères à inclure dans un processus de reconnaissance. Le système n'entamera pas le processus de reconnaissance sur les plaques d'immatriculation contenant des caractères d'une hauteur supérieure à la valeur spécifiée.

Lorsque vous avez modifié les paramètres de votre caméra LPR, validez votre configuration (voir "Valider la configuration" á la page 349) pour voir si le système reconnaît bien les plaques d'immatriculation comme escompté.

Paramètres avancés

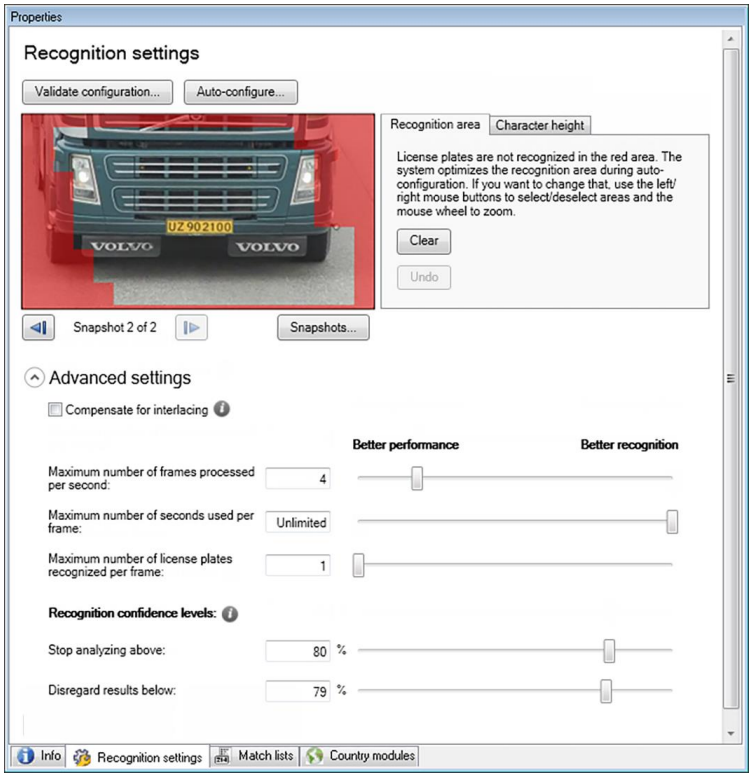
Le système optimise les paramètres avancés au cours de la configuration automatique, mais vous pouvez les modifier manuellement.

Le processus de reconnaissance peut être divisé en deux étapes : trouver la ou les plaques et reconnaître les caractères inscrits sur les plaques. Les paramètres avancés vous permettent de trouver un compromis entre la vitesse de traitement et la qualité de reconnaissance.

En règle générale, une qualité de reconnaissance élevée :

- nécessite un plus grand effort de calcul,
- entraîne une charge plus élevée du processeur,

- requiert plus de temps pour présenter des résultats.



En ajustant les paramètres avancés, vous définissez le compromis. Le processus de reconnaissance s'arrête si l'un des critères d'arrêt est rempli et renvoie la plaque d'immatriculation reconnue à ce moment-là.

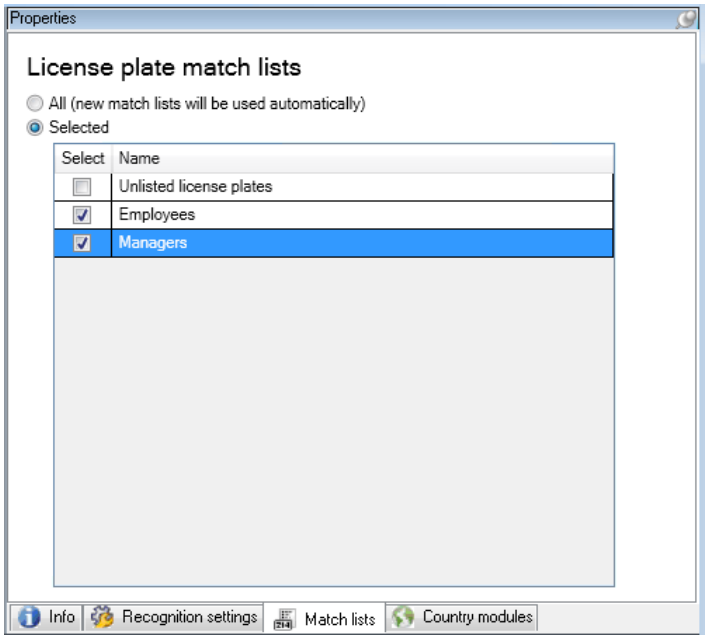
Nom	Description
Compensation du désentrelacement	Lorsque votre caméra LPR envoie une vidéo entrelacée et que vous observez des effets de peigne dans les images désentrelacées sur la LPR, vous pouvez activer cette fonction. Ceci peut améliorer la qualité de l'image et, par conséquent, vos résultats de reconnaissance.
Sélectionner le nombre maximum d'images traitées par seconde	Spécifie une limite quant au nombre d'images que votre solution LPR traite par seconde. Si vous gardez un nombre d'images faible pour les processus LPR, vous pouvez appliquer une fluidité d'image plus élevée sur la caméra afin de pouvoir enregistrer sans ajouter de charge inutile sur le serveur LPR. **Illimité** signifie que vous n'avez pas défini de critère pour ce paramètre.
Nombre maximum de secondes utilisées par image	Spécifie une limite quant au nombre de secondes que votre solution LPR est autorisée à passer sur la reconnaissance d'une image. Si ce paramètre est ajusté, la valeur recommandée est de *200* ms par image. **Illimité** signifie que vous n'avez pas défini de critère pour ce paramètre.

Nom	Description
Nombre maximum de plaques d'immatriculation reconnues par image	Spécifie une limite quant au nombre de plaques d'immatriculation reconnues renvoyé par image. Veuillez ne changer ce paramètre que si c'est absolument nécessaire, si vous procédez à une détection sur plusieurs voies à l'aide d'une seule caméra LPR, par exemple. **Illimité** signifie que vous n'avez pas défini de critère pour ce paramètre.
Arrêter l'analyse au-dessus de	Spécifie un niveau de confiance minimum (en pourcentage). Le processus de reconnaissance se poursuit jusqu'à ce que le système puisse renvoyer une plaque d'immatriculation avec un niveau de confiance supérieur ou égal à la valeur spécifiée.
Ignorer les résultats en dessous de	Le système rejette les plaques d'immatriculation lorsque le niveau de confiance est inférieur ou égal à la valeur spécifiée. En règle générale, plus la différence entre les valeurs **Arrêter l'analyse au-dessus de** et **Ignorer les résultats en dessous de** est faible, plus la charge du processus est faible et plus le système renvoie les résultats de reconnaissance rapidement.

Lorsque vous avez modifié les paramètres de votre caméra LPR, validez votre configuration (voir "Valider la configuration" á la page 349) pour voir si le système reconnaît bien les plaques d'immatriculation comme escompté.

Onglet Listes de correspondance

Dans cet onglet, vous pouvez sélectionner la ou les listes de correspondance de plaques d'immatriculation que vous souhaitez qu'une caméra LPR spécifique utilise pour procéder à la vérification des plaques d'immatriculation. Vous pouvez créer autant de listes que vous le souhaitez (voir "Ajouter de nouvelles listes de correspondance de plaques d'immatriculation" á la page 351).



Nom	Description
Tous	Les plaques d'immatriculation sont vérifiées par rapport à toutes les listes disponibles et futures.
Sélectionné	Les plaques d'immatriculation sont vérifiées par rapport aux listes sélectionnées uniquement. Sélectionnez une ou plusieurs des listes disponibles.

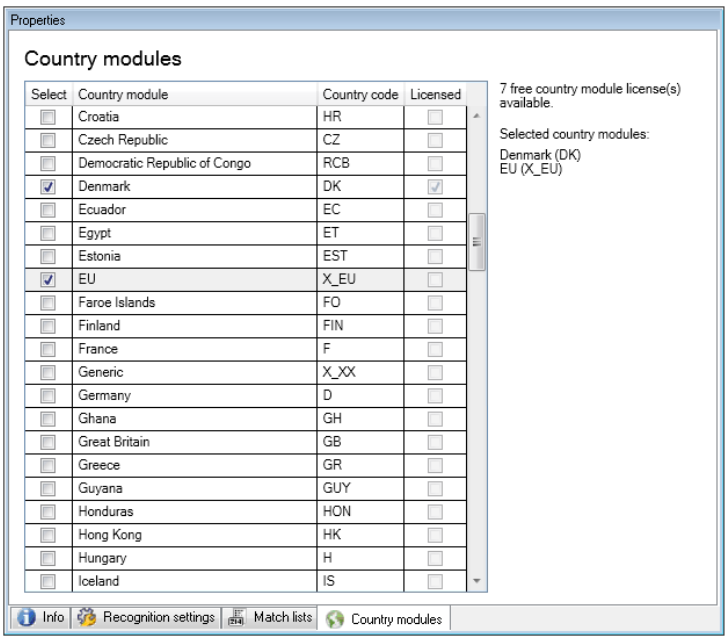
Lorsque vous avez modifié les paramètres de votre caméra LPR, validez votre configuration (voir "Valider la configuration" á la page 349) pour voir si le système reconnaît bien les plaques d'immatriculation comme escompté.

Onglet Modules de pays

Ici, vous pouvez sélectionner les modules de pays que vous souhaitez utiliser avec une caméra LPR spécifique. La liste dans laquelle vous pouvez faire votre choix dépend des modules installés et de vos licences (voir "Licences LPR" á la page 322).

Un module de pays est une série de règles définissant les plaques d'immatriculation d'un certain type et d'une certaine forme appartenant à un certain pays, état ou une certaine région.

Les modules déjà sous licence sont accompagnés d'une coche dans la colonne **Licence**. Si le module du pays que vous recherchez n'apparaît pas dans la liste, veuillez contacter votre fournisseur.



Nom	Description
Sélectionner	Cliquez pour sélectionner ou désélectionner un module de pays. La liste des modules de pays sélectionnés présentée sur le côté droit est mise à jour automatiquement.
Module de pays	Affiche les modules de pays installés.

Nom	Description
Code de pays	Lettres identifiant un module de pays.
Licence	Indique si un module de pays est déjà sous licence. Vous pouvez sélectionner un module de pays sous licence pour un nombre illimité de caméras.

Lorsque vous avez modifié les paramètres de votre caméra LPR, validez votre configuration (voir "Valider la configuration" á la page 349) pour voir si le système reconnaît bien les plaques d'immatriculation comme escompté.

Sélectionner des instantanés

Lors de la configuration initiale de la LPR à l'aide de l'assistant **Ajouter une caméra LPR**, vous avez également ajouté des instantanés (voir "À propos des instantanés" á la page 339). Vous pouvez toujours ajouter des instantanés représentatifs supplémentaires afin d'améliorer l'optimisation de la configuration.

1. Sélectionnez la caméra pertinente.
2. Dans l'onglet **Paramètres de reconnaissance**, cliquez sur **Instantanés**.
3. Capturez les instantanés à partir d'une vidéo en direct ou importez-les à partir d'un emplacement externe. Cliquez sur **Suivant**.

   Le système analyse les instantanés que vous avez sélectionnés pour la caméra.
4. Sur la page suivante, approuvez ou rejetez chacun des instantanés. Si le système ne parvient pas à reconnaître des plaques d'immatriculation, cliquez sur **Précédent** pour ajouter de nouveaux instantanés de meilleure qualité. Si le système ne parvient toujours pas à procéder à des reconnaissances correctes, vous devrez probablement modifier votre configuration. Vérifiez que la caméra a bien été installée et configurée correctement (voir "À propos de la préparation des caméras pour LPR" á la page 323).
5. Lorsque vous avez approuvé tous les instantanés, cliquez sur **Suivant** et fermez l'assistant.
6. Dans l'onglet **Paramètres de reconnaissance**, cliquez sur **Valider la configuration** (á la page 349).

Valider la configuration

Vous pouvez valider votre configuration actuelle pour voir si vous devez modifier des paramètres ou fournir plus d'instantanés. La fonction de validation vous indique le nombre de plaques d'immatriculation reconnues par votre système et si elles sont reconnues correctement ou non.

Elle peut vous aider à décider si le niveau de confiance est réglé correctement et si la configuration de votre système est optimale.

1. Sélectionnez la caméra pertinente.
2. Dans l'onglet **Paramètres de reconnaissance**, cliquez sur **Valider la configuration**.

   Sur la base des paramètres actuels, le système analyse les captures d'écran que vous avez sélectionnées pour la caméra et fournit un récapitulatif des résultats :

- **Plaques d'immatriculation détectées :** Le nombre de plaques d'immatriculation reconnues, par exemple, 3 sur 3
- **Indice de confiance moyen :** Le pourcentage de confiance moyen avec lequel les plaques d'immatriculation ont été reconnues.
- **Durée moyenne de traitement** : La durée moyenne nécessaire pour analyser une capture d'écran et renvoyer un résultat, mesurée en ms.

License plates detected:	**2 of 2**
Average confidence:	**91 %**
Average processing time:	**112 ms**

3. Si la configuration actuelle répond à vos exigences, cliquez sur **Fermer**.
4. Si vous souhaitez procéder à un examen plus approfondi des résultats, cliquez sur **Suivant**. Vous pouvez alors passer en revue les résultats pour chaque capture d'écran. Ceci peut vous aider à identifier les situations problématiques.

Vous pouvez valider la configuration autant de fois que vous le souhaitez, sur n'importe quelle caméra LPR et avec différents paramètres.

Auto-configuration

La configuration automatique de la caméra LPR remplace toute modification manuelle apportée aux paramètres. Vous pouvez sélectionner cette option si, par exemple, vous avez apporté des modifications manuelles qui ne vous ont pas donné de résultats de reconnaissance satisfaisants.

1. Dans l'onglet **Paramètres de reconnaissance**, cliquez sur **Configuration automatique**.

   Une nouvelle fenêtre de dialogue s'affiche alors.

2. Confirmez que vous souhaitez revenir aux paramètres configurés automatiquement en cliquant sur **Suivant**.

   Le système optimise les paramètres.

3. Cliquez sur **Fermer.**
4. Si vous y êtes invité, confirmez pour sauvegarder la configuration.
5. Passez en revue et validez (voir "Valider la configuration" á la page 349) les nouveaux paramètres.

Travailler avec des listes de correspondance de plaques d'immatriculation

À propos des listes de correspondance de plaques d'immatriculation

Les listes de plaques d'immatriculation sont des collections de plaques d'immatriculation que vous souhaitez voir traitées de façon spéciale par votre solution LPR. Les reconnaissances de plaques d'immatriculation sont comparées avec ces listes et, en cas de concordance, le système déclenche

un événement LPR. Les événements sont enregistrés sur le serveur d'événements et peuvent faire l'objet de recherches et être consultés dans l'ongle **LPR** de XProtect Smart Client.

Par défaut, les événements ne sont conservés que pendant 24 heures. Pour modifier ce paramètre, ouvrez la fenêtre de dialogue **Options** dans le Management Client et dans l'onglet **Paramètres du serveur d'événements**, dans le champ **Conserver les événements pendant**, saisissez un nouveau délai.

Une fois qu'une liste de correspondance de plaques d'immatriculation est spécifiée, vous pouvez configurer des événements et alarmes supplémentaires à déclencher en cas de concordance.

Exemples :

- Le siège social d'une entreprise utilise une liste des plaques d'immatriculation des véhicules professionnels de la direction afin que les directeurs puissent accéder à une zone de stationnement privilégiée. Lorsque les plaques d'immatriculation des directeurs sont reconnues, la solution LPR déclenche un signal de sortie qui ouvre la barrière de la zone de stationnement.
- Une chaîne de stations-services crée une liste de plaques d'immatriculation à partir des véhicules qui ont précédemment quitté des stations-services sans payer. Lorsque de telles plaques d'immatriculation sont reconnues, la solution LPR déclenche des signaux de sortie qui activent une alarme et bloquent l'approvisionnement en carburant de certaines pompes à titre temporaire.

Les événements déclenchés peuvent également être utilisés pour procéder à un enregistrement vidéo de haute qualité ou une autre action similaire. Vous pouvez même utiliser un événement pour déclencher des combinaisons de telles actions.

À propos de la liste de plaques d'immatriculation n'appartenant à aucune liste

Vous souhaiterez souvent déclencher un événement en cas de reconnaissance d'une plaque d'immatriculation incluse dans une liste, mais vous pouvez également déclencher un événement avec une plaque d'immatriculation qui n'est **pas** incluse dans une liste.

Exemple : Un parking privé utilise une liste de plaques d'immatriculation pour accorder l'accès au parking aux véhicules des résidents. Si un véhicule doté d'une plaque d'immatriculation ne figurant pas sur la liste s'approche du parking, la solution LPR déclenche un signal de sortie qui allume un panneau expliquant au conducteur qu'il doit obtenir une carte d'invité auprès du bureau de la sécurité.

Pour déclencher un événement du système de surveillance en cas de reconnaissance d'une plaque d'immatriculation ne figurant **pas** dans une liste, utilisez la liste **de plaques d'immatriculation ne figurant dans aucune liste**. Vous pouvez la sélectionner comme toute autre liste (voir "Onglet Listes de correspondance" á la page 347) pour quelque caméra que ce soit et la configurer comme toute autre liste (voir "Événements déclenchés par la solution LPR " á la page 355).

Ajouter de nouvelles listes de correspondance de plaques d'immatriculation

1. Dans le **Panneau Navigation du Site**, sélectionnez **Listes de correspondance de plaques d'immatriculation**, cliquez avec le bouton droit et sélectionnez **Ajouter nouveau**.
2. Dans la fenêtre qui s'affiche, donnez un nom à la liste et cliquez sur **OK**.

Dès que vous avez créé une liste de plaques d'immatriculation, celle-ci apparaît dans la **Liste de correspondance de plaques d'immatriculation** et dans l'onglet **Listes de correspondance** pour toutes vos caméras LPR.

3. Si vous souhaitez ajouter des colonnes à la liste de correspondances, cliquez sur **Champ personnalisé** et spécifiez les colonnes dans la fenêtre de dialogue qui s'ouvre (voir "Modifier les propriétés des champs personnalisés" á la page 355).

4. Pour mettre à jour la liste de correspondances, utilisez les boutons (voir "Modifier les listes de correspondance de plaques d'immatriculation" á la page 352) **Ajouter**, **Modifier**, **Supprimer**.

5. Au lieu de définir la liste de correspondances directement dans le Management Client, vous pouvez importer un fichier (voir "Importer/Exporter des listes de correspondance de plaques d'immatriculation" á la page 352).

6. Si vous y êtes invité, confirmez pour sauvegarder les modifications.

Modifier les listes de correspondance de plaques d'immatriculation

1. Dans le **Panneau Navigation du Site**, sélectionnez **Listes de correspondance de plaques d'immatriculation**.

2. Allez au panneau Vue d'ensemble Cliquez sur la liste pertinente.

3. La fenêtre d'**Informations concernant la liste de correspondance de plaques d'immatriculations** s'ouvre alors.

4. Pour ajouter de nouvelles lignes à votre liste, cliquez sur **Ajouter** et remplissez les champs :

   - N'incluez aucun espace.
   - Utilisez toujours des lettres majuscules.

     Exemples : *ABC123* (correct), *ABC 123* (incorrect), *abc123* (incorrect)

   - Vous pouvez utiliser des caractères génériques dans vos listes de correspondance de plaques d'immatriculation. Pour ce faire, définissez des plaques contenant plusieurs ? et la ou les lettres et/ou chiffres qui doivent apparaître à des emplacements spécifiques.

     Exemples : *?????A*, *A?????*, *???1??*, *22??33*, *A?B?C?* ou d'autres combinaisons similaires.

5. Si vous y êtes invité, confirmez pour sauvegarder les modifications.

Importer/Exporter des listes de correspondance de plaques d'immatriculation

Vous pouvez importer un fichier contenant une liste de plaques que vous souhaitez utiliser dans une liste de correspondance de plaques d'immatriculation. Vous disposez des options d'importation suivantes :

- Ajouter des plaques d'immatriculation à la liste existante.
- Remplacer la liste existante.

Cette option peut s'avérer utile si, par exemple, les listes sont gérées à partir d'un emplacement central. Toutes les installations locales peuvent ensuite être mises à jour en distribuant un fichier.

De même, vous pouvez exporter la liste complète de plaques d'immatriculation vers un emplacement externe à partir d'une liste de correspondances.

Les formats de fichiers pris en charge sont .txt ou .csv.

Pour importer :

1. Dans le **Panneau Navigation du Site**, cliquez sur **Listes de correspondance des plaques d'immatriculation** et sélectionnez la liste pertinente.
2. Pour importer un fichier, cliquez sur **Importer**.
3. Dans la fenêtre de dialogue, indiquez l'emplacement du fichier d'importation et le type d'importation. Cliquez sur **Suivant**.
4. Patientez jusqu'à ce que la confirmation s'affiche, puis cliquez sur **Fermer**.

Pour exporter :

1. Pour exporter un fichier, cliquez sur **Exporter**.
2. Dans la fenêtre de dialogue, indiquez l'emplacement du fichier d'exportation et cliquez sur **Suivant**.
3. Cliquez sur **Fermer.**
4. Vous pouvez ouvrir et modifier le fichier exporté dans Microsoft Excel, par exemple.

Propriétés des listes de correspondance des plaques d'immatriculation

Nom	Description
Nom	Affiche le nom de la liste. Si besoin, vous pouvez modifier ce nom.
Champs personnalisés	Cliquez pour indiquer les colonnes de saisie des plaques d'immatriculation auxquelles vous ou l'utilisateur du client pouvez ajouter des informations supplémentaires. Voir Champs personnalisés (propriétés) (voir "Modifier les propriétés des champs personnalisés" á la page *355*).
Rechercher	Effectuez une recherche dans la liste pour trouver des plaques d'immatriculation, chiffres, motifs ou autres éléments spécifiques similaires. Si besoin est vous pouvez utiliser *?* en tant que caractère générique unique

Nom	Description
Ajouter	Cliquez pour ajouter une plaque d'immatriculation. • N'incluez aucun espace. • Utilisez toujours des lettres majuscules. **Exemples :** *ABC123* (correct), *ABC 123* (incorrect), *abc123* (incorrect) • Vous pouvez utiliser des caractères génériques dans vos listes de plaques d'immatriculation. Pour ce faire, définissez des plaques contenant plusieurs ? et la ou les lettres et/ou chiffres qui doivent apparaître à des emplacements spécifiques. **Exemples :** *?????A*, *A?????*, *???1??*, *22??33*, *A?B?C?* et d'autres combinaisons similaires. Certaines zones régionales peuvent disposer d'exceptions à ces règles. Il peut s'agir, par exemple, de plaques personnalisées contenant des espaces. Des plaques avec deux séries de caractères qui doivent être reconnues séparément par un trait de soulignement (_). Ou encore, les plaques de certaines régions dont des lettres apparaissent sur une couleur d'arrière-plan différente sur une ou plusieurs parties de la plaque d'immatriculation. **Exemple :** 
Modifier	Cliquez pour modifier une plaque d'immatriculation. Vous pouvez sélectionner plusieurs lignes pour les modifier.
Supprimer	Cliquez pour supprimer la ou les plaques d'immatriculation sélectionnées.
Importer	Cliquez pour importer des plaques d'immatriculation à partir d'un fichier séparé par des virgules, comme, par exemple, un fichier .txt ou .csv (voir "Importer/Exporter des listes de correspondance de plaques d'immatriculation" á la page *352*).
Export	Cliquez pour exporter la liste complète de plaques d'immatriculation vers d'un fichier séparé par des virgules, comme, par exemple, un fichier .txt ou .csv (voir "Importer/Exporter des listes de correspondance de plaques d'immatriculation" á la page *352*).
Lignes par page	Sélectionnez le nombre de plaques d'immatriculation à afficher sur une page (un écran). Vous pouvez choisir entre 50 et 1 000 lignes.
Événements déclenchés par une correspondance avec une liste	Sélectionnez le ou les événements qui doivent être déclenchés par une correspondance avec une liste (voir "Événements déclenchés par la solution LPR " á la page *355*). Vous pouvez choisir parmi tous les types d'événements disponibles définis dans votre système.

Modifier les propriétés des champs personnalisés

Vous pouvez ajouter des colonnes à vos listes de correspondance des plaques d'immatriculation pour y ajouter des informations supplémentaires. Vous pouvez définir le nom et le nombre de colonnes, ainsi que le contenu des champs.

Les utilisateurs XProtect Smart Client peuvent mettre les informations à jour dans les colonnes, mais pas les colonnes en elles-mêmes.

Nom	Description
Ajouter	Ajoute une colonne dans la liste de correspondance. Saisissez un nom pour la colonne.
Modifier	Cliquez pour modifier le nom de la colonne si nécessaire.
Supprimer	Supprime une colonne.
Haut	Modifie l'ordre des colonnes.
Bas	Modifie l'ordre des colonnes.

Événements déclenchés par la solution LPR

Après avoir créé des listes de correspondance de plaques d'immatriculation (voir "Ajouter de nouvelles listes de correspondance de plaques d'immatriculation" á la page 351), vous pouvez les associer à tous les types d'événements définis dans votre système.

Le type d'événements disponible dépend de la configuration de votre système. Dans le cadre du système LPR, les événements sont utilisés pour déclencher des signaux de sortie pour lever une barrière de parking ou produire des enregistrements de haute qualité à partir des caméras, par exemple. Vous pouvez également utiliser un événement pour déclencher des combinaisons de telles actions. Voir À propos des listes de correspondance de plaques d'immatriculation (á la page 350) pour obtenir d'autres exemples d'applications.

Configurer des événements système déclenchés par des correspondances avec des listes

1. Développez **Serveurs**, cliquez sur **Liste de correspondance de plaques d'immatriculation** et sélectionnez la liste à laquelle vous souhaitez associer un événement.
2. Dans la fenêtre **Informations concernant la liste de correspondance de plaques d'immatriculation**, à côté du champ de sélection **Événements déclenchés par une correspondance avec une liste**, cliquez sur **Sélectionner**.
3. Dans la fenêtre de dialogue **Sélectionner des événements déclenchés**, sélectionnez un ou plusieurs événements.
4. Si vous y êtes invité, confirmez pour sauvegarder les modifications.
5. L'événement est maintenant associé aux reconnaissances sur la liste de correspondance de plaques d'immatriculation sélectionnée.

Pour déclencher un événement du système de surveillance en cas de reconnaissance d'une plaque d'immatriculation ne figurant **pas** dans une liste, configurez la liste de **plaques d'immatriculation ne figurant dans aucune liste**.

Alarmes déclenchées par la solution LPR

Vous pouvez associer certains types d'alarmes à des événements à partir de XProtect LPR. Procédez de la manière suivante :

1. Créez la liste de correspondance de plaques d'immatriculation (voir "Ajouter de nouvelles listes de correspondance de plaques d'immatriculation" á la page 351) par rapport à laquelle vous souhaitez vérifier les plaques d'immatriculation.
2. Ajoutez et configurez votre ou vos caméra(s) LPR (voir "Ajouter une caméra LPR" á la page 341).
3. Dans le **Panneau Navigation du Site**, développez **Alarmes**, cliquez avec le bouton droit sur **Définitions des alarmes**, et sélectionnez l'option pour créer une nouvelle alarme.
4. La fenêtre **Informations sur les définitions d'alarme** s'affiche. Sélectionnez les propriétés (voir "Définitions d'alarmes pour la solution LPR" á la page 356) pertinentes.
5. Si vous y êtes invité une fois terminé, confirmez pour sauvegarder les modifications.
6. Configurer les paramètres des données d'alarmes pour la LPR (voir "Paramètres des données d'alarmes pour la LPR" á la page 357).

Définitions d'alarmes pour la solution LPR

À l'exception de la définition des **Événements déclencheurs**, les paramètres des **Définitions d'alarme** sont les mêmes pour la LPR que pour le reste du système.

Pour définir des événements déclencheurs en lien avec la LPR, sélectionnez le message d'événement à utiliser en cas de déclenchement de l'alarme :

a) Dans le champ **Événements déclencheurs**, en haut du menu déroulant, décidez du type d'événements à utiliser pour l'alarme. La liste propose des événements (voir "Travailler avec des listes de correspondance de plaques d'immatriculation" á la page 350) de **Listes de correspondance de plaques d'immatriculation** et de **serveur LPR**.

b) Dans le deuxième menu déroulant, sélectionnez le message de l'événement spécifique à utiliser. Si vous avez sélectionné des **Listes de correspondance de plaques d'immatriculation** dans le menu déroulant situé au-dessus, sélectionnez une liste de plaques d'immatriculation. Si vous avez sélectionné **Serveur LPR**, sélectionnez le message d'événement du serveur LPR pertinent :

- Connexion avec la caméra LPR perdue
- Caméra LPR en fonctionnement
- Le serveur LPR ne répond pas
- Réponse du serveur LPR

Pour plus d'informations sur les paramètres de définition des alarmes restants, veuillez vous reporter à la rubrique **Alarmes**.

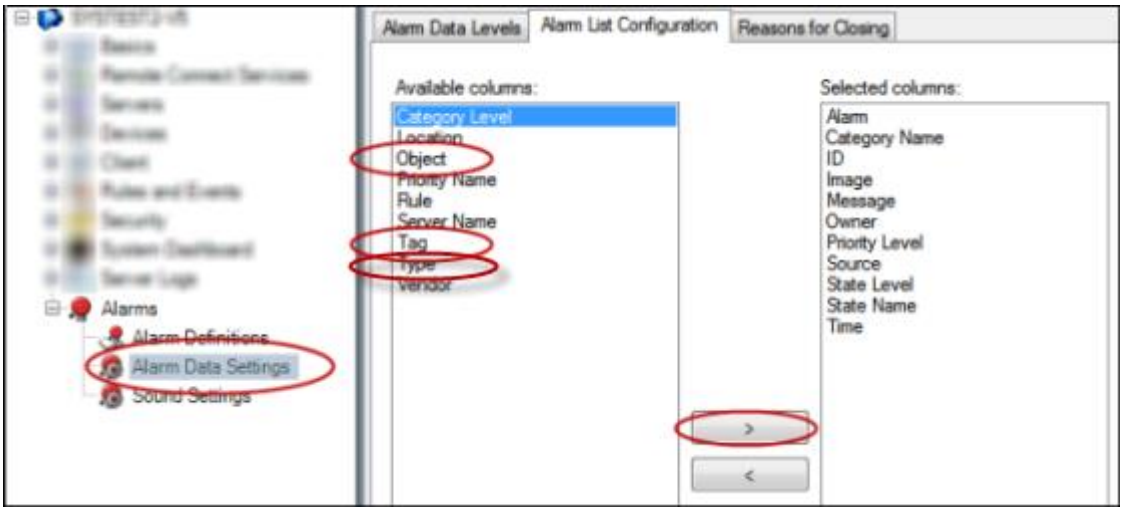
Paramètres des données d'alarmes pour la LPR

Dans le Management Client, vous devez mettre à disposition deux éléments spécifiques de **Configuration de la liste d'alarmes** pour qu'ils puissent être sélectionnés dans XProtect Smart Client.

Ces deux éléments sont utilisés pour configurer des listes d'alarmes dans l'onglet **Gestionnaire d'alarme** de XProtect Smart Client. Les éléments pertinents sont **Objet**, **Balise**, et **Type**, qui sont essentiels pour reconnaître des numéros de plaques d'immatriculation (Objet) et des codes de pays (Balise).

Dans le Management Client, procédez comme suit :

1. Dans le **Panneau Navigation du Site**, développez **Alarmes** et sélectionnez **Paramètres des données d'alarmes**.
2. Dans l'onglet de **Configuration des listes d'alarmes**, sélectionnez **Objet**, **Balise**, et **Type** puis cliquez sur **>**.



3. Si vous y êtes invité, confirmez pour sauvegarder les modifications.

Maintenance de la solution LPR

À propos de LPR Server Manager

Lorsqu'un serveur LPR est installé, vous pouvez vérifier l'état de ses services à l'aide du gestionnaire de serveur XProtect LPR. Vous pouvez, par exemple, démarrer et arrêter le Service LPR Server, consulter les messages d'état et lire les fichiers journaux.

- Vous pouvez accéder aux informations d'état du serveur LPR par le biais de l'icône **LPR Server Manager** dans la zone de notification de l'**ordinateur exécutant le serveur LPR**.

Exemple : Icône LPR Server Manager dans la zone de notification.

Dans le Management Client, vous pouvez obtenir un aperçu complet de l'état de tous vos serveurs LPR (voir "Consulter les informations relatives au serveur LPR" á la page 337).

Démarrer et arrêter le service LPR Server

Le service LPR Server démarre automatiquement après l'installation. Si vous avez arrêté le service manuellement, vous pouvez le redémarrer manuellement.

1. Cliquez sur l'icône **LPR Server Manager** avec le bouton droit de la souris dans la zone de notification.
2. Dans le menu qui s'affiche, sélectionnez **Démarrer le service LPR Server**.
3. Si nécessaire, sélectionnez **Arrêter le service LPR Server** pour arrêter le service à nouveau.

Afficher l'état du serveur LPR

1. Sur votre serveur LPR, cliquez sur l'icône **LPR Server Manager** avec le bouton droit de la souris dans la zone de notification.
2. Dans le menu qui s'affiche, sélectionnez **Afficher l'état du serveur LPR**.

   Si le système fonctionne sans problèmes, l'état sera : *Toutes les caméras LPR fonctionnent*.

   Les autres états sont :

   - *Le service ne répond pas*
   - *Pas de connexion au système de surveillance*
   - *Le service n'est pas en cours d'exécution*
   - *Le serveur d'événements n'est pas connecté*
   - *Erreur inconnue*
   - *X caméras LPR sur Y fonctionnent*

Afficher le journal du serveur LPR

Les fichiers journaux sont un outil utile pour surveiller l'état du service du serveur LPR et résoudre les problèmes y ayant trait. Toutes les entrées sont horodatées, les plus récentes étant présentées en bas.

1. Dans la zone de notification, cliquer avec le bouton droit sur l'icône **LPR Server Manager**.
2. Dans le menu qui s'affiche, sélectionnez **Afficher le fichier journal du serveur LPR**.

   Un programme d'affichage du journal présente toutes les activités horodatées du serveur.

Modifier les paramètres du serveur LPR

Le serveur LPR doit pouvoir communiquer avec le serveur de gestion de votre système. Pour ce faire, vous spécifiez l'adresse IP/nom d'hôte du serveur de gestion lors de l'installation du serveur LPR.

S'il est nécessaire de modifier l'adresse du serveur de gestion, procédez comme suit :

1. Arrêtez (voir "Démarrer et arrêter le service LPR Server" á la page 358) le service LPR Server.
2. Dans la zone de notification, cliquer avec le bouton droit sur l'icône **LPR Server Manager**.
3. Dans le menu qui apparaît, sélectionnez **Modifier les paramètres**. La fenêtre **Paramètres du service LPR Server** s'affiche.
4. Indiquez les nouvelles valeurs et cliquez sur **OK**.
5. Redémarrez le service LPR Server.

Désinstaller XProtect LPR

Si vous souhaitez supprimer XProtect LPR de votre système, désinstallez les deux composants séparément à l'aide de la procédure de suppression ordinaire de Windows :

- Pour les ordinateurs sur lesquels le module d'extension LPR est installé, désinstallez le *module d'extension Milestone XProtect LPR [version].*
- Pour les ordinateurs sur lesquels le serveur LPR est installé, désinstallez l*e serveur Milestone XProtect LPR [version].*

XProtect Transact

Introduction de XProtect Transact

À propos de XProtect Transact

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits pour de plus amples informations.

XProtect Transact est un produit complémentaire aux solutions de vidéo surveillance IP XProtect Advanced VMS et XProtect Professional VMS de Milestone.

XProtect Transact est un outil servant à observer les transactions en cours et à enquêter sur des transactions antérieures. Les transactions sont connectées aux systèmes de surveillance vidéo numériques contrôlant les transactions. Cela permet par exemple d'apporter des preuves en cas de fraude ou de vol. Il existe une relation directe entre les lignes de transaction et les images vidéo.

Les données de transaction peuvent provenir de différents types de sources. La plupart du temps, ces sources sont des systèmes de points de vente ou des distributeurs automatiques de billets.

Architecture de système XProtect Transact

Il existe plusieurs composants dans le flux de communication de XProtect Transact. Les données entrantes proviennent des caméras de vidéosurveillance et des sources de transaction fournissant les données de transaction, par exemple des caisses enregistreuses ou des distributeurs automatiques. Les données de transaction sont enregistrées sur le serveur d'événements, alors que le flux vidéo est enregistré sur le serveur d'enregistrement. Les données passent du serveur au XProtect Smart Client.

Si vous utilisez Advanced VMS, il peut y avoir plusieurs serveurs d'enregistrement.

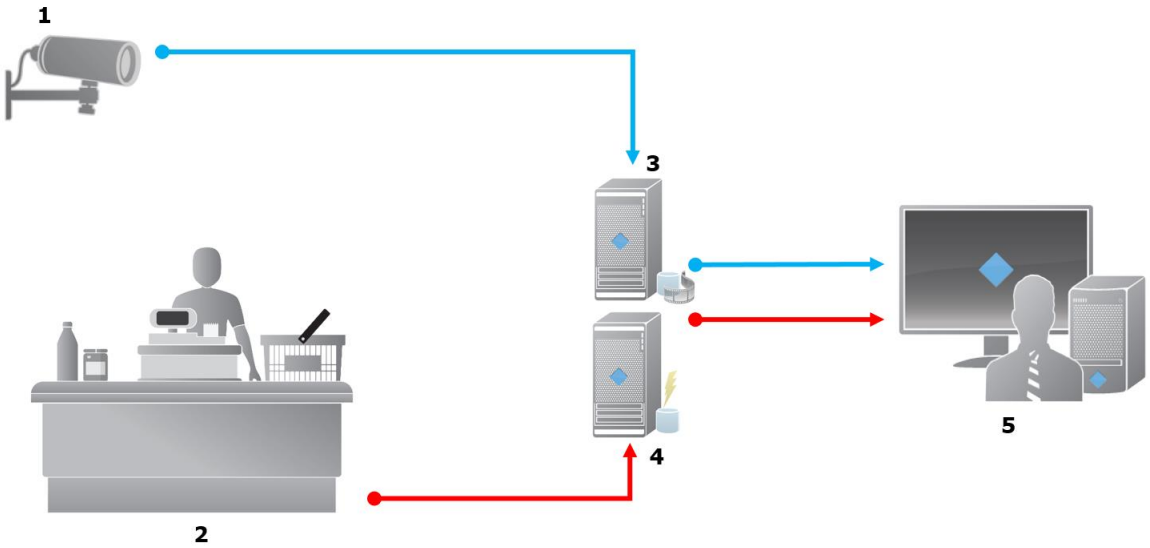


Illustration :

- 1 = Caméra.
- 2 = Caisse enregistreuse.
- 3 = Serveur d'enregistrement.
- 4 = Serveur d'événements.
- 5 = Smart Client.
- Les flèches bleues représentent les enregistrements vidéo du système de surveillance.
- Les flèches rouges représentent les données de transaction des sources de transaction.

Par défaut, XProtect Transact prend en charge deux types de sources de transactions :

- Clients de port série.
- Clients serveur TCP.

Des types supplémentaires de sources de transaction peuvent être pris en charge grâce à des connecteurs personnalisés développés par le kit de développement logiciel MIP (SDK). Par exemple, un connecteur qui récupère des données de transaction à partir d'un système de planification des ressources (ERP).

À propos des connecteurs

Un connecteur permet d'importer des données de transaction brutes à partir d'une source de transaction, par exemple le distributeur automatique, vers le serveur d'événements correspondant à l'aide de video management software.

Les connecteurs intégrés disponibles sont décrits dans le tableau suivant :

Nom	Description
Connecteur client TCP	Utilisé lorsque la source de transaction fournit les données de transaction via une interface de serveur TCP. Ce connecteur possède deux paramètres pouvant être spécifiés : nom d'hôte et numéro de port.
Connecteur de port série	Utilisé lorsque les données de transaction arrivent sur le port de série sur le serveur d'événements.

Des connecteurs mis au point par le kit de développement logiciel (MIP) sont aussi disponibles.

Voir également

Ajouter une source de transaction (assistant)

À propos des définitions de transactions

Une définition de transaction est un groupe de paramètres vous permettant de contrôler l'affichage des enregistrements vidéo et des données brutes provenant des sources de transaction sur XProtect Smart Client. La sortie est dans un format lisible ressemblant à un vrai ticket. Par exemple, un ticket de caisse ou un ticket de distributeur automatique.

Plus précisément, les définitions de transaction vous permettent de :

- définir le début et la fin de chaque transaction.
- insérer des sauts de ligne le cas échéant.
- supprimer les caractères non désirés ou les chaînes de texte, par exemple si les données proviennent d'une d'imprimante et contiennent des caractères ne pouvant pas être imprimés comme les caractères indiquant un saut de page ou l'extrémité du ticket.
- remplacer des caractères par d'autres caractères.

Vous pouvez utiliser la même définition de transaction pour plusieurs sources de transaction.

Voir également

Ajouter des définitions de transaction

À propos des événements de transaction

Un événement de transaction correspond à l'occurrence de mots, de chiffres ou de caractères spécifiques dans le flux de données de transaction circulant des sources de transactions, telles que les caisses, vers le serveur d'événements. En tant qu'administrateur de système, vous devez définir ce que sont ces événements. Ceci permet à l'opérateur de suivre les événements de transaction dans XProtect et de mener des enquêtes à leur sujet. Pour chaque événement, une méthode (type de correspondance) doit être spécifiée afin d'identifier des chaînes dans les données de transaction : correspondance exacte, symbole de remplacement ou expression régulière.

Voir également

Définir un événement de transaction (voir "Définir des événements de transaction" á la page 368)

Créer une alarme de transaction (voir "Créer des alarmes basées sur des événements de transaction" á la page 369)

Compatibilité

XProtect Transact 2016 est compatible avec la version 2016 des produits suivants :

- XProtect Corporate
- XProtect Expert

Démarrage

La fonctionnalité XProtect Transact est standard sur Management Client. Les fonctions seront disponibles immédiatement après avoir activé la licence de base et les licences de source de transaction. Avant d'utiliser les fonctions XProtect Transact dans XProtect Smart Client, vous devriez :

1. Vérifier que votre licence de base pour XProtect Transact a été activée. Vérifier que vous disposez d'une licence de source de transaction pour chaque source nécessaire pour contrôler. Les informations sur la licence sont disponibles sous le nœud **Bases**.

   Si vous ne possédez pas le nombre suffisant de licences de source de transactions, assurez-vous d'obtenir des licences supplémentaires avant l'expiration de la période de grâce de 30 jours.

2. Ajoutez et configurez les sources fournissant les données de transaction, par exemple les caisses enregistreuses. Pour en savoir plus, consultez la rubrique Ajouter une source de transaction (assistant) (á la page 363).

3. (facultatif) Définissez les événements de transaction et configurez-les pour déclencher des règles ou des alarmes. Dans XProtect Smart Client, l'opérateur peut enquêter les événements de transaction.

Même si vous n'avez pas acheté de licences XProtect Transact, vous pouvez essayer XProtect Transact avec une licence d'essai. Pour plus d'informations, consultez la rubrique Licence d'essai XProtect Transact (á la page 362).

Voir également

Configurer des transactions :

Configurer des transactions : (voir "Configuration d'alarmes et d'événements de transaction" á la page 368)

Licence d'essai XProtect Transact

Avec une licence d'essai XProtect Transact, vous pouvez essayer la fonction XProtect Transact pendant 30 jours. Toutes les fonctions associées sont activées et vous pouvez ajouter une source de transaction, par exemple une caisse enregistreuse. Au terme de la période d'essai de 30 jours, toutes les fonctions XProtect Transact sont désactivées, y compris l'espace de travail **Transact** et les éléments de vue de transaction. Après l'achat et l'activation d'une licence de base XProtect Transact et des licences de source de transaction nécessaires, vous pouvez à nouveau utiliser XProtect Transact, et vos paramètres et données sont conservés.

Si vous utilisez des produits de la suite de produit Advanced VMS, vous devez obtenir la licence d'essai auprès de Milestone. L'administrateur du système doit activer la licence d'essai dans la configuration.

Si vous utilisez des produits de la suite de produit Professional VMS, la licence d'essai est déjà comprise. La licence d'essai est activée lorsque les administrateurs du système ajoutent une source de transaction dans la configuration.

Configuration XProtect Transact

Configurer des transactions :

Dans cette section, vous apprendrez comment ajouter et configurer les sources de transaction et comment créer les définitions de transaction.

Ajouter une source de transaction (assistant)

Pour connecter des données d'une source de transaction à XProtect Transact, vous devez ajouter les sources de transaction, par exemple un distributeur automatique. Dans l'assistant, sélectionnez un connecteur pour connecter une ou plusieurs caméras.

Si vous ne possédez pas de licence de source de transaction pour la source que vous souhaitez ajouter, le système fonctionnera pendant les 30 jours de la période de grâce. Assurez-vous d'obtenir une licence de source de transaction supplémentaire et de l'activer à temps.

Étapes :

1. Dans le **Panneau Navigation du Site**, développez **Transact**.
2. Allez au panneau Vue d'ensemble Cliquez sur le nœud **Sources de transaction** avec le bouton droit de la souris et sélectionnez **Ajouter une source**. L'assistant apparaît.
3. Suivez les instructions présentées dans l'assistant.
4. En fonction du connecteur sélectionné, vous devez remplir différents champs. Pour plus d'informations, voir la rubrique Sources de transaction (propriétés) (á la page 363). Vous pouvez modifier ces paramètres une fois l'assistant terminé.
5. Si la définition de transaction nécessaire n'est pas disponible, cliquez sur **Ajouter nouvelle** pour créer une nouvelle définition de transaction.

Voir également

Ajouter des définitions de transaction

À propos des connecteurs

Sources de transaction (propriétés)

Les paramètres pour les sources de transaction sont décrits dans le tableau.

Nom	Description
Activer	Si vous souhaitez désactiver la source de transaction, décochez cette case. Le flux de données de transaction s'arrête, mais les données déjà importées restent sur le serveur d'événements. Vous pouvez toujours afficher les transactions des sources de transaction désactivées dans XProtect Smart Client au cours de sa durée de rétention. Même une source de transaction désactivée nécessite une licence de source de transaction.
Nom	Si vous souhaitez modifier le nom, veuillez saisir un nouveau nom ici.
Connecteur	Vous ne pouvez pas modifier le connecteur sélectionné lors de la création de la source de transaction. Pour sélectionner un connecteur différent, vous devez créer une nouvelle source de transaction et sélectionnez le connecteur désiré au cours de l'assistant d'installation.
Définition de la transaction	Vous pouvez sélectionner une définition de transaction différente qui définit comment transformer les données de transaction en transactions et en lignes de transaction. Ceci définit : • le début et la fin de la transaction. • l'affichage des transactions dans XProtect Smart Client.
Durée de rétention	Précisez le nombre de jours durant lesquels les données de transaction seront conservées sur le serveur d'événements. La durée de rétention par défaut est de 30 jours. Une fois la durée de rétention expirée, les données sont supprimées automatiquement. Ceci permet de ne pas dépasser la capacité de stockage de la base de données. La valeur minimum est 1 jour et la valeur maximum est 1000 jours.
Connecteur client TCP	Si vous avez sélectionné le **connecteur client TCP**, veuillez spécifier les paramètres suivants : • **Nom d'hôte** : saisissez le nom d'hôte du serveur TCP correspondant à la source de transaction. • **Port** : saisissez le nom du port du serveur TCP correspondant à la source de transaction.

Nom	Description
Connecteur de port série	Si vous avez sélectionné le **Connecteur de port série**, veuillez spécifier ces paramètres et vous assurer qu'ils correspondent aux paramètres de la source de transaction : • **Port série** : sélectionnez le port COM. • **Vitesse de transmission** : veuillez préciser le nombre d'octets transmis par seconde. • **Parité** : veuillez préciser la méthode de détection des erreurs dans les transmissions. Par défaut, l'option **Aucun** est sélectionnée. • **Bits de données** : veuillez préciser le nombre d'octets utilisés pour représenter un caractère de données. • **Bits d'arrêt** : veuillez spécifier le nombre d'octet pour indiquer lorsqu'un octet est transmis. La plupart des périphériques nécessite 1 octet. • **Établissement d'une liaison** : veuillez préciser la méthode de liaison pour déterminer le protocole de communication entre la source de transaction et le serveur d'événements.

Voir également

Ajouter une source de transaction (assistant) (á la page 363)

Ajouter des définitions de transaction

Ajouter des définitions de transaction

Pour définir une source de transaction, vous devez préciser une définition de la source. Une définition transforme les données brutes en données présentables, afin que les utilisateurs puissent afficher les données dans XProtect Smart Client dans un format qui correspond aux vrais tickets de caisse. Ceci est nécessaire car les données brutes prennent généralement la forme d'une seule série de données, et il est parfois difficile d'identifier le début et la fin de chaque transaction.

Étapes :

1. Dans le **Panneau Navigation du Site**, développez **Transact**.
2. Sélectionner des **Définitions de transaction**.
3. Allez au panneau Vue d'ensemble Cliquez sur **Définition de transaction** avec le bouton droit de la souris et sélectionnez **Ajouter une nouvelle**. Plusieurs paramètres apparaissent dans la section **Propriétés**.
4. Utilisez les champs **Tendance de début** et **Tendance de fin** pour spécifier les données qui définissent le début et la fin de chaque ticket.
5. Cliquez sur **Démarrer la collecte des données** pour recueillir les données brutes de la source de données connectée. Plus vous recueillez des données, moins vous avez de chance de rater les caractères que vous souhaitez remplacer ou omettre, par exemple des caractères de contrôle.

6. Dans la section **Données brutes**, sélectionnez les caractères que vous souhaitez remplacer ou omettre. Si vous voulez saisir les caractères manuellement, sautez cette étape et cliquez sur **Ajouter un filtre.**
7. Cliquez sur **Ajouter un filtre** pour définir l'affichage des caractères sélectionnés des données de source de transaction dans XProtect Smart Client.
8. Pour chaque filtre, sélectionnez une action pour déterminer la manière de transformer les caractères. La section **Aperçu** vous donne un aperçu de l'affichage des données avec les filtres définis.

Pour obtenir des informations détaillées au sujet des champs, voir Définitions de transaction (propriétés) .

Vous pouvez également charger des données préalablement recueillies et stockées dans votre ordinateur. Pour ce faire, cliquez sur **Charger à partir d'un fichier**.

Définitions de transaction (propriétés)

Les paramètres pour les définitions de transaction sont décrits dans le tableau.

Nom	Description
Nom	Saisissez un nom.
Encodage	Sélectionnez le jeu de caractères utilisé par la source de transaction, par exemple la caisse. Ceci aide XProtect Transact à convertir les données de transaction en texte intelligible que vous pouvez utiliser lors de la configuration de la définition. Si vous sélectionnez le mauvais encodage, il se peut que les données soient inintelligibles.
Démarrer la collecte des données	Collecte des données de transaction à partir de la source de transaction connectée. Vous pouvez utiliser les données pour configurer une définition de transaction. Attendez qu'une (ou plusieurs de préférence) transaction soit terminée.
Arrêter la collecte des données	Lorsque vous avez recueilli suffisamment de données pour configurer la définition, cliquez sur ce bouton.
Charger à partir d'un fichier	Si vous souhaitez importer des données d'un fichier existant, cliquez sur ce bouton. C'est habituellement un fichier que vous avez créé en format .capture. Bien qu'un autre format soit possible. Le plus important c'est que l'encodage du fichier importé corresponde à l'encodage sélectionné pour la définition en cours.
Enregistrer dans un fichier	Si vous souhaitez enregistrer les données brutes dans un fichier, cliquez sur ce bouton. Vous pourrez toujours les réutiliser ultérieurement.

Nom	Description
Type de correspondance	Sélectionnez le type de correspondance à utiliser pour rechercher le masquage de début et de fin dans les données brutes recueillies : • Utiliser une correspondance exacte : La recherche identifie les séries qui contiennent exactement ce que vous avez saisi dans les champs **Masquage de début** et **Masquage de fin**. • Utiliser des jokers : La recherche identifie les séries qui contiennent ce que vous avez saisi dans les champs **Masquage de début** et **Masquage de fin** en présence d'un symbole joker (*, #, ?). * correspond à n'importe quel nombre de caractères. Par exemple, si vous avez saisi "Commencer la tra*tion", la recherche identifie les séries qui contiennent "Commencer la transaction". # correspond à un chiffre. Si vous avez saisi "# pastèque", la recherche identifie les séries qui contiennent par exemple "1 pastèque". ? correspond à un caractère. Par exemple, vous pouvez saisir "Commencer la trans?ction" pour identifier les séries qui contiennent "Commencer la transaction". • Utiliser une expression régulière : Utilisez ce type de correspondance pour identifier les séries qui contiennent des méthodes ou conventions de notation spécifiques, par exemple un format de date ou un numéro de carte bancaire. Pour plus d'informations, voir le site web de Microsoft https://msdn.microsoft.com/en-us/library/az24scfc(v=vs.110).aspx.
Données brutes	Les séries de données de transaction provenant de la source de transaction connectée s'affichent dans cette section.
Masquage de début	Précisez un masquage de début pour indiquer le début de la transaction. Les lignes horizontales sont insérées dans le champ **Aperçu** afin de visualiser le début et la fin de la transaction. Elles permettront également de séparer les différentes transactions.
Masquage de fin	Précisez un masquage de fin pour indiquer la fin de la transaction. Un masquage de fin n'est pas obligatoire mais peut s'avérer utile si les données reçus contiennent des informations inutiles entre chaque transaction, telles que des informations relatives aux heures d'ouverture ou aux offres spéciales. Si vous ne précisez pas de masquage de fin, la fin du ticket de caisse sera définie en fonction du début du ticket suivant. Le début du ticket est défini par le champ de **Masquage de début**.

Nom	Description
Ajouter un filtre	Utilisez le bouton **Ajouter un filtre** pour indiquer les caractères à omettre dans XProtect Smart Client ou à remplacer par d'autres caractères ou un saut de ligne. Le fait de remplacer des caractères s'avère utile lorsque la série de la source de transaction contient des caractères de commande n'étant pas destinés à être imprimés. Il est nécessaire d'ajouter un saut de ligne pour reproduire l'apparence du ticket d'origine dans XProtect Smart Client.
Filtrer le texte	Affiche les caractères sélectionnés dans la section des **Données brutes**. Si vous souhaitez omettre ou remplacer des caractères qui ne sont pas présents dans la série des données brutes recueillies, vous pouvez les saisir manuellement dans le champ **Caractère.** S'il s'agit d'un caractère de commande, vous devez saisir sa valeur d'octet hexadécimale. Utilisez ce format pour la valeur d'octet : {XX} et {XX,XX,...} si le caractère contient plus d'un octet.
Action	Pour chaque filtre ajouté, vous devez préciser la manière dont les caractères sélectionnés sont traités : • Omettre : les caractères sélectionnés sont omis. • Remplacer : les caractères sélectionnés sont remplacés par les caractères spécifiés. • Ajouter un saut de ligne : les caractères sélectionnés sont remplacés par un saut de ligne.
Substitution	Saisissez le texte devant remplacer les caractères sélectionnés. Uniquement requis si vous avez sélectionné l'action **Remplacer**.
Aperçu	Utilisez la section **Aperçu** pour vérifier que vous avez identifié et filtré les caractères non désirés. Le résultat ressemble à un vrai ticket de caisse dans XProtect Smart Client.

Voir également

Ajouter des définitions de transaction

Configuration d'alarmes et d'événements de transaction

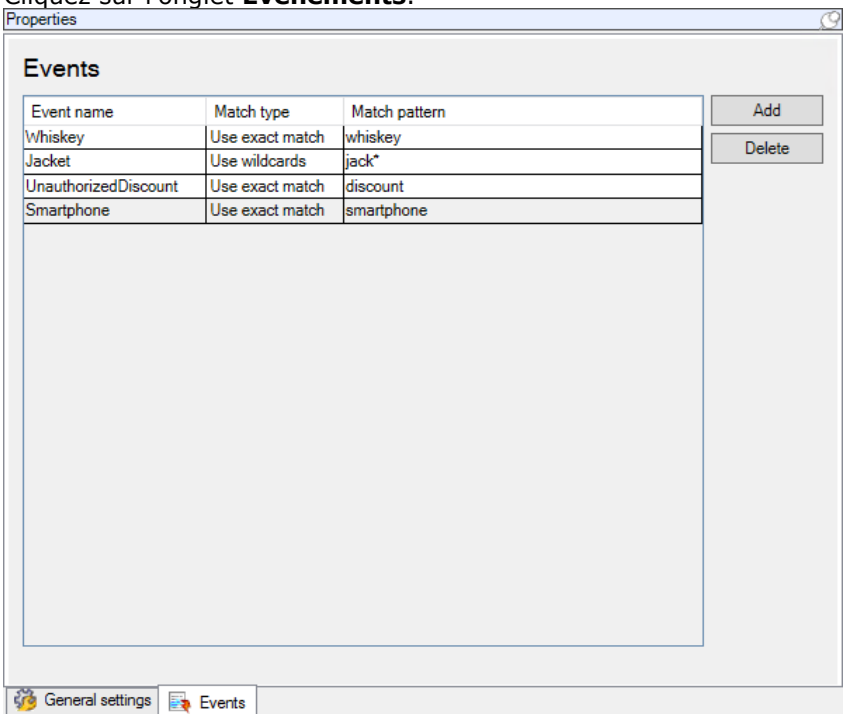
Dans cette section, vous apprendrez comment définir des événements de transaction et configurer des alarmes.

Définir des événements de transaction

Pour suivre des événements de transaction dans XProtect Smart Client et mener des enquêtes à leur sujet, vous devez d'abord définir ce que sont ces événements. Il peut s'agir, par exemple, de l'acquisition d'un smartphone. Vous pouvez définir les événements de transaction à partir d'une définition de transaction, de sorte que les événements définis s'appliquent à toutes les sources de transactions, telles que les caisses, utilisant la définition de transaction.

Étapes :

1. Dans le **Panneau Navigation du Site**, développez **Transact**.
2. Allez au panneau Vue d'ensemble Sélectionnez la définition de transaction, dans laquelle vous souhaitez définir un événement.
3. Cliquez sur l'onglet **Événements**.



4. Dans le volet **Propriétés**, cliquez sur **Ajouter**. Une nouvelle ligne apparaît.
5. Saisissez un nom d'événement.
6. Sélectionnez le type de correspondance à utiliser pour identifier une chaîne spécifique des données de transaction en tant qu'événement. Vous pouvez faire votre choix parmi une correspondance exacte, des symboles de remplacement et des expressions régulières. Pour de plus amples informations, voir la description du type de correspondance dans la Définitions de transaction (propriétés) .
7. Dans la colonne **Mode de correspondance**, spécifiez ce que vous souhaitez que le système identifie comme un événement, « smartphone » par exemple.
8. Pour chaque événement, répétez les étapes ci-dessus.

Voir également

À propos des règles et événements (á la page 174)

À propos des définitions de transactions (á la page 361)

Créer des alarmes basées sur des événements de transaction

Pour notifier l'opérateur XProtect Smart Client lorsqu'un événement de transaction spécifique a lieu, vous devez d'abord créer une alarme de transaction dans Management Client. L'alarme apparaîtra dans l'onglet **Gestionnaire d'alarme** dans XProtect Smart Client pour permettre à l'opérateur de mener une enquête au sujet de l'événement et, si nécessaire, de prendre des mesures.

Étapes :

1. Dans le **Panneau Navigation du Site**, développez **Alarmes**.
2. Allez au panneau Vue d'ensemble Cliquez sur le nœud **Définitions des alarmes** avec le bouton droit de la souris et sélectionnez**Ajouter nouveau...**. Les paramètres du volet **Propriétés** sont activés.
3. Saisissez un nom pour l'alarme et, dans le champ **Description**, vous pouvez ajouter des instructions sur les mesures que l'opérateur XProtect Smart Client devrait prendre.
4. Dans le menu déroulant **Événements de transaction**, sélectionnez **Événements de transaction.**
5. Dans le menu déroulant situé en dessous d'**Événements de transaction**, sélectionnez l'événement spécifique.
6. Dans le champ **Sources**, cliquez sur le bouton **Sélectionner...**. Une fenêtre contextuelle s'affiche.
7. Cliquez sur l'onglet **Serveur** et sélectionnez la source de transactions.
8. Spécifiez des paramètres supplémentaires. Pour de plus amples informations, voir Définitions des alarmes (voir "Définitions d'alarmes (Propriétés)" á la page 264).

Voir également

Définir des événements de transaction (á la page 368)

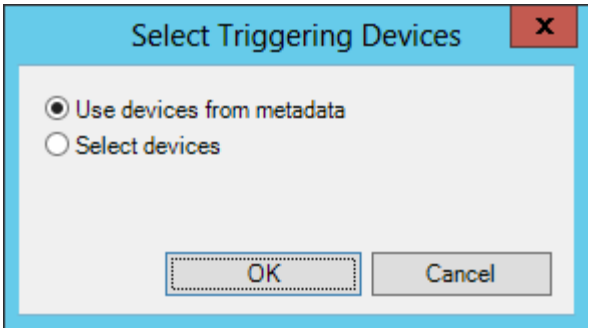
Configurer des règles pour un événement

Pour déclencher une action lorsqu'un événement de transaction spécifique se produit, vous devez configurer une règle, pour laquelle vous sélectionnez un événement et indiquez ce que vous souhaitez voir se produire. Il peut s'agir du déclenchement de l'enregistrement sur une caméra ou de l'envoi d'un e-mail, par exemple.

Étapes :

1. Dans le **Panneau Navigation du Site**, développez **Règles et événements**.
2. Allez au panneau Vue d'ensemble Cliquez sur **Règles** avec le bouton droit de la souris et sélectionnez **Ajouter une règle...**. Un assistant apparaît.
3. Suivez les instructions présentées dans l'assistant.
4. Assurez-vous que le bouton radio **Réaliser une action lors de l'événement <event>** est sélectionné.
5. Sélectionnez l'événement de transaction sous **Transact** > **Événements de transaction**.
6. Si une action implique un enregistrement et si vous souhaitez utiliser les caméras associées aux sources de transactions, telles que des caisses, sélectionnez le bouton radio **Utiliser les périphériques à partir de métadonnées** dans la fenêtre de dialogue apparaissant

dans l'assistant.



Voir également

Définir des événements de transaction (á la page 368)

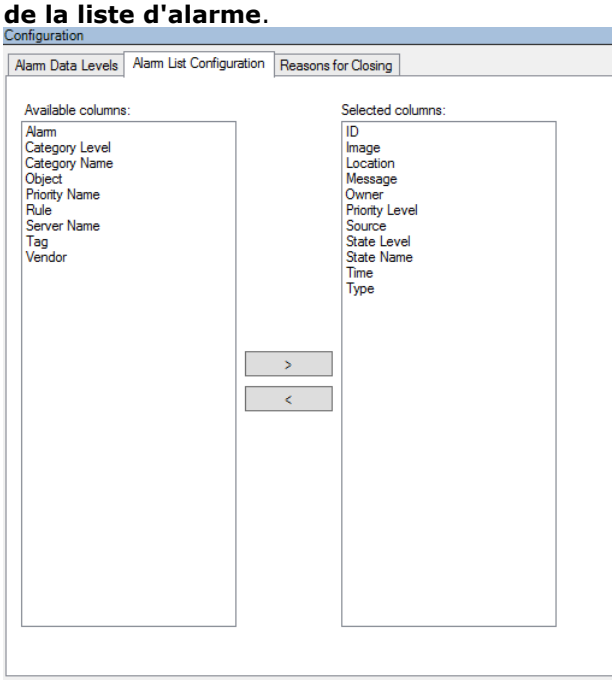
À propos des règles et événements (á la page 174)

Activer le filtrage des événements de transaction ou des alarmes

Si vous souhaitez que l'opérateur XProtect Smart Client soit en mesure de filtrer des événements ou des alarmes par transactions, vous devez d'abord activer le champ **Type** dans Management Client. Une fois activé, le champ est disponible dans la section des filtres de l'onglet **Gestionnaire d'alarmes** dans XProtect Smart Client.

Étapes :

1. Dans le **Panneau Navigation du Site**, développez **Alarmes**
2. Sélectionnez **Paramètres des données de l'alarme** et cliquez sur l'onglet **Configuration de la liste d'alarme**.



3. Dans la section **Colonnes disponibles**, sélectionnez le champ **Type**.
4. Ajoutez le champ aux **Colonnes sélectionnées**.

5. Sauvegardez les modifications apportées. Maintenant, le champ est disponible dans XProtect Smart Client.

Maintien de la configuration de transaction

Dans cette section, vous apprendrez comment modifier, désactiver et supprimer des sources de transaction.

Modifier les paramètres de source de transaction

Une fois la source de transaction ajoutée, vous pouvez modifier le nom ou sélectionner une définition de transaction différente. Selon le connecteur sélectionné, vous pouvez modifier des paramètres supplémentaires, par exemple le nom d'hôte et le numéro de port d'un serveur TCP connecté. Vous pouvez également désactiver la source de transaction. Ceci interrompra le flux des données de transaction de la source au serveur d'événements.

Une fois le connecteur sélectionné, vous ne pourrez pas le modifier.

Étapes :

1. Dans le **Panneau Navigation du Site**, développez **Transact**.
2. Sélectionnez les **Sources de transaction**.
3. Allez au panneau Vue d'ensemble Cliquez sur la source de transactions. Les propriétés s'affichent.
4. Apportez les modifications nécessaires et enregistrez-les. Pour en savoir plus, consultez la rubrique Sources de transaction (propriétés) (á la page 363).

Voir également

Ajouter une source de transaction (assistant)

Désactiver les sources de transaction (á la page 372)

Désactiver les sources de transaction

Vous pouvez désactiver une source de transaction, par exemple si un distributeur automatique est temporairement indisponible ou si le service d'une caisse est désactivé. Le flux des données de transaction vers le serveur d'événements est interrompu.

Étapes :

1. Dans le **Panneau Navigation du Site**, développez **Transact**.
2. Sélectionnez les **Sources de transaction**.
3. Allez au panneau Vue d'ensemble Cliquez sur la source de transactions. Les propriétés s'affichent.
4. Décochez la case **Activer** et enregistrez les modifications. La source de transaction est désactivée.

Voir également

Ajouter une source de transaction (assistant)

Supprimer la source de transaction (voir "Supprimer les sources de transaction" á la page 373)

Supprimer les sources de transaction

Vous pouvez supprimer les sources de transaction que vous avez ajoutées. Les données de transaction enregistrées provenant de la source sont supprimées du serveur d'événements.

Alternativement, vous pouvez désactiver la source de transaction pour éviter de supprimer des données de transaction enregistrées. Une source de transaction désactivée nécessite aussi une licence de source de transaction.

Étapes :

1. Dans le **Panneau Navigation du Site**, développez **Transact**.
2. Sélectionnez les **Sources de transaction**.
3. Allez au panneau Vue d'ensemble Cliquez sur **Sources de transaction**. Faites un clic droit sur la source que vous souhaitez supprimer.
4. Sélectionnez **Supprimer.** Une fenêtre de dialogue s'affiche.
5. Cliquez sur **OK** pour confirmer la suppression de la source de transaction.

Voir également

Ajouter une source de transaction (assistant)

Vérifier la configuration de XProtect Transact

Une fois la configuration de XProtect Transact et de ses composants terminée, vous pouvez vérifier que Transact fonctionne correctement dans XProtect Smart Client.

1. Vérifiez que toutes les sources de transaction nécessaires ont été ajoutées correctement dans Management Client :
    1. Ouvrez XProtect Smart Client et cliquez sur l'onglet **Transact**.
    2. Cliquez sur le menu déroulant **Toutes les sources** et vérifiez que toutes les sources de transaction apparaissent.
2. Vérifiez que toutes les définitions de transaction ont été correctement configurées dans Management Client. Si la configuration est bonne, il existe un ticket par transaction et les sauts de ligne sont corrects :
    1. Ouvrez XProtect Smart Client et cliquez sur l'onglet **Transact**.
    2. Sélectionnez une source de transaction active et cliquez sur  . Les lignes de transaction d'aujourd'hui apparaissent.
    3. Cliquez sur une ligne pour afficher le ticket et les enregistrements vidéo correspondants.
3. Vérifiez que les événements de transaction sont correctement configurés :

1. Définissez un événement de test de transaction dans Management Client, par exemple un article qui sera certainement acheté et enregistré sur une source de transaction connectée, comme une caisse par exemple.
2. Une fois l'événement terminé, ouvrez XProtect Smart Client et cliquez sur l'onglet **Gestionnaire d'alarme**.
3. Ouvrez la liste des alarmes et sélectionnez **Événement**. Les événements les plus récents s'affichent en haut de la liste. L'événement de test que vous avez créé apparaît dans la liste.

Milestone Mobile

Présentation de Milestone Mobile

À propos de Milestone Mobile

Milestone Mobile est constitué de trois composants :

- **Client Milestone Mobile**
- **Serveur Milestone Mobile**
- **Module d'extension Milestone Mobile**

Le client Milestone Mobile est une application de surveillance mobile que vous pouvez installer et utiliser sur votre périphérique Android, Apple ou Windows 8. Vous pouvez utiliser autant d'installations du client Milestone Mobile que nécessaire.

Pour de plus amples informations, téléchargez le guide de l'utilisateur du client Milestone Mobilesur le site Internet http://www.milestonesys.com/support/manuals-and-guides/ de Milestone Systems.

Le serveur Milestone Mobile et le module d’extension Milestone Mobile sont abordés dans ce manuel.

Pré-requis pour l'utilisation de Milestone Mobile

Avant de pouvoir commencer à utiliser Milestone Mobile, vous devez vous assurer d'avoir les éléments suivants :

- Un VMS en fonctionnement, installé et configuré avec au moins un utilisateur.
- Des caméras et des vues configurées dans XProtect® Smart Client.
- Un périphérique portable fonctionnant sous Android, iOS ou Windows 8, avec accès à Google Play, l'App Store℠ ou le Windows Phone Store, sur lequel vous pouvez télécharger l'application du client Milestone Mobile.

Configuration Milestone Mobile

À propos du serveur Milestone Mobile

Le serveur Milestone Mobile gère les ouvertures de session sur le système à partir du client Milestone Mobile à partir d'un appareil mobile ou XProtect Web Client.

Un serveur Milestone Mobile distribue les flux vidéo des serveurs d'enregistrement vers les clients Milestone Mobile. Ainsi, la configuration est sécurisée, dans la mesure où les serveurs d'enregistrements ne sont jamais connectés à Internet. Lorsqu'un serveur Milestone Mobile reçoit des flux vidéo des serveurs d'enregistrement, il gère également la conversion complexe des codecs et des formats permettant la diffusion de vidéos sur le périphérique mobile.

Vous devez installer le serveur Milestone Mobile sur n'importe quel ordinateur à partir duquel vous souhaitez accéder aux serveurs d'enregistrement. Lorsque vous installez le serveur Milestone

Mobile, assurez-vous de vous connecter à l'aide d'un compte doté de droits d'administrateur. Autrement, il est possible que votre installation échoue.

À propos de Milestone Federated Architecture et des serveurs maître/asservi

Si votre système prend en charge Milestone Federated Architecture ou les serveurs en configuration maître/asservi, vous pouvez accéder à ces serveurs à l'aide de votre client Milestone Mobile. Utilisez cette fonction pour accéder à toutes les caméras de tous les serveurs asservis en vous connectant au serveur maître.

Dans une configuration Milestone Federated Architecture, vous accédez aux sites enfants par le biais du site central. Installez le serveur Milestone Mobile uniquement sur le site central.

Autrement dit, lorsque des utilisateurs du client Milestone Mobile se connectent à un serveur pour voir les caméras de tous les serveurs de votre système, ils doivent se connecter à l'adresse IP du serveur maître. Les utilisateurs doivent disposer de droits d'administrateur sur tous les serveurs du système afin que les caméras s'affichent dans le client Milestone Mobile.

Ajouter ou modifier un serveur Mobile

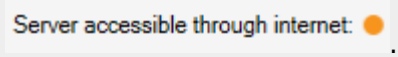
1. Aller dans **Serveurs** > **Serveurs mobiles.** Sélectionnez **Créer nouveau** dans le menu qui s'affiche. Saisissez ou modifiez les paramètres.

Important : Si vous modifiez les paramètres **Procédé de connexion**, **Toutes les caméras** et **Sorties et événements**, alors que vous ou d'autres personnes êtes connecté(e)(s) au client Milestone Mobile, vous devez redémarrer le client Milestone Mobile pour que les nouveaux paramètres prennent effet.

Configurer Smart Connect

Activez le dispositif de découverte Plug and Play universel sur votre routeur

Pour faciliter la connexion d'appareils mobiles sur les serveurs Milestone Mobile, vous pouvez activer la fonction Plug and Play universelle (UPnP) sur votre routeur. UPnP permet au serveur Milestone Mobile de configuration automatiquement le transfert de port. Cependant, vous pouvez également configurer le transfert de port manuellement sur votre routeur à l'aide de son interface web. Le processus de configuration de cartographie des ports peut varier selon le routeur. Si vous n'êtes pas sûr(e) de savoir comment configurer le transfert de ports sur votre routeur, veuillez consulter la documentation pour ce périphérique.

Remarque : Toutes les cinq minutes, le service du serveur Milestone Mobile vérifie que le serveur est mis à la disposition des utilisateurs sur Internet. L'état s'affiche dans le coin supérieur gauche du volet **Propriétés** : 

.

Configuration

- Votre serveur Milestone Mobile doit utiliser une adresse IP publique. L'adresse peut être statique ou dynamique, mais il est généralement conseillé d'utiliser des adresses IP statiques.
- Vous devez disposer d'une licence valide pour Smart Connect.

Configurer les paramètres de connexion

1. Dans Management Client, dans le volet de navigation, développez **Serveurs**, et sélectionnez **Mobile Server**.
2. Sélectionnez le serveur mobile puis cliquez sur l'onglet **Connectivité**.
3. Utilisez les options du groupe **Général** pour spécifier les éléments suivants :
   - Pour faciliter la connexion de périphériques mobiles sur les serveurs Milestone Mobile pour les utilisateurs, cochez la case **Activer Smart Connect**.
   - Spécifiez le protocole à utiliser dans le champ **Type de connexion**.
   - **Remarque :** Si vous activez les connexions sécurisées, les périphériques utilisant iOS 9.0 ou une version ultérieure, ou un téléphone Windows Phone, ne peuvent se connecter que si vous détenez un certificat émis par une autorité de certification (CA) installée sur votre serveur Milestone Mobile. Les CAs émettent des certificats numériques qui vérifient les identités des utilisateurs et les sites Internet qui échangent des données sur Internet. Parmi les exemples de CAs, on compte des sociétés telles que Comodo, Symantec et GoDaddy.
   - Avec d'activer les connexions sécurisées, assurez-vous de bien vous familiariser avec les certificats numériques. Pour apprendre comment ajouter un certificat sur le serveur Milestone Mobile, voir Modifier les certificats (voir "Modifier le certificat" á la page 392).
   - Spécifiez le nombre de secondes avant que la connexion expire.
   - Pour permettre aux périphériques mobiles de trouver les serveurs Milestone Mobile se trouvant à proximité, cochez la case **Activer la découverte UPnP**.
   - Pour activer des routeurs afin d'acheminer les périphériques mobiles vers un port spécifique, cochez la case **Activer la cartographie automatique des ports**.

Envoyez un message par e-mail pour aider les utilisateurs à se connecter

Vous pouvez faciliter l'introduction de Milestone Mobile pour vos utilisateurs en leur envoyant un e-mail contenant des informations de connexion. Vous pouvez envoyer le message directement à partir de Management Client, ou vous pouvez copier l'information vers le programme de messagerie que vous utilisez.

1. Dans le champ **Invitation par e-mail à**, saisissez l'adresse e-mail du destinataire, puis spécifiez une langue.
2. Ensuite, suivrez l'une de ces méthodes :
   - Pour envoyer le message, cliquez sur **Envoyer**.
   - Copiez les informations vers le programme de messagerie que vous utilisez.

Activez les connexions sur un réseau complexe

Si vous avez un réseau complexe doté de paramètres personnalisés, vous pouvez fournir les informations dont les utilisateurs ont besoin pour se connecter.

Dans le groupe **Accès Internet**, spécifiez les éléments suivants :

- Si vous utilisez la cartographie de ports UPnP pour diriger les connexions vers une connexion spécifique, cochez la case **Configurer un accès personnalisé à Internet**. Ensuite, fournissez l'**adresse IP ou le nom d'hôte**, et le port à utiliser pour la connexion.

Par exemple, vous devrez peut-être procéder ainsi si votre routeur ne prend pas en charge UPnP ou si vous avez une chaîne de routeurs.

- Si vos adresses IP changent souvent, cochez la case **Vérifier pour une récupération dynamique des adresses IP**.

Configurer les enquêtes

Configurez les enquêtes de façon à ce que les gens puissent utiliser Web Client et Milestone Mobile pour accéder à la vidéo enregistrer et mener des enquêtes sur les incidents, mais aussi préparer et télécharger des preuves vidéo.

Pour configurer les enquêtes, suivez ces étapes :

1. Dans Management Client, cliquez sur le serveur mobile, puis cliquez sur l'onglet **Enquêtes**.
2. Cochez la case **Activé**. Par défaut, la case est cochée.
3. Dans le champ **Répertoire d'enquêtes**, spécifiez où vous souhaitez stocker la vidéo aux fins des enquêtes.
4. Dans le champ **Limiter la taille des enquêtes à**, saisissez le nombre maximum de méga-octets que le répertoire d'enquête peut contenir.
5. Facultatif : Pour permettre aux utilisateurs d'accéder aux enquêtes créées par d'autres utilisateurs, sélectionnez la case **Voir les enquêtes créées par d'autres**. Si vous ne cochez pas cette case, les utilisateurs ne peuvent voir que leurs propres enquêtes.
6. Facultatif : Pour inclure la date et l'heure de téléchargement d'une vidéo, cochez la case **Inclure l'horodatage pour les exports AVI**.
7. Dans le champ **Codec utilisé pour les exports AVI**, sélectionnez le format de compression à utiliser lors de la préparation de paquets AVI à télécharger.

   Remarque : Les codecs de la liste peuvent être différents selon votre système d'exploitation. Si vous ne voyez pas le codec que vous souhaitez utiliser, vous pouvez l'installer sur l'ordinateur exécutant Management Client et il s'affichera alors dans cette liste.

   Par ailleurs, les codecs peuvent utiliser différents taux de compression, ce qui peut affecter la qualité de la vidéo. Des taux de compression plus élevés réduisent les exigences de stockage mais peuvent également réduire la qualité de la vidéo. Des taux de compression moins élevés nécessitent plus d'espace de stockage et de capacité du réseau mais accroissent la qualité de la vidéo. Il est conseillé d'effectuer des recherches au sujet des codecs avant d'en sélectionner un.
8. Dans le champ **Échec d'export des données (pour les exports MKV et AVI)**, spécifiez s'il faut conserver les données qui ont bien été téléchargées, bien qu'elles puissent être incomplètes, ou s'il faut les supprimer.
9. Pour permettre aux utilisateurs de sauvegarder des enquêtes, vous devez accorder les permissions suivantes au rôle de sécurité assigné aux utilisateurs :
   - Dans les produits XProtect Advanced VMS, accordez la permission **Export**.
   - Dans les produits XProtect Professional VMS, accordez la permission **Base de données**.

Nettoyer les enquêtes

Si vous avez des enquêtes ou des exports de vidéo que vous ne souhaitez plus conserver, vous pouvez les supprimer. Par exemple, ceci peut s'avérer utile si vous souhaitez libérer plus d'espace disponible sur le serveur.

- Pour supprimer une enquête et tous les exports de vidéos créés pour celle-ci, sélectionnez l'enquête dans la liste puis cliquez sur **Supprimer**.
- Pour supprimer des fichiers vidéo individuels qui ont été exportés pour une enquête, mais conserver l'enquête, sélectionnez l'enquête dans la liste. Dans le groupe **Détails de l'enquête**, cliquez sur l'icône **Supprimer** à droite des champs **Base de données**, **AVI**, ou **MKV** pour les exports.

À propos de l'envoi de notifications

Vous pouvez activer Milestone Mobile pour informer les utilisateurs de la survenance d'un événement, tel qu'un déclenchement d'alarme ou un problème au niveau d'un périphérique ou d'un serveur. Lorsque Milestone Mobile est ouvert sur le périphérique portable, l'application fournit la notification. Les utilisateurs peuvent spécifier les types de notifications qu'ils souhaitent recevoir. Par exemple, un utilisateur peut choisir de recevoir des notifications pour les éléments suivants :

- Toutes les alarmes
- Uniquement les alarmes dont ils sont propriétaires
- Uniquement les alarmes relatives au système Il peut s'agir des alarmes information de la mise hors tension ou du redémarrage d'un serveur.

Vous pouvez également utiliser des notifications push pour informer les utilisateurs qui n'ont pas ouvert Milestone Mobile. Ces notifications sont appelées des notifications push. Les notifications push sont envoyées sur le périphérique portable, et représentent un excellent moyen pour que les utilisateurs restent au courant de la situation pendant leurs déplacements.

Utiliser les notifications push

Remarque : Pour utiliser les notifications push, votre système doit avoir accès à Internet.

Les notifications push utilisent des services en nuage d'Apple, Microsoft et Google :

- le service Apple Push Notification (APN)
- Microsoft Azure Notification Hub
- le service Google Cloud Messaging Push Notification

Il y a une limite quant au nombre de notifications que votre système est autorisé à envoyer au cours d'une période donnée. Si votre système dépasse la limite, il ne peut envoyer qu'une seule notification toutes les 15 minutes au cours de la période suivante. La notification contient un résumé des événements qui se sont produits au cours des 15 minutes. Après la période suivante, les limites sont levées.

Exigences pour les notifications push

Les exigences suivantes doivent être respectées pour utiliser les notifications push :

- Vous devez associer une ou plusieurs alarmes à un ou plusieurs événements et règles. Ceci est exigé pour les notifications système.

- Assurez-vous que votre accord Milestone Care™ avec Milestone Systems est à jour.

Envoyer des notifications vers des périphériques mobiles.

Vous pouvez activer Milestone Mobile pour informer les utilisateurs de la survenance d'un événement, tel qu'un déclenchement d'alarme ou un problème au niveau d'un périphérique ou d'un serveur.

Configurer les notifications système

Pour envoyer les notifications en lien avec le système, lorsqu'un serveur est mis hors ligne, par exemple, suivez les étapes suivantes :

1. Dans Management Client, sélectionnez le serveur mobile, puis cliquez sur l'onglet **Notifications**.
2. Cochez la case **Notifications.**

Configurer les notifications push sur le serveur Milestone Mobile

Pour configurer les notifications push, suivez ces étapes :

1. Dans Management Client, sélectionnez le serveur mobile, puis cliquez sur l'onglet **Notifications**.
2. Pour envoyer des notifications à tous les appareils mobiles se connectant au serveur, sélectionnez la case à cocher **Notifications**.
3. Pour stocker des informations au sujet des utilisateurs et appareils mobiles se connectant au serveur, cochez la case **Maintenir l'inscription de l'appareil**.

   Remarque : Le serveur envoie des notifications uniquement aux périphériques portables de cette liste. Si vous décochez la case **Maintenir l'inscription de l'appareil** et sauvegardez la modification, le système efface la liste. Pour recevoir les notifications push à nouveau, les utilisateurs doivent reconnecter leur périphérique.

Arrêter d'envoyer des notifications push à des périphériques portables ou à tous les périphériques portables

Il existe plusieurs façons d'arrêter l'envoi de notifications push à des périphériques mobiles.

1. Dans Management Client, sélectionnez le serveur mobile, puis cliquez sur l'onglet **Notifications**.
2. Procédez comme suit :
   - Pour les périphériques individuels, décochez la case **Activé** pour chaque périphérique portable. L'utilisateur peut utiliser un autre périphérique pour se connecter au serveur Milestone Mobile.
   - Pour tous les périphériques, décochez la case **Notifications**.

Pour arrêter temporairement l'envoi vers tous les périphériques, décochez la case **Maintenir l'inscription des périphériques** et sauvegardez votre modification. Le système enverra à nouveau des notifications lorsque les utilisateurs se reconnecteront.

À propos de l'utilisation de vidéo push pour diffuser la vidéo

Vous pouvez configurer vidéo push de façon à ce que les utilisateurs puissent tenir d'autres personnes informées au sujet d'une situation, ou enregistrer une vidéo à des fins d'examen ultérieur, en transmettant la vidéo de la caméra de leur périphérique portable vers votre système de surveillance XProtect.

Configuration de vidéo push pour diffuser la vidéo

Pour permettre aux utilisateurs de transmettre la vidéo de leur périphérique portable vers un système de surveillance XProtect, configurez vidéo push sur un serveur Milestone Mobile.

Dans Management Client, suivez ces étapes dans l'ordre indiqué :

1. Configurez un canal que le périphérique portable peut utiliser pour transmettre la vidéo au serveur d'enregistrement.
2. Ajouter le pilote vidéo push en tant que périphérique système sur le serveur d'enregistrement. Le pilote simule une caméra afin que vous puissiez transmettre la vidéo au serveur d'enregistrement.
3. Affectez le périphérique du pilote vidéo push au canal.

Ce sujet décrit chacune de ces étapes.

Configurer un canal pour diffuser la vidéo

Remarque : Chaque canal nécessite une licence de périphérique.

Pour ajouter un canal, procédez de la manière suivante :

1. Dans le volet de navigation, choisissez **Mobile Server** puis sélectionnez le serveur portable.
2. Dans l'onglet **Vidéo Push**, cochez la case **Vidéo Push**.
3. En bas à droite, cliquez sur **Ajouter** pour ajouter un canal de vidéo push sous **mappage des canaux**.
4. Saisissez le nom d'utilisateur du compte utilisateur qui utilisera ce canal. Ce compte utilisateur doit être autorisé à accéder au serveur Milestone Mobile et au serveur d'enregistrement.

   Remarque : Pour utiliser vidéo push, les utilisateurs doivent se connecter à Milestone Mobile sur leur périphérique portable à l'aide de l'identifiant et du mot de passe relatifs à ce compte.
5. Notez bien le numéro de port. Vous en aurez besoin lorsque vous ajouterez le pilote vidéo push en tant que périphérique sur le serveur d'enregistrement.
6. Cliquez sur **OK** pour fermer la fenêtre de dialogue du canal vidéo push et sauvegarder le canal.

Ajouter le pilote vidéo push en tant que périphérique au système

1. Dans le volet Navigation sur le site, cliquez sur **Serveurs d'enregistrement**.
2. Effectuez un clic droit sur le serveur auquel vous souhaitez transmettre la vidéo, et cliquez sur **Ajouter matériel** pour ouvrir l'assistant **Ajouter matériel**.

3. Sélectionnez la méthode de détection de matériel **Manuelle,** puis cliquez sur **Suivant**.
4. Saisissez les coordonnées de la caméra comme suit :
   - Pour utiliser les coordonnées par défaut d'usine de l'usine de fabrication de la caméra, cliquez sur **Suivant**. En règle générale, les paramètres d'usine sont utilisés.
   - Si vous avez modifié les coordonnées sur l'appareil, saisissez ces informations, puis cliquez sur **Suivant**.

   Remarque : Il s'agit des coordonnées relatives au matériel, et non à l'utilisateur. Celles-ci ne sont pas liées au nom d'utilisateur pour le canal.
5. Dans la liste de pilotes, développez **Autre**, cochez la case **Pilote Vidéo Push**, puis cliquez sur **Suivant**.

   Remarque : Le système génère une adresse MAC pour le périphérique du pilote vidéo push. Nous vous recommandons d'utiliser cette adresse. Changez-la uniquement si vous rencontrez des problèmes avec le périphérique du pilote vidéo push. Par exemple, si vous devez ajouter une nouvelle adresse et un numéro de port.
6. Dans le champ **Adresse**, saisissez l'adresse IP de l'ordinateur sur lequel le serveur Milestone Mobile est installé.
7. Dans le champ **Port**, saisissez le numéro de port pour le canal que vous avez créé pour diffuser la vidéo. Le numéro de port a été assigné au moment de la création du canal.
8. Dans la colonne **Modèle du matériel**, choisissez **Pilote vidéo push**, et cliquez sur **Suivant**.
9. Lorsque le système détecte le nouveau matériel, cliquez sur **Suivant**.
10. Dans le champ **Modèle de nom du matériel**, indiquez s'il faut afficher soit le modèle du matériel soit son adresse IP ou le modèle uniquement.
11. Indiquez s'il faut activer les périphériques associés en cochant la case **Activé**. Vous pouvez ajouter des périphériques associés à la liste pour **Pilote vidéo push**, même s'ils ne sont pas activés. Vous pourrez les activer ultérieurement.

    Remarque : Si vous souhaitez utiliser les informations géographiques au moment de la diffusion de la vidéo, vous devez activer le port **Métadonnées**.
12. Sélectionnez les groupes par défaut pour les périphériques associés à gauche, ou sélectionnez un groupe spécifique dans le champ **Ajouter au groupe**. L'ajout de périphériques au groupe peut faciliter l'application simultanée des paramètres à tous les périphériques ou le remplacement de périphériques.

Ajouter le périphérique du pilote vidéo push au canal pour la diffusion vidéo

1. Dans le volet de **Navigation sur le site**, cliquez sur **Serveurs portables**, puis cliquez sur l'onglet **Vidéo push**.
2. Cliquez sur **Trouver des caméras**. Si l'opération réussit, le nom de la caméra du pilote vidéo push s'affiche dans le champ Nom de la caméra.
3. Enregistrez votre configuration.

Supprimer un canal dont vous n'avez pas besoin

Vous pouvez supprimer les canaux que vous n'utilisez plus.

- Sélectionnez le canal à supprimer, puis cliquez sur **Supprimer** dans le coin inférieur droit.

À propos des actions

Vous pouvez gérer la disponibilité de l'onglet **Actions** dans le client Milestone Mobile en activant ou désactivant cette fonction dans l'onglet du serveur mobile. Les **Actions** sont activées par défaut et toutes les actions disponibles pour les périphériques connectés sont affichées ici.

À propos de l'attribution d'un nom à une sortie à des fins d'utilisation dans Milestone Mobile

Afin que les actions s'affichent correctement avec la caméra actuelle, il est important que la sortie porte exactement le même nom que la caméra.

Exemple :

Si vous avez une caméra nommée « AXIS P3301,P3304 - 10.100.50.110 - Camera 1 », vous devez également appeler l'action « AXIS P3301,P3304 - 10.100.50.110 - Camera 1 ».

Vous pouvez ajouter une description plus complète au titre par la suite, par exemple « AXIS P3301,P3304 - 10.100.50.110 - Caméra 1 - Interrupteur éclairage ».

Important : Si vous ne suivez pas ces conventions, les actions ne seront pas disponibles dans la liste d'actions pour la vue de caméra associée. Au lieu de cela, les actions apparaîtront dans la liste d'autres actions de l'onglet **Actions**.

Ajouter une règle d'export automatique

1. Dans le Management Client, cliquez sur l'onglet du serveur mobile pertinent **> Export**.
2. Dans **Exports automatiques**, cliquez sur **Ajouter** pour ouvrir la fenêtre **Règle d'export automatique.**
3. Réglez les Paramètres de la fenêtre de règle d'export automatique pertinents.
4. Lorsque vous avez fini, cliquez sur **OK**.

Paramètres du serveur mobile

Généralités

Le tableau suivant décrit les paramètres de cet onglet.

Nom	Description
Nom du serveur	Saisissez un nom de serveur Milestone Mobile.
Description	Saisissez une description facultative du serveur Milestone Mobile.

Nom	Description
Serveur mobile	Choisissez entre tous les serveurs Milestone Mobile actuellement installés au système spécifique. Seuls les serveurs Milestone Mobile en cours d'exécution sont présentés dans la liste.
Méthode de connexion	Sélectionnez la méthode d'authentification à utiliser lorsque des utilisateurs se connectent au serveur. Vous pouvez choisir entre les options suivantes : **Automatique**, **Authentification Windows** ou **Authentification basique**.
Activer XProtect Web Client	Activez l'accès à XProtect Web Client.
Activer la vue de toutes les caméras	Incluez la vue **Toutes les caméras.** Cette vue affiche toutes les caméras qu'un utilisateur est autorisé à consulter sur un serveur d'enregistrement.
Activer les actions (sorties et événements)	Activez l'accès aux actions dans les clients Milestone Mobile.
Activer les images-clés	Diffusez uniquement les images-clés lors de la diffusion de vidéos. Ceci utilise moins de bande passante.
Activer les images en mode plein écran	Activer le serveur Milestone Mobile pour envoyer des images en mode plein écran au client Milestone Mobile ou XProtect Web Client. Notez que l'activation des images en mode plein écran utilise plus de bande passante. De plus, l'activation de cette option désactive toutes les règles configurées dans les paramètres **Performance**.
Activer la diffusion directe	Choisissez la façon dont la diffusion directe sera gérée dans XProtect Web Client. Choisissez entre faire appliquer l'utilisation de la diffusion directe, la faire appliquer dans la mesure du possible ou ne jamais la faire appliquer.
Activé	Activer / désactiver la journalisation des actions du client Milestone Mobile dans un fichier journal à part.
Emplacement du fichier journal	Chemin où les fichiers journaux sont enregistrés.
Activer les journaux pendant	Nombre de jour de conservation des journaux (par défaut, trois jours).
Sauvegarde de la configuration	Importez ou exportez votre configuration de serveur Milestone Mobile. Votre système enregistre la configuration dans un fichier XML.

Connectivité

Dans la rubrique **Généralités**, spécifiez les éléments suivants :

Nom	Description
Type de connexion	Choisissez comment les clients doivent se connecter au serveur Milestone Mobile. Vous pouvez choisir entre les options suivantes : **HTTP uniquement**, **HTTP et HTTPS** ou **HTTPS uniquement**. **Remarque :** Si vous choisissez **HTTPS uniquement**, les périphériques utilisant iOS 9.0 ou une version ultérieure, ou un téléphone Windows Phone, ne peuvent se connecter que si vous détenez un certificat émis par une autorité de certification (CA) installée sur votre serveur Milestone Mobile. Les CAs émettent des certificats numériques qui vérifient les identités des utilisateurs et les sites Internet qui échangent des données sur Internet. Parmi les exemples de CAs, on compte des sociétés telles que Comodo, Symantec et GoDaddy. Avec d'activer les connexions sécurisées, assurez-vous de bien vous familiariser avec les certificats numériques. Pour apprendre comment ajouter un certificat sur le serveur Milestone Mobile, voir Modifier le certificat (á la page *392*).
Délai client expiré (HTTP)	Définissez un délai de fréquence à laquelle le client Milestone Mobile doit indiquer au serveur mobile qu'il est opérationnel. La valeur par défaut est de 30 secondes. Milestone vous recommande de ne **pas** augmenter le délai.

Les paramètres de la rubrique **Accès Internet** sont utilisés pour les tâches suivantes :

- Configurer les paramètres de connexion
- Envoyer un message par e-mail pour aider les utilisateurs à connecter leur périphérique portable aux serveurs Milestone Mobile
- Activez les connexions aux serveurs Milestone Mobile sur un réseau complexe

Pour des descriptions étape par étape de ces tâches, voir Configurer Smart Connect (á la page 376).

État du serveur

Voir les détails de l'état pour votre mobile. Les détails sont en lecture seule :

Nom	Description
Serveur en cours d'exécution depuis	Indique la durée d'exécution du serveur mobile depuis son dernier arrêt.
Utilisation du processeur	Indique l'utilisation réelle du processeur sur le serveur mobile.
Bande passante interne	Indique la bande passante interne réelle utilisée entre le serveur mobile et le serveur d'enregistrement pertinent.
Bande passante externe	Indique la bande passante externe réelle utilisée entre le périphérique mobile et le serveur mobile.

Nom	Description
Colonne nom d'utilisateur	Indique le(s) nom(s) d'utilisateur(s) des utilisateur(s) du serveur mobile connectés au serveur mobile.
Colonne état	Indique la relation réelle entre le mobile et l'utilisateur client Milestone Mobile en question. L'utilisateur est-il connecté (un état préliminaire aux serveurs échangeant des clés et des certificats cryptés) ou est-il identifié ? Les états possibles sont les suivants : **Relié** et **Connecté** à XProtect.
Colonne utilisateur de la bande passante	Indique le niveau de bande passante utilisé par l'utilisateur client-serveur mobile en question.
Colonne flux en direct	Indique le nombre de vidéo de flux en direct actuellement ouvert pour l'utilisateur client Milestone Mobile en question.
Colonne flux enregistrés	Indique le nombre de vidéo de flux enregistré actuellement ouvert pour l'utilisateur client mobile pertinent.
Flux Vidéo Push	Indique le nombre de flux vidéo push actuellement ouvert pour l'utilisateur client mobile en question.
Flux directs	Indique le nombre de flux vidéo en direct utilisant la diffusion directe qui sont actuellement ouverts pour l'utilisateur mobile pertinent.

Vidéo Push

Indiquez les paramètres suivants si vous utilisez de la vidéo push.

Nom	Description
Vidéo push	Activer le vidéo push sur le serveur mobile.
Nombre de canaux	Indiquez le nombre de canaux sur lesquels la vidéo push est activée dans votre système XProtect.
Colonne canal	Présente le nombre de canal pour le canal adéquat. N'est pas modifiable.
Port	Numéro de port pour le canal vidéo push adéquat
MAC	Adresse MAC pour le canal vidéo push adéquat
Nom d'utilisateur	Indiquez le nom d'utilisateur associé au canal vidéo push adéquat.
Nom de la caméra	Affiche le nom de la caméra, si la caméra a été identifiée.

Une fois que vous avez terminé toutes les étapes nécessaires (voir "Configuration de vidéo push pour diffuser la vidéo" á la page 381), cliquez sur **Rechercher Caméras** pour rechercher la caméra correspondante.

Enquêtes

Vous pouvez activer les enquêtes de façon à ce que les gens puissent utiliser XProtect Web Client et Milestone Mobile pour accéder à la vidéo enregistrer et mener des enquêtes sur les incidents, mais aussi préparer et télécharger des preuves vidéo.

Le tableau suivant décrit les paramètres pour les enquêtes.

Nom	Description
Répertoire Enquêtes	Spécifiez l'emplacement de stockage des vidéos aux fins des enquêtes.
Limiter la taille des enquêtes à	Saisissez le nombre maximum de méga--octets que le répertoire Enquêtes peut contenir.
Voir les enquêtes créées par d'autres	Cochez cette case pour permettre aux utilisateurs pour accéder aux enquêtes qu'ils n'ont pas créées.
Inclure l'horodatage pour les exports AVI	Cochez cette case pour inclure la date et l'heure auxquelles le fichier AVI a été téléchargé.
Codec utilisé pour les fichiers AVI	Sélectionnez le format de compression à utiliser lors de la préparation de paquets AVI à télécharger. Les codecs que vous pouvez choisir peuvent être différents selon votre système d'exploitation. Si vous ne voyez pas le codec souhaité, vous pouvez l'ajouter à la liste en l'installation sur l'ordinateur exécutant le serveur Milestone Mobile.
Échec d'export des données (pour les exports MKV et AVI)	Indiquez s'il faut conserver les données qui n'ont pas été préparées correctement à des fins de téléchargement dans une enquête, ou les supprimer.

Notifications

Utilisez l'onglet **Notifications** pour activer ou désactiver les notifications du système et les notifications push.

Si vous activez les notifications et si vous avez configuré un ou plusieurs événements et alarmes, Milestone Mobile informe les utilisateurs de la survenance d'un événement. Lorsque l'application est ouverte, les notifications sont présentées dans Milestone Mobile sur le périphérique portable. Les notifications push informent les utilisateurs qui n'ont pas ouvert Milestone Mobile. Ces notifications sont fournies directement au périphérique portable.

Pour de plus amples informations, voir Envoyer des notifications vers des périphériques portables (voir "Envoyer des notifications vers des périphériques mobiles." á la page 380).

Le tableau suivant décrit les paramètres de cet onglet.

Nom	Description
Notifications	Cochez la case pour activer les notifications.
Maintenir l'inscription de l'appareil	Cochez cette case pour stocker des informations au sujet des périphériques et des utilisateurs qui se connectent au serveur. Le système envoie des notifications à ces périphériques. En décochant cette case, vous effacez également la liste de périphériques. Pour que les utilisateurs recommencent à recevoir des notifications, vous devez cocher la case et les utilisateurs doivent reconnecter leurs périphériques au serveur.
Activé	Cochez cette case pour envoyer des notifications au périphérique.
Périphériques enregistrés	Une liste des périphériques portables qui se sont connectés au serveur. Vous pouvez commencer ou arrêter d'envoyer des périphériques spécifiques en cochant ou décochant la case **Activé.**

Performance

Dans l'onglet **Performance**, vous pouvez configurer les limites suivantes concernant la performance du serveur Milestone Mobile :

Niveau 1

Le niveau 1 est la limite par défaut affectée au serveur Milestone Mobile. Toute limite configurée ici est toujours appliquée au flux vidéo Milestone Mobile.

Nom	Description
Niveau 1	Cochez la case pour activer le premier niveau de limites à la performance du serveur Milestone Mobile.
FPS maximum	Fixez une limite pour le nombre maximum d'images par seconde (FPS) devant être envoyé du serveur Milestone Mobile aux clients.
Résolution maximale des images	Fixez une limite pour le nombre maximum d'images par seconde (FPS) devant être envoyé du serveur Milestone Mobile aux clients.

Niveau 2

Si vous souhaitez plutôt exécuter un niveau de limites différent du **Niveau 1** par défaut, vous pouvez alors sélectionner la case **Niveau 2**. Vous ne pouvez pas régler les paramètres à un niveau plus élevé que celui fixé au premier niveau. Ainsi, par exemple, si vous avez réglé le FPS max sur 45 au **Niveau 1**, vous ne pouvez régler le FPS max du **Niveau 2** que sur 44 ou moins.

Nom	Description
Niveau 2	Cochez la case pour activer le deuxième niveau de limites à la performance du serveur Milestone Mobile.
Seuil de CPU	Fixez un seuil de charge du CPU sur le serveur Milestone Mobile avant que le système n'applique les limites du flux vidéo.
Seuil de bande passante	Fixez un seuil de bande passante sur le serveur Milestone Mobile avant que le système n'applique les limites du flux vidéo.
FPS maximum	Fixez une limite pour le nombre maximum d'images par seconde (FPS) devant être envoyé du serveur Milestone Mobile aux clients.
Résolution maximale des images	Fixez une limite pour le nombre maximum d'images par seconde (FPS) devant être envoyé du serveur Milestone Mobile aux clients.

Niveau 3

Vous pouvez également cocher une case **Niveau 3** pour créer un troisième niveau de limites. Vous ne pouvez pas régler les paramètres à un niveau plus élevé que celui fixé aux **Niveau 1** et **Niveau 2**. Ainsi, par exemple, si vous avez réglé le **FPS max** sur 45 au **Niveau 1** et sur 32 au **Niveau 2**, vous ne pouvez régler le **FPS max** du **Niveau 3** que sur 31 ou moins.

Nom	Description
Niveau 3	Cochez la case pour activer le deuxième niveau de limites à la performance du serveur Milestone Mobile.
Seuil de CPU	Fixez un seuil de charge du CPU sur le serveur Milestone Mobile avant que le système n'applique les limites du flux vidéo.
Seuil de bande passante	Fixez un seuil de bande passante sur le serveur Milestone Mobile avant que le système n'applique les limites du flux vidéo.
FPS maximum	Fixez une limite pour les images par seconde (FPS) devant être envoyées du serveur Milestone Mobile aux clients.
Résolution maximale des images	Fixez une limite pour le nombre maximum d'images par seconde (FPS) devant être envoyé du serveur Milestone Mobile aux clients.

Le système ne bascule pas instantanément d'un niveau à un autre. Si votre seuil de CPU ou de bande passante dépasse les niveaux indiqués de moins de cinq pour cent, le niveau actuel continue d'être utilisé.

Veuillez noter qu'en cas d'activation de l'option **Activer les images en mode plein écran** dans l'onglet **Général**, aucun des niveaux de **Performance** n'est appliqué.

Paramètres des journaux

Remplissez et spécifiez les paramètres de journaux suivants :

Nom	Description
Activé	Activer / désactiver la journalisation des actions clients de Milestone Mobile dans un fichier journal à part.
Emplacement du fichier journal :	Chemin où les fichiers journaux sont enregistrés.
Conserver les journaux pendant :	nombre de jour de conservation des journaux (par défaut, 3 jours)
Utilisation du processeur :	Niveau d'utilisation par défaut du processeur qui déclenchera un avertissement sur le journal.
Bande passante interne :	Bande passante interne par défaut qui déclenchera un avertissement sur le journal.
Bande passante externe :	Bande passante externe par défaut qui déclenchera un avertissement sur le journal.
Vérifier toutes les :	Délai par défaut (30 sec) de vérification des niveaux d'avertissement.

Mobile Server Manager

À propos de Mobile Server Manager

Le Mobile Server Manager est une fonctionnalité contrôlé par barre d'état connecté au serveur mobile. Un clic droit sur l'icône Mobile Server Manager dans la barre d'état système ouvre un menu dans lequel vous pouvez facilement accéder aux fonctionnalités du serveur mobile.

Vous pouvez :

- Ouvrir XProtect Web Client (voir "Accès à XProtect Web Client" á la page 390)
- Démarrer, arrêter et redémarrer Mobile service (voir "Démarrer, arrêter et redémarrer le service Mobile" á la page 393)
- Compléter ou modifier les informations d'identification du serveur de surveillance (voir "Compléter/modifier les informations d'identification du serveur de surveillance" á la page 392)
- Afficher/modifier les numéros de port (á la page 393)
- Modifier le certificat (á la page 392)
- Ouvrir le fichier journal d'aujourd'hui (voir "À propos de l'accès aux journaux et aux exportations" á la page 391)
- Ouvrir un dossier de journaux (voir "À propos de l'accès aux journaux et aux exportations" á la page 391)
- Ouvrir le dossier d'export (voir "À propos de l'accès aux journaux et aux exportations" á la page 391)
- Afficher l'état du serveur mobile (voir "À propos de Afficher l'état" á la page 391)

Accès à XProtect Web Client

Si un serveur Milestone Mobile est installé sur votre ordinateur, vous pouvez utiliser le XProtect Web Client pour accéder à vos caméras et vues. Comme il est inutile d'installer XProtect Web Client, vous pouvez y accéder depuis l'ordinateur sur lequel est installé le serveur Milestone Mobile ou depuis tout ordinateur que vous souhaitez utiliser à cette fin.

1. Configurez le serveur Milestone Mobile dans le Management Client.
2. Si vous utilisez l'ordinateur sur lequel le serveur Milestone Mobile est installé, vous pouvez cliquer avec le bouton droit sur l'icône du serveur Milestone Mobile dans la barre des tâches du système et sélectionner **Ouvrir XProtect Web Client**.
3. Si vous n'utilisez pas l'ordinateur sur lequel le serveur Milestone Mobile est installé, vous pouvez y accéder à partir d'un navigateur. Passez à l'étape 4 de ce processus.
4. Ouvrez un navigateur Internet (Internet Explorer, Mozilla Firefox, Google Chrome ou Safari).
5. Saisissez l’adresse IP externe (c’est-à-dire votre adresse externe et le port du serveur sur lequel le serveur de serveur Milestone Mobile s’exécute).

Exemple : Le serveur Milestone Mobile est installé sur un serveur dont l'adresse IP est 127.2.3.4. Il est configuré pour accepter les connexions HTTP sur le port 8081 et les connexions HTTPS sur le port 8082 (les valeurs par défaut du programme d'installation).

Dans la barre d'adresses de votre navigateur, saisissez : http://1.2.3.4:8081 ou https://1.2.3.4:8082, selon que vous utilisez une connexion HTTP standard ou une connexion HTTPS sécurisée. Vous pouvez alors commencer à utiliser XProtect Web Client.

6. Ajoutez l'adresse en tant que signet dans votre navigateur pour faciliter l'accès à XProtect Web Client ultérieurement. Si vous utilisez XProtect Web Client sur l'ordinateur local sur lequel vous avez installé le serveur Milestone Mobile, vous pouvez également utiliser le raccourci de bureau créé par le programme d'installation. Cliquez sur le raccourci pour lancer votre navigateur par défaut et ouvrir le XProtect Web Client.

Les navigateurs Internet exécutant le XProtect Web Client doivent avoir leur cache effacé avant de pouvoir utiliser une nouvelle version de XProtect Web Client Les administrateurs système doivent demander à leurs utilisateurs de XProtect Web Client de vider le cache de leur navigateur après la mise à niveau ou de forcer cette action à distance (vous pouvez effectuer cette action uniquement sur Internet Explorer dans un domaine).

À propos de Afficher l'état

Faites un clic droit sur l'icône du Mobile Server Manager et sélectionnez **Afficher l'état** ou double-cliquez sur l'icône Mobile Server Manager pour ouvrir une fenêtre affichant l'état du serveur mobile. Vous pouvez voir les informations suivantes :

Nom	Description
Serveur en cours d'exécution depuis	Heure et date du dernier lancement du serveur mobile
Utilisateurs connectés	Nombre d'utilisateurs actuellement connectés au serveur mobile
Décodage du matériel	Indique si le décodage accéléré du matériel fonctionne sur le serveur mobile.
Utilisation du processeur	Combien de % du processeur est actuellement utilisé par le serveur mobile.
Historique de l'utilisation de l'unité centrale	Un graphique détaillant l'historique de l'utilisation du processeur par le serveur mobile.

À propos de l'accès aux journaux et aux exportations

Le Mobile Server Manager vous permet d'accéder rapidement au fichier journal de la journée, ouvrez le dossier dans lequel les fichiers journaux sont enregistrés, et ouvrez le dossier dans lequel les exportations sont enregistrées.

Pour ouvrir l'un de ces éléments, faites un clic droit sur le Mobile Server Manager et sélectionnez **Ouvrir le journal d'aujourd'hui**, **Ouvrir le dossier journal** ou **Ouvrir le dossier d'export** respectivement**.**

Important : Si vous désinstallez Milestone Mobile de votre système, ses fichiers journaux ne sont pas supprimés. Les administrateurs disposant des droits appropriés peuvent accéder à ces fichiers journaux plus tard, ou décider de les supprimer s'ils ne sont pas nécessaires plus longtemps. L'emplacement par défaut des fichiers journaux se trouve dans le dossier ProgramData. Si vous modifiez l'emplacement par défaut des fichiers journaux, les journaux existants ne sont pas copiés vers le nouvel emplacement et ne sont pas supprimés.

Modifier le certificat

Si vous voulez utiliser un protocole sécurisé HTTPS pour établir la connexion entre un serveur Milestone Mobile et votre appareil mobile ou le XProtect Web Client, vous devez avoir un certificat valide pour le périphérique ou le navigateur Web pour l'accepter sans avertissement. Le certificat atteste que le titulaire du certificat est autorisé à établir la connexion.

Lorsque vous installez le serveur Milestone Mobile, vous générez un certificat auto-signé si vous exécutez une installation **Typique** . Si vous exécutez une installation **Personnalisée**, vous pouvez choisir entre la génération d'un certificat auto-signé ou le chargement d'un fichier contenant un certificat délivré par un autre site de confiance.

Remarque : Si vous souhaitez activer les connexions sécurisées (HTTPS), les périphériques utilisant iOS 9.0 ou une version ultérieure, ou un téléphone Windows Phone, ne peuvent se connecter que si vous détenez un certificat émis par une autorité de certification (CA) installée sur votre serveur Milestone Mobile. Les CAs émettent des certificats numériques qui vérifient les identités des utilisateurs et les sites Internet qui échangent des données sur Internet. Parmi les exemples de CAs, on compte des sociétés telles que Comodo, Symantec et GoDaddy. Avec d'activer les connexions sécurisées, assurez-vous de bien vous familiariser avec les certificats numériques.

Si vous souhaitez utiliser un certificat différent, vous pouvez procéder comme suit.

1. À partir d'un ordinateur sur lequel Management Client est installé, effectuez un clic droit sur l'icône **Serveur Milestone Mobile** et sélectionnez **Modifier certificat...**
2. Choisissez l'une des options suivantes :
   - Générer un certificat auto-signé
   - Charger un fichier de certificat

Générer un certificat auto-signé

1. Choisissez l'option **Générer un certificat auto-signé** et cliquez sur **OK**.
2. Attendez quelques secondes que le système installe le certificat.
3. Une fois cette opération terminée, une fenêtre s'ouvre et vous informe que le certificat a été installé avec succès. Le service mobile redémarre pour appliquer la modification.

Trouver un fichier de certificat

1. Choisissez l'option **Charger un fichier de certificat**.
2. Remplissez le chemin du fichier de certificat ou cliquez sur la case ... pour ouvrir une fenêtre dans laquelle vous pouvez rechercher le fichier.
3. Remplissez le mot de passe relié au fichier de certificat.
4. Lorsque vous avez fini, cliquez sur **OK**.

Compléter/modifier les informations d'identification du serveur de surveillance

1. Faites un clic droit sur le Mobile Server Manager et sélectionnez **Identifiant du serveur de surveillance...**

2. Remplissez l'**URL du serveur**
3. Sélectionnez sous quel utilisateur vous souhaitez vous connecter
   - Administrateur système local (aucun identifiant nécessaire) ou
   - Un compte d'utilisateur spécifié (identifiants nécessaires)
4. Si vous avez choisi un compte d'utilisateur spécifié, remplissez **Nom d'utilisateur** et **Mot de passe**.
5. Lorsque vous avez fini, cliquez sur **OK**.

Afficher/modifier les numéros de port

1. Faites un clic droit sur le Mobile Server Manager et sélectionnez **Afficher/modifier les numéros de port...**
2. Pour modifier les numéros de port, saisissez le numéro du port concerné. Vous pouvez indiquer un numéro de port standard (pour les connexions HTTP) et/ou un numéro de port sécurisé (pour les connexions HTTPS).
3. Lorsque vous avez fini, cliquez sur **OK**.

Démarrer, arrêter et redémarrer le service Mobile

Si nécessaire, vous pouvez démarrer, arrêter et redémarrer le service mobile du Mobile Server Manager.

- Pour effectuer ces tâches, faites un clic droit sur **Mobile Server Manager** et sélectionnez **Démarrer le service Mobile**, **Arrêter le service Mobile** ou **Redémarrer le service Mobile** respectivement**.**

Foire aux Questions (FAQs)

1. **Pourquoi ne puis-je pas me connecter à mes enregistrements/mon serveur Milestone Mobile à partir de mon client Milestone Mobile ?**

   Afin de vous connecter à vos enregistrements, le serveur Milestone Mobile doit être installé sur le serveur exécutant votre système XProtect ou sur un serveur dédié. Les paramètres Milestone Mobile pertinents sont également requis dans votre configuration de gestion de la vidéo XProtect. Ceux-ci sont installés soit sous forme de modules d'extension ou dans le cadre d'une installation ou mise à niveau de produit. Pour plus d'informations sur la façon d'obtenir le serveur Milestone Mobile et de l'intégrer aux paramètres du client Milestone Mobile de votre système XProtect, voir la rubrique configuration (voir "Configuration Milestone Mobile" á la page 375).

2. **J'ai installé le serveur Milestone Mobile sur XProtect Corporate, mais je n'arrive pas à me connecter au serveur à partir de mon appareil. Quel est le problème ?**

   Après avoir installé le serveur Milestone Mobile sur votre XProtect Corporate (4.0+), vous devez installer le module d’extension Milestone Mobile pour voir le serveur Milestone Mobile dans votre configuration XProtect Corporate (voir "Installer le serveur Milestone Mobile" á la page 48). Une fois le module d’extension Milestone Mobile installé, trouvez le module d'extension dans **Serveurs** > **Serveurs mobiles** et cliquez avec le bouton droit de la

souris pour ajouter un nouveau serveur mobile. Ici, vous ajoutez les détails se rapportant à votre serveur Milestone Mobile (Nom du serveur, description (facultatif), adresse du serveur, port et bien plus encore). Lorsque vous avez terminé, redémarrez le service Milestone Mobile (à partir des Services Windows) et essayez de reconnecter votre périphérique.

3. **Comment puis-je ajouter un serveur/emplacement/site Milestone Mobile sur mon client Milestone Mobile ?**

   Vous pouvez y parvenir à partir du client Milestone Mobile. Lorsque vous l'ouvrez pour la première fois, vous devez ajouter un ou plusieurs serveurs mobiles afin de récupérer la vidéo sur vos caméras. Vos serveurs Milestone Mobile ajoutés seront répertoriés alphabétiquement. Vous pouvez ajouter autant de serveurs Milestone Mobile que nécessaire, dans la mesure où vous disposez des informations de connexion nécessaires.

4. **Pourquoi la qualité de l'image est-elle parfois mauvaise lorsque je consulte la vidéo dans le client Milestone Mobile ?**

   Le serveur Milestone Mobile ajuste automatiquement la qualité d'image en fonction de la bande passante disponible entre le serveur et le client Si vous observez une qualité de l'image inférieure à celle du XProtect® Smart Client, il se peut que votre bande passante soit trop faible pour vous permettre d'obtenir des images de haute résolution par le biais du client Milestone Mobile. Il est possible que cela soit dû à une bande passante trop faible en amont du serveur ou à une bande passante trop faible dans le client. Reportez-vous au **Manuel de l'utilisateur XProtect Smart Client** que vous pouvez télécharger sur notre site Internet http://www.milestonesys.com/support/manuals-and-guides/.

   Si vous êtes dans une région à bande passante sans fil variable, vous remarquerez peut-être que la qualité de l'image s'améliore lorsque vous entrez dans une zone dotée d'une meilleure bande passante.

5. **Comment puis-je créer des vues ?**

   Vous ne pouvez pas créer ou configurer de vues dans le Milestone Mobile. Il utilise des vues et noms associés déjà créés dans le XProtect Smart Client. Si aucune vue n'est configurée, vous pouvez utiliser la vue **Toutes les caméras** pour voir toutes les caméras de votre système. Vous pouvez toujours ajouter d'autres vues dans le XProtect Smart Client ultérieurement.

6. **Comment puis-je ajouter un nouvel utilisateur Milestone Mobile ?**

   Un utilisateur Milestone Mobile est exactement comme tout autre utilisateur XProtect. Vous pouvez ajouter un nouvel utilisateur Milestone Mobile de la même manière qu'un nouvel utilisateur normal dans votre Management Client : effectuez un clic droit sur **Utilisateurs** dans le volet de navigation et sélectionnez **Ajouter un nouvel utilisateur basique** ou **Ajouter un nouvel utilisateur Windows**. Si vous sélectionnez un nouvel utilisateur basique, vous devez changer de méthode de connexion au serveur et choisir **Automatique** ou **Basique uniquement** selon votre système. Vous pouvez changer votre méthode de connexion au serveur de à partir du menu déroulant **Méthode de connexion** dans l'onglet **Général** de l'entrée du serveur mobile, sous **Serveurs** > **Serveurs mobiles** dans le Management Client.

7. **Puis-je contrôler mes caméras pan-tilt-zoom (PTZ) et utiliser les préréglages du client Milestone Mobile ?**

   Oui, dans le client Milestone Mobile, vous pouvez contrôler vos caméras PTZ connectées et utiliser les préréglages en mode En direct.

8. **Comment puis-je parcourir mes enregistrements ?**

Android : Vous pouvez parcourir vos enregistrements en mode Lecture. Sélectionnez la caméra que vous souhaitez consulter en mode Lecture et choisir **Menu** > **Lecture**. Une fois en mode Lecture, vous pouvez parcourir vos enregistrements à l'aide des boutons de commande. Vous pouvez également vous rendre à un instant spécifique en choisissant **Menu** > **Aller à l'instant**. Une fois que vous avez choisi **Aller à l'instant**, sélectionnez la date et l'heure que vous souhaitez examiner.

iOS : Vous pouvez parcourir vos enregistrements en mode Lecture. Sélectionnez la caméra que vous souhaitez consulter en mode Lecture et tapez sur Lecture. Une fois en mode Lecture, vous pouvez parcourir vos enregistrements à l'aide des boutons de commande. Vous pouvez également vous rendre à un instant spécifique en choisissant **Menu** > **Aller à l'instant**. Une fois que vous avez choisi **Aller à l'instant**, sélectionnez la date et l'heure que vous souhaitez examiner et cliquez sur **Confirmer**.

9. **Puis-je voir des vidéos en direct et enregistrées en même temps ?**

   Oui, en mode Lecture, votre écran contient une petite image insérée (PiP) représentant la vue en direct de la même caméra.

10. **Puise-je utiliser le client Milestone Mobile sans abonnement de données 3G ?**

    Oui, vous pouvez utiliser Milestone Mobile par le biais du réseau Wi-Fi. Localement, sur le même réseau que votre système XProtect ou à partir d'un emplacement différent, tel qu'un réseau public dans un café ou un réseau personnel. Veuillez noter que la bande passante des réseaux publics varie et qu'elle peut affecter la qualité de l’image des flux vidéo.

11. **Puise-je utiliser le client Milestone Mobile avec un abonnement de données 4G/LTE ?**

    Oui, vous pouvez utiliser toute connexion de données sur votre périphérique portable vous permettant d'accéder à Internet pour vous connecter au système de gestion vidéo XProtect.

12. **Puis-je ajouter plusieurs serveurs au client Milestone Mobile ?**

    Lorsque vous ouvrez le client Milestone Mobile pour la première fois, vous devez ajouter un ou plusieurs serveurs mobiles afin de récupérer la vidéo sur vos caméras. Ces serveurs mobiles sont répertoriés dans l'ordre alphabétique. Si vous souhaitez récupérer des vidéos à partir de serveurs supplémentaires, répétez ce processus. Vous pouvez ajouter autant de serveurs mobiles que nécessaire, dans la mesure où vous disposez des informations de connexion pertinentes.

13. **Pourquoi la qualité de l’image est-elle mauvaise lorsque je me connecte à mon système de gestion vidéo XProtect à la maison, à partir de la WiFi de mon bureau ?**

    Vérifiez la bande passante de votre connexion Internet personnelle. De nombreuses connexions privées à Internet ont des bandes passantes différentes pour le téléchargement et le chargement, souvent décrites comme suit : 20 Mbit/2 Mbit. En effet, les utilisateurs particuliers ont rarement besoin de charger de grandes quantités de données sur Internet, mais consomment beaucoup de données. Le système de gestion vidéo XProtect a besoin d'envoyer la vidéo au client Milestone Mobile et est limité par la vitesse de chargement de votre connexion. Si vous rencontrez une mauvaise qualité d'image à divers endroits alors que la vitesse de téléchargement du réseau du client Milestone Mobile est bonne, le problème pourrait être résolu en augmentant la vitesse de chargement de votre connexion Internet personnelle.

14. **Où sont sauvegardés mes instantanés ?**

    Android : Les instantanés sont sauvegardés sur la carte SD de votre appareil sur : **/mnt/sdcard/XProtect**.

iOS : Les instantanés sont sauvegardés sur votre périphérique et sont accessibles par le biais du menu **Photos** sur votre périphérique.

Vous ne pouvez pas modifier les paramètres par défaut sur Android ou iOS.

15. **Comment puis-je éviter l'avertissement de sécurité lorsque j'exécute XProtect Web Client par le biais d'une connexion HTTPS ?**

    L'avertissement s'affiche parce que les informations du certificat concernant l'adresse du serveur sont incorrectes. La connexion restera cryptée.
    Le certificat auto-signé du serveur Milestone Mobile doit être remplacé par votre propre certificat correspondant à l'adresse du serveur utilisée pour connecter le serveur Milestone Mobile. Ces certificats sont obtenus par le biais d'autorités officielles de signature de certificats telles que Verisign. Consultez l'autorité de signature de votre choix pour obtenir de plus amples informations.
    Le serveur Milestone Mobile n'utilise pas Microsoft IIS. Cela signifie que les instructions fournies pour la production de fichiers de demande de signature d'un certificat (CSR) par l'autorité signataire utilisant IIS ne s'appliquent pas au serveur Milestone Mobile. Vous devez créer un fichier CSR manuellement en utilisant des outils de certification à ligne de commande ou d'autres applications tierces similaires. Veuillez noter que ce processus doit être entrepris uniquement par des administrateurs du système ou des utilisateurs avancés.

16. **Mon processeur supporte-t-il le décryptage avec accélération matérielle ?**

    Seuls les processeurs les plus récents d'Intel supportent le décryptage avec accélération matérielle. Consultez le site Internet d'Intel http://ark.intel.com/search/advanced?s=t&MarketSegment=DT&QuickSyncVideo=true pour savoir si votre processeur est pris en charge.

    Dans le menu, assurez vous que **Technologies** > **Intel Quick Sync Video** est réglé sur **Oui**.

    Si votre processeur est pris en charge, le décryptage avec accélération matérielle est activé par défaut. Vous pouvez voir l'état actuel dans **Afficher l'état** dans le Mobile Server Manager (voir "À propos de Afficher l'état" á la page 391).

17. **Mon système d'exploitation supporte-t-il le décryptage avec accélération matérielle ?**

    Seuls Windows 8 et Windows Server 2012 ou les versions plus récentes de ces systèmes d'exploitation sont pris en charge.

    Assurez-vous d'installer les pilotes graphiques les plus récents sur votre système à partir du site Internet d'Intel. Ces pilotes ne sont pas disponibles à partir de Windows Update.

    Le décryptage avec accélération matérielle n'est pas supporté si le serveur mobile est installé dans un environnement virtuel.

18. **Comment puis-je désactiver le décryptage avec accélération matérielle sur le serveur mobile ? (Avancé)**

    Si le processeur du serveur mobile prend en charge le décryptage avec accélération matérielle, celui-ci est activé par défaut. Pour désactiver le décryptage avec accélération matérielle, procédez comme suit :

    1. Trouvez le fichier VideoOS.MobileServer.Service.exe.config. En règle générale, le chemin d'accès est le suivant : C:\Program Files\Milestone\Milestone Mobile Server\VideoOS.MobileServer.Service.exe.config.

    2. Ouvrez le fichier dans Notepad ou un éditeur de texte similaire. Si nécessaire, associez le type de fichier .config à Notepad.

3. Trouvez le champ <add key="HardwareDecodingMode" value="Auto" />.
4. Remplacez la valeur « Auto » par « Off ».
5. Enregistrez et fermez le fichier.

19. **Je viens d'activer mon pare-feu et, maintenant, je ne peux pas connecter de périphérique portable à mon serveur. Pourquoi ?**

    Si votre pare-feu était désactivé au cours de l'installation de votre serveur Milestone Mobile, vous devez activer manuellement les communications TCP et UDP.

Milestone ONVIF Bridge

À propos de Milestone ONVIF Bridge

Les fonctions disponibles dépendent du système que vous utilisez. Voir le tableau de comparaison des produits pour de plus amples informations.

ONVIF est un forum mondial ouvert qui œuvre pour standardiser et sécuriser la communication des produits de vidéosurveillance IP. Le but est de faciliter l'échange de données vidéo et audio. Par exemple, pour permettre aux autorités, centres de surveillance ou organisations similaires d'accéder rapidement à des flux vidéo en direct et enregistrés dans tout système de surveillance IP.

Milestone Systems souhaite soutenir cet objectif et a développé Milestone ONVIF Bridge dans ce but. Milestone ONVIF Bridge fait partie de la plateforme ouverte Milestone et offre une interface prenant en charge les parties de la norme ONVIF liées à la récupération des vidéos en direct et enregistrées depuis n'importe quel NVR Milestone Husky™ ou produit VMS XProtect®.

Ce document fournit les informations suivantes :

- Informations sur la norme ONVIF et liens vers les matériels de référence.
- Instructions pour installer et configurer Milestone ONVIF Bridge dans un produit VMS XProtect.
- Exemples de la manière de mettre en œuvre différents types de clients ONVIF pour diffuser de la vidéo en direct et enregistrée depuis les produits VMS XProtect.

Milestone ONVIF Bridge et la norme ONVIF

La norme ONVIF facilite l'échange d'informations en définissant un protocole commun. Le protocole contient les profils ONVIF qui sont des collections de spécifications d'interopérabilité entre les périphériques conformes à ONVIF.

Milestone ONVIF Bridge est conforme avec les parties des profils ONVIF G et S, fournissant un accès à la vidéo en direct et enregistrée, et la capacité de contrôler les caméras Pan/Tilt/Zoom :

- Profil G - Supporte l'enregistrement, le stockage, la recherche et l'extraction de la vidéo Pour en savoir plus, consultez Caractéristiques du profil G ONVIF (https://www.onvif.org/Portals/0/documents/specs/ONVIF_Profile_G_Specification_v1-0.pdf.)
- Profil S - Supporte la diffusion de la vidéo en direct avec le codec H.264, la diffusion audio et les commandes pan-tilt-zoom (PTZ). Pour en savoir plus, consultez Caractéristiques du profil G ONVIF (http://www.onvif.org/Portals/0/documents/op/ONVIF_Profile_S_Specification_v1-1-1.pdf)

Pour en savoir plus sur la norme ONVIF, consultez le site Internet ONVIF® http://www.onvif.org/.

Les profils ONVIF supportent les fonctions « obtenir » qui récupèrent les données et les fonctions « définir » qui configurent les paramètres. Chaque fonction est obligatoire, conditionnelle ou optionnelle. Pour des raisons de sécurité, Milestone ONVIF Bridge supporte uniquement les fonctions « obtenir » obligatoires, optionnelles et conditionnelles qui font les choses suivantes :

- Requête vidéo
- Authentification utilisateurs

- Flux vidéo
- Lecture vidéo enregistrée

Remarque : Bien qu'Milestone ONVIF Bridge prenne actuellement en charge uniquement les profils ONVIF S et G, nous travaillons sur l'incorporation de la prise en charge d'autres profils ONVIF.

À propos des clients ONVIF

Les clients ONVIF peuvent être des serveurs, des ponts comme Milestone ONVIF Bridge, des lecteurs de médias ou des systèmes de surveillance basés sur IP.

Real Time Streaming Protocol (RTSP) est utilisé pour établir et contrôler les sessions médias entre au moins deux points terminaux. Milestone ONVIF Bridge utilise le profil ONVIF S et RTSP pour gérer les demandes de vidéo d'un client ONVIF, et pour diffuser la vidéo en direct depuis une installation XProtect video management software vers le client ONVIF.

Par défaut, la communication entre les clients ONVIF et le serveur ONVIF Bridge utilise les ports suivants :

- ONVIF port 580. Les clients ONVIF utilisent ce port pour envoyer des demandes de flux vidéo
- RTSP port 554. Milestone ONVIF Bridge utilise ce port pour diffuser des vidéos aux clients ONVIF

Les clients ONVIF peuvent accéder au port RTSP directement sur Milestone ONVIF Bridge. Par exemple, le lecteur de médias VLC ou un module d'extension VLC dans un navigateur peut extraire et afficher la vidéo. Ceci est décrit plus bas dans ce document dans une section intitulée Utiliser un lecteur de médias pour se connecter à un flux en direct.

Vous pouvez utiliser les différents ports, par exemple, pour éviter un conflit de ports. Si vous changez les numéros de port, vous devez aussi actualiser le flux RTSP pour l'URL client ONVIF.

RTSP supporte uniquement le codec H.264. Les caméras doivent pouvoir diffuser la vidéo sous le codec H.264.

Contrôles de sécurité Milestone ONVIF Bridge

Milestone ONVIF Bridge exécute l'autorisation utilisateur des clients ONVIF. Celle-ci contrôle la capacité du client ONVIF à accéder aux caméras, et les types d'opérations que peuvent réaliser les clients ONVIF. Par exemple, si les clients ONVIF peuvent utiliser les commandes pan-tilt-zoom (PTZ) sur les caméras.

Milestone vous recommande de créer et ajouter un compte utilisateur dédié pour Milestone ONVIF Bridge, et pour chaque client ONVIF, de la manière suivante :

1. Créez un utilisateur basique dans Management Client, ou un utilisateur Windows dans Active Directory.
2. Affectez à l'utilisateur un rôle qui peut accéder aux caméras, et spécifiez les permissions pour le groupe de sécurité ONVIF Bridge dans l'onglet Sécurité globale pour le rôle.
3. Affectez l'utilisateur à Milestone ONVIF Bridge pendant l'installation, puis dans Management Client ou Management Application pour chaque client ONVIF ensuite.

Milestone ONVIF Bridge permet uniquement aux clients ONVIF de demander et recevoir des flux vidéo depuis les caméras. Les clients ONVIF ne peuvent pas configurer les paramètres du système VMS XProtect ou d'Milestone ONVIF Bridge.

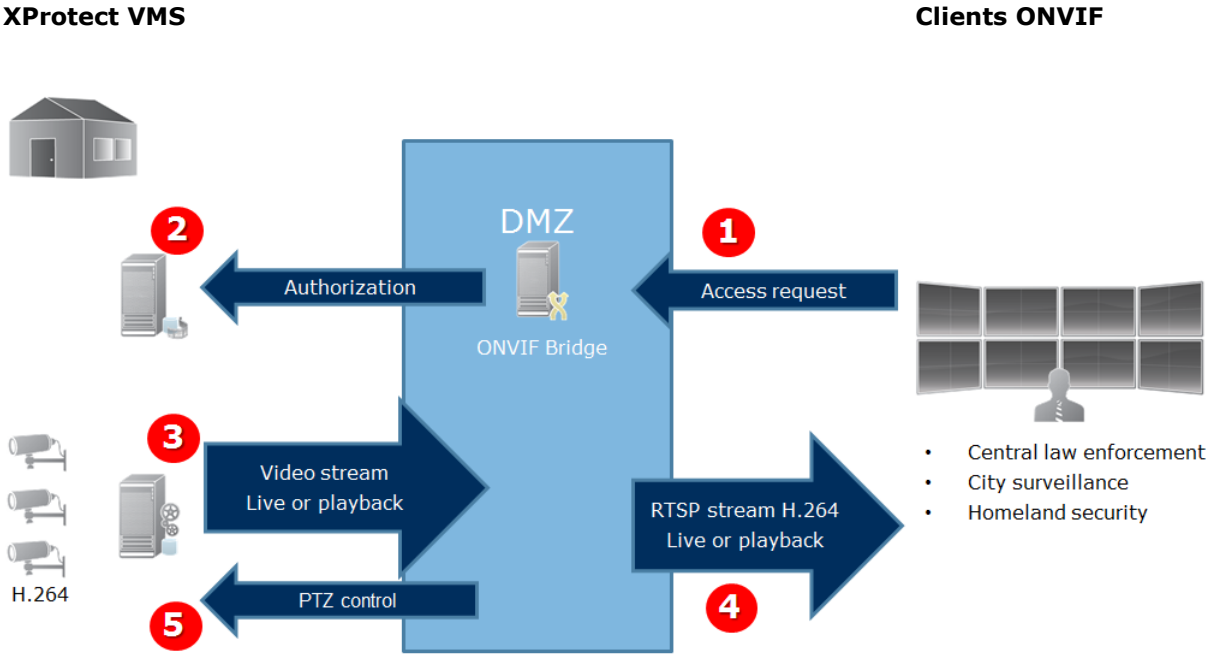
À titre de précaution, Milestone vous recommande d'installer le serveur ONVIF Bridge dans une zone démilitarisée (DMZ). Si vous installez le pont dans un DMZ, vous devez aussi configurer le transfert de port pour les adresses IP internes et externes.

Architecture Milestone ONVIF Bridge

Le Milestone ONVIF Bridge comporte les composants suivants :

- Serveur Milestone ONVIF Bridge
- Module complémentaire 32 bits Milestone ONVIF Bridge pour Management Application
- Module complémentaire 64 bits Milestone ONVIF Bridge pour Management Client

L'image suivante présente une vue de haut niveau de l'interopérabilité entre un client ONVIF, Milestone ONVIF Bridge et XProtect VMS.



1. Un client ONVIF se connecte au VMS XProtect via le serveur ONVIF Bridge sur Internet. Pour cela, le client ONVIF doit avoir l'adresse IP ou le nom de domaine (domain/hostname) du serveur où est installé Milestone ONVIF Bridge, et le numéro de port ONVIF.
2. Le serveur ONVIF Bridge se connecte au serveur de gestion pour autoriser l'utilisateur du client ONVIF.
3. Une fois l'autorisation accordée, le serveur d'enregistrement commence à envoyer les flux vidéo H.264 des caméras au serveur ONVIF Bridge.

   Remarque : Si une caméra prend en charge les flux multiples, seul le flux par défaut est envoyé.
4. Le serveur ONVIF Bridge envoie la vidéo en tant que flux RTSP au client ONVIF.
5. L'utilisateur du client ONVIF peut Pan/Tilt/Zoom les caméras PTZ, si ces fonctions sont disponibles.

Remarque : Milestone vous recommande d'installer le serveur ONVIF Bridge dans une zone démilitarisée (DMZ).

Licence

Milestone ONVIF Bridge ne nécessite aucune licence supplémentaire. Vous pouvez télécharger et installer le logiciel gratuitement depuis le site web de Milestone Systems.

Installation de Milestone ONVIF Bridge

Quand vous installez Milestone ONVIF Bridge, vous installez un serveur et un module d'extension pour Management Client, qui sont les composants de gestion centraux des produits XProtect Advanced VMS et XProtect Professional VMS respectivement. Par exemple, vous utilisez ces composants pour gérer les caméras, configurer les utilisateurs, accorder des permissions etc.

Vous pouvez installer et ajouter plusieurs Milestone ONVIF Bridge à votre système. Mais cela augmente la charge sur le réseau et peut avoir un impact sur la performance. En général, un seul Milestone ONVIF Bridge est ajouté à un système car plusieurs clients ONVIF peuvent se connecter via un seul pont.

Versions prises en charge des produits XProtect video management software et Milestone Husky

Vous pouvez utiliser Milestone ONVIF Bridge avec n'importe quelle version du produit XProtect video management software ou Milestone Husky.

Configuration système

L'ordinateur sur lequel vous voulez installer le composant de serveur Milestone ONVIF Bridge doit avoir accès à Internet et avoir le logiciel suivant installé :

- Microsoft® .NET Framework 3.5.
- Microsoft® .NET Framework 4.5.1 ou supérieur.
- Visual C++ Redistributable Package for Visual Studio 2013 (x64).

Important : Les caméras doivent prendre en charge les flux H.264 via Internet.

Quels composants sont installés ?

Pendant l'installation, les composants suivants sont installés :

- Le serveur Milestone ONVIF Bridge, y compris le service Milestone ONVIF Bridge, le service Milestone RTSP Bridge et Milestone ONVIF Bridge Manager.
- Le module d'extension Milestone ONVIF Bridge. Ce module d'extension sera disponible dans le nœud des serveurs dans Management Client. Ceci se produit automatiquement si vous utilisez une méthode d'installation **Typique**. Si vous choisissez une installation **Personnalisée**, vous l'installerez durant une seconde étape.

L'installation fait également les choses suivantes :

- Inscrit et lance le service Milestone ONVIF Bridge et le service Milestone RTSP Bridge
- Lance Milestone ONVIF Bridge Manager, disponible dans la zone de notification Windows sur le serveur où le serveur ONVIF Bridge est installé

Remarque : Les actions dans ONVIF Bridge Manager s'appliquent au service Milestone ONVIF Bridge et au service Milestone RTSP Bridge. Par exemple, quand vous démarrez ou arrêtez le service ONVIF Bridge, le service Milestone RTSP Bridge démarre ou s'arrête également.

Avant de commencer

Avant de commencer l'installation, obtenez les informations suivantes :

- Le nom de domaine et le mot de passe du compte utilisateur dédié créé pour Milestone ONVIF Bridge. Pour en savoir plus, consulter la section intitulée Contrôles de sécurité Milestone ONVIF Bridge (voir "À propos de Milestone ONVIF Bridge" á la page 398).
- L'URL ou l'adresse IP et le numéro de port du serveur de gestion.

Vous aurez besoin de ces informations pendant l'installation.

Installation d'Milestone ONVIF Bridge

Téléchargez le fichier d'installation :

1. Sur l'ordinateur où vous souhaitez installer Milestone ONVIF Bridge, rendez-vous sur le site web https://www.milestonesys.com/support/download-software/ de Milestone et localisez le produit Milestone ONVIF Bridge.
2. Cliquez sur le fichier d'installation Milestone ONVIF Bridge.
3. Sélectionnez **Exécuter** ou **Enregistrer** et suivez les instructions.

Lancez l'installateur :

1. Choisissez la langue que vous souhaitez utilisez puis cliquez sur **Continuer**.
2. Lisez et acceptez les conditions du contrat de licence et cliquez sur Continuer.
3. Sélectionnez le type d'installation de la manière suivante :
   - Cliquez sur **Typique** pour installer le serveur et le module d'extension ONVIF Bridge sur un ordinateur, et appliquer les paramètres par défaut. Allez à l'étape 7.
   - Cliquez sur **Personnalisé** pour installer le serveur et le module d'extension ONVIF Bridge sur plusieurs ordinateurs. Utilisez cette méthode si vous avez un système distribué. Si vous choisissez **Personnalisé**, sélectionnez l'option serveur puis cliquez sur **Continuer**.
4. Pour établir une connexion au serveur de gestion, spécifiez les informations suivantes :
   - L'URL ou l'adresse IP et le numéro de port du serveur de gestion. Port par défaut : 80. Si vous omettez le numéro de port, le système utilisera le port 80.
   - Le nom et le mot de passe de l'utilisateur de domaine de l'utilisateur Windows ou basique que le service utilisera. Cliquez sur **Continuer**.
   - **Remarque :** Laissez **Compte utilisateur** dans le champ **Connexion en tant que**.
5. Sélectionnez l'emplacement du fichier et la langue du produit et cliquez sur **Installer**.
6. Une fois l'installation terminée, une liste de composants correctement installés s'affiche. En fonction de la méthode d'installation choisie, faites l'une des choses suivantes :
   - Si vous avez choisi une installation **Typique**, cliquez sur **Fermer**.
   - Si vous avez choisi une installation **Personnalisée**, cliquez sur Fermer puis installez le module d'extension ONVIF Bridge sur l'ordinateur où Management Client est installé. Pour installer le module d'extension, exécutez à nouveau l'installateur sur cet ordinateur.

Les composants suivants sont à présent installés :

- Serveur Milestone ONVIF Bridge.
- Le module complémentaire Milestone ONVIF Bridge visible dans Management Client dans le nœud **Serveurs**.
- Le Gestionnaire Milestone ONVIF Bridge en cours d'exécution et accessible dans la zone notification sur le serveur avec le serveur ONVIF Bridge installé.
- Le service Milestone ONVIF Bridge enregistré en tant que service.

Vous êtes prêt pour la configuration initiale (voir "Configuration d'Milestone ONVIF Bridge" á la page 403).

Configuration d'Milestone ONVIF Bridge

Après avoir installé Milestone ONVIF Bridge, le service ONVIF Bridge fonctionne et l'icône dans la barre d'état du système devient verte. Ensuite :

- Ajoutez le module d'extension ONVIF Bridge au Management Client
- Activez les clients ONVIF pour qu'ils puissent accéder à votre produit XProtect video management software

Ajoutez un Milestone ONVIF Bridge au Management Client

1. Ouvrez le Management Client.
2. Déroulez **Serveurs**, faites un clic-droit sur **ONVIF Bridge**, et sélectionnez **Ajouter nouveau**.
3. Saisissez un nom pour le Milestone ONVIF Bridge et cliquez sur **OK**.

Configurez les paramètres utilisateur pour un client ONVIF

Avant de pouvoir terminer ces étapes, vous devez déjà avoir créé un utilisateur basique dans Management Client, ou un utilisateur Windows dans Active Directory pour le client ONVIF. Un rôle ayant la permission d'afficher les caméras et d'accéder à Milestone ONVIF Bridge doit être attribué à l'utilisateur. Pour en savoir plus, consultez la section intitulée « Contrôles de sécurité Milestone ONVIF Bridge » dans À propos d'Milestone ONVIF Bridge (voir "À propos de Milestone ONVIF Bridge" á la page 398). Pour avoir des informations à propos de la manière de configurer un utilisateur basique dans Management Client, consultez l'aide de ces programmes.

Pour donner à un client ONVIF l'accès à votre XProtect video management software, suivez les étapes ci-dessous :

1. Ouvrez le Management Client.
2. Déroulez **Serveurs**, sélectionnez **ONVIF Bridge** et sélectionnez le pont que vous venez d'ajouter.
3. Dans l'onglet **Paramètres utilisateur**, saisissez le nom d'utilisateur de domaine (domain/user) et le mot de passe de l'utilisateur dédié créé pour le client ONVIF.
4. Cliquez sur le bouton **Ajouter utilisateur**.

Le nom de l'utilisateur du client ONVIF s'affiche dans la liste des **Identifiants d'utilisateur ONVIF**.

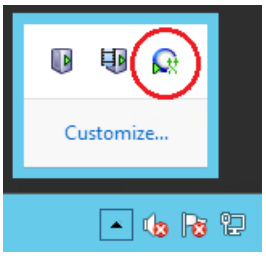
Gestion de Milestone ONVIF Bridge

Après avoir configuré Milestone ONVIF Bridge, vous pouvez surveiller le service et modifier les paramètres de configuration de plusieurs manières.

Vérifier l'état du service ONVIF Bridge

Pour afficher l'état du service ONVIF Bridge, suivez les étapes ci-dessous.

1. Sur l'ordinateur où est installé le serveur ONVIF Bridge, regardez dans la zone des notifications. L'icône de la barre ONVIF Bridge indique l'état du service ONVIF Bridge. Si le service est en cours d'exécution, l'icône est verte.



2. S'il n'est pas en cours d'exécution, l'icône est jaune ou rouge. Faites un clic droit sur l'icône et sélectionnez **Démarrer le service ONVIF Bridge**.

Afficher des journaux

Le Gestionnaire ONVIF Bridge enregistre les informations de connexion du serveur ONVIF Bridge et les flux RTSP.

1. Dans la zone notification de l'ordinateur sur lequel le serveur ONVIF Bridge est installé, faites un clic droit sur l'icône de la barre ONVIF Bridge.
2. Sélectionnez **Afficher le journal ONVIF le plus récent** ou **Afficher le journal RTSP le plus récent**.

Changez le niveau des informations dans vos journaux

Le Gestionnaire ONVIF Bridge enregistre les informations de connexion du serveur ONVIF Bridge et les flux RTSP.

Pour changer le niveau d'information, suivez ces étapes :

1. Cliquez droit sur l'icône de la barre ONVIF Bridge puis arrêtez le service ONVIF Bridge.
2. Faites de nouveau un clic droit sur l'icône de la barre ONVIF Bridge et sélectionnez **Configuration**.
3. Dans les champs **Niveau de journalisation pour ONVIF** et **Niveau de journalisation pour RTSP**, spécifiez le type d'information et la quantité d'information que vous souhaitez enregistrer dans vos journaux ONVIF et RTSP. La valeur par défaut est Information.

   Remarque : Du haut en bas dans la liste, les options sont organisées du niveau le plus bas au niveau le plus haut. Chaque niveau inclut le niveau supérieur dans la liste. Par exemple,

le niveau Avertissement inclut le niveau Erreur. Si vous le pouvez, utilisez seulement les niveaux d'information Erreur, Avertissement et Informations. Les niveaux Tracé et Message capturent plus d'informations et utilisent plus d'espace sur le disque, ce qui peut réduire la performance.

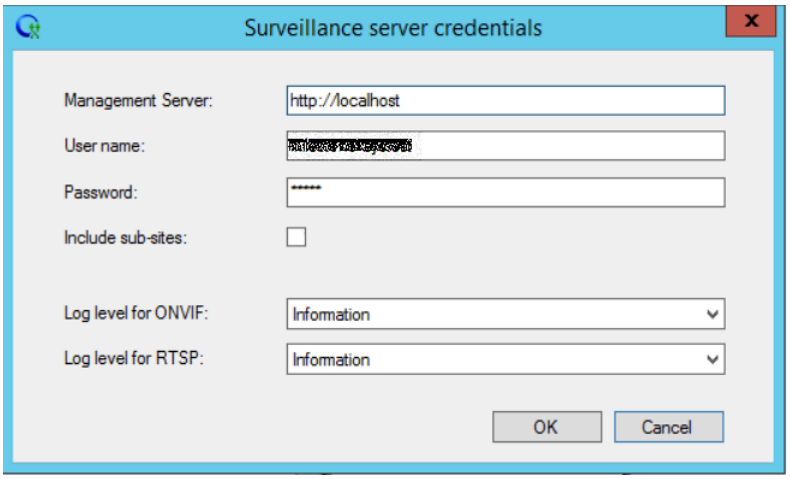
4. Cliquez sur **OK**.
5. Cliquez droit sur l'icône de la barre ONVIF Bridge puis démarrez le service ONVIF Bridge.

Changez les paramètres de configuration pour Milestone ONVIF Bridge

Si vous modifiez l'adresse IP ou le nom d'hôte du serveur de surveillance ou si vous avez modifié les comptes d'utilisateur ayant accès au service du serveur de surveillance, vous devez également mettre à jour ces informations pour Milestone ONVIF Bridge, pour permettre au service ONVIF Bridge de continuer à fonctionner.

Pour changer l'adresse VMS ou les paramètres de connexion, suivez ces étapes :

1. Sur l'ordinateur où le serveur Milestone ONVIF Bridge est installé, cliquez droit sur l'icône de la barre ONVIF Bridge puis arrêtez le service ONVIF Bridge.
2. Faites de nouveau un clic droit sur l'icône de la barre ONVIF Bridge et sélectionnez **Configuration**.



3. Indiquez les nouvelles informations puis cliquez sur **OK**.

Remarque : Vous devez utiliser le nom de domaine qualifié complet ou l'adresse IP du serveur où le serveur de gestion est installé.

4. Cliquez droit sur l'icône de la barre ONVIF Bridge puis démarrez le service ONVIF Bridge.

Le service ONVIF Bridge est à présent en cours d'exécution et l'icône de la barre devient verte.

Inclure les sous-sites

Par défaut, Milestone ONVIF Bridge est configuré pour exclure les sous-sites. Cela signifie que les utilisateurs du client ONVIF ne peuvent pas accéder à la vidéo à partir des caméras installées dans les sous-sites.

Vous pouvez modifier ce paramètre pour inclure les sous-sites. Mais Milestone vous recommande de le faire uniquement pour les systèmes où les sous-sites ne contiennent pas de grands nombres de caméras. En effet, Milestone ONVIF Bridge agrège et affiche toutes les caméras, y compris

celles des sous-sites, dans une seule liste. Par exemple, si le système et les sous-sites contiennent plus de 50 caméras, la liste devient difficile à utiliser.

Astuce : Si vous devez inclure les sous-sites, envisagez d'installer Milestone ONVIF Bridge sur chaque serveur de gestion. Vous aurez plusieurs listes de caméras, mais les caméras seront plus faciles à identifier et à naviguer.

Pour inclure les sous-sites.

1. Cliquez droit sur l'icône de la barre ONVIF Bridge puis arrêtez le service ONVIF Bridge.
2. Faites de nouveau un clic droit sur l'icône de la barre ONVIF Bridge et cliquez sur **Configuration**.
3. Sélectionnez l'option **Inclure sous-sites** et cliquez sur **OK**.
4. Cliquez droit sur l'icône de la barre ONVIF Bridge puis démarrez le service ONVIF Bridge.

Conseils et astuces

La configuration créée par le Gestionnaire ONVIF Bridge est enregistrée localement dans un fichier situé à ProgramData\Milestone\Milestone ONVIF Bridge. Le nom du fichier est serverconfiguration.xml. Si ce fichier est supprimé, vous devez actualiser la configuration dans ONVIF Bridge Manager.

Pour actualiser une configuration, suivez les étapes décrites dans la section de ce document intitulée Modifier les paramètres de configuration d'un Milestone ONVIF Bridge.

Propriétés d'Milestone ONVIF Bridge

Cette section donne des informations à propos des paramètres de gestion des utilisateurs et des connexions, et des paramètres de configuration des caméras.

Onglet Paramètres utilisateur (propriétés)

Le tableau ci-dessous décrit les paramètres du serveur ONVIF Bridge et des clients ONVIF.

Nom	Description
Port ONVIF	Le numéro du port ONVIF. Les clients ONVIF utilisent ce port pour se connecter au serveur ONVIF Bridge. Le numéro de port par défaut est 580.
Port RTSP	Le numéro du port RTSP. Le serveur ONVIF Bridge envoie les flux vidéo RTSP aux clients ONVIF via ce port. Le numéro de port par défaut est 554.
Identifiants d'utilisateur ONVIF	Liste des utilisateurs client ONVIF qui ont accès au système XProtect VMS via le serveur ONVIF Bridge.
Nom d'utilisateur	Le nom de l'utilisateur de domaine de l'utilisateur créé pour un client ONVIF. Préalable : Vous avez configuré les utilisateurs client ONVIF comme utilisateurs dans Management Client pour leur donner accès aux caméras et au Milestone ONVIF Bridge.
Mot de passe	Le mot de passe de l'utilisateur du client ONVIF.

Nom	Description
Ajouter un utilisateur	Une fois que vous avez saisi un nom d'utilisateur domaine et un mot de passe, cliquez sur le bouton **Ajouter l'utilisateur** pour l'ajouter.
Supprimer un utilisateur	Empêche un client ONVIF d'accéder à Milestone ONVIF Bridge. Supprime un utilisateur sélectionné de la liste des **identifiants utilisateur ONVIF**.

Onglet paramètres avancés (propriétés)

Les paramètres avancés pour ONVIF Bridge répertorient les paramètres par défaut de toutes les caméras qu'ONVIF Bridge fournit aux clients ONVIF lorsque les clients se connectent et demandent des flux vidéo.

Les paramètres ne reflètent pas la configuration réelle des caméras et n'ont aucune incidence sur le flux vidéo. Le système utilise ces paramètres pour accélérer l'échange de vidéo entre ONVIF Bridge et le client ONVIF. Le client ONVIF utilisera les paramètres réels du flux RTSP.

Vous pouvez modifier les paramètres par défaut qu'ONVIF Bridge fournit au client ONVIF, par exemple si vous voulez que les valeurs reflètent la configuration réelle des caméras.

Nom	Description
Jours de rétention max	La valeur par défaut est 30.
Images par seconde	La valeur par défaut est 5.
Largeur	La valeur par défaut est 1920. Ceci correspond à la qualité full HD.
Hauteur	La valeur par défaut est 1080. Ceci correspond à la qualité full HD.
Débit binaire Kbps	La valeur par défaut est 512.
Taille GOP	La valeur par défaut est 5.
Codec	Sélectionnez l'un des profils de codec H.264. La valeur par défaut est le Profil de base H.264.
Utiliser des configurations de caméras	Activez cela pour utiliser la configuration actuelle des caméras au lieu des valeurs moyennes par défaut définies ci-dessus. **Remarque :** Si vous activez ce paramètre, le temps de réponse entre le système XProtect et les clients ONVIF augmente.

Utiliser les clients ONVIF pour voir les flux vidéo

Les clients ONVIF peuvent être de nombreuses choses différentes, qui vont de systèmes de surveillance personnalisés avancés à des lecteurs média basiques.

Cette section donne des exemples de la manière de connecter un client réseau vidéo et un lecteur média au Milestone ONVIF Bridge.

Utiliser un client réseau vidéo pour voir un flux en direct

Cet exemple décrit comment installer le gestionnaire de périphériques ONVIF et le configurer pour diffuser des vidéos en direct depuis une installation XProtect Advanced VMS.

Le dispositif de périphériques ONVIF est un client réseau vidéo en source ouverte gratuit de iDeviceDesign conforme aux normes ONVIF. Cet outil est largement utilisé car il facilite la découverte et la visualisation des vidéos provenant de caméras compatibles ONVIF sur un réseau. Notez cependant que vous pouvez utiliser le gestionnaire de périphériques ONVIF uniquement pour diffuser des vidéos en direct. Vous ne pouvez pas non plus capturer et enregistrer les données vidéo du flux.

Avant de commencer, obtenez les informations suivantes auprès de la personne qui gère l'installation XProtect Advanced VMS :

- Les identifiants de connexion utilisateur créés pour Milestone ONVIF Bridge.

L'adresse IP ou le nom de l'ordinateur où est installé le Milestone ONVIF Bridge Pour installer le gestionnaire de périphériques ONVIF, suivez les étapes ci-dessous :

1. Allez à https://sourceforge.net/projects/onvifdm (https://sourceforge.net/projects/onvifdm), puis téléchargez et exécutez l'installateur. Vous pouvez installer le gestionnaire de périphériques ONVIF sur n'importe quel ordinateur.
2. Une fois l'installation terminée, une icône apparaît sur votre bureau. Double cliquez l'icône pour lancer le gestionnaire de périphériques ONVIF.
3. Quand vous démarrez le gestionnaire de périphériques ONVIF, il découvre automatiquement les périphériques conformes à ONVIF sur le réseau. Mais il est possible qu'il ne découvre pas Milestone ONVIF Bridge.
   - S'il le découvre, passez à l'étape 6.
   - S'il ne le découvre pas, ajoutez ONVIF Bridge manuellement. Passez à l'étape 4.
4. Pour ajouter un Milestone ONVIF Bridge, cliquez sur **AJOUTER**.
5. Dans la boîte de dialogue **Ajouter un périphérique**, dans le champ **URL**, indiquez le nom ou l'adresse IP de l'ordinateur où est installé Milestone ONVIF Bridge, et le numéro de port ONVIF. Par exemple, la chaîne devrait prendre cette forme : http://<IP address>:580/onvif/device_service.
6. Lorsque vous avez ajouté ONVIF Bridge, il est disponible en bas de la liste **Périphériques**. Sélectionnez-le.
7. Saisissez les identifiants de l'utilisateur basique créé pour le client ONVIF en haut de la liste. Pour le nom de l'utilisateur, vous devez saisir le nom de l'utilisateur du domaine.
8. Redémarrez le service ONVIF Bridge pour appliquer le changement.

Utiliser un lecteur média pour afficher un flux vidéo

Cet exemple décrit comment utiliser le lecteur média VLC pour récupérer et afficher un flux vidéo en direct ou une vidéo enregistrées depuis une caméra dans une installation XProtect Advanced VMS.

Le lecteur média VLC est un lecteur multimédia en source ouverte gratuit de VideoLan qui prend en charge différents protocoles de diffusion, dont RTSP. Par exemple, l'utilisation du lecteur média VLC est utile quand vous souhaitez un moyen très rapide de vous connecter à une caméra ou simplement pour tester la connexion à une caméra.

Quand vous vous connectez à une caméra pour afficher une vidéo enregistrée, le Milestone ONVIF Bridge diffuse les séquences vidéo en commençant par la première.

Avant de commencer, obtenez les informations suivantes auprès de la personne qui gère l'installation XProtect Advanced VMS :

- Les identifiants de connexion du compte utilisateur affecté au Milestone ONVIF Bridge.
- L'adresse IP ou le nom de l'ordinateur où est installé le Milestone ONVIF Bridge.
- Le GUID du périphérique depuis lequel vous voulez diffuser la vidéo.

Astuce : Le GUID de la caméra est disponible dans Management Client. Pour trouver le GUID, sélectionnez le serveur d'enregistrement où la caméra a été ajoutée puis sélectionnez la caméra. Cliquez sur l'onglet **Infos,** appuyez longuement sur CTRL sur votre clavier puis cliquez sur l'aperçu vidéo de la caméra.

Cette description est basée sur VLC 2.2.4 pour Windows.

Pour installer le lecteur média VLC et le connecter à un XProtect Advanced VMS, suivez ces étapes :

1. Allez à http://www.videolan.org/vlc/index.html et téléchargez l'installateur du lecteur média VLC.
2. Exécutez l'installateur et suivez les instructions à chaque étape.
3. Sur la barre d'outils, cliquez sur **Média**, puis sélectionnez **Ouvrir le flux réseau**.
4. Dans la boîte de dialogue **Ouvrir média**, saisissez la chaîne RSTP suivante. Remplacez les variables entre crochets « <ONVIF Bridge IP Address> » et « <Camera GUID> » par les informations correctes :
   - Pour voir un flux vidéo en direct, saisissez **rtsp://<ONVIF Bridge IP Address>:554/live/<Camera GUID>**
   - Pour voir une vidéo enregistrée, saisissez **rtsp://<ONVIF Bridge IP Address>:554/vod/<Camera GUID>**
5. Cliquez sur **Lecture**, puis saisissez l'identifiant et le mot de passe du compte utilisateur qui a été ajouté à Milestone ONVIF Bridge.

Multi-domaines avec confiance à sens unique

Configuration avec approbation à sens unique

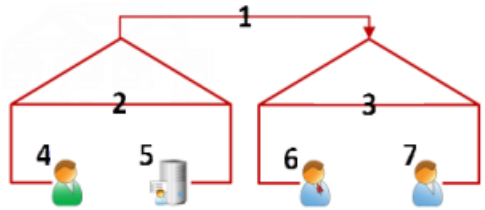
Si vous exploitez votre système dans un environnement multi-domaines, vous pouvez configurer cette installation avec une approbation à sens unique. Le système est installé sur le domaine **d'approbation** et les utilisateurs se connectent depuis les domaines **d'approbation** et les domaines **approuvés**.

1. Créez un compte de service dans le domaine **approuvé**. Vous pouvez le nommer comme vous le souhaitez, par exemple, **svcMilestone**.
2. Ajoutez le nouveau compte de service aux groupes d'utilisateurs Windows locaux suivants sur le serveur exploitant le système, dans le domaine **d'approbation** :

- Administrateurs
- IIS_IUSRS (Windows Server 2008, nécessaire pour les pools d'applications Internet Information Services (IIS))
- IIS_WPG (Windows Server 2003, nécessaire pour les pools d'applications IIS).

3. Veillez à ce que le compte de service possède des droits d'administrateur système sur votre base de données SQL ou SQL Server Express, soit directement soit par le biais du groupe **BUILTIN\Administrators**.
4. Configurez l'identité du pool d'applications **ManagementServerAppPool** dans l'IIS sur le compte de service.
5. Redémarrez le serveur pour garantir la prise d'effet de tous les changements d'adhésion et d'autorisation du groupe.

Important : Pour ajouter des utilisateurs du domaine **approuvé** aux rôles nouveaux ou existants du système XProtect, connectez-nous sur Windows en tant qu'utilisateur du domaine **approuvé**. Ensuite, lancez le Management Client et connectez-vous en tant qu'utilisateur du domaine d'**approbation** ou du domaine **approuvé**. Si vous vous connectez sur Windows en tant qu'utilisateur du domaine **d'approbation**, vous devez indiquer vos identifiants pour le domaine **approuvé** pour pouvoir rechercher des utilisateurs.



Exemple d'illustration d'environnements multi-domaines avec approbation à sens unique.

Légende :

1. Approbation à sens unique du domaine sortant
2. MyDomain.local
3. OtherDomain.edu
4. Utilisateur du domaine d'approbation
5. Serveur de gestion
6. Compte de service Milestone
7. Utilisateur du domaine approuvé

SNMP

À propos du support de service SNMP

Votre système supporte le Simple Network Management Protocol (SNMP), un protocole standard pour surveiller et contrôler les périphériques réseau, pour gérer leur configuration, collecter des statistiques, etc.

Le système agit en tant qu'agent SNMP capable de générer un trap SNMP après activation d'une règle déclenchée. Une console de gestion SNMP tierce peut ensuite recevoir les informations sur

l'événement déclenché par règle, et les opérateurs de la console de gestion SNMP peuvent configurer leur système pour d'autres actions le cas échéant.

La mise en œuvre utilise le service SNMP Microsoft® Windows® pour déclencher les traps SNMP. Cela signifie que vous devez installer le service SNMP sur les serveurs d'enregistrement. Une fois que vous avez configuré le service SNMP via sa propre interface utilisateur, cela permet aux serveurs d'enregistrement d'envoyer des fichiers .mib (Management Information Base) à la console de gestion SNMP.

Installer le Service SNMP

1. Sur les serveurs d'enregistrement concernés, ouvrez la fonction **Programmes et fonctionnalités** de Windows.
2. Sur le côté gauche de la boîte de dialogue **Programmes et fonctionnalités**, cliquez sur **Activer ou désactiver des fonctionnalités Windows**. Cela ouvre la fenêtre **Fonctionnalité Windows**.
3. Dans la boîte de dialogue, cochez la case à côté de **Simple Network Management Protocol (SNMP)**, puis cliquez sur **OK**.

Configurer le Service SNMP

1. Sur les serveurs d'enregistrement requis, sélectionnez **Démarrer** > **Panneau de Configuration** > **Outils administratifs** > **Services**.
2. Double cliquez sur le Service SNMP.
3. Sélectionnez l'onglet **Traps**.
4. Spécifiez un nom de communauté, et cliquez sur le bouton **Ajouter à la liste**.
5. Sélectionnez l'onglet **Destinations**.
6. Cliquez sur le bouton **Ajouter**, et spécifiez l'adresse IP ou le nom d'hôte du serveur qui exécute le logiciel du poste de gestion SNMP tiers.
7. Cliquez sur **OK**.

Serveurs XProtect Enterprise

À propos des serveurs XProtect Enterprise

Cette section n'est pertinente que si vous utilisez :

- XProtect Corporate
- votre système n'utilise pas IPv6, et
- vous avez des installations dotées de XProtect Enterprise version 7 ou supérieure.

Dans tous les autres cas, utilisez Milestone Federated Architecture ou Milestone Interconnect.

Vous pouvez ajouter des serveurs XProtect Enterprise à votre système XProtect Corporate. Lorsqu'ils sont ajoutés, les serveurs agissent comme des serveurs d'enregistrement et leurs vidéos peuvent être visualisées par les clients.

Dans le Management Client, vous pouvez voir l'état des serveurs XProtect Enterprise ajoutés. Vous devez tout de même définir tous les paramètres du serveur XProtect Enterprise (caméras, planification, droits d'utilisateur, etc.) dans le Management Application de XProtect Enterprise. Voir la documentation XProtect Enterprise.

Pour que les utilisateurs aient accès aux vidéos des serveurs XProtect Enterprise, vous devez faire correspondre les rôles dans XProtect Corporate avec les droits d'utilisateur définis sur les serveurs XProtect Enterprise.

- Ajout de serveurs XProtect Enterprise (á la page 412)
- Définir des rôles avec accès aux serveurs XProtect Enterprise (á la page 412)
- Modifier les serveurs XProtect Enterprise (á la page 413)

Ajout de serveurs XProtect Enterprise

Même si le système XProtect Enterprise possède une configuration interne maître/esclave, vous ne pouvez pas la réutiliser dans votre système XProtect Corporate. Vous devez ajouter individuellement chaque serveur XProtect Enterprise dont les données des périphériques vous sont nécessaires.

Pour ajouter un serveur XProtect Enterprise existant à votre système, procédez comme suit :

1. À partir du menu **Outils** du Management Client, sélectionnez **Serveurs Enterprise**.
2. Dans la boîte de dialogue **Ajouter/Supprimer serveurs Enterprise**, cliquez sur **Ajouter**.
3. Saisissez l'adresse IP ou le nom d'hôte du serveur XProtect Enterprise.
4. Saisissez le numéro de port utilisé par le serveur XProtect Enterprise.

   Le numéro de port par défaut est 80. En cas de doute, vous trouverez le numéro de port dans l'application de gestion de XProtect Enterprise, dans Accès au serveur.
5. Saisissez les certificats utilisateur pour l'administrateur du serveur XProtect Enterprise afin de vous conférer des droits illimités pour les données des périphériques à partir de celui-ci.
6. Si le système XProtect Corporate accède au serveur XProtect Enterprise par le biais d'une connexion Internet, cliquez sur **Réseau** pour spécifier l'adresse WAN du serveur de gestion de XProtect Corporate. Vous devez définir l'adresse WAN une seule fois.

L'étape suivante consiste à permettre aux utilisateurs d'accéder aux périphériques à partir du serveur XProtect Enterprise.

Définir des rôles avec accès aux serveurs XProtect Enterprise

Pour permettre aux utilisateurs d'accéder aux périphériques à partir des serveurs XProtect Enterprise :

1. Sur le serveur XProtect Enterprise, ouvrez l'application de gestion pour trouver un utilisateur XProtect Enterprise qui possède des droits d'utilisateur que vous pouvez réutiliser et associer à un rôle dans votre système XProtect Corporate. Sinon, créez un

nouvel utilisateur XProtect Enterprise qui correspond au rôle dans votre système XProtect Corporate.

2. Veuillez noter soigneusement le nom d'utilisateur, le mot de passe et le type d'authentification (basique ou Windows) de l'utilisateur XProtect Enterprise. Le système XProtect Corporate ne vérifie pas que les informations que vous spécifiez ultérieurement dans ces étapes correspondent à un utilisateur défini dans XProtect Enterprise.
3. Dans le volet **Navigation du Site** du Management Client XProtect Corporate, développez l'onglet **Sécurité** et sélectionnez **Rôles**.
4. Sélectionnez le rôle que vous souhaitez utiliser ou définissez un nouveau rôle.
5. Au bas du volet **Paramètres des rôles**, sélectionnez l'onglet **Serveurs** puis le serveur XProtect Enterprise.
6. Sélectionnez l'utilisateur XProtect Enterprise avec les droits d'utilisateur que vous souhaitez associer à votre rôle.
7. Cliquez sur **Enregistrer**.

Modifier les serveurs XProtect Enterprise

Pour ajouter un serveur XProtect Enterprise ajouté à votre système, procédez comme suit :

1. À partir du menu **Outils**, sélectionnez **Serveurs Enterprise**.
2. Sélectionnez le serveur XProtect Enterprise dans la liste et cliquez sur **Modifier**.
3. Modifiez les paramètres concernés et cliquez sur **OK.**

Maintenance du système

Ports utilisés par le système

Les ports sont entrants et sortants, sauf indication contraire. Les numéros de port sont les numéros par défaut. En cas de besoin, vous pouvez modifier les numéros de port. Contactez l'assistance Milestone si vous avez besoin de modifier des ports ne pouvant pas être configurés par le biais du Management Client.

Numéro de port	Protocole	Utilisé par	Objectif
25	SMTP	Serveurs d'enregistrement	Écouter des messages depuis des périphériques pour activer des événements et pour recevoir des images pré et post-enregistrement. Le port est désactivé par défaut.
80	HTTP	Les IIS sur le serveur de gestion	L'exécution du service de serveur de gestion.
443	HTTPS	Serveur de gestion et canal de service	Authentification des utilisateurs de base.
554	RTSP	Serveurs d'enregistrement	Trafic qui contrôle le flux à partir de caméras.
1234	TCP/UDP	Serveur d'événements	Écouter des événements génériques de systèmes ou de périphériques externes.
1235	TCP	Serveur d'événements	Écouter des événements génériques de systèmes ou de périphériques externes.
1433	TCP	Tous les processus dans le système (entre autres le serveur de gestion, le serveur de journaux et le serveur d'événements)	Communication avec le serveur SQL.
5210	TCP	Serveurs d'enregistrement, et les serveurs d'enregistrement de basculement.	Fusion des bases de données après l'exécution d'un serveur d'enregistrement de basculement.

Numéro de port	Protocole	Utilisé par	Objectif
5432	TCP	Serveurs d'enregistrement	Écouter des messages d'événements à partir des périphériques.
7474	TCP	Serveurs d'enregistrement	Communication avec l'agent d'extension SNMP. N'utilisez pas le port à d'autres fins, même si votre système n'applique pas SNMP.
7475	TCP	Serveur de gestion	Communication avec l'agent d'extension SNMP. N'utilisez pas le port à d'autres fins, même si votre système n'applique pas SNMP.
7563	TCP	Serveurs d'enregistrement et XProtect Smart Client	Communication avec l'interface ImageServer. Également la gestion des commandes de contrôle des caméras PTZ et pour la récupération de flux d'images à partir des clients, etc.
7609	HTTP	Le serveur de rapports et le service Server Data Collector	La communication entre les deux. Le port doit toujours être ouvert surle serveur exécutant le service Serveur Data Collector.
8080	UDP	Serveur de gestion	La communication entre les processus internes du serveur.
8844	UDP	Serveurs d'enregistrement de redondance	La communication entre les serveurs.
8990	TCP	Serveur de gestion	Suivi de l'état du service du serveur de basculement.
9090	TCP	Serveur d'événements	Écouter les événements analytiques des systèmes ou des dispositifs externes.
9993	TCP	Serveurs d'enregistrement et serveur de gestion	La communication entre les deux.
11000	TCP	Serveurs d'enregistrement de redondance	Interrogation de l'état des serveurs d'enregistrement.

Numéro de port	Protocole	Utilisé par	Objectif
12345	TCP	Serveur de gestion et XProtect Smart Client	Communication entre le système et les bénéficiaires Matrix. En cas de besoin, vous pouvez modifier le numéro de port dans le Management Client.
22331	TCP	Serveur d'événements, XProtect Smart Client et Management Client	L'entrée doit être activée pour créer des produits complémentaires XProtect, des plans XProtect Smart Client, des listes d'alarmes XProtect Smart Client et faire fonctionner les modules complémentaires MIP.
52111	TCP	XProtect Screen Recorder et les serveurs d'enregistrement	La communication entre les deux. En cas de besoin, vous pouvez modifier le numéro de port dans le Management Client.
65101	UDP	Serveurs d'enregistrement	Écouter des notifications d'événements des pilotes.

Sauvegarde et restauration de la configuration du système

À propos de la sauvegarde et de la restauration de la configuration de votre système

Milestone vous recommande de faire des sauvegardes régulières de la configuration de votre système comme mesure préventive de la récupération d'urgence. Bien que la perte de votre configuration soit un phénomène rare, cela peut arriver dans des circonstances malheureuses. Heureusement, la sauvegarde de votre configuration actuelle ne prend qu'une minute.

Le système offre une fonctionnalité intégrée qui sauvegarde toute la configuration du système que vous pouvez définir dans le Management Client. Notez que la base de données du serveur de journaux et les fichiers journaux, y compris les fichiers journaux d'audit, ne sont pas inclus dans cette sauvegarde.

Si votre système est grand, Milestone vous recommande de définir des sauvegardes planifiées. Cela se fait avec l'outil tiers : Microsoft® SQL Server Management Studio. Cette sauvegarde contient les mêmes données qu'une sauvegarde manuelle.

Lors d'une sauvegarde, le système reste en ligne. Selon la configuration de votre système, votre matériel, et le fait que vous ayez installé le serveur SQL, le service de serveur d'événements et le client de gestion sur un serveur unique ou sur plusieurs serveurs (une installation distribuée), la sauvegarde de la configuration du système peut prendre un certain temps.

Chaque fois que vous effectuez une sauvegarde à la fois manuelle et programmée, le fichier journal de transaction de SQL Server est vidé. Pour plus d'informations sur la façon de vider ce fichier journal, consultez le site Internet de Microsoft et recherchez « journal des transactions SQL Server ».

Sauvegarder la base de données du serveur de journaux

Gérer la base de données **Serveur journaux de surveillance** en utilisant la méthode que vous utilisez lorsque vous gérez la configuration du système comme décrit précédemment. La base de données **Serveur journaux de surveillance** (le nom peut être différent si vous avez renommé la base de données de configuration du système) contient tous vos journaux système, y compris les erreurs rapportées par les caméras et serveurs d'enregistrement.

La base de données se situe là où le service Serveur journaux SQL server est installé, à savoir généralement au même endroit que votre serveur de gestion de SQL server. La sauvegarde de cette base de données n'est pas vitale car elle ne contient aucune configuration du système. Toutefois, il est possible que vous appréciiez éventuellement d'avoir accès aux journaux système précédant la restauration/sauvegarde du serveur de gestion.

Sauvegarde et restauration manuelles de la configuration du système

À propos de la sauvegarde manuelle de la configuration de votre système

Si vous souhaitez effectuer une sauvegarde manuelle de la configuration de votre système, assurez-vous que votre système reste en ligne. Voici quelques éléments à considérer avant de commencer la sauvegarde :

- Vous ne pouvez pas utiliser une sauvegarde pour copier des configurations pour d'autres systèmes.
- La sauvegarde de votre configuration peut prendre un certain temps. Cela dépend de la configuration de votre système, de votre matériel, et si votre SQL server, votre serveur de gestion et Management Client sont installés sur le même ordinateur.
- Les journaux (y compris les journaux d'audit) ne font **pas** partie de la sauvegarde de la configuration.

À propos de la sauvegarde et de la restauration de la configuration du serveur d'événements

Le contenu de la configuration de votre serveur d'événements est inclus lorsque vous sauvegardez et restaurez la configuration du système.

La première fois que vous exécutez le serveur d'événements, tous ses fichiers de configuration sont automatiquement déplacés sur le serveur SQL. Vous pouvez appliquer la configuration restaurée au serveur d'événements sans avoir besoin de redémarrer le serveur d'événements, et le serveur d'événements peut démarrer et d'arrêter toutes les communications externes pendant que la restauration de la configuration est en cours de chargement.

À propos des scénarios de problème et d'échec de sauvegarde/restauration

Si, après votre dernière sauvegarde de la configuration du système, vous avez déplacé le serveur d'événements ou d'autres services enregistrés tels que le serveur de journaux, vous devez sélectionner la configuration du service enregistrée que vous souhaitez pour le nouveau système.

Vous pouvez décider de conserver la nouvelle configuration après que le système ait été restauré avec l'ancienne configuration. Vous choisissez en regardant les noms d'hôte des services.

Si votre restauration de la configuration du système échoue parce que le serveur d'événements ne se trouve pas à la destination spécifiée (par exemple, si vous avez choisi l'ancienne configuration de service enregistrée), effectuez une nouvelle restauration.

Sauvegarde manuelle de la configuration système

1. À partir de la barre de menu, sélectionnez **Fichier > Configuration de sauvegarde...**
2. Lisez la note dans la boîte de dialogue et cliquez sur **Sauvegarder.**
3. Entrez un nom de fichier pour le fichier .cnf.
4. Saisissez un dossier de destination et cliquez sur **Enregistrer.**
5. Attendez que la sauvegarde soit terminée, puis cliquez sur **Fermer**.

Remarque : Tous les fichiers de configuration du système concernés sont regroupés dans un seul fichier .cnf, qui est sauvegardé à un emplacement spécifique. Pendant la sauvegarde, tous les fichiers de sauvegarde sont d'abord exportés vers un dossier de sauvegarde temporaire du système sur le serveur de gestion. Vous pouvez sélectionner un autre dossier temporaire par un clic droit sur l'icône du service du serveur de gestion de la zone de notification et en sélectionnant Sélectionner le dossier de sauvegarde partagé.

Restauration d'une configuration système à partir d'une sauvegarde manuelle

Informations importantes :

- L'utilisateur qui installe et celui qui restaure doivent tous deux être des administrateurs locaux de la base de données sur le serveur de gestion **et** sur le serveur SQL.
- À l'exception de vos serveurs d'enregistrement, votre système est complètement éteint pendant la durée de la restauration, qui peut prendre plusieurs minutes.
- Une sauvegarde ne peut être restaurée que sur l'installation du système où elle a été créée. Assurez-vous que la configuration est aussi similaire que possible au moment où la sauvegarde a été effectuée. Autrement, la restauration peut échouer.
- Si vous sauvegardez la base de données et la restaurez sur un serveur SQL propre, les erreurs de la base de données ne fonctionneront pas et vous ne recevrez que des messages d'erreurs généraux du serveur SQL. Pour éviter ça, réinstallez d'abord votre système XProtect à l'aide du serveur SQL propre et restaurez la sauvegarde par-dessus.
- Si la restauration échoue au cours de la phase de validation, vous pouvez démarrer l'ancienne configuration car vous n'avez apporté aucun changement.
  Si la restauration échoue à un autre moment, vous ne pourrez pas utiliser l'ancienne configuration.
  Tant que le fichier de sauvegarde n'est pas corrompu, vous pouvez effectuer une autre restauration.
- La restauration remplace la configuration actuelle. Cela signifie que toute modification apportée à la configuration depuis la perte de la dernière sauvegarde est perdue.
- Aucun journal, y compris les journaux d'audit, n'est restauré.

- Une fois que la restauration a commencé, vous ne pouvez pas l'annuler.

Restauration :

1. Cliquez droit sur l'icône service du serveur de gestion de la zone de notification et sélectionnez **Restaurer la Configuration**
2. Lisez la note importante et cliquez sur **Restaurer.**
3. Dans la boîte de dialogue d'ouverture de fichier, naviguez vers l'emplacement du fichier de configuration de sauvegarde, sélectionnez-le, et cliquez sur **Ouvrir.**

   Le fichier de sauvegarde se trouve sur l'ordinateur Management Client. Si le Management Client est installé sur un autre serveur, copiez le fichier de sauvegarde de ce serveur avant de sélectionner la destination.
4. La fenêtre **Restaurer la configuration** s'affiche. Attendez la fin de la restauration et cliquez sur **Fermer.**

Sélectionner le fichier de sauvegarde partagé

Avant de sauvegarder et de restaurer une configuration système, vous devez créer un fichier de sauvegarde à cette fin

1. Cliquez droit sur l'icône du service serveur de gestion de la zone de notification et sélectionnez **Sélectionner le fichier de sauvegarde partagé**.
2. Dans la fenêtre qui s'affiche, naviguez vers l'emplacement de fichier désiré.
3. Cliquez deux fois sur **OK**.
4. S'il vous est demandé si vous souhaitez supprimer des fichiers dans le fichier de sauvegarde actuel, cliquez sur **Oui** ou **Non** en fonction de vos besoins.

Sauvegarde et restauration programmées

À propos de la sauvegarde et la restauration programmées de la configuration du système

Milestone vous recommande de faire des sauvegardes régulières de la configuration de votre système comme mesure préventive de la récupération d'urgence. Bien que la perte de votre configuration soit un phénomène rare, cela peut arriver dans des circonstances malheureuses. Heureusement, la sauvegarde de votre configuration actuelle ne prend qu'une minute. Des sauvegardes régulières ont également l'avantage supplémentaire de vider le journal de transactions de votre serveur Microsoft ® SQL Server®.

Si vous avez une configuration plus petite et n'avez pas besoin de sauvegardes programmées, vous pouvez sauvegarder la configuration de votre système manuellement. Pour les instructions, voir Sauvegarde et restauration manuelles de la configuration du système (á la page 417).

Le serveur de gestion sauvegarde la configuration de votre système dans une base de données. Lorsque vous sauvegardez/restaurez le/les serveur(s) de gestion, assurez-vous que cette base de données est incluse dans la sauvegarde/restauration.

Prérequis pour l'utilisation de la sauvegarde et la restauration programmées

Microsoft® SQL Server Management Studio est un outil téléchargeable gratuitement sur son site web http://www.microsoft.com/downloads.

Outre la gestion des bases de données SQL Server, l'outil comprend des fonctions de sauvegarde et de restauration faciles à utiliser. Téléchargez et installez l'outil sur votre serveur de gestion.

À propos du Journal des transactions du serveur SQL

À chaque fois qu'une modification des données du système intervient, le Serveur SQL journalise cette modification dans son journal des transactions, que ce soit un Serveur SQL sur votre réseau ou une édition SQL Server Express.

Le journal des transactions est essentiellement une fonction de sécurité qui permet de revenir à la version précédente et d'annuler des modifications apportées à la base de données Serveur SQL. Par défaut, SQL Server stocke son journal de transactions indéfiniment et au fil du temps le journal des transactions accumulent de plus en plus d'entrées. Le journal des transactions du serveur SQL est situé par défaut sur le lecteur système et, s'il continue de croître, il peut finir par empêcher le bon fonctionnement de Windows.

Pour éviter un tel scénario, il est recommandé de purger le journal des transactions du serveur SQL de temps à autres. Cependant, la purge en elle-même ne diminue pas la taille du journal de transaction, mais elle l'empêche de croître et devenir hors de contrôle. Cependant, votre système ne purge pas automatiquement le journal des transactions du serveur SQL à intervalles spécifiques. Vous pouvez également réaliser plusieurs tâches directement sur le serveur SQL pour conserver la taille réduite du journal des transactions.

Pour plus d'informations à ce sujet, allez sur la page d'assistance Microsoft http://support.microsoft.com et recherchez journal de transaction du Serveur SQL.

Sauvegarder la configuration du système avec une sauvegarde programmée

1. Dans le menu Windows **Démarrer**, ouvrez Microsoft® SQL Server Management Studio.
2. Lors de la connexion, spécifiez le nom du serveur SQL requis. Utilisez le compte sous lequel vous avez créé la base de données.
   a) Trouvez la base de données **Surveillance** qui contient toute votre configuration du système, incluant le serveur d'événements, les serveurs d'enregistrement, les caméras, les entrées, les sorties, les utilisateurs, les règles, les profils de patrouille, entre autres.

      Nous supposons que la base de données utilise le nom par défaut.

   b) Faites une sauvegarde de la base de données **Surveillance** et assurez-vous de :
      - Vérifiez que la base de données sélectionnée est **Surveillance.**
      - Vérifiez que le type de sauvegarde est **complète.**
      - Établissez la programmation pour la sauvegarde récurrente. Vous pouvez obtenir de plus amples informations sur les sauvegardes programmées et automatiques sur le site web de Microsoft https://support.microsoft.com/en-us/kb/2019698.
      - Vérifiez que le chemin proposé est satisfaisant ou sélectionnez un autre chemin

- Sélectionner **Vérifier la sauvegarde en fin d'opération** et **Effectuer une somme de contrôle avant d'écrire sur le support**.

3. Suivez les instructions de l'outil jusqu'à la fin.

Envisagez également la sauvegarde de la base de données **JournalSurveillance** en procédant de la même manière.

Sauvegarder et restaurer la configuration du serveur d'événements

Le contenu de la configuration de votre serveur d'événements est inclus lorsque vous sauvegardez et restaurez la configuration du système. La première fois que vous exécutez le serveur d'événements, tous ses fichiers de configuration sont automatiquement déplacés sur le serveur SQL. Vous pouvez appliquer la configuration restaurée au serveur d'événements sans avoir besoin de redémarrer le serveur d'événements, et le serveur d'événements est capable de démarrer et d'arrêter toutes les communications externes pendant que la restauration de la configuration est en cours de chargement.

Restauration d'une configuration système à partir d'une sauvegarde programmée

Préalable : Afin d'empêcher les modifications de configuration pendant que vous restaurez la base de données de la configuration système, arrêtez le :

- Service Management Server (voir "Services du serveur de gestion" á la page 429)
- Service Event Server (cette démarche peut être effectuée à partir du menu **Services** de Windows (recherchez **services.msc** sur votre ordinateur. Dans **Services**, trouvez **Serveur d'événement Milestone XProtect**))
- World Wide Web Publishing Service, également connu sous le nom d'Internet Information Service (IIS). Pour découvrir comment arrêter l'IIS http://technet.microsoft.com/en-us/library/cc732317(WS.10).aspx, consultez :

Ouvrez Microsoft® SQL Server Management Studio à partir du menu **Démarrer** de Windows.

Dans l'outil, procédez comme suit :

1. Lors de la connexion, spécifiez le nom du serveur SQL requis. Utilisez le compte sous lequel la base de données a été créée.
2. Trouvez la base de données **Surveillance** qui contient toute votre configuration du système, incluant le serveur d'événements, les serveurs d'enregistrement, les caméras, les entrées, les sorties, les utilisateurs, les règles, les profils de patrouille, etc.
3. Faites une restauration de la base de données **Surveillance** et assurez-vous de :
    - Sélectionner Sauvegarder **à partir** d'un périphérique
    - Sélectionner sauvegarde du support de type **fichier**
    - Trouver et sélectionner votre fichier de sauvegarde **Surveillance.bak**
    - Sélectionner **écraser la base de données existante**.
4. Suivez les instructions de l'outil jusqu'à la fin.

Si vous avez également sauvegardé la base de données **JournalSurveillance** de l'ancien serveur de journaux, restaurez-la sur le nouveau serveur de journaux en procédant de la même façon.

Veuillez noter que le système ne fonctionne pas tant que le service Management Server est à l'arrêt. Il est important de se rappeler de démarrer les services une fois que vous avez terminé la restauration de la base de données.

Déplacer le serveur de gestion

À propos du déplacement du serveur de gestion

Vous pouvez parfois devoir déplacer l'installation du serveur de gestion d'un serveur physique à un autre. Le serveur de gestion sauvegarde la configuration de votre système dans une base de données. Si vous déplacez le serveur de gestion d'un serveur physique à un autre, il est primordial que vous vous assuriez que votre nouveau serveur de gestion a également accès à cette base de données. La base de données de la configuration système peut être enregistrée de deux manières différentes :

- **Serveur SQL réseau :** Si vous enregistrez la configuration de votre système dans une base de données sur un serveur SQL existant de votre réseau, vous pouvez identifier l'emplacement de la base de données sur le Serveur SQL lors de l'installation du logiciel du serveur de gestion sur votre nouveau serveur de gestion. Dans ce cas, seul le paragraphe suivant sur l'adresse IP et le nom d'hôte du serveur de gestion s'applique et vous devez ignorer le reste de ce thème :

  Nom d'hôte et adresse IP du serveur de gestion : Lorsque vous déplacez le serveur de gestion d'un serveur physique à un autre serveur physique, la solution la plus facile consiste à donner au nouveau serveur le même nom d'hôte et la même adresse IP que l'ancien serveur. Ceci s'explique par le fait que le serveur d'enregistrement se connecte au nom d'hôte et à l'adresse IP de l'ancien serveur de gestion. Si vous avez donné un nouveau nom d'hôte et/ou une adresse IP au nouveau serveur de gestion, le serveur d'enregistrement ne peut pas trouver le serveur de gestion. Arrêtez manuellement chaque serveur d'enregistrement de votre système, modifiez l'URL de leur serveur de gestion et, lorsque vous avez terminé, redémarrez-les.

- **Serveur SQL local :** Si vous enregistrez la configuration de votre système dans une base de données locale SQL Server directement sur le serveur de gestion, il est important que vous sauvegardiez la base de données de configuration système du serveur de gestion existant avant le déplacement. En sauvegardant la base de données, et ensuite en la restaurant sur le nouveau serveur, vous évitez d'avoir à reconfigurer vos caméras, règles, profils de temps etc. après le déplacement.

Conditions préalables

- **Votre fichier d'installation logicielle pour installation sur le nouveau serveur de gestion**.

- **Votre fichier de licence logicielle (.lic)**, que vous avez reçu lors de l'achat et de l'installation initiale de votre système. Vous ne devriez pas utiliser le fichier de licence logicielle activé que vous avez reçu après une activation manuelle des licences hors ligne. Un fichier de licence logicielle contient des informations relatives au serveur spécifique sur lequel le système est installé. Par conséquent un fichier de licence logicielle activé ne peut pas être réutilisé lors du déplacement vers un nouveau serveur.

Notez que si vous mettez également à jour le logiciel de votre système conjointement au déplacement, vous aurez reçu un nouveau fichier de licence logicielle. Il vous suffira alors d'utiliser ce dernier.

- **SQL Server local réservé aux utilisateurs : Microsoft® SQL Server Management Studio**.
- Que se passe-t-il lorsque le serveur de gestion est indisponible ? (voir "À propos des serveurs de gestion indisponibles" á la page 423)
- Copier la base de données du serveur de journaux (voir "Sauvegarder la base de données du serveur de journaux" á la page 417)

À propos des serveurs de gestion indisponibles

- **Les serveurs d'enregistrement peuvent encore enregistrer :** Tout serveur d'enregistrement en cours de fonctionnement a reçu une copie de sa configuration du serveur de gestion, donc il peut fonctionner et sauvegarder les enregistrements automatiquement pendant que le serveur de gestion est hors service. Par conséquent, l'enregistrement programmé et par détection de mouvement fonctionne, et l'enregistrement déclenché par les événements fonctionne également sous réserve d'être basé sur des événements associés au serveur de gestion ou tous autres serveurs d'enregistrement puisque ces derniers passent par le serveur de gestion.
- **Les serveurs d'enregistrement sauvegardent temporairement les données de journaux localement :** Ils envoient automatiquement les données de journaux au serveur de gestion lorsqu'il redevient disponible.
  - **Les clients ne peuvent pas s'identifier :** L'accès des clients est autorisé via le serveur de gestion. Sans le serveur de gestion, les clients ne peuvent se connecter.
  - **Les clients qui sont déjà connectés peuvent rester connectés pendant une heure :** Lorsque les clients se connectent, ils sont autorisés par le serveur de gestion et peuvent communiquer avec les serveurs d'enregistrement pour une durée d'une heure. Si vous pouvez organiser le nouveau serveur de gestion et le faire fonctionner en une heure, beaucoup de vos utilisateurs ne sont pas affectés.
  - **Impossibilité de configurer le système :** Sans le serveur de gestion, vous ne pouvez pas modifier la configuration du système.

Milestone vous recommande que vous informiez vos utilisateurs du risque de perte de contact avec le système de surveillance pendant que le serveur de gestion est hors service.

Déplacer la configuration du système

Déplacer votre configuration système est un processus en trois étapes :

1. Faites une sauvegarde de votre configuration système. Ceci est identique à une sauvegarde programmée (voir "Sauvegarder la configuration du système avec une sauvegarde programmée" á la page 420).
2. Installez le nouveau serveur de gestion sur le nouveau serveur. Voir sauvegarde programmée, étape 2.
3. Restaurez la configuration de votre système sur le nouveau système. Voir Restauration d'une configuration système à partir d'une sauvegarde programmée (á la page 421).

Gérer SQL server

À propos de la mise à jour de l'adresse de SQL server

Lorsque vous installez un système dans sa version d'essai, ou si vous restructurez une grande installation, vous devrez peut-être utiliser une base de données SQL différente. Vous pouvez le faire avec l'outil **Mettre à jour l'adresse du SQL Server**.

Avec l'outil, vous pouvez modifier les adresses des serveurs SQL utilisés par le serveur de gestion, le serveur d'événements ou encore le serveur de journaux. La seule limite vient du fait que vous ne pouvez pas changer l'adresse SQL du serveur de gestion et du serveur d'événements en même temps que l'adresse SQL du serveur de journaux. Vous pouvez le faire l'une après l'autre.

Vous devez faire des mises à jour SQL localement sur l'ordinateur où vous avez installé le serveur de gestion/d'événements **ou** le serveur de journaux. Vous ne pouvez pas le faire à partir du Management Client. Si votre serveur de gestion et votre serveur d'enregistrement ne sont pas situés sur le même ordinateur, vous pouvez quand même utiliser l'outil, mais vous devez l'exécuter sur les deux ordinateurs sur lesquels le serveur de gestion est installé, et sur l'ordinateur sur lequel le serveur d'événements est installé.

Vous devez copier les bases de données SQL avant de poursuivre.

Mettre à jour l'adresse SQL du serveur de journaux

Le serveur de gestion et le serveur de journaux situés sur le même ordinateur

1. Allez sur l'ordinateur sur lequel le serveur de gestion est installé.
2. Allez dans la zone de notification de la barre des tâches. Cliquez avec le bouton droit sur l'icône **Serveur de gestion**, puis sélectionnez **Mettre à jour l'adresse SQL**. La boîte de dialogue **Mettre à jour l'adresse du serveur SQL** s'affiche.
3. Sélectionnez **Serveur de journaux** et cliquez sur **Suivant**.
4. Entrez l'adresse du nouveau site et cliquez sur **Suivant**.
5. Sélectionnez la nouvelle base de données SQL et cliquez sur **Sélectionner**.
6. Patientez pendant que la modification de l'adresse a lieu. Cliquez sur **OK** pour confirmer.

Le serveur de gestion et le serveur de journaux situés sur des ordinateurs différents.

1. Allez sur l'ordinateur où votre serveur de gestion est installé et copiez le répertoire *%ProgramFiles%\Milestone\XProtect Management Server\Tools\ChangeSqlAddress* (et son contenu) vers un répertoire temporaire sur le serveur d'événements.
2. Collez le répertoire que vous avez copié sur un emplacement temporaire de l'ordinateur sur lequel le serveur de journaux est installé et exécutez le fichier inclus :*VideoOS.Server.ChangeSqlAddress.exe*. La boîte de dialogue **Mettre à jour l'adresse du serveur SQL** s'affiche.

3. Sélectionnez **Serveur de journaux** et cliquez sur **Suivant**.
4. Entrez l'adresse du nouveau site et cliquez sur **Suivant**.
5. Sélectionnez la nouvelle base de données SQL et cliquez sur **Sélectionner**.
6. Patientez pendant que la modification de l'adresse a lieu. Cliquez sur **OK** pour confirmer.

Mettre à jour l'adresse SQL du serveur de gestion ou du serveur d'événements

1. Si votre serveur de gestion et votre serveur d'événements sont situés :

   a) ensemble sur le même ordinateur et que vous souhaitez mettre à jour les deux adresses SQL, allez sur l'ordinateur où le serveur de gestion est installé.

   b) sur différents ordinateurs et que vous souhaitez mettre à jour l'adresse SQL du serveur de gestion (puis l'adresse SQL du serveur d'événements), allez sur l'ordinateur où le serveur de gestion est installé.

   c) sur différents ordinateurs et que vous souhaitez mettre à jour uniquement l'adresse SQL du serveur d'événements (ou que vous l'avez déjà mise à jour sur le serveur de gestion), allez sur l'ordinateur où votre serveur de gestion est installé et copiez le répertoire *%ProgramFiles%\Milestone\XProtect Management Server\Tools\ChangeSqlAddress* (et son contenu) vers un répertoire temporaire sur le serveur d'événements.

2. Si :

   - **a** et **b**, allez dans la zone de notification de la barre des tâches. Cliquez avec le bouton droit sur l'icône **Serveur de gestion**, puis sélectionnez **Mettre à jour l'adresse SQL**.
   - **c,** collez le répertoire que vous avez copié sur un emplacement temporaire de l'ordinateur sur lequel le serveur d'événements est installé et exécutez le fichier inclus :*VideoOS.Server.ChangeSqlAddress.exe*.

3. La boîte de dialogue **Mettre à jour l'adresse du serveur SQL** s'affiche. Sélectionnez **Serveur de gestion et serveur d'événements** et cliquez sur **Suivant**.
4. Entrez l'adresse du nouveau site et cliquez sur **Suivant**.
5. Sélectionnez la nouvelle base de données SQL et cliquez sur **Sélectionner**.
6. Patientez pendant que la modification de l'adresse a lieu. Lorsqu'un message de confirmation s'affiche, cliquez sur **OK**.

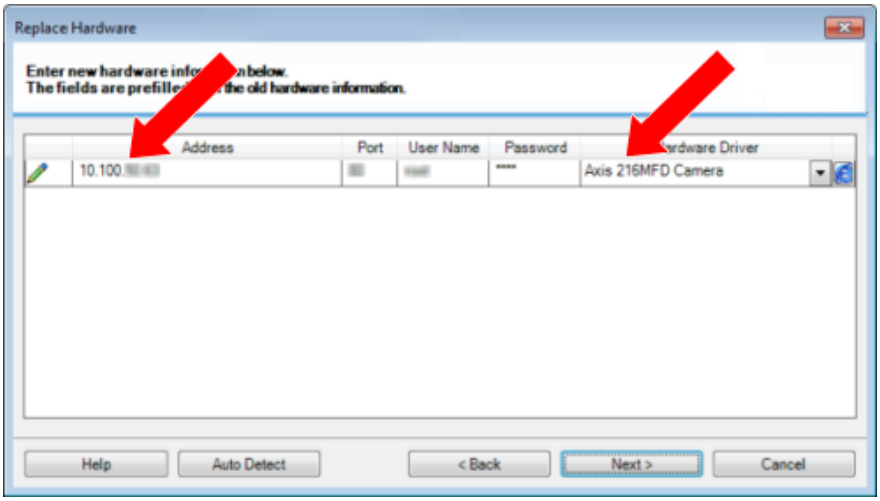
Si vous avez bien rempli l'étape **2 b**, vous avez maintenant mis à jour uniquement l'adresse SQL du **serveur de gestion**. Vous devez répéter cette procédure pour mettre à jours l'adresse SQL du **serveur d'événements**. Ce faisant, assurez-vous de sélectionner le scénario présenté à l'étape **2 c.**

Remplacer le matériel

Lorsque vous remplacez un périphérique par un autre périphérique sur votre réseau, vous devez connaître l'adresse IP, le port, le nom d'utilisateur et le mot de passe du nouveau périphérique.

Si vous n'avez pas activé l'activation automatique des licences (voir "À propos de l'activation automatique des licences" á la page 71) et si vous avez utilisé tous les changements apportés aux périphériques sans activation (voir "À propos des changements apportés aux périphériques sans activation" á la page 69), vous devez activer manuellement vos licences **après** avoir remplacé les périphériques. Si le nombre de périphériques dépasse le nombre total de licences de périphérique, vous devrez acheter de nouvelles licences.

1. Agrandissez le serveur d'enregistrement requis et faites un clic droit sur le matériel que vous souhaitez remplacer.
2. Sélectionnez **Remplacer le matériel**.
3. L'assistant **Remplacer le matériel** apparaît. Cliquez sur **Suivant**.
4. Dans l'assistant, saisissez l'adresse IP du nouveau matériel dans le champ **Adresse** (marqué par une flèche rouge dans l'illustration). Si vous le connaissez, sélectionnez le pilote pertinent dans la liste déroulante **Pilote matériel**. Autrement, sélectionnez **Détection automatique**. Si le port, le nom d'utilisateur ou le mot de passe sont différents pour le nouveau matériel, corrigez ces informations **avant de lancer le processus de détection automatique, le cas échéant**.



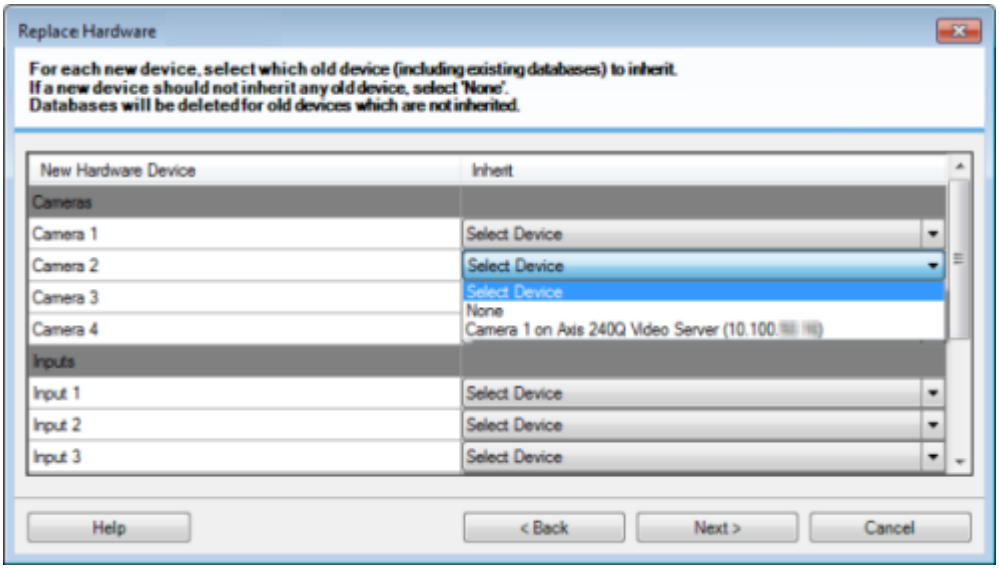
   L'assistant contient déjà les données relatives au matériel existant. Si vous le remplacez par un périphérique similaire, vous pouvez réutiliser certaines de ces informations, comme, par exemple, les informations concernant le port et le pilote.

5. Procédez comme suit :
   - Si vous avez sélectionné le pilote de périphérique requis directement dans la liste, cliquez sur **Suivant**.
   - Si vous avez sélectionné **Détection automatique** dans la liste, cliquez sur le bouton **Détection automatique**, attendez que ce processus se termine correctement (cela sera indiqué par un ✓ à gauche), cliquez sur **Suivant**.

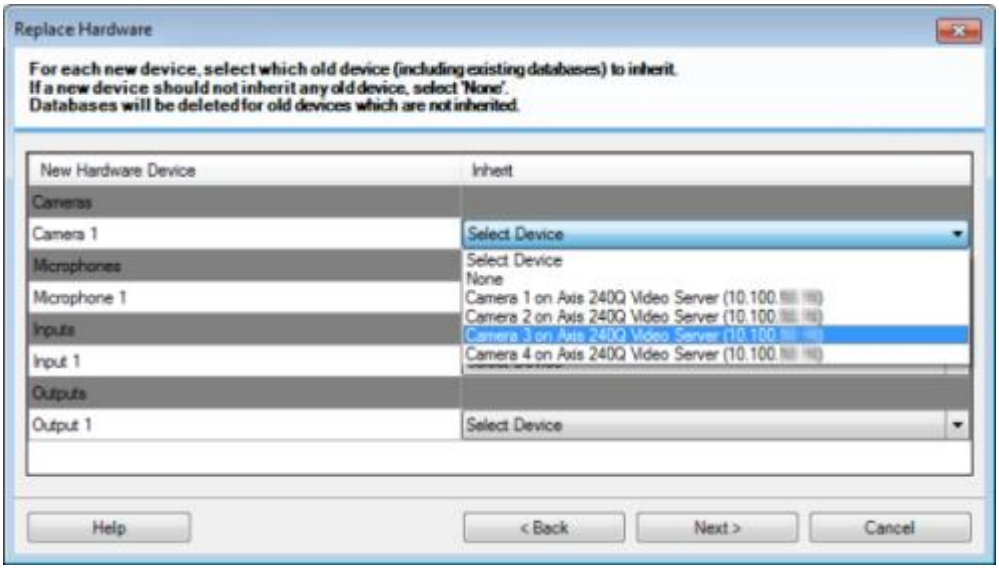
   Cette étape est conçue pour vous aider à cartographier vos périphériques et leurs bases de données, en fonction du nombre de caméras, micros, entrées et sorties individuels, etc., connectés respectivement à l'ancien périphérique et au nouveau.

   Il est important de réfléchir à la **façon** de cartographier les bases de donnée de l'ancien périphérique avec celles du nouveau périphérique. Vous pouvez cartographier des périphériques individuels, etc. en sélectionnant une caméra, un micro, une entrée, une sortie correspondante ou **Aucune** dans la colonne de droite.

Important : Veillez à cartographier **toutes** les caméras, les microphones, les entrées, les sorties, etc. Le contenu cartographié à **Aucun** est **perdu**.



Exemple d'un ancien périphérique ayant plus de périphériques individuels que le nouveau.



Cliquez sur **Suivant**.

6. Une liste s'affiche alors. Elle contient une liste de matériel à ajouter, remplacer ou supprimer. Cliquez sur **Confirmer**.
7. L'étape finale est un résumé des périphériques ajoutés, remplacés et hérités et de leurs paramètres. Cliquez sur **Copier dans le presse-papier** pour copier le contenu vers le presse-papier Windows ou/et **Fermer** pour mettre fin à l'assistant.

Remplacer un serveur d'enregistrement

Si un serveur d'enregistrement fonctionne mal et que vous souhaitez le remplacer par un nouveau serveur qui hérite des paramètres de l'ancien serveur d'enregistrement, procédez comme suit :

1. Récupérez l'identifiant du serveur d'enregistrement auprès de l'ancien serveur d'enregistrement.
   1. Sélectionnez **Serveurs d'enregistrement**, puis dans le volet **Vue d'ensemble**, sélectionnez l'ancien serveur d'enregistrement.
   2. Sélectionnez l'onglet **Stockage**.
   3. Appuyez sur la touche CTRL de votre clavier et maintenez-la enfoncée tout en sélectionnant l'onglet **Infos**.
   4. Copiez l'identifiant du serveur d'enregistrement indiqué dans la partie inférieure de l'onglet **Infos**. Ne copiez pas le terme *ID*, mais seulement le numéro.

2. Remplacez l'identifiant du serveur d'enregistrement sur le nouveau serveur d'enregistrement :
   1. Arrêtez le service Recording Server sur l'ancien serveur d'enregistrement, puis, dans la fenêtre **Services** de Windows, réglez le **Type de démarrage** du service sur **Désactivé**.

      Il est très important de ne pas démarrer simultanément deux serveurs d'enregistrement dotés d'identifiants identiques.

   2. Sur le nouveau serveur d'enregistrement, ouvrez l'explorateur et allez sur *C:\ProgramData\Milestone\XProtect Recording Server* ou le chemin où se situe votre serveur d'enregistrement.
   3. Ouvrez le fichier *RecorderConfig.xml*.
   4. Effacez l'identifiant indiqué entre les balises *<id>* et *</id>*.

   5. Collez l'identifiant du serveur d'enregistrement copié entre les balises *<id>* et *</id>*. Enregistrez le fichier *RecorderConfig.xml*.
   6. Allez au répertoire : *HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation*.
   7. Ouvrez **RecorderIDOnMachine** et changez l'ancien ID du serveur d'enregistrement au profit du nouvel ID.
   8. Redémarrez le service Recording Server. Dès que le nouveau service Recording Server démarre, le serveur d'enregistrement hérite de tous les paramètres de l'ancien serveur d'enregistrement.

Pilotes des périphériques vidéo

À propos des pilotes de périphériques vidéo

Votre système utilise les pilotes de périphériques vidéo pour contrôler et communiquer avec les périphériques de type caméra connectés à un serveur d'enregistrement. Vous devez installer les pilotes de périphérique vidéo sur chaque serveur d'enregistrement de votre système.

Lorsque vous installez votre système, les pilotes de périphérique vidéo font partie du processus d'installation initiale. Milestone publie de nouvelles versions des pilotes de périphérique vidéo à intervalles réguliers et les met à disposition sur la page de téléchargements http://www.milestonesys.com/downloads de notre site web. Lorsque vous mettez à jour les pilotes de périphériques vidéo, vous pouvez installer la dernière version de toute version que vous avez déjà installée. Arrêtez le Recording Server avant de procéder à l'installation, sinon vous devrez redémarrer l'ordinateur.

Nous vous recommandons de toujours utiliser la dernière version des pilotes de périphérique vidéo pour garantir des performances optimales.

À propos de la suppression des pilotes de périphériques vidéo

Si vous souhaitez supprimer un pilote de périphérique vidéo de votre ordinateur, vous pouvez supprimer les packs de périphérique de votre système. Pour ce faire, suivez la procédure Windows standard pour la suppression de programmes.

Si vous supprimez des pilotes de périphériques vidéo, le serveur d'enregistrement et les périphériques de type caméra ne pourront plus communiquer entre eux. Ne supprimez pas les packs de périphériques lorsque vous procédez à une mise à niveau parce que vous installez une nouvelle version en la superposant à une ancienne. Le pack de périphériques ne doit être supprimé qu'en cas de désinstallation du système complet.

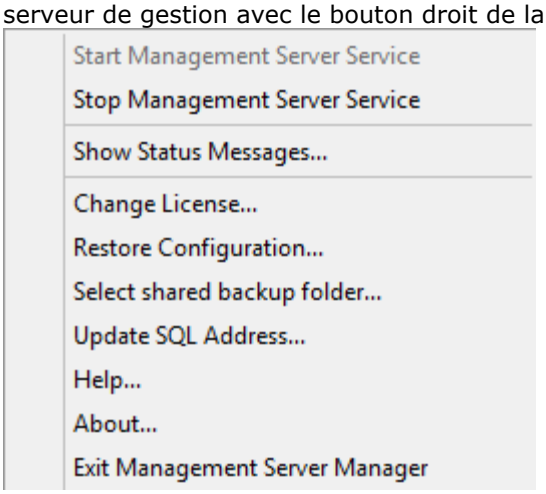
Services du serveur de gestion

L'ordinateur exécutant les serveurs contient une zone de notification dotée d'icônes de la barre des tâches. Avec ces icônes, vous pouvez accéder aux informations relatives aux services du serveur et effectuer certaines actions. Par exemple, ceci peut inclure la vérification de l'état des services, la consultation des journaux ou encore des messages d'état, ainsi que le démarrage et l'arrêt des services.

Démarrer ou arrêter le service Management Server

Dans la zone de notification, une icône de la barre des tâches indique l'état du service Management Server, par exemple : **Running** (en cours d'exécution). Par le biais de cette icône, vous pouvez démarrer ou arrêter le service Management Server. Si vous arrêtez le service Management Server, vous ne pouvez pas utiliser le Management Client.

1. Dans la zone de notification, cliquez sur l'icône de la barre des tâches correspondant au serveur de gestion avec le bouton droit de la souris. Un menu contextuel s'affiche.



2. Si le service s'est arrêté, cliquez sur **Démarrer le service Management Server** pour le lancer. L'icône de la barre des tâches reflète son nouvel état.

3. Pour arrêter le service, cliquez sur **Arrêter le service Management Server**.

Pour de plus amples informations au sujet des icônes de la barre des tâches, voir À propos des icônes de la barre des tâches (á la page 434).

Voir également

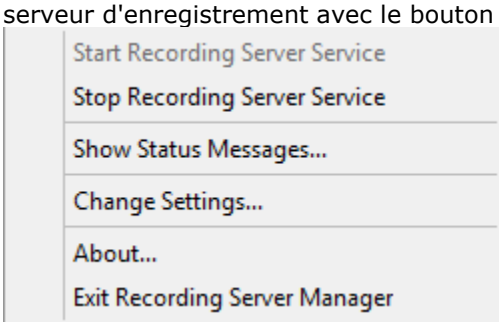
Démarrer, arrêter ou redémarrer le service Event Server (á la page 432)

Démarrer ou arrêter le service Recording Server (á la page 431)

Démarrer ou arrêter le service Recording Server

Dans la zone de notification, une icône de la barre des tâches indique l'état du service Recording Server, par exemple : **Running** (en cours d'exécution). Par le biais de cette icône, vous pouvez démarrer, arrêter ou redémarrer le service Recording Server. Si vous arrêtez le service Recording Server, votre système ne peut pas interagir avec les périphériques connectés au serveur. Cela signifie que vous ne pouvez pas visualiser la vidéo en direct ou enregistrer des vidéos.

1. Dans la zone de notification, cliquez sur l'icône de la barre des tâches correspondant au serveur d'enregistrement avec le bouton droit de la souris. Un menu contextuel s'affiche.



2. Si le service s'est arrêté, cliquez sur **Démarrer le service Recording Server** pour le lancer. L'icône de la barre des tâches reflète son nouvel état.

3. Pour arrêter le service, cliquez sur **Arrêter le service Recording Server**.

Pour de plus amples informations au sujet des icônes de la barre des tâches, voir À propos des icônes de la barre des tâches (á la page 434).

Voir également

Démarrer, arrêter ou redémarrer le service Event Server (á la page 432)

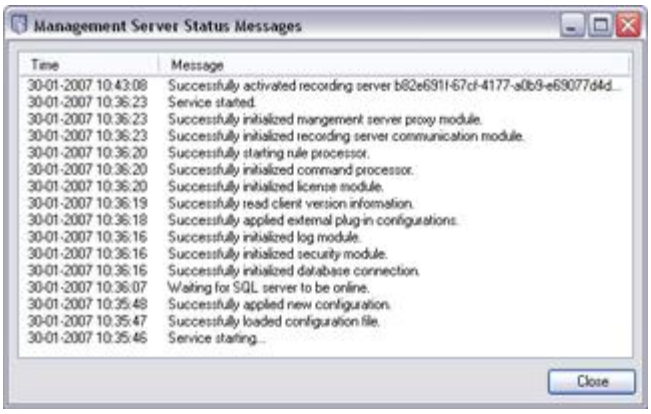
Démarrer ou arrêter le service Management Server (á la page 430)

Consulter les messages d'état relatifs au serveur de gestion ou au serveur d'enregistrement

Dans la zone de notification de l'ordinateur exécutant les serveurs, les icônes de la barre des tâches indiquent l'état du serveur de gestion et du serveur d'enregistrement. Vous pouvez consulter des messages d'état, tels que « Service démarré », à partir de ces icônes.

1. Dans la zone de notification, cliquer avec le bouton droit sur l'icône pertinente de la barre des tâches. Un menu contextuel s'affiche.

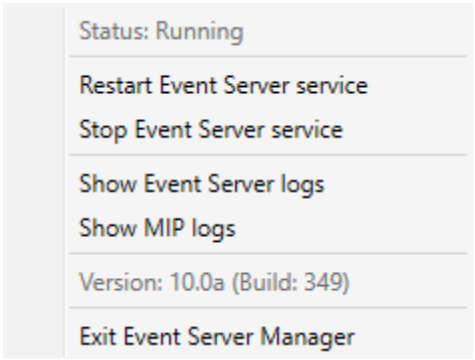
2. Sélectionnez **Afficher les messages d'état**. En fonction du type de serveur, s'affiche soit la fenêtre **Messages d'état du serveur de gestion** soit la fenêtre **Messages d'état du serveur d'enregistrement**, établissant la liste des messages d'état horodatés :



Démarrer, arrêter ou redémarrer le service Event Server

Dans la zone de notification, une icône de la barre des tâches indique l'état du service Event Server, par exemple : **Running** (en cours d'exécution). Par le biais de cette icône, vous pouvez démarrer, arrêter ou redémarrer le service Event Server. Si vous arrêtez le service, certains parties du système ne fonctionneront pas, et notamment les événements et les alarmes. Cependant, vous pourrez continuer à afficher et enregistrer des vidéos. Pour de plus amples informations, voir Arrêter le service Event Server.

1. Dans la zone de notification, cliquez sur l'icône de la barre des tâches correspondant au serveur d'événements avec le bouton droit de la souris. Un menu contextuel s'affiche.



2. Si le service s'est arrêté, cliquez sur **Démarrer le service Event Server** pour le lancer. L'icône de la barre des tâches reflète son nouvel état.

3. Pour redémarrer ou arrêter le service, cliquez sur **Redémarrer le service Event Server** ou **Arrêter le service Event Server**.

Pour de plus amples informations au sujet des icônes de la barre des tâches, voir À propos des icônes de la barre des tâches (á la page 434).

Voir également

Démarrer ou arrêter le service Recording Server (á la page 431)

Arrêter le service Event Server

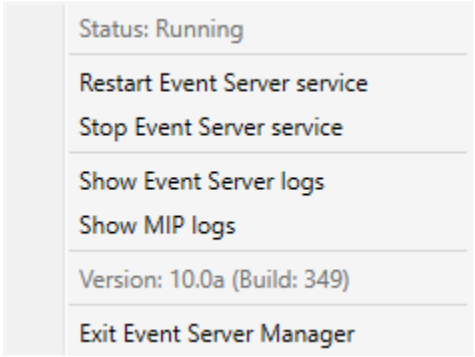
Lors de l'installation de modules d'extension MIP sur le serveur d'événements, vous devez d'abord arrêter le service Event Server puis le redémarrer une fois la procédure terminée. Cependant, lorsque le service sera à l'arrêt, de nombreuses parties du système VMS ne fonctionneront pas.

- Aucun événement ou alarme ne sera stocké dans le serveur d'événements. Cependant, les événements système et les événements de périphériques déclencheront encore des actions, telles que le démarrage de l'enregistrement.
- XProtect Access, XProtect LPR, et XProtect Transact ne fonctionnent pas dans cette configuration ou dans XProtect Smart Client.
- Les événements analytiques ne fonctionnent pas.
- Les événements génériques ne fonctionnent pas dans XProtect Advanced VMS.
- Aucune alarme n'est déclenchée.
- Dans XProtect Smart Client, les éléments de vue des plans, les éléments de vue de la liste d'alarmes et l'espace de travail du gestionnaire d'alarmes ne fonctionnent pas.
- Les modules d'extension MIP qui se trouvent dans le serveur d'événements ne peuvent pas fonctionner.
- Les modules d'extension MIP dans Management Client et XProtect Smart Client ne fonctionnent pas correctement.

Consulter le serveur d'événements ou les journaux MIP

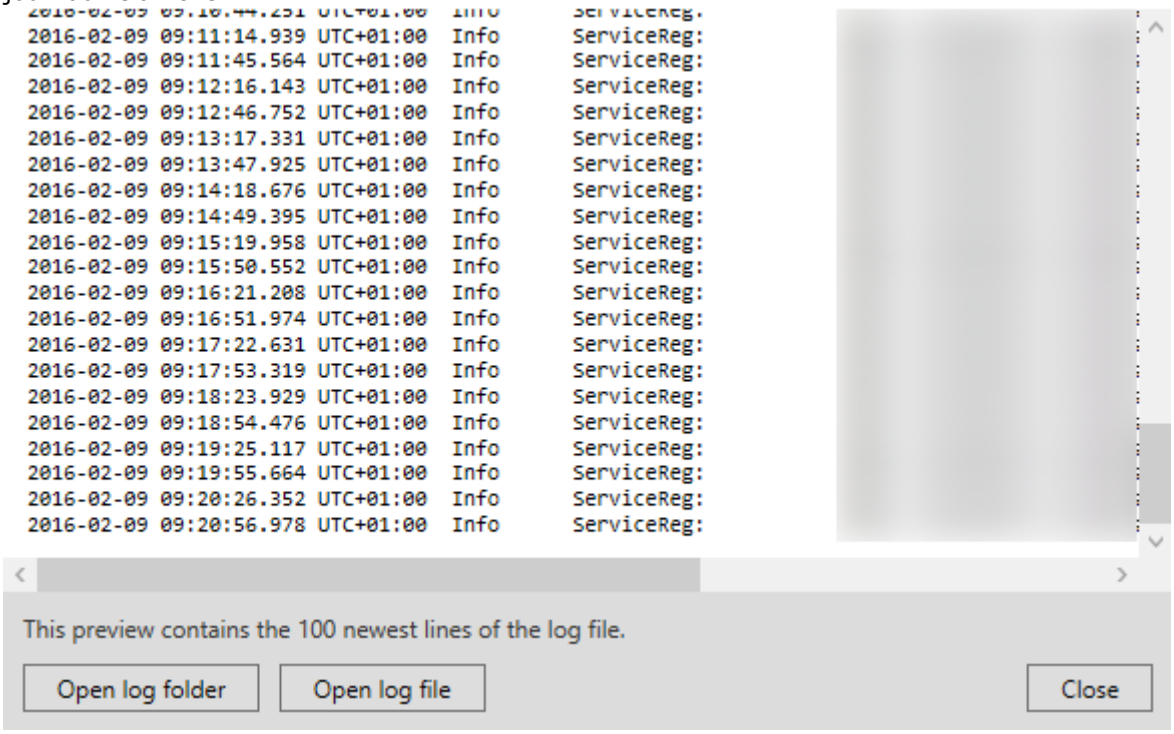
Vous pouvez consulter des informations horodatées au sujet des activités du serveur d'événements dans le journal du serveur d'événements. Des informations au sujet des intégrations tierces sont consignées dans le journal MIP, dans un sous-répertoire du répertoire **Event Server (Serveur d'événements)**.

1. Dans la zone de notification, cliquer avec le bouton droit sur l'icône pertinente de la barre des tâches. Un menu contextuel s'affiche.



2. Pour afficher les 100 lignes les plus récentes du journal du serveur d'événements, cliquez sur **Afficher les journaux du serveur d'événements**. Un programme d'affichage des

journaux s'affiche.



1. Pour consulter le journal, cliquez sur **Ouvrir le journal**.

2. Pour ouvrir le répertoire du journal, cliquez sur **Ouvrir le répertoire du journal**.

3. Pour consulter les 100 lignes les plus récentes du journal MIP, rendez-vous dans le menu contextuel et cliquez sur **Afficher les journaux MIP**. Un programme d'affichage des journaux s'affiche.

Si quelqu'un supprime les journaux du répertoire des journaux, les éléments du menu sont grisés. Pour ouvrir le programme d'affichage des journaux, vous devez d'abord copier les journaux dans l'un de ces répertoires : *C:\ProgramData\Milestone\XProtect Event Server\logs* ou*C:\ProgramData\Milestone\XProtect Event Server\logs\MIPLogs*.

À propos des icônes de la barre des tâches

Les icônes de la barre des tâches contenues dans le tableau représentent les états possibles des services exécutés sur le serveur de gestion, le serveur d'enregistrement, le serveur d'enregistrement de redondance et le serveur d'événements. Ces icônes sont toutes visibles sur les ordinateurs sur lesquels les serveurs sont installés, dans la zone de notification :

Icône du service Management Server	Icône du service Recording Server	Icône du service Event Server	Icône du service Failover Recording Server	Description
				**En cours** S'affiche lorsqu'un service de serveur est activé et démarré. Si le service Failover Recording Server fonctionne, il peut prendre le relais en cas de panne des serveurs d'enregistrement.
				**Arrêté** S'affiche lorsqu'un service de serveur s'est arrêté. Si le service Failover Recording Server s'arrête, il ne peut pas prendre le relais en cas de panne du serveur d'enregistrement.
				**Démarrage en cours** S'affiche lorsqu'un service de serveur est en cours de démarrage. Normalement, après quelques instants, l'icône de la barre des tâches change et indique **En cours**.
				**Arrêt en cours** S'affiche lorsqu'un service de serveur est en cours d'arrêt. Normalement, après quelques instants, l'icône de la barre des tâches change et indique **Arrêté**.
				**Dans un état indéterminé** S'affiche lorsque le service du serveur est initialement chargé et jusqu'à ce que les premières informations soient reçues, à la suite de quoi l'icône de la barre des tâches, dans des circonstances normales, changera au profit de l'icône **Démarrage**, puis de l'icône **En cours**.
				**Fonctionnement hors ligne** S'affiche généralement lorsque le service Recording Server ou Failover Recording Server est en cours de fonctionnement, mais pas le service Management Server.

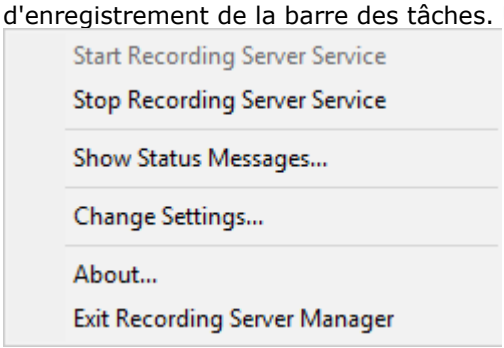
Icône du service Management Server	Icône du service Recording Server	Icône du service Event Server	Icône du service Failover Recording Server	Description
				**Nécessite l'autorisation de l'administrateur** S'affiche lorsque le service Recording Server est chargé pour la première fois. Les administrateurs autorisent le serveur d'enregistrement par le biais du Management Client : Agrandissez la liste **Serveurs**, sélectionnez le nœud **Serveur d'enregistrement** et dans le volet **Vue d'ensemble**, faites un clic droit sur le serveur d'enregistrement concerné et sélectionnez **Autoriser le serveur d'enregistrement**.

Modifier les paramètres pour le service Recording Server

Vous pouvez modifier les paramètres de base du service Recording Server, tels que les numéros de port à utiliser, procédez comme suit :

Conditions préalables : Pour modifier les paramètres, vous devez d'abord arrêter le service Recording Server. Tant que le service Recording Server est arrêté, votre système ne peut pas interagir avec les périphériques connectés au serveur d'enregistrement. Cela signifie que vous ne pouvez pas visualiser la vidéo en direct ou enregistrer des vidéos.

1. Dans la zone de notification, cliquer avec le bouton droit sur l'icône serveur d'enregistrement de la barre des tâches. Un menu contextuel s'affiche.



2. Sélectionnez **Arrêter le service Recording Server**.
3. Cliquez à nouveau sur l'icône avec le bouton droit.
4. Sélectionnez **Modifier les paramètres**. La fenêtre **Paramètres du serveur d'enregistrement** s'affiche. Modifiez les paramètres concernés.

Voir également

Paramètres du serveur d'enregistrement (á la page 437)

Paramètres du serveur d'enregistrement

Lorsque vous configurez les paramètres du serveur d'enregistrement, indiquez les propriétés suivantes :

Nom	Description
Adresse	Adresse IP (exemple : 123.123.123.123) ou non d'hôte (exemple : notre serveur) du serveur de gestion avec lequel le serveur de redondance pourra communiquer. Cette information est nécessaire pour que le serveur d'enregistrement puisse communiquer avec le serveur de gestion.
Port	Numéro de port à utiliser lors de la communication avec le serveur de gestion. Le port par défaut est 9993. Vous pouvez le modifier si nécessaire.
Port du serveur web	Numéro de port à utiliser pour gérer les demandes de serveurs web, par exemple, pour gérer les commandes des caméras PTZ et pour les demandes en direct et de consultation de XProtect Smart Client. Le port par défaut est 7563. Vous pouvez le modifier si nécessaire.
Port du serveur d'alerte	Le numéro de port à utiliser lorsque le serveur d'enregistrement reçoit des données TCP (certains périphériques utilisent TCP pour envoyer des messages d'événement). Le port par défaut est 5432. Vous pouvez le modifier si nécessaire.
Port du serveur SMTP	Le numéro de port à utiliser lorsque le serveur d'enregistrement est à la recherche d'informations de type protocole SMTP (SMTP). SMTP est une norme d'envoi de messages e-mail entre serveurs. Certains périphériques utilisent SMTP pour envoyer des messages d'événements ou des images au serveur du système de surveillance par e-mail. Le port par défaut est le port 25, que vous pouvez activer et désactiver En cas de besoin, vous pouvez modifier le numéro de port si nécessaire.

À propos du service Data Collector Server

Votre système installe automatiquement le service Data Collector Server sur les mêmes machines que le serveur de gestion, le serveur d'enregistrement, le serveur de journaux, le serveur d'événements et le serveur Milestone Mobile.

Généralement, le service Data Collector Server ne nécessite pas de maintenance, mais s'il **s'arrête**, aucun flux en direct ne sera envoyé au moniteur système. Ceci est indiqué dans le Moniteur système au moyen de messages d'erreur.

1. Sur l'ordinateur sur lequel le service Data Collector Server est installé :
2. Dans le menu **Démarrer** de Windows, sélectionnez **Panneau de configuration**, puis :
   - Si vous utilisez la vue par **Catégorie**, cherchez la catégorie **Système et sécurité** et cliquez sur **Outils administratifs**.
   - Si vous utilisez des **petites icônes** ou des **grandes icônes,** cliquez sur **Outils administratifs**.
3. Double-cliquez sur **Services**.

4. Trouvez le **service Data Collector Server Milestone XProtect**. Faites un clic droit et sélectionnez **Démarrer** pour redémarrer le service.

Services enregistrés

Occasionnellement, il y a des serveurs et/ou des services qui devraient pouvoir communiquer avec le système même s'ils ne font pas directement partie du système. Certains services (et non pas tous) peuvent s'enregistrer automatiquement dans le système. Les services pouvant être automatiquement enregistrés sont :

- Service du serveur d'événements
- Service du serveur de journaux
- Service du canal de service

Les services automatiquement enregistrés apparaissent dans la liste des services enregistrés.

Il est possible de préciser manuellement les serveurs/services dans le Management Client comme services enregistrés :

À propos du canal de service

Le canal de service permet de communiquer automatiquement et en toute transparence les paramètres entre différents serveurs et clients de l'installation de votre système. Par exemple, c'est le canal de service qui s'assure que lorsqu'une vue partagée est modifiée sur un client, la modification est immédiatement reflétée sur les autres clients qui utilisent la vue partagée en question. Le canal de service facilite également la communication associée à la configuration entre les serveurs et les clients pour les cas où vous utilisez plusieurs modules d'extension ou produits complémentaires avec votre système.

Le canal de service est généralement installé dans le cadre de l'installation du serveur de gestion et réside sur l'ordinateur du serveur de gestion mais, si nécessaire, vous pouvez l'installer sur un autre serveur dans votre système de surveillance.

Une fois installé, le canal de service peut s'enregistrer automatiquement avec votre système (ce qui signifie qu'il est automatiquement répertorié par la fonction services enregistrés du Management Client). Son emplacement est connu par le système, et les clients qui se connectent au système peuvent automatiquement en bénéficier.

Si ultérieurement vous modifiez l'adresse IP ou le nom d'hôte du serveur qui exécute le service Service Channel, vous devez modifier manuellement les informations dans **Outils** > **Services enregistrés** dans le Management Client. De même, si ultérieurement il vous faut modifier l'utilisateur sous lequel le service canal de service a été installé, vous devez supprimer le service Service Channel et le réinstaller ensuite sous le nouvel utilisateur.

Il est important que l'heure de toute instance de XProtect Smart Client soit synchronisée avec celle de l'ordinateur exploitant le service Service Channel. Si l'heure d'un XProtect Smart Client n'est pas synchronisée avec celle du serveur de gestion et de l'ordinateur exploitant le service Service Channel, le XProtect Smart Client n'est pas mis à jour avec les informations relatives aux changements de configuration effectués par les autres utilisateurs dans XProtect Smart Client. Cela signifie que les utilisateurs risquent d'écraser les modifications de configuration des uns et des autres. Si les XProtect Smart Client ne sont pas temporellement synchronisés avec l'ordinateur qui exécute le service Service Channel, vous verrez un message d'erreur vous en informant.

Ajouter et modifier des services enregistrés

1. Dans la fenêtre **Ajouter/Supprimer des services enregistrés**, cliquez sur le bouton **Ajouter** ou **Modifier**, en fonction de vos besoins.
2. Dans la fenêtre **Ajouter un service enregistré** ou **Modifier un service enregistré** (en fonction de votre sélection précédente), spécifiez ou modifiez les paramètres.
3. Cliquez sur **OK**.

Gérer la configuration du réseau

Avec les paramètres de configuration réseau, vous pouvez indiquer les adresses serveur WAN et LAN du serveur de gestion afin que le serveur de gestion et les serveurs fiables puissent communiquer.

1. Dans la fenêtre **Ajouter/supprimer des services enregistrés**, cliquez sur **Réseau.**
2. Spécifiez l'adresse IP LAN et/ou WAN du serveur de gestion.

   Si tous les serveurs concernés (le serveur de gestion et les serveurs approuvés) sont sur votre réseau local, vous pouvez simplement spécifier l'adresse LAN. Si un ou plusieurs serveurs concernés accèdent au système par le biais d'une connexion Internet, vous devez également spécifier l'adresse WAN.

3. Cliquez sur **OK**.

Propriétés des services enregistrés

Dans la fenêtre **Ajouter un service enregistré** ou **Modifier un service enregistré**, spécifiez les éléments suivants :

Composant	Exigences
Type	Champ pré-rempli.
Nom	Nom du service enregistré. Le nom est utilisé à des fins d'affichage dans le Management Client.

Composant	Exigences
URL	Cliquez sur **Ajouter** pour ajouter l'adresse IP ou le nom d'hôte du service enregistré. Si vous spécifiez un nom d'hôte comme partie intégrante d'une URL, l'hôte en question doit exister et être accessible sur le réseau. Les URL doivent commencer par *http://* ou *https://* et ne doivent contenir aucun des caractères suivants : *< > & ' " * ? | [ ] "*. **Exemple** d'un format typique d'URL : http://adresseip:port/répertoire (où le port et le répertoire sont facultatifs). Notez que vous pouvez ajouter plusieurs URL le cas échéant.
De confiance	Sélectionnez si le service enregistré doit être reconnu immédiatement (c'est souvent le cas, mais l'option vous donne la possibilité d'ajouter le service enregistré puis de le marquer comme fiable en modifiant le service enregistré ultérieurement). Notez que modifier l'état de confiance modifie également l'état des autres services enregistrés partageant plusieurs URL définies pour le service enregistré pertinent.
Description	Description du service enregistré. La description est utilisée à des fins d'affichage dans le Management Client.
Avancée	Lorsqu'un service est avancé, il dispose de son propre modèle d'URL (par exemple, http, https, tcp ou udp) qui doit être configuré pour chaque adresse d'hôte que vous définissez. Une adresse d'hôte a donc de multiples extrémités, ayant chacune leur propre modèle, adresse d'hôte et port IP pour ce modèle.

Index

À propos des systèmes Milestone

Milestone Systems est une société internationale leader de l'édition de logiciels de gestion vidéo IP sur plateforme ouverte, fondée en 1998. Elle opère maintenant en tant que société autonome du Groupe Canon. La technologie Milestone est facile à gérer, fiable et éprouvée au travers de milliers d'installations. Elle offre une flexibilité en matière de choix de matériel pour la mise en réseau et l'intégration à d'autres systèmes. Vendues par l'intermédiaire de partenaires dans plus de 100 pays, les solutions Milestone aident les organisations à gérer les risques, à protéger les personnes et les biens, à optimiser les processus et à réduire les frais. Pour plus d'informations, rendez-vous à l'adresse suivante : http://www.milestonesys.com.