MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS 2025 R2

Manuel de l'administrateur

XProtect Corporate
XProtect Expert
XProtect Professional+
XProtect Express+

milestone

Table des matières

Droit d’auteur, marques et exclusions

Marques de commerce

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 de commerce de Google Inc.

Toutes les autres marques de commerce mentionnées dans le présent document sont des marques de commerce 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’institutions utilisés dans les exemples de ce document sont fictifs. Toute ressemblance avec des institutions 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 de votre système Milestone.

Vue d’ensemble

Manuel de l’administrateur XProtect VMS

Ce manuel constitue un guide complet conçu pour aider les administrateurs à gérer le logiciel de gestion des vidéos Milestone XProtect VMS. Il fournit des instructions détaillées sur divers aspects du système, notamment l’installation, la configuration et la maintenance de XProtect VMS.

Ce manuel regroupe toutes les informations utiles pour pouvoir gérer efficacement et optimiser le système XProtect VMS. Il inclut des instructions étape par étape pour l’installation et la configuration des composants système comme XProtect Management Client, XProtect Smart Client et les serveurs d’enregistrement.

Les tâches qui y sont décrites sont notamment les suivantes :

- Sécurisation du système par le biais des rôles utilisateur et des autorisations
- Préservation de la confidentialité grâce aux profils utilisateur et au masquage de confidentialité
- Activation du cryptage et configuration des bases de données de façon sécurisée
- Activation de diverses méthodes d’authentification
- Gestion du basculement
- Résolution des problèmes liés à divers composants système

Ce document se destine notamment aux administrateurs système, aux experts IT et au personnel technique responsables de l’installation, de la configuration et de la maintenance de Milestone XProtect VMS.

Quelles sont les nouveautés ?

Dans Management Client 2025 R2

Aucune mise à jour pour cette version.

Dans Management Client 2025 R1

XPCO prend en charge la synchronisation des identités via le système de gestion des identités inter-domaines (SCIM). SCIM permet la fourniture automatique des utilisateurs, et toutes les modifications apportées aux autorisations d’utilisateur sont instantanément répercutées dans le VMS sans nécessiter de nouvelle connexion.

Dans Management Client 2024 R2

XProtect Management Client

Le filtre de périphérique Afficher les périphériques désactivés a été renommé et inversé

La logique de filtrage de l'option **Afficher les périphériques désactivés**, dans le volet **Vue d'ensemble**, a été inversée et renommée **Masquer les périphériques désactivés**. L'option de filtrage est désactivée par défaut, ce qui signifie que l'arborescence des périphériques affiche désormais tous les périphériques, y compris ceux qui sont désactivés.

Les critères de filtrage des périphériques spécifiés sont désormais conservés, mais sont réinitialisés si le Management Client est redémarré. Les utilisateurs peuvent encore supprimer manuellement les critères de filtrage des périphériques pour réinitialiser les filtres. Par conséquent, la touche de raccourci **F5** ne réinitialise plus les critères de filtrage des périphériques.

Auparavant, les périphériques récemment créés, mais désactivés, pouvaient être difficiles à localiser, car le filtre **Afficher les périphériques désactivés** était désactivé par défaut et pouvait facilement passer inaperçu.

Nouvelles images XProtect Management Client

Les images de la documentation technique ont été mises à jour pour refléter l'environnement actuel.

Fin de la prise en charge

Les options suivantes ne sont plus prises en charge :

- Plusieurs instances Recording Server

  Plusieurs instances Recording Server ne sont plus prises en charge. Consultez cet article de la base de connaissances qui décrit comment mettre à jour une installation qui utilise plusieurs instances Recording Server.

- Fichiers d'aide Management Client installés

  Le Management Client repose désormais sur l'aide en ligne du site Web de Milestone. Les fichiers d'aide installés ne sont plus disponibles. Si un poste de travail qui exécute le Management Client n'a pas d'accès à Internet, un lien vers la rubrique d'aide correspondante sera disponible dans le client. Si nécessaire, les fichiers d'aide peuvent être téléchargés et installés manuellement. Voir Fichiers d'aide.

- Prise en charge de Microsoft SQL Server 2014

  La prise en charge étendue de Microsoft SQL Server 2014 a pris fin le 9 juillet 2024. Plus aucune mise à jour de sécurité Microsoft ne sera publiée pour ce serveur.

- Transcodage JPEG dans le Smart Client

  Le réglage du transcodage JPEG (qualité de l'image) en mode configuration n'est plus disponible dans le volet des propriétés. Utilisez désormais le flux adaptatif.

- Événements SMTP de la caméra

  Par défaut, les caméras ne peuvent plus charger d'image sur le serveur XProtect VMS via SMTP. Cette fonctionnalité était utilisée par certains anciens modèles de caméras. En raison des normes de sécurité actuelles, les ports ouverts pour les communications non cryptées ne sont pas sécurisés.

Dans Management Client 2024 R1

XProtect Management Client

Documentation Management Client en russe

L'aide pour le Management Client est maintenant disponible en russe.

Installation d'un serveur d'enregistrement de basculement / d'un serveur d'enregistrement

Lorsque vous installez un serveur d'enregistrement ou un serveur d'enregistrement de basculement, les fichiers de chaque serveur respectif sont désormais placés dans des dossiers distincts du dossier Milestone : **XProtect Serveur de basculement** et **XProtect serveur d'enregistrement**.

Si vous mettez à niveau XProtect, ces dossiers sont également créés au cours de la procédure de mise à niveau et les fichiers de chaque type de serveur se trouvent dans ces dossiers.

Auparavant, les fichiers du serveur d'enregistrement de basculement et du serveur d'enregistrement étaient installés dans le même dossier, ce qui pouvait poser des problèmes lorsque vous mettiez des produits à l'échelle ou que vous utilisiez différentes versions de Microsoft .NET.

Dans Management Client 2023 R3

XProtect Management Client

Azure Active Directory peut désormais être utilisé pour l'authentification. Lors de l'installation, vous pouvez choisir entre l'**Authentification Windows** et **Azure Active Directory Integrated** pour la sécurité intégrée.

Pour en savoir plus sur l'installation XProtect avec la sécurité intégrée d'Azure, voir Installer votre système - option personnalisée on page 166.

XProtect Management Client

Une option (ne pas faire confiance au certificat du serveur) est désormais disponible pour l'Authentification Windows et pour Azure Active Directory Integrated. Pour Azure Active Directory Integrated, cette option est obligatoire. L'option (ne pas faire confiance au certificat du serveur) garantit que les certificats du serveur sont validés et vérifiés avant l'installation.

XProtect Management Client:

Une nouvelle autorisation utilisateur **Modifier les paramètres d'alarme** a été introduite pour les alarmes. Elle permet aux administrateurs de modifier les définitions, les états, les catégories, les sons et la rétention des alarmes, ainsi que la rétention des événements. Les autorisations de modification correspondantes pour les définitions des alarmes ont été supprimées de l'autorisation utilisateur existante **Gérer**, et les administrateurs devront disposer des deux autorisations utilisateur (**Modifier les paramètres d'alarme** et **Gérer**) pour gérer les paramètres des alarmes.

Le nouveau droit d'utilisateur **Modifier les paramètres d'alarme** n'est pas appliqué aux utilisateurs existants et doit être attribué manuellement aux utilisateurs qui ont besoin d'un accès de niveau administrateur pour configurer les alarmes après l'installation ou la mise à niveau.

Pour en savoir plus sur l'installation personnalisée, voir Rôles (noeud Sécurité) on page 552

Dans Management Client 2023 R2

XProtect Management Client:

Le flux adaptatif peut désormais être configuré pour être utilisé en mode lecture. Cette méthode est appelée lecture adaptative. Pour plus d'informations, voir Lecture adaptative (expliquée) on page 251

XProtect Management Client:

Lorsque vous installez les composants XProtect, vous pouvez désormais choisir d'utiliser une base de données pré-créée dans le cadre d'une installation personnalisée. Pour en savoir plus sur l'installation personnalisée, voir Installer votre système - option personnalisée on page 166

XProtect Management Client:

De nouvelles autorisations utilisateur pour les restrictions vidéo ont été introduites. Elles permettent aux administrateurs de configurer et d'attribuer des droits de création, de visualisation, de modification et de suppression aux utilisateurs. Pour de plus amples informations, voir Rôles (noeud Sécurité) on page 552

Dans Management Client 2023 R1

XProtect Incident Manager :

- Pour se conformer au RGPD ou aux autres lois applicables concernant les données à caractère personnel, les administrateurs de XProtect Management Client peuvent à présent définir une durée de rétention pour les projets d'incident.

Dans Management Client 2022 R3

XProtect Incident Manager :

- L'extension XProtect Incident Manager est désormais également compatible avec la version 2022 R3 ou ultérieure de XProtect Expert, XProtect Professional+ et XProtect Express+.
- XProtect Incident Manager peut afficher plus de 10 000 projets d'incident.

Dans Management Client 2022 R2

XProtect Incident Manager :

- La première version de cette extension.
- L'extension XProtect Incident Manager est compatible avec la version 2022 R2 et supérieure de XProtect Corporate, ainsi qu'avec la version 2022 R2 et supérieure de XProtect Smart Client.

XProtect LPR :

- Les styles de plaque d'immatriculation, qui font partie des modules de pays, sont désormais répertoriés dans un seul endroit.
- Pour faciliter la gestion des styles de plaque d'immatriculation, vous pouvez les regrouper en des alias selon vos besoins de reconnaissance de plaque.
- Les listes de correspondances prennent désormais en charge les alias.

Dans Management Client 2022 R1

Cryptage du serveur d'événements :

- Vous pouvez chiffrer la connexion bilatérale entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements , y compris le LPR Server.

  Pour plus d'informations, voir Activer le chiffrement du serveur d'événements on page 328.

Connexion via un IDP externe :

- Vous pouvez maintenant vous connecter au Milestone XProtect VMS à l'aide d'un IDP externe. La connexion via un IDP externe est une alternative à la connexion en tant qu'utilisateur Active Directory ou en tant qu'utilisateur standard. Grâce à la méthode de connexion à l'IDP externe, vous pouvez ignorer les exigences de configuration d'un utilisateur standard et être toujours autorisé à accéder aux composants et aux périphériques dans XProtect.

  Pour de plus amples informations, consultez IDP externe (explications).

Mettre à jour les données de matériel

- Vous pouvez maintenant voir la version de firmware du périphérique matériel qui est détecté par le système dans le Management Client.

  Pour plus d'informations, voir Mettre à jour vos données de matériel on page 374.

XProtect Management Server Failover

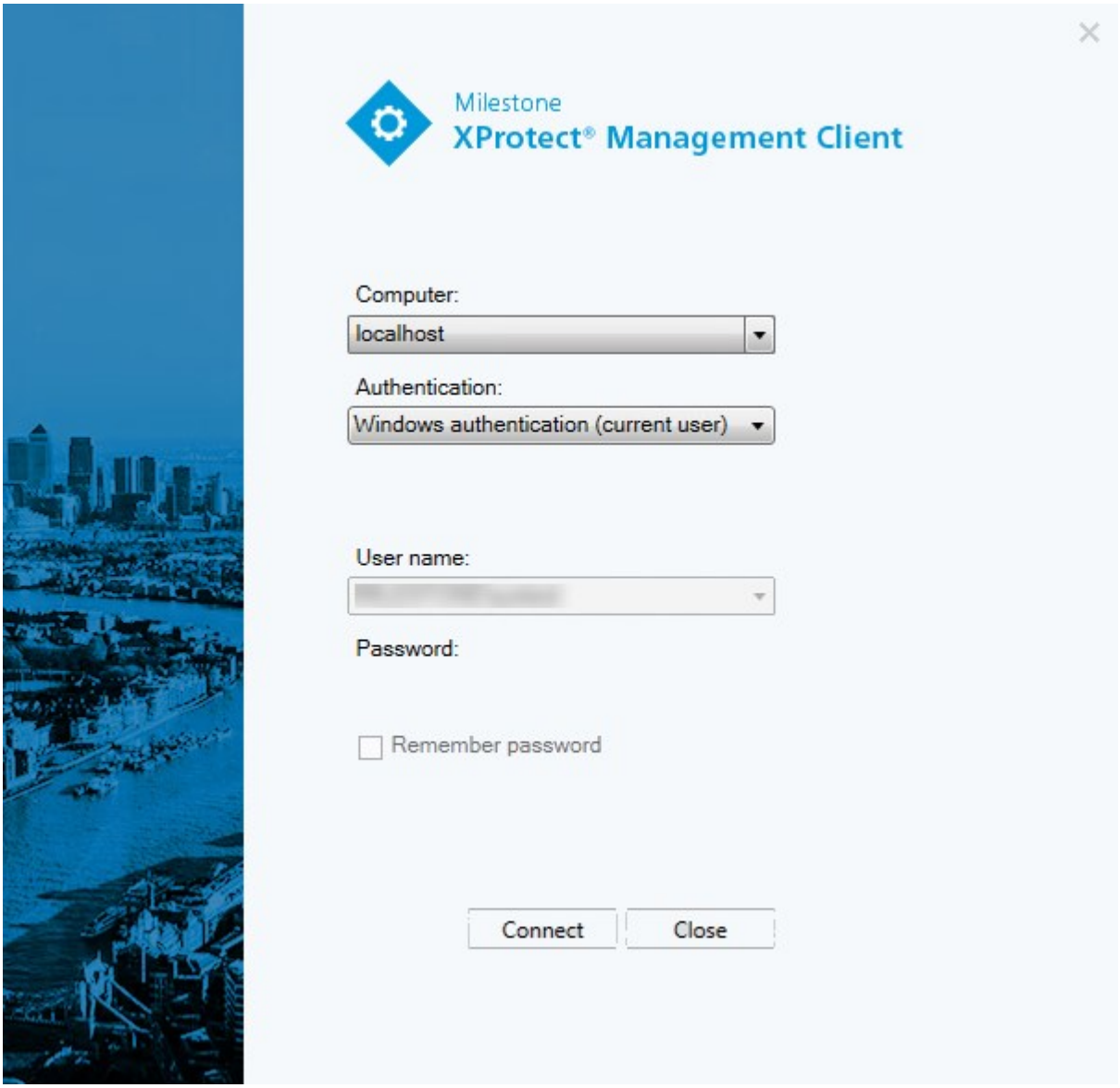
- Vous pouvez maintenant bénéficier d'une disponibilité élevée de votre système en configurant un serveur de gestion de basculement entre deux ordinateurs redondants. Si l'ordinateur qui exécute le serveur de gestion tombe en panne, le deuxième prend le relais. La réplication des données en temps réel s'assure que les bases de données du serveur de gestion, du serveur de journaux et du serveur d'événements sont identiques sur les deux ordinateurs.

  Pour plus d'informations, voir XProtect Management Server Failover on page 56

Se connecter (explications)

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 des versions plus récentes sont installées, vous pouvez vous connecter aux systèmes exécutant des versions plus anciennes du produit après avoir installé un correctif. Les versions prises en charge sont XProtect Corporate 2013 et XProtect Expert 2013 ou toute autre version plus récente.



Autorisation de connexion (explications)

Le système permet aux administrateurs de configurer des utilisateurs de façon à ce qu'ils puissent uniquement se connecter à un système si un deuxième utilisateur disposant d'autorisations suffisantes 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.

Les utilisateurs qui se connectent via un IDP externe ne peuvent pas être configurés avec une exigence d'autorisation par un deuxième utilisateur.

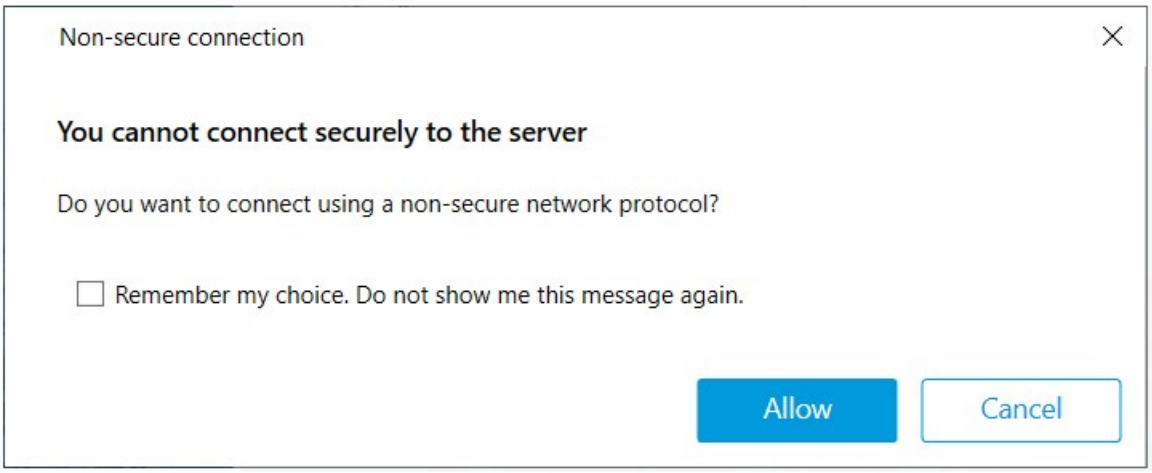
Pour associer l'autorisation de connexion à un rôle :

- Configurez l'**autorisation de connexion requises** pour le rôle sélectionné dans l'onglet **Info** (voir Paramètres des rôles) sous **Rôles**, pour qu'il soit demandé à l'utilisateur une autorisation supplémentaire lors de la connexion
- Configurer l'option **Authoriser des utilisateurs** pour le rôle sélectionné dans l'onglet **Sécurité générale** (voir Paramètres des rôles) sous **Rôles**, afin que l'utilisateur puisse autoriser d'autres utilisateurs à se connecter

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.

Se connecter en utilisant une connexion non-sécurisée

Lorsque vous vous connectez dans le Management Client, il peut vous être demandé si vous souhaitez vous connecter en utilisant un protocole réseau non-sécurisé.



- Cliquez sur **Autoriser** pour vous connecter en ignorant la notification. Pour ne plus recevoir cette notification, cochez la case **Se souvenir de mon choix. Ne pas afficher ce message à nouveau.** ou cliquez sur **Outils** > **Options** puis sélectionnez **Autoriser la connexion non-sécurisée au serveur (redémarrage de Management Client requis)**.

Pour de plus amples informations sur les communications sécurisées, consultez Communication sécurisée (explications) on page 158.

Changer votre mot de passe d'utilisateur de base

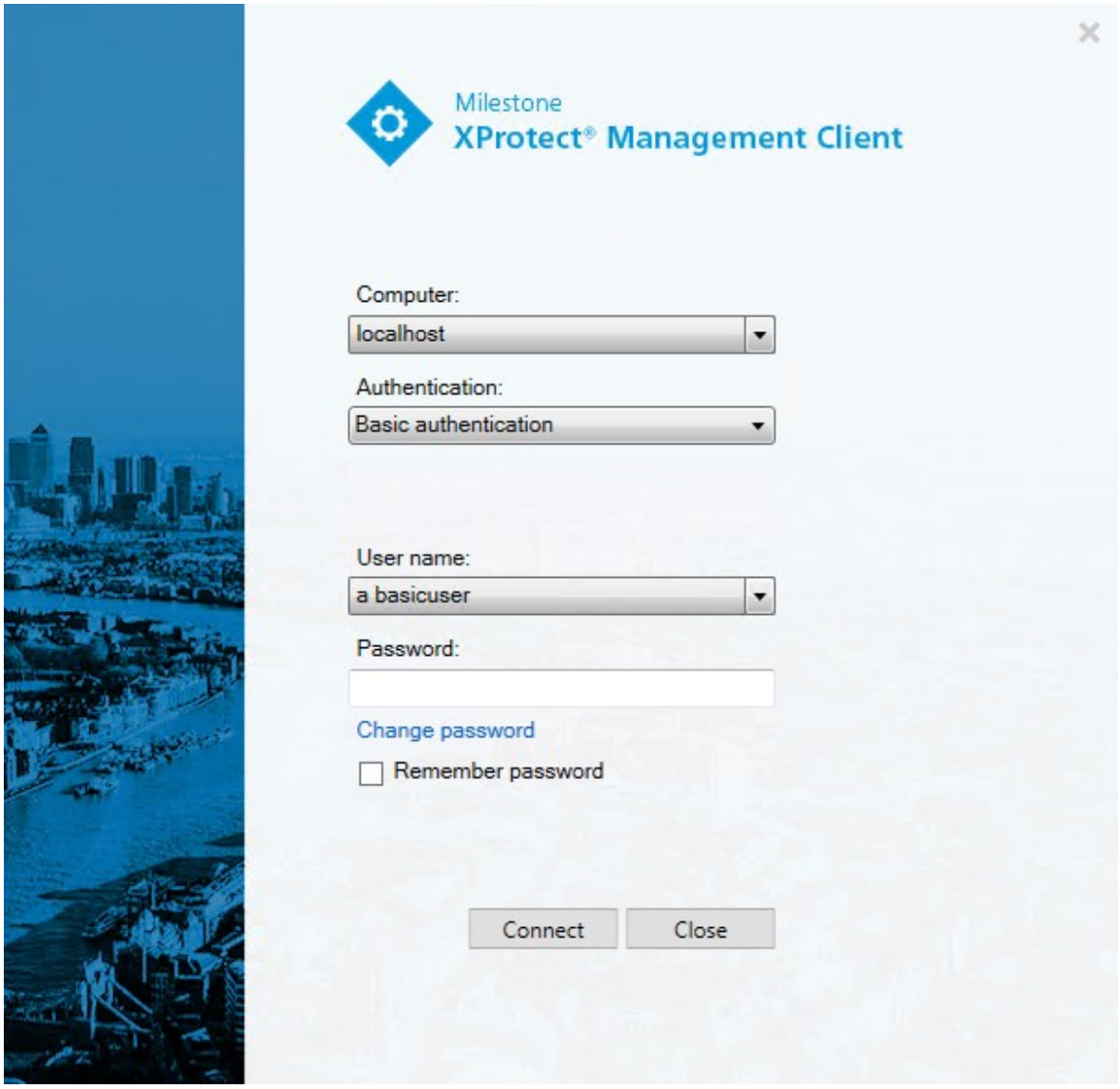
Si vous vous connectez en tant qu'**utilisateur de base**, vous pouvez modifier votre mot de passe. Si vous choisissez une méthode d'authentification différente, seul votre administrateur de système pourra modifier votre mot de passe. Modifier souvent votre mot de passe permet d'augmenter la sécurité de votre système VMS XProtect.

Prérequis

La version de votre système VMS XProtect doit être 2021 R1 ou une version plus récente.

Étapes :

1. Démarrer Management Client. La fenêtre de connexion apparaît.
2. Indiquez vos informations de connexion. Dans la liste **Authentification**, sélectionnez **Authentification basique**. Un lien avec le texte **Modifier le mot de passe** s'affiche.



3. Cliquez sur le lien. Une fenêtre de navigateur s'ouvre.
4. Suivez les instructions et enregistrez vos modifications.
5. Vous pouvez maintenant vous connecter à Management Client avec votre nouveau mot de passe.

Présentation générale du produit

Les produits VMS XProtect constituent un logiciel de gestion vidéo conçu pour les installations de toutes formes et de toutes tailles. Que vous souhaitiez protéger votre magasin contre le vandalisme ou gérer une installation de haute sécurité sur plusieurs sites, XProtect vous permet d'y parvenir. Les solutions apportent 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 composants suivants :

- Le **serveur de gestion** : au cœur de votre installation, il se compose de plusieurs serveurs
- Un ou plusieurs **serveurs d'enregistrement**
- Une ou plusieurs installations de **XProtect Management Client**
- **XProtect Download Manager**
- Une ou plusieurs installations de **XProtect® Smart Client**
- Une ou plusieurs utilisations de **XProtect Web Client** et/ou des installations de client **XProtect Mobile** si nécessaire

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 sur les serveurs virtualisés ou sur plusieurs serveurs physiques dans une configuration distribuée. Voir également Une configuration distribuée du système on page 100.

Le système offre également la possibilité d'inclure un XProtect® Smart Client – Player indépendant lors de l'export de preuves vidéo 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.

Lorsque des produits riches en fonctionnalités sont installés (voir Comparaison des produits on page 125), votre système peut gérer un nombre illimité de caméras, serveurs et utilisateurs et ce, sur plusieurs sites si besoin. Votre système peut supporter IPv4 ainsi que IPv6.

Composants du système

Serveur de gestion (explications)

Le serveur de gestion est le composant central du VMS. Il conserve la configuration du système de surveillance dans une base de données SQL Server, sur SQL Server sur l'ordinateur du serveur de gestion lui-même ou sur SQL Server séparé sur le réseau. Il gère également l'authentification de l'utilisateur, les autorisations utilisateur, le système de règles, entre autres.

Pour améliorer les performances du système, vous pouvez exécuter plusieurs serveurs de gestion comme une 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.

SQL Server installations et bases de données (explications)

Le serveur de gestion, le serveur d'événements, le serveur de journaux, XProtect Incident Manager, et le Identity Provider stockent, entre autres, la configuration du système, les alarmes, les événements et les messages de journaux dans les bases de données SQL Server suivantes :

- **Surveillance : Serveur de gestion et d'événements**
- **Surveillance_IDP : IDP**
- **Surveillance_IM : Incident Manager**
- **LogserverV2 : LogServer**

Le serveur de gestion et le serveur d'événements partagent la même base de données SQL Server alors que le serveur de journaux, XProtect Incident Manager, et le Identity Provider ont chacun leur propre base de données SQL Server. L'emplacement par défaut des bases de données est `C:\Program Files\Microsoft SQL Serv-er\MSSQL16.MSSQLSERVER\MSSQL\DATA`, où \{nn} est la version de SQL Server.

Le programme d'installation du système inclut Microsoft SQL Server Express, qui est une version gratuite de SQL Server.

Pour de très grands systèmes ou des systèmes avec beaucoup de transactions provenant de bases de données et allant vers des bases de données SQL Server, Milestone vous recommande d'utiliser l'édition Microsoft® SQL Server® Standard ou Microsoft® SQL Server® Enterprise de SQL Server sur un ordinateur dédié sur le réseau et sur un disque dur dédié qui n'est pas utilisé à d'autres fins. L'installation de SQL Server sur ses propres périphériques améliore la performance de l'intégralité du système.

Pour consulter la liste des versions de SQL Server prises en charge, allez à https://www.milestonesys.com/systemrequirements/.

Pour plus d'informations sur le Identity Provider, voir Identity Provider (explications) on page 73.

Pour plus d'informations sur la base de données XProtect Incident Manager et savoir comment s'y connecter, voir le manuel d'administrateur séparé pour XProtect Incident Manager.

Serveur d'enregistrement (explications)

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 périphériques

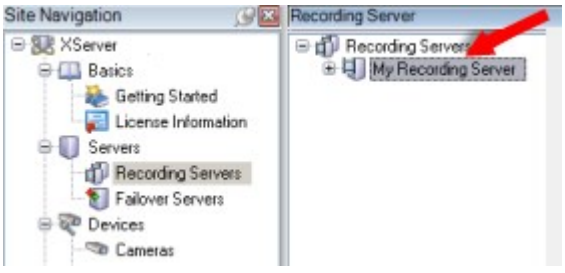
- Les caméras réseau et les encodeurs vidéo communiquent via un pilote de périphérique développé spécifiquement pour les périphériques individuels ou une série de périphériques semblables du même fabricant.
- À partir de la version 2018 R1, les pilotes de périphériques sont répartis en deux packs de pilotes de périphériques : le pack de pilotes de périphériques régulier équipé des pilotes plus récents et un pack de pilotes de périphériques hérités doté de pilotes plus anciens
- Le pack de pilotes de périphériques régulier est installé automatiquement au moment où vous installez le serveur d'enregistrement. Par la suite, vous pouvez mettre à jour les pilotes en téléchargeant et en installant une version plus récente du pack de pilotes de périphériques
- Le pack de pilotes de périphériques hérités ne peut être installé que si un pack de pilotes de périphériques régulier est installé dans le système. Les pilotes relevant du pack de pilotes de périphériques hérités sont installés automatiquement si une version précédente est déjà installée sur votre système. Ils sont disponibles au téléchargement manuel et à l'installation sur la page de téléchargement du logiciel (https://www.milestonesys.com/download/)

Base de données Multimédia

- Le serveur d'enregistrement stocke les données audio et vidéo récupérées 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 telles que l'archivage en plusieurs étapes, le groupage de vidéo, le cryptage et l'ajout d'une signature numérique aux enregistrements.

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

Les serveurs d'enregistrement sont des ordinateurs où vous avez installé le programme Recording Server, et où vous l'avez configuré pour communiquer avec le 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**.



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.

Le serveur d'enregistrement prend en charge le chiffrement des flux de données sur les clients et les services :

- Activer le cryptage pour les clients et les serveurs on page 330
- Voir le status du cryptage vers les clients on page 314

Le serveur d'enregistrement prend également en charge le chiffrement de la connexion avec le serveur de gestion:

- Activer le cryptage depuis et vers le serveur de gestion on page 325

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

- Ajouter un matériel on page 231
- Déplacer du matériel on page 367
- Supprimer tous les périphériques matériels sur un serveur d'enregistrement on page 388
- Supprimer un serveur d'enregistrement on page 387

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, arrêtez le service Recording Server, fermez le programme accédant au(x) fichier (s) ou répertoire(s) multimédia en question, et redémarrez tout simplement le service Recording Server.

Serveur mobile (explications)

Le serveur mobile est responsable de permettre au client XProtect Mobile et aux utilisateurs de XProtect Web Client d'accéder au système.

En outre, pour agir en temps que passerelle du système pour les deux clients, le serveur mobile peut transcoder la vidéo, car le flux vidéo de la caméra d'origine est bien souvent d'une taille trop importante pour rentrer dans la bande passante disponible pour les utilisateurs du client.

Si vous procédez à une installation **Distribuée** ou **Personnalisée**, Milestone vous recommande d'installer le serveur mobile sur un serveur dédié.

Serveur d'événements (explications)

Le serveur d'événements gère plusieurs tâches liées aux événements, alarmes et plans et potentiellement des intégrations tierces via le 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 l'interface des événements génériques ou des événements analytiques

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 la même base de données SQL Server que celle que le serveur de gestion utilise

Messages

- La communication des messages est gérée par le serveur d'événements, ce qui permet aux modules d'extension d'envoyer des messages en temps réel entre les environnements, tels que XProtect Smart Client, Management Client, le serveur d'événements et les services autonomes.

Plans

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

MIP SDK

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

Serveur de journaux (explications)

Le serveur de journaux stocke tous les messages du journal pour l'ensemble du système dans une base de données SQL Server. Cette base de données de messages du journal peut exister sur le même SQL Server que la base de données de configuration du système du serveur de gestion ou sur SQL Server distinct. Le serveur de journaux est généralement installé sur le même serveur que le serveur de gestion, cependant, afin d'augmenter les performances des serveurs de gestion et de journaux, il peut être installé sur un serveur distinct.

API Gateway (explications)

Le MIP VMS API fournit une API RESTful unifiée, selon les protocoles standard du secteur, tels que OpenAPI, pour accéder aux fonctionnalités XProtect VMS, simplifiant ainsi les projets d'intégration et servant de base pour la communication connectée dans le cloud.

Le XProtect VMSAPI Gateway prend en charge ces options d'intégration via le Milestone Integration Platform VMS API (MIP VMS API).

Le API Gateway est installé sur site et est destiné à servir de front-end et de point d'entrée commun pour les services API RESTful et API de messagerie WebSocket sur tous les composants du serveur VMS actuels (serveur

de gestion, serveur d'événements, serveurs d'enregistrement, serveur de journaux, etc.). Un service API Gateway peut être installé sur le même hôte que le serveur de gestion ou séparément, et plus d'un service peut être installé (chacun sur son propre serveur).

RESTful API est mis en œuvre en partie par chaque composant du serveur VMS spécifique, et le API Gateway peut simplement passer ces requêtes et réponses, alors que pour d'autres requêtes, le API Gateway convertira les requêtes et réponses appropriées.

Actuellement, la configuration API, hébergée par le serveur de gestion, es disponible en tant qu'API RESTful. L'API d'événements RESTful, l'API de messagerie Websockets et l'API d'alarmes RESTful, hébergées par le serveur d'événements, sont également disponibles.

Pour plus d'informations, voir le manuel de l'administrateur API Gateway et la documentation de référence Milestone Integration Platform VMS API.

Redondance

Serveur de gestion de basculement

Le serveur de gestion est le composant central du VMS. Il conserve la configuration du système de surveillance dans une base de données SQL Server, sur SQL Server sur l'ordinateur du serveur de gestion lui-même ou sur SQL Server séparé sur le réseau. Il gère également l'authentification de l'utilisateur, les autorisations utilisateur, le système de règles, entre autres.

Pour minimiser les temps d'arrêt du système, vous pouvez configurer un serveur de gestion de basculement en installant le serveur de gestion dans un cluster. Le cluster garantira alors qu'un autre ordinateur reprendra la fonction de serveur de gestion si le premier ordinateur tombe en panne.

Vous pouvez installer le serveur de gestion dans un cluster à l'aide de :

XProtect Management Server Failover

XProtect Management Server Failover est une extension de XProtect VMS qui peut vous aider dans les cas suivants :

- Un serveur tombe en panne : vous pouvez exécuter les composants du système depuis un autre ordinateur pendant que vous résolvez les problèmes.
- Vous devez appliquer les mises à jour du système et les correctifs de sécurité : l'application de correctifs de sécurité dans un serveur de gestion autonome peut prendre du temps, ce qui provoquera des temps d'arrêt. Lorsque vous avez un cluster de basculement, vous pouvez appliquer des mises à jour du système et des correctifs de sécurité avec peu de temps d'arrêt.
- Vous avez besoin d'une connexion transparente : les utilisateurs bénéficient d'un accès continu à la vidéo en direct et en lecture, ainsi qu'à la configuration du système à tout moment.

Pour configurer XProtect Management Server Failover, vous devez installer le serveur de gestion, le serveur de journaux et le serveur d'événements sur deux ordinateurs. Si le premier ordinateur cesse de fonctionner, les

composants VMS commencent à s'exécuter sur le deuxième ordinateur. En outre, vous pouvez bénéficier d'une réplication sécurisée en temps réel des bases de données VMS lorsque SQL Server s'exécute dans le cluster de basculement.

Pour plus d'informations, voir le manuel de l'administrateur pour XProtect Management Server Failover.

Windows Server Failover Clustering (WSFC)

WSFC est une fonctionnalité du système d'exploitation Microsoft Windows Server pour la tolérance aux pannes et la haute disponibilité (HA) des applications et des services. Elle permet à plusieurs ordinateurs d'héberger des services partagés et, en cas de défaillance des services sur un nœud, les nœuds restants prennent automatiquement en charge l'hébergement des services.

Vous pouvez installer le serveur de gestion sur au moins deux nœuds au sein d'un cluster. Un nœud exécute Management Server et Data Collector, et échange des fréquences avec les autres nœuds du cluster. Si le serveur de gestion actif et ses services associés cessent de s'exécuter sur un nœud ou s'exécutent très lentement, les services VMS commencent à s'exécuter sur un autre nœud du cluster.

Pour plus d'informations, consultez le guide Clustering de basculement.

Serveur d'enregistrement de basculement (explications)

> Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Un serveur d'enregistrement de basculement est un serveur d'enregistrement supplémentaire qui peut prendre le relais du serveur d'enregistrement standard si celui-ci devient indisponible. Vous pouvez configurer un serveur d'enregistrement de basculement avec deux modes, en tant que **serveur d'enregistrement de basculement à froid** ou en tant que **serveur de basculement à affectation unique (à chaud)**.

Les serveurs d'enregistrement de basculement sont installés comme les serveurs d'enregistrement standard (voir Installer un serveur d'enregistrement de basculement via Download Manager on page 183). Une fois que vous avez installé les serveurs d'enregistrement de basculement, ils sont visibles dans le Management Client. Milestone vous recommande d'installer chaque serveur d'enregistrement de basculement sur un ordinateur distinct. Assurez-vous de configurer les serveurs d'enregistrement de basculement avec la bonne adresse IP ou le bon nom d'hôte du serveur de gestion. Les autorisations utilisateur pour le compte d'utilisateur sous lequel s'exécute le service du serveur de basculement sont fournies lors du processus d'installation. Il s'agit des :

- Autorisations Marche/Arrêt pour démarrer et arrêter le serveur d'enregistrement de basculement
- Autorisations d'accès en Lecture/Écriture pour lire ou modifier le fichier RecorderConfig.xml

Si un certificat est sélectionné pour le cryptage, alors l'administrateur doit accorder l'autorisation Lire à l'utilisateur du serveur de basculement sur la clé privée sélectionnée.

Si le serveur d'enregistrement de basculement prend le contrôle depuis le serveur d'enregistrement utilisant le cryptage, Milestone recommande de préparer également le serveur d'enregistrement de basculement pour qu'il utilise le cryptage. Pour plus d'informations, voir Communication sécurisée (explications) on page 158 et Installer un serveur d'enregistrement de basculement via Download Manager on page 183.

Vous pouvez spécifier quel type d'assistance de basculement vous souhaitez pour chaque périphérique. Pour chaque périphérique d'un serveur d'enregistrement, vous pouvez sélectionner un basculement complet, uniquement en direct ou aucune assistance de basculement. Ceci vous aide à accorder une priorité à vos ressources de basculement 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.

Lorsque votre système se trouve en mode de basculement, vous ne pouvez pas remplacer ou déplacer un matériel, mettre à jour le serveur d'enregistrement, ou changer les configurations du périphérique telles que les paramètres de stockage ou les paramètres du flux vidéo.

Serveurs d'enregistrement de basculement à froid

Dans une configuration de serveur de basculement à froid, vous regroupez plusieurs serveurs d'enregistrement de basculement dans un groupe de basculement. L'ensemble du groupe de basculement se consacre à prendre le relais de plusieurs serveurs d'enregistrement présélectionnés au cas où l'un d'entre eux ne serait plus disponible. Vous pouvez créer autant de groupes que vous le souhaitez (voir Serveurs d'enregistrement de basculement groupes pour une veille à froid on page 228).

Le regroupement a un avantage évident : par la suite, lorsque vous spécifiez les serveurs d'enregistrement de basculement devant prendre le relais d'un serveur d'enregistrement, vous sélectionnez un groupe de serveurs d'enregistrement de basculement. Si le groupe choisi contient plus d'un serveur d'enregistrement de basculement, vous savez que vous avez plus d'un serveur d'enregistrement de basculement à disposition si jamais un serveur d'enregistrement était indisponible. Vous pouvez spécifier un groupe de serveurs de basculement secondaire, qui prendra le relais du groupe primaire si tous les serveurs d'enregistrement du groupe primaire sont occupés. Un serveur d'enregistrement de basculement peut uniquement faire partie d'un seul groupe à la fois.

Les serveurs d'enregistrement de basculement d'un groupe de basculement sont classés de façon séquentielle. Cette séquence détermine l'ordre dans lequel les serveurs d'enregistrement de basculement doivent prendre le relais d'un serveur d'enregistrement. Par défaut, la séquence reflète l'ordre dans lequel vous avez incorporé les serveurs d'enregistrement de basculement dans le groupe de basculement ; le premier arrivé étant classé en premier dans la séquence. Vous pouvez le modifier si nécessaire.

Serveurs d'enregistrement de basculement à affectation unique

Dans une configuration de serveur d'enregistrement de basculement à affectation unique, vous pouvez dédier un serveur d'enregistrement de basculement pour qu'il prenne le relais d'**un** seul serveur d'enregistrement. Pour cette raison, le système peut conserver ce serveur d'enregistrement de basculement en mode « veille », ce qui signifie qu'il est synchronisé avec la configuration correcte/actuelle du serveur d'enregistrement auquel il est dédié et qu'il peut prendre le relais bien plus rapidement qu'un serveur d'enregistrement de basculement à froid. 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 assigner des serveurs de basculement qui font déjà partie d'un groupe de basculement en tant que serveurs d'enregistrement à affectation unique.

Validation du serveur d'enregistrement de basculement

Pour valider une fusion des données vidéo d'un serveur de basculement au serveur d'enregistrement, vous devez rendre le serveur d'enregistrement indisponible en arrêtant le service du serveur d'enregistrement ou en éteignant l'ordinateur du serveur d'enregistrement.

Toute interruption manuelle du réseau que vous pouvez provoquer en débranchant le câble réseau ou en bloquant le réseau avec un outil de test ne constitue pas une méthode valide.

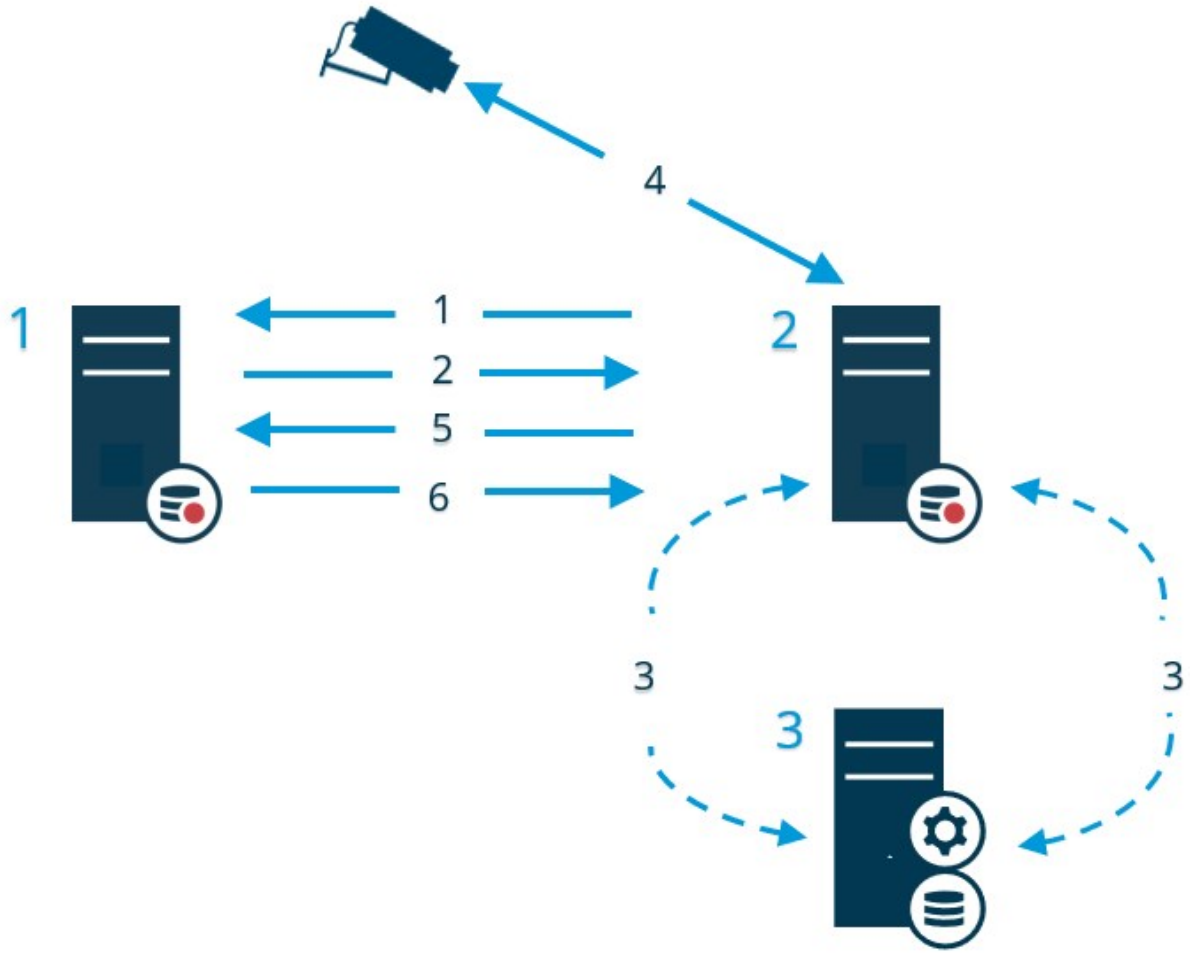
Fonctionnalité du serveur d'enregistrement de basculement (explications)

- Un serveur d'enregistrement de basculement vérifie l'état des serveurs d'enregistrement concernés chaque 0,5 seconde. 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 basculement prend le relais.
- Un serveur d'enregistrement de basculement à froid prend le relais du serveur d'enregistrement qui est devenu indisponible après cinq secondes plus le temps nécessaire à la connexion aux caméras. Par contre, un serveur d'enregistrement de basculement 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 basculement. Les enregistrements stockés par le serveur d'enregistrement de basculement sont automatiquement fusionnés dans les bases de données du serveur d'enregistrement standard. Le temps requis par le processus de fusion 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 basculement a pris le relais.
- Si un serveur d'enregistrement de basculement doit prendre le relais d'un autre serveur d'enregistrement lors du processus de fusion dans une configuration de serveur d'enregistrement de basculement à froid, 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 basculement reprend le processus de fusion et permet aux serveurs d'enregistrement A et B de fusionner à nouveau les enregistrements simultanément.
- Dans une configuration à affectation unique, un serveur de basculement 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 basculement 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 basculement prend le relais. Une brève coupure se produit, généralement pendant quelques secondes seulement, au moment où le serveur d'enregistrement de basculement 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 basculement a pris le relais. Comme les enregistrements récents sont stockés sur le serveur d'enregistrement de basculement, ils peuvent lire les enregistrements effectués après la prise de relais par le serveur d'enregistrement de basculement. 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 basculement. 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 basculement 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 basculement a pris le relais.

- Dans une configuration de redondance à froid, la configuration d'un serveur d'enregistrement de basculement en soutien d'un autre serveur d'enregistrement de basculement n'est pas nécessaire. La raison est que vous attribuez des groupes de basculement et non des serveurs d'enregistrement de basculement particuliers pour prendre le relais des serveurs d'enregistrement spécifiques. Un groupe de basculement doit comprendre au moins un serveur d'enregistrement de basculement, mais vous pouvez ajouter autant de serveurs d'enregistrement de basculement que nécessaire. Si un groupe de basculement contient plusieurs serveurs d'enregistrement de basculement, plusieurs serveurs d'enregistrement de basculement peuvent prendre le relais.
- Dans une configuration à affectation unique, vous ne pouvez pas configurer des serveurs d'enregistrement de basculement ou des serveurs à affectation unique en tant que serveur de basculement à affectation unique.

Étapes de basculement (explications)



Description
Serveurs impliqués (numéros en bleu) : 1. Recording Server 2. Failover Recording Server 3. Management Server
Étapes de basculement pour les configurations **à veille à froid** : 1. Pour vérifier si elle fonctionne ou non, un serveur d'enregistrement de basculement dispose d'une connexion TCP permanente avec le serveur d'enregistrement. 2. Cette connexion est interrompue. 3. Le serveur d'enregistrement de basculement 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 basculement reçoit la configuration et commence à enregistrer pour le compte du serveur d'enregistrement. 4. Le serveur d'enregistrement de basculement et la/les caméra(s) échangent des données vidéo. 5. Le serveur d'enregistrement de basculement essaie continuellement de rétablir la connexion avec le serveur d'enregistrement. 6. Une fois la connexion au serveur d'enregistrement rétablie, le serveur d'enregistrement récupère les données vidéo (le cas échéant) enregistrées pendant son temps d'arrêt et les fusionne avec sa base de données.
Étapes de basculement pour les configurations **à affectation unique** : 1. Pour vérifier si elle fonctionne ou non, un serveur de basculement à affectation unique dispose d'une connexion TCP 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 basculement 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 basculement à affectation unique et la ou les caméra(s) pertinente(s) échangent des données vidéo.

Description
5. Le serveur de basculement 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 basculement 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.

Services du serveur d'enregistrement de basculement (explications)

Un serveur d'enregistrement de basculement 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 basculement d'agir comme un serveur d'enregistrement.

  Dans une configuration de redondance à froid, ce service n'est démarré que lorsqu'il est requis, c'est-à-dire lorsque le serveur d'enregistrement de basculement à froid prend le relais du serveur d'enregistrement. Démarrer ce service prend généralement quelques secondes, mais peut prendre plus de temps en fonction des paramètres de sécurité locaux, etc.
  Dans une configuration à affectation unique, ce service fonctionne en permanence et permet au serveur de basculement à affectation unique de prendre le relais plus rapidement que le serveur d'enregistrement de basculement à froid.

Haute disponibilité des bases de données SQL Server

Les services XProtect stockent les données dans différentes bases de données SQL Server :

- **Surveillance** pour les services Management Server et Event Server
- **Surveillance_IDP** pour Identity Provider
- **Surveillance_IM** pour XProtect Incident Manager
- **LogserverV2 : LogServer** pour le service Log Server

Pour assurer la redondance des bases de données SQL Server, vous devez vous assurer que les services et les composants peuvent accéder aux bases de données. En fonction de vos besoins, différentes options de haute disponibilité s'offrent à vous :

Groupes de disponibilité Always On

Les groupes de disponibilité Always On (AG) protègent les bases de données en conservant des copies des bases de données sur d'autres hôtes, appelés réplicas, qui peuvent prendre le relais en cas de défaillance de l'hôte principal.

Pour en savoir plus sur les AG, consultez Qu'est-ce qu'un groupe de disponibilité Always On ?.

Instances de cluster de basculement

Les instances de cluster de basculement (FCI) offrent une haute disponibilité pour l'ensemble de l'instance SQL Server, garantissant que tous les composants, y compris les bases de données et les tâches, sont déplacés vers un autre hôte en cas de panne.

Pour en savoir plus sur les FCI, consultez Instances de cluster de basculement Always On (SQL Server).

Expédition de journaux

Avec l'expédition de journaux SQL Server, vous pouvez copier le fichier journal des transactions d'une instance SQL Server à une autre.

Pour en savoir plus sur l'expédition de journaux, consultez À propos de l'expédition de journaux (SQL Server).

Clients

Management Client (explications)

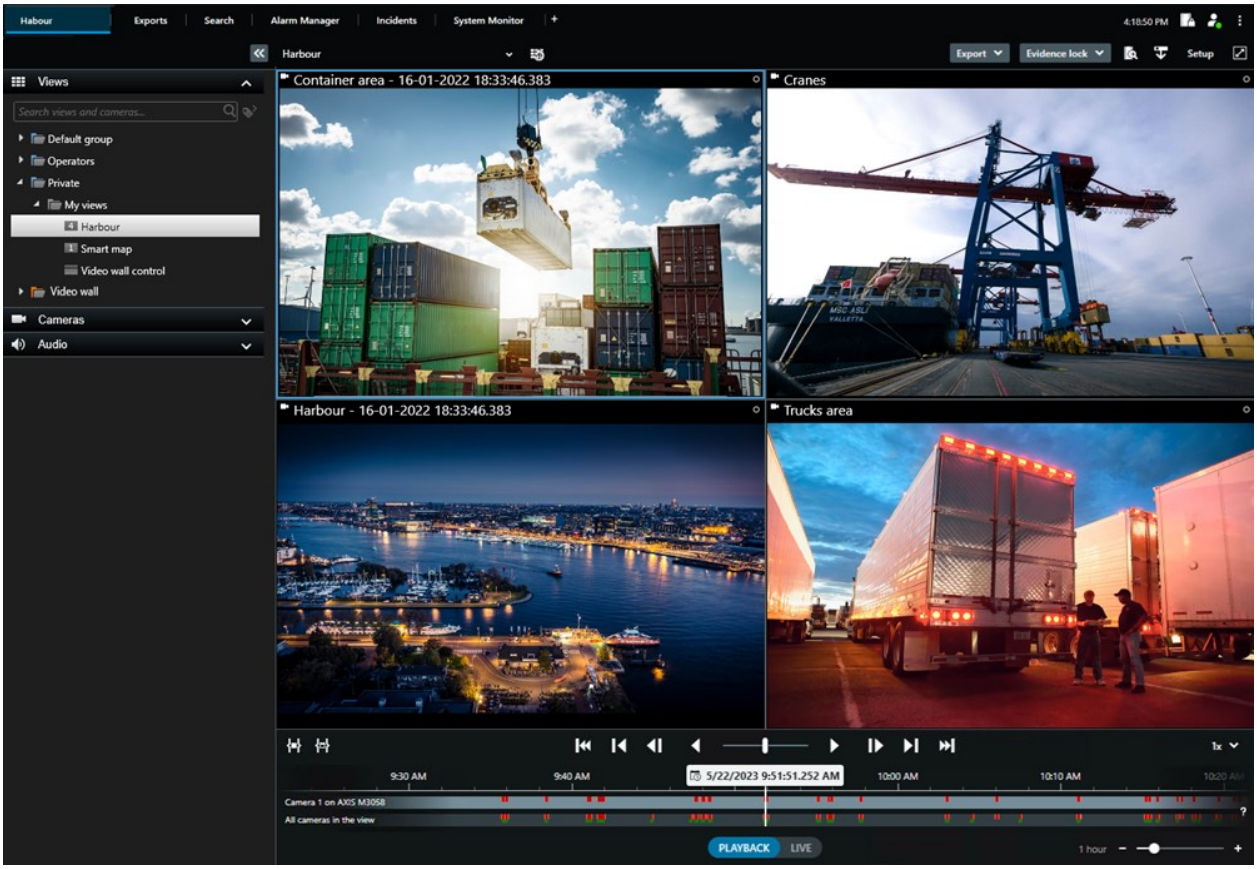
Le Management Client est un client d'administration riche en fonctionnalités pour la configuration et la gestion quotidienne de votre système. Disponible en plusieurs langues.

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

XProtect Smart Client (explications)

XProtect Smart Client est une application de bureau conçue pour vous aider à gérer vos caméras de surveillance IP. Elle offre un contrôle intuitif sur les installations de sécurité en conférant aux utilisateurs l'accès à la vidéo en direct et enregistrée, un contrôle instantané des caméras et périphériques de sécurité connectés et la possibilité d'effectuer des recherches avancées dans les enregistrements et métadonnées.

Disponible dans de nombreuses 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 visualisation afin de spécifier votre environnement de travail en sélectionnant un thème clair ou sombre. Il dispose également d'onglets de travail optimisé et d'une chronologie principale des opérations de surveillance facilitées.

En utilisant MIP SDK, les utilisateurs peuvent intégrer différents types de systèmes de sécurité, de gestion et des applications d'analyse vidéo, que vous gérez à travers XProtect Smart Client.

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

XProtect Mobile client (explications)

Le client XProtect Mobile est une solution de surveillance mobile étroitement intégrée au reste de votre configuration de surveillance XProtect. Il s'exécute sur votre tablette ou smartphone Android ou sur votre tablette, smartphone, lecteur de musique Apple® et vous donne accès aux caméras, vues et autre fonctionnalité configurée dans la gestion des clients.

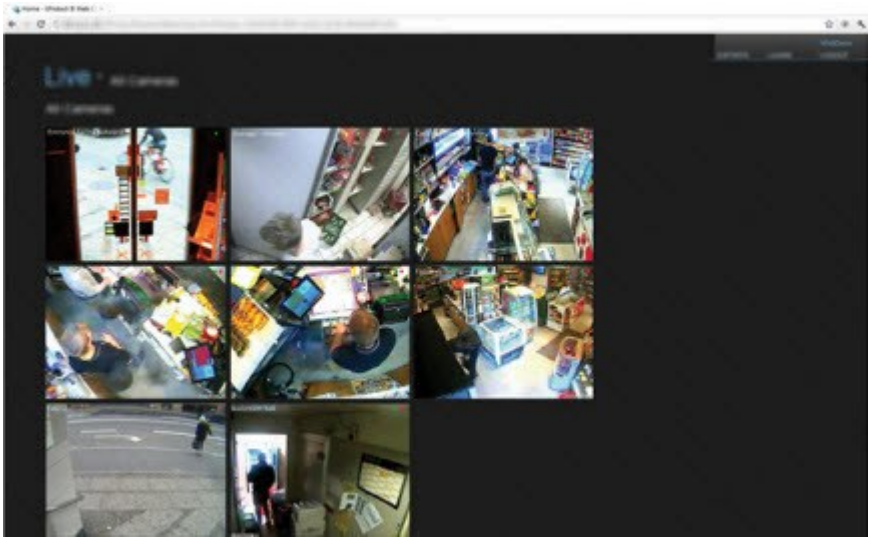
Utilisez le client XProtect Mobile pour voir et lire la vidéo en direct et enregistrée à partir d'une ou de plusieurs caméras, des caméras de contrôle PTZ (pan-tilt-zoom), de la sortie de déclenchement et des événements. Utilisez la fonctionnalité vidéo push pour envoyer de la vidéo à partir de votre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

Si vous souhaitez utiliser le client XProtect Mobile avec votre système, vous devez disposer d'un serveur XProtect Mobile afin d'établir la connexion entre le client XProtect Mobile et votre système. Une fois que le serveur XProtect Mobile est configuré, téléchargez le client XProtect Mobile gratuitement depuis Google Play ou App Store pour commencer à utiliser XProtect Mobile.

Vous avez besoin d'une licence de périphérique par périphérique qui puisse lancer la vidéo dans votre système XProtect.

XProtect Web Client (explications)

XProtect Web Client est une application client en ligne permettant de consulter, 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 autorisations utilisateur individuelles qui sont configurées dans Management Client.



Pour pouvoir utiliser le XProtect Web Client, vous devez avoir un serveur XProtect 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 XProtect Mobile configuré, vous pouvez contrôler votre système XProtect n'importe où à partir de n'importe quel ordinateur ou tablette disposant d'un accès Internet (si vous connaissez l'adresse externe/Internet correcte, le nom d'utilisateur et le mot de passe).

Extensions XProtect

À propos des extensions XProtect

Milestone a développé plusieurs extensions. Les extensions sont des éléments qui étendent les fonctionnalités des produits XProtect VMS en y ajoutant des fonctions spécialisées supplémentaires.

> Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

XProtect Access pour les administrateurs

XProtect Access est une extension de XProtect. Lorsqu'un module d'extension XProtect dédié existe, il permet aux organisations d'intégrer leurs systèmes de contrôle d'accès à XProtect.

Pour utiliser cette extension, vous devez acheter ce qui suit :

- 1 (une) licence de base pour chaque système XProtect que vous souhaitez utiliser avec XProtect Access
- 1 (une) licence pour chaque porte que vous souhaitez contrôler via XProtect

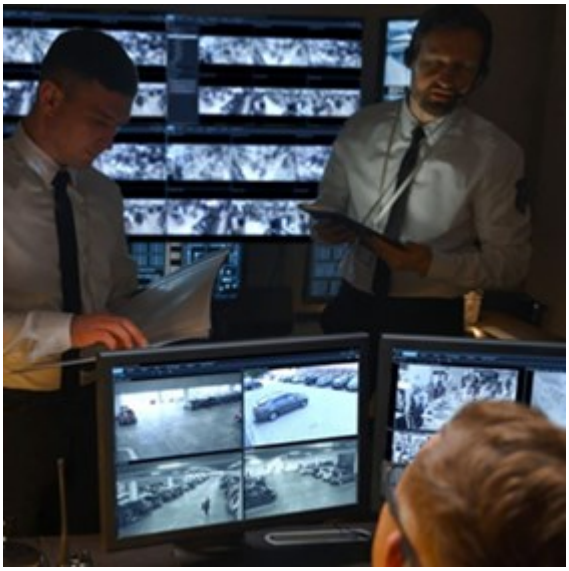
XProtect Access comprend les éléments suivants :

- Une interface utilisateur partagée destinée aux opérateurs pour les systèmes de contrôle d'accès dans XProtect Smart Client
- L'intégration puissante de systèmes de contrôle d'accès
- La surveillance en direct des événements et des points d'accès
- Des demandes d'accès assistées par opérateur
- Des intégrations avec des plans
- Des définitions d'alarmes pour les événements de contrôle d'accès
- La possibilité d'enquêter 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

Chaque fois qu'un utilisateur de XProtect Smart Client effectue une action liée à l'accès, comme l'ouverture d'une porte ou le refus d'entrée, le système l'enregistre dans le **journal d'activité**.

XProtect Incident Manager pour les administrateurs

XProtect Incident Manager est une extension qui permet aux organisations de documenter les incidents et de les associer à des preuves sous forme de séquences (vidéo et potentiellement audio) provenant du VMS XProtect.



Les utilisateurs de XProtect Incident Manager peuvent en outre enregistrer en vidéo l'intégralité des informations de l'incident dans les projets d'incident. Depuis les projets d'incident, ils peuvent suivre l'état et les activités de chaque incident. De cette manière, les utilisateurs peuvent gérer efficacement les incidents et partager en toute facilité des preuves fortes de l'incident, que ce soit en interne avec leurs collègues ou de manière externe avec les autorités.

XProtect Incident Manager offre aux organisations un aperçu et une compréhension globale des incidents qui surviennent dans les zones étudiées. Cette connaissance permet aux organisations de mettre en place des étapes afin de minimiser les risques de répétition d'incidents similaires.

Dans XProtect Management Client, les administrateurs d'un VMS XProtect d'une organisation peuvent définir les propriétés de l'incident disponibles dans XProtect Incident Manager en fonction des besoins de celle-ci. Les opérateurs de XProtect Smart Client démarrent, enregistrent et gèrent les projets d'incident et ajoutent plusieurs informations aux projets d'incident. Celles-ci comprennent du texte libre, des propriétés de l'incident définies par les administrateurs, ainsi que des séquences provenant du VMS XProtect. Pour une traçabilité intégrale, le VMS XProtect consigne quand les administrateurs définissent et éditent les propriétés de l'incident et quand les opérateurs créent et mettent à jour les projets d'incident.

XProtect LPR pour les administrateurs

XProtect LPR vous permet d'utiliser l'analyse de contenu vidéo (VCA) et la reconnaissance des plaques d'immatriculation des véhicules en interaction avec votre système de surveillance et votre XProtect Smart Client.

Pour lire les caractères d'une plaque, XProtect LPR utilise la reconnaissance optique de caractères sur des images assistées par des paramètres de caméra spécialisés.

Vous pouvez associer la reconnaissance de plaque (License Plate Recognition, LPR) à d'autres fonctionnalités de surveillance telles que l'enregistrement et l'activation de sorties en fonction d'événements.

Exemples d'événements dans XProtect LPR :

- Activer l'enregistrement dans une certaine qualité
- Déclencher les alarmes
- Établir la correspondance avec des listes de correspondances positives et négatives
- Ouvrir des barrières
- Allumer la lumière
- Afficher automatiquement l'enregistrement d'un incident sur les écrans du personnel de sécurité désigné
- Envoyer des SMS sur certains téléphones portables

Avec un événement, vous pouvez activer des alarmes dans XProtect Smart Client.

XProtect Smart Wall pour les administrateurs

XProtect Smart Wall est une extension avancée qui permet aux entreprises de créer des murs vidéo qui répondent à leurs besoins spécifiques en matière de sécurité. XProtect Smart Wall fournit une vue d'ensemble de toutes les données vidéo dans le système VMS[1] XProtect et prend en charge n'importe quelle quantité ou combinaison de moniteurs.

[1]Abréviation pour "Logiciel de gestion des vidéos".

XProtect Smart Wall permet aux opérateurs de voir des murs vidéo statiques, tels que définis par leur administrateur système, avec un ensemble de caméras et de dispositions de moniteurs fixe. Cependant, le mur vidéo est également dirigé par l'opérateur, c'est-à-dire que ce dernier peut contrôler ce qui est affiché. Cela inclut :

- Déplacer des caméras et autres types de contenus vers le mur vidéo, comme des images, du texte, des alarmes et des Smart Map
- Envoyant des vues aux moniteurs
- Appliquer d'autres préréglages[1] pour certains événements.

Enfin, les changements d'affichage peuvent être contrôlés par des règles qui changent automatiquement les préréglages en fonction d'événements spécifiques ou de plannings bien définis.

XProtect Transact pour les administrateurs

XProtect Transact est une extension des solutions de vidéosurveillance IP de Milestone qui vous permet d'observer les transactions en cours et d'enquêter sur des transactions passées. Les transactions sont connectées aux systèmes de surveillance vidéo numériques contrôlant les transactions. Cela permet par

[1]Une couche prédéfinie pour un ou plusieurs moniteurs Smart Wall dans XProtect Smart Client. Les préréglages déterminent les caméras affichées et la manière dont le contenu est structuré sur chaque moniteur du mur vidéo.

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. Lors de la sélection d’une ligne de transaction, une image vidéo fixe provenant de chacune des caméras associées est affichée dans une zone d’aperçu qui vous permet de consulter les enregistrements. En dessous de la zone d’aperçu, la transaction associée à la ligne sélectionnée est affichée dans un justificatif.

XProtect Management Server Failover

Si un ordinateur autonome exécutant le serveur de gestion ou SQL Server connaît une défaillance matérielle, cela n’affecte pas les enregistrements ou le serveur d’enregistrement. Cependant, ces pannes matérielles peuvent provoquer des temps d’arrêt pour les opérateurs et les administrateurs qui ne sont pas connectés dans les clients.

XProtect Management Server Failover est une extension de XProtect VMS qui peut vous aider dans les cas suivants :

- Un serveur tombe en panne : vous pouvez exécuter les composants du système depuis un autre ordinateur pendant que vous résolvez les problèmes.
- Vous devez appliquer les mises à jour du système et les correctifs de sécurité : l’application de correctifs de sécurité dans un serveur de gestion autonome peut prendre du temps, ce qui provoquera des temps d’arrêt. Lorsque vous avez un cluster de basculement, vous pouvez appliquer des mises à jour du

système et des correctifs de sécurité avec peu de temps d'arrêt.

- Vous avez besoin d'une connexion transparente : les utilisateurs bénéficient d'un accès continu à la vidéo en direct et en lecture, ainsi qu'à la configuration du système à tout moment.

Pour configurer XProtect Management Server Failover, vous devez installer le serveur de gestion, le serveur de journaux et le serveur d'événements sur deux ordinateurs. Si le premier ordinateur cesse de fonctionner, les composants VMS commencent à s'exécuter sur le deuxième ordinateur. En outre, vous pouvez bénéficier d'une réplication sécurisée en temps réel des bases de données VMS lorsque SQL Server s'exécute dans le cluster de basculement.

XProtect Hospital Assist

XProtect Hospital Assist est conçu exclusivement pour les services hospitaliers accueillant des patients qui nécessitent une observation continue.

Cette extension VMS XProtect est une solution adaptée à la surveillance à distance des patients ; elle permet à l'hôpital de :

- Améliorer l'efficacité du personnel.
- Réagir rapidement aux incidents.
- Fournir des soins de haute qualité.

Avec cette extension XProtect, les utilisateurs XProtect Smart Client peuvent :

- Ajouter une pense-bête aux vues de la caméra à l'aide de Sticky Notes.
- Flouter le flux vidéo en direct à l'aide du floutage de confidentialité.
- Recevoir une alarme lorsqu'un patient tombe grâce à la Détection de chute.
- Écouter plusieurs pièces et parler avec un patient à distance à l'aide de Multipièces Audio.

Husky IVO System Health

L'interface Husky IVO System Health vous permet d'obtenir un aperçu rapide de l'état général de toutes les unités Husky IVO que vous avez spécifiquement connectées au serveur de gestion XProtect afin de signaler les données relatives à l'intégrité du système.

Les données relatives à l'intégrité du système pour les unités Husky IVO qui n'ont pas été spécifiquement connectées au serveur de gestion XProtect pour l'envoi de données relatives à l'intégrité du système ne seront pas affichées.

L'état des unités Husky IVO connectées est affiché dans le nœud Husky IVO System Health dans XProtect Management Client. Le Husky IVO System Health n'affiche que les données d'intégrité du système des unités Husky IVO.

Installation du module d'extension requise

Le nœud Husky IVO System Health n'est accessible qu'après l'installation du module d'extension Husky IVO System Health sur le serveur de gestion XProtect.

Version bêta

Le nœud Husky IVO System Health est actuellement publié en tant que version bêta. L'apparence et les fonctions de la version finale peuvent différer de celles de la version bêta.

Indicateurs d'état de l'intégrité du système

Les indicateurs d'état général affichés sur le nœud d'aperçu de Husky IVO System Health sont les suivants :

- **Tout va bien** : Aucun problème n'est à signaler.
- **À besoin d'attention** : Un ou plusieurs problèmes ont été détectés et requièrent votre attention.
- **Données manquantes** : L'état ne peut pas être signalé en raison de l'insuffisance des données.

Vérifier l'intégrité du système d'une unité spécifique

Il est également possible d'afficher les données relatives à l'intégrité du système d'unités spécifiques Husky IVO. Sélectionnez le nom d'une unité dans le nœud d'aperçu de l'intégrité du système pour ouvrir une nouvelle page où sont affichées les principales statistiques relatives à l'intégrité du système pour cette unité.

Les données relatives à l'intégrité du système d'une unité donnée affichent généralement les indicateurs d'état clés suivants :

- **État du stockage des données** : L'état du stockage de l'appareil ainsi que l'option de gestion du stockage sélectionnée.
- **Utilisation RAM** : La capacité totale de la RAM en Go ainsi que la capacité actuelle de la RAM libre en Go.
- **Charge CPU** : La charge actuelle du CPU, mesurée en pourcentage de la charge théorique maximale.
- **La température du CPU** : La température du CPU en Celsius et en Fahrenheit.
- **Réseau** : L'état en ligne/hors ligne de tous les emplacements NIC enregistrés sur l'unité.

Certaines données relatives à l'intégrité du système dépendent du matériel de l'unité, par exemple les données relatives à l'alimentation électrique seront affichées pour les unités qui contiennent des options d'alimentation électrique double (redondante) et les données relatives à la charge et à la température du GPU seront affichées pour les unités qui contiennent des cartes GPU discrètes.

Connexion à l'intégrité du système Husky

Chaque unité Husky IVO doit être connectée manuellement au Management Client à l'aide de son logiciel Husky Assistant local.

Les révisions Husky IVO suivantes peuvent se connecter au nœud Husky IVO System Health :

• Milestone Husky IVO 150D, révision 2 ou ultérieure

• Milestone Husky IVO 350T, révision 3 ou ultérieure

• Milestone Husky IVO 350R ou ultérieure

• Milestone Husky IVO 700R, révision 2 ou ultérieure

• Milestone Husky IVO 1000R, révision 2 ou ultérieure

• Milestone Husky IVO 1800R ou ultérieure

Comme le processus de connexion à l'intégrité du système est lancé sur la page **Intégrité du système** dans le Husky Assistant, il se peut que vous deviez mettre à jour le Husky Assistant sur les unités individuelles Husky IVO vers la version la plus récente afin d'accéder à la page **Intégrité du système** .

Il n'est pas possible de connecter en masse ou de connecter automatiquement plusieurs appareils Husky IVO pour envoyer des données sur l'intégrité du système au serveur de gestion XProtect.

Pour connecter une unité Husky IVO, vous devez cliquer sur le bouton **Connecter** de la page **Intégrité du système** dans le Husky Assistant de l'unité Husky IVO et fournir l'adresse de l'ordinateur du Management Client ainsi que les informations d'identification de l'administrateur.

Résolution des problèmes Husky IVO

Vous ne pouvez pas dépanner ou résoudre les problèmes signalés pour les unités Husky IVO à partir du serveur de gestion XProtect. Vous devez donc accéder directement aux unités en question pour procéder à l'atténuation ou au dépannage.

Périphériques

Matériel (explications)

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 ou un module E/S.
- Un serveur d'enregistrement sur un site distant dans une configuration Milestone Interconnect

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

> 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.

Configuration matérielle (explications)

Certains fabricants exigent que les identifiants soient configurés dans le matériel dès sa sortie de la boîte, soit avant d'ajouter le matériel à un système VMS pour la première fois. Il s'agit de la préconfiguraiton du matériel et elle s'effectue via l'assistant **Préconfigurer des périphériques** qui apparaît lorsque ledit matériel est détecté par l'assistant Ajouter un matériel on page 231.

Ci-dessous des informations importantes à prendre en compte concernant l'assistant **Préconfigurer le matériel** :

- Un matériel qui requiert des identifiants de base avant son ajout dans un système VMS ne peut être ajouté via les identifiants par défaut habituels. Il doit être configuré via l'assistant ou en vous connectant directement au matériel
- Les identifiants (nom d'utilisateur et mot de passe) peuvent être ajoutés uniquement dans les champs marqués comme **non configuré**
- Une fois que l'**état** du matériel est paramétré sur **configuré**, vous ne pouvez plus changer les identifiants de connexion (nom d'utilisateur ou mot de passe)
- La préconfiguration s'applique aux matériels prêts à l'emploi et ne doit être faite qu'une seule fois. Une fois préconfiguré, le matériel peut être géré comme n'importe quel autre matériel dans Management Client
- Après avoir fermé l'assistant **Préconfigurer des périphériques**, le matériel préconfiguré apparaîtra dans l'assistant Ajouter un matériel on page 231, et pourra désormais être ajouté à votre système

> Il est fortement recommandé d'ajouter un matériel préconfiguré à votre système via l'assistant Ajouter un matériel on page 231 après avoir fermé l'assistant **Préconfigurer des périphériques**. Management Client ne conservera pas les identifiants préconfigurés si vous n'ajoutez pas le matériel à votre système.

Périphériques (explications)

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 Web de Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

Les sections suivantes décrivent chacun des types de périphériques que vous pouvez ajouter.

Caméras

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 l'autorisation des utilisateurs de visualiser la vidéo.

Microphones

Vous pouvez relier des micros externes sur de nombreux périphériques. Certains périphériques sont équipés de micros intégrés.

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 afin de recevoir des événements spécifiques au microphone qui déclenchent les actions concernées.

Les rôles déterminent l'autorisation des utilisateurs d'écouter les microphones. Vous ne pouvez pas écouter les micros depuis le Management Client.

Haut-parleurs

Vous pouvez relier des haut-parleurs externes sur de nombreux périphériques. Certains périphériques disposent de haut-parleurs intégrés.

Le système envoie un flux audio vers les haut-parleurs lorsque l'utilisateur appuie sur le bouton de conversation dans XProtect Smart Client. Vous pouvez également utilise cette fonctionnalité à partir de XProtect Web Client et de XProtect® Mobile. L'audio des haut-parleurs n'est enregistré que lorsqu'un utilisateur parle. Les rôles déterminent l'autorisation 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 l'autorisation des utilisateurs de 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.

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.
- 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.

Les rôles déterminent l'autorisation des utilisateurs de visualiser les métadonnées.

Entrées

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.

Sorties

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.

Groupes de périphériques (explications)

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 maintenir 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.

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 des caméras de groupe dans des groupes de périphériques, mais le principe s'applique pour tous les périphériques

Ajouter un groupe de périphériques

Spécifier les périphériques à inclure dans un groupe de périphériques

Spécifier les propriétés communes pour tous les périphériques d'un groupe de périphériques

Stockage de supports

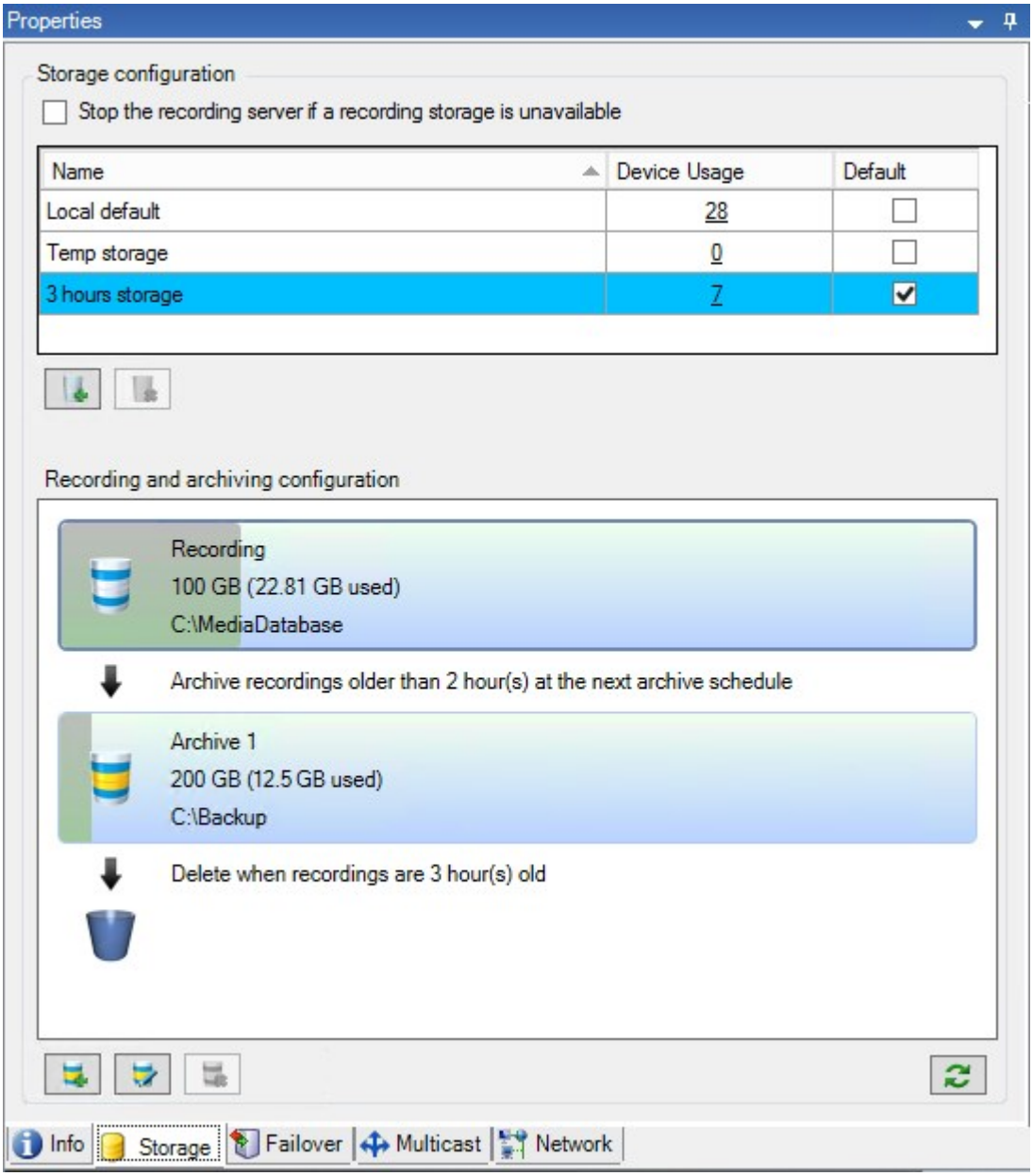
Stockage et archivage (explications)

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Dans l'onglet **Stockage**, vous pouvez configurer, gérer et visualiser des emplacements de stockage pour un serveur d'enregistrement sélectionné.

Pour le stockage et l'archivage des enregistrements, la barre horizontale affiche la quantité d'espace libre. Vous pouvez spécifier le comportement du serveur d'enregistrement au cas où le stockage des enregistrements est indisponible. Cela est particulièrement utile si votre système comprend des serveurs de basculement.

Si vous utilisez le **Verrouillage des preuves**, une ligne rouge s'affiche pour indiquer l'espace utilisé pour la séquence de verrouillage des preuves.



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 stockage se compose d'un stockage d'enregistrement qui 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 la surcharge de la base de données des enregistrements, vous pouvez créer des stockages supplémentaires Ajouter un nouvel emplacement de stockage on page 214). Vous pouvez également créer des archives (voir Créer une archive dans un emplacement de stockage on page 215) dans chaque stockage et démarrer un processus d'archivage pour stocker des 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 chaque 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.

Si un disque dur est endommagé et que le stockage d'enregistrement devient indisponible, la barre horizontale devient rouge. Il sera encore possible de visualiser des vidéos en direct dans XProtect Smart Client, mais l'enregistrement et l'archivage seront interrompus jusqu'à la restauration du disque dur. Si votre système est configuré avec des serveurs d'enregistrement de basculement, vous pouvez spécifier le serveur d'enregistrement pour arrêter l'exécution, pour que les serveurs de basculement prennent le relais (voir Spécifier le comportement lorsque le stockage des enregistrements n'est pas disponible on page 213).

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.

Milestone vous recommande d'utiliser un disque dur dédié pour le stockage et l'archivage d'enregistrements afin d'éviter 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 en lire plus sur l'affectation de la taille des unités et trouver de l'aide sur le site Web de Microsoft (https://learn.microsoft.com/en-us/windows-server/storage/file-server/ntfs-overview).

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, les tentatives d'écriture dans la base de données peuvent échouer et dans ce cas, 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.

Pour les systèmes conformes aux normes FIPS 140-2 comportant des exportations et des bases de données multimédias archivées à partir des versions de XProtect VMS antérieures à 2017 R1 qui sont cryptées avec un cryptage non conforme aux normes FIPS, il est nécessaire d'archiver les données dans un emplacement auquel il est possible d'accéder après l'activation du mode FIPS. Pour de plus amples informations sur comment configurer votre XProtect VMS pour qu'il s'exécute conformément au mode FIPS 140-2, voir la section de conformité aux normes FIPS 140-2 dans le guide de durcissement.

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 on page 215.

Archivage efficace

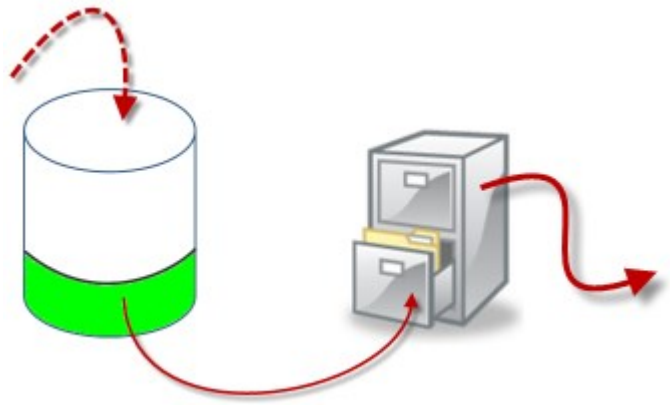
Lorsque vous activez l'archivage d'une caméra ou d'un groupe de caméras, le contenu de la base de données de la caméra est automatiquement déplacé vers une archive à des intervalles que vous définissez.

Selon vos exigences, vous pouvez configurer une ou plusieurs archives pour chacun de vos stockages. 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.

En configurant votre archivage de manière efficace, vous pouvez optimiser vos besoins de stockage. 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 configurerez un archivage efficace à partir de l'onglet **Stockage** d'un serveur d'enregistrement en réglant plusieurs paramètres interdépendants :

- Conservation du stockage d'enregistrements
- Taille du stockage des enregistrements
- Durée de rétention des archives
- Taille de l'archive
- Calendrier d'archivage
- Cryptage
- Images par seconde (Frames per second - FPS).

Les champs de taille définissent la taille du stockage d'enregistrements, comme illustré par ce cylindre et sa/ses archive(s) respective(s) :



En termes de durée de rétention et de paramètre de taille pour le stockage 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.

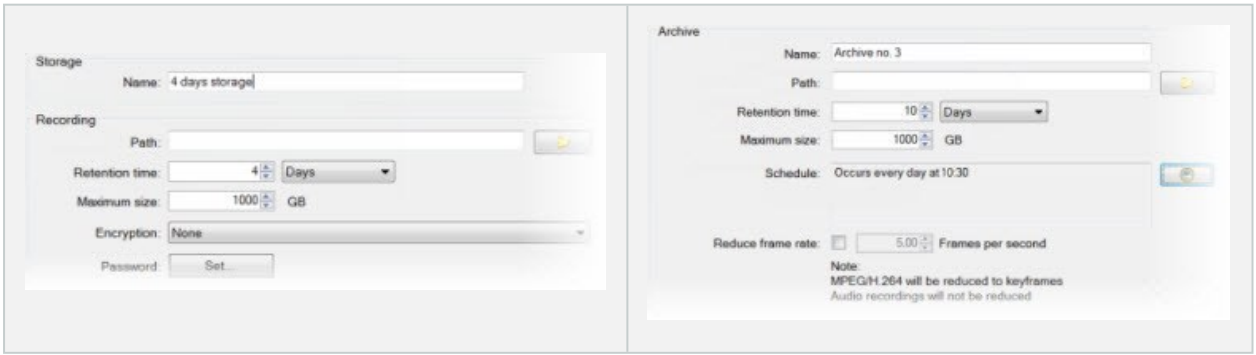
La durée de rétention et le paramétrage de taille des archives définissent la durée pendant laquelle les enregistrements demeurent dans l'archive. Les enregistrements demeurent dans l'archive pendant la période spécifiée, ou jusqu'à ce que l'archive atteigne la limite de taille spécifiée. Lorsque ces 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 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 (image à droite) a une durée de rétention de 10 jours. L'archivage est réglé de façon à se produire tous les jours à 10h30, 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.

Structure des archives (explication)

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 (stockage de bord 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

```
...[Storage Path]\[Storage name]\[device-name] - plus date and time of most
recent recording]\
```

Si les données proviennent du stockage de bord :

```
...[Storage Path]\[Storage name]\[device-name] (Edge) - plus date and time of
most recent recording]\
```

Si les données proviennent de SMTP :

```
...[Storage Path]\[Storage name]\[device-name] (SMTP) - plus date and time of
most recent recording]\
```

Exemple réel

```
...F:\OurArchive\Archive1\Camera 1 on Axis Q7404 Video Encoder(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.

- **Multimédia** : Le dossier contient les fichiers multimédia réels vidéo ou audio (l'un ou l'autre)
- **MotionLevel**: Ce dossier contient les grilles de niveau de mouvement créées à partir des données vidéo à l'aide de notre algorithme de détection de mouvement. Ces données permettent à la fonctionnalité Smart Search de XProtect Smart Client d'effectuer des recherches très rapides
- **Mouvement** : C'est dans ce dossier que le système stocke les séquences de mouvement. Une séquence de mouvement est la tranche de temps durant laquelle un mouvement a été détecté dans les données vidéo. Ces informations sont par exemple utilisées pour la ligne de temps de XProtect Smart Client
- **Enregistrement** : C'est dans ce dossier que le système stocke les séquences d'enregistrement. Une séquence d'enregistrement est une tranche de temps pour laquelle il existe des enregistrements cohérents de données multimédia. Ces informations permettent, par exemple de tracer la ligne de temps dans XProtect Smart Client
- **Signature** : Ce répertoire contient les signatures générées pour les données médias (dans le répertoire Médias). Grâce à ces renseignements, vous pouvez vérifier que les données médias n'ont pas été falsifiées depuis qu'elles ont été enregistrées

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 on Axis Q7404 Video Encoder(10.100.50.137) -
2011-10-05T11:23:47+02:00\
```

Pré-enregistrement et stockage des enregistrements (explications)

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

Stockage des enregistrements pré-enregistrés temporaires

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.

Authentification

Active Directory (explications)

Active Directory est un service d'annuaire distribué et 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 de base sans Active Directory. Le système est soumis à certaines limites au niveau des utilisateurs basiques.

Utilisateurs (explications)

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 basiques**, 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. 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 basiques

Si votre système n'a pas accès à Active Directory, créez un utilisateur basique. Pour plus d'informations sur comment configurer les utilisateurs basiques, voir Créer des utilisateurs de base on page 312.

Identity Provider (explications)

Identity Provider app pool (IDP) est une entité du système qui crée, conserve et gère les informations d'identité des utilisateurs basiques.

Identity Provider fournit également des services d'authentification et d'enregistrement aux applications ou services concernés, dans ce cas : serveur d'enregistrement, serveur de gestion, Data Collector et serveur de rapport.

Lorsque vous vous connectez aux clients et services XProtect en tant qu'utilisateur basique, votre demande est envoyée au Identity Provider. Une fois authentifié, l'utilisateur peut appeler le serveur de gestion.

Identity Provider exécute l'IIS comme faisant partie du serveur de gestion en utilisant le même SQL Server avec une base de données distincte et il est responsable de la création et la conservation des jetons de communication OAuth utilisés par les services pour communiquer (Surveillance_IDP).

Les journaux Identity Provider sont disponibles dans : `\\ProgramData\Milestone\IDP\Logs`.

IDP externe (explications)

IDP est un acronyme pour Identity Provider. Un IDP externe est une application et un service externes où vous pouvez stocker et gérer les informations d'identité de l'utilisateur et fournir des services d'authentification de l'utilisateur à d'autres systèmes. Vous pouvez associer un IDP externe avec le VMS XProtect.

XProtect prend en charge les IDP externes compatibles avec Connect (OIDC) OpenID.

Authentification des utilisateurs

Lorsqu'un IDP externe est configuré, les clients XProtect prennent en charge l'utilisation d'IDP externes en tant qu'option d'authentification supplémentaire.

Lorsque l'adresse de l'ordinateur dans l'écran de connexion du client pointe vers un VMS XProtect avec un IDP externe configuré, un appel d'API sera déclenché et l'option d'authentification pour l'IDP externe sera disponible sur l'écran de connexion. L'appel d'API est activé au démarrage du client et à chaque fois que l'adresse est modifiée.

L'API particulière que le client interroge est une API publique qui ne nécessite aucune authentification de l'utilisateur, de sorte que ces informations peuvent toujours être lues par le client.

Revendications

Une demande est un énoncé qu'une entité comme un utilisateur ou une application formule sur lui ou elle-même.

La revendication se compose d'un nom de revendication et d'une valeur de revendication. Par exemple, le nom de la demande peut être un nom standard qui décrit le contenu de la valeur de demande, et la valeur de demande peut être le nom d'un groupe. Voir plus d'exemples de revendications d'un IDP externe : Exemple de demandes à partir d'un IDP externe.

Les revendications ne sont pas obligatoires. Cependant, elles sont nécessaires pour relier automatiquement les utilisateurs d'IDP externes à des rôles dans le VMS XProtect afin de déterminer les autorisations des utilisateurs. Les revendications sont incluses dans le jeton d'identification de l'utilisateur provenant de l'IDP externe et, par le biais de l'association avec les rôles, elles déterminent les autorisations de l'utilisateur dans XProtect.

Si les revendications liées aux rôles du VMS XProtect ne sont pas fournies pour les utilisateurs d'IDP externes, ces derniers peuvent être créés dans le VMS XProtect lorsqu'ils se connectent pour la première fois. Dans ce cas, les utilisateurs d'IDP externes ne sont liés à aucun rôle. L'administrateur du VMS XProtect doit alors ajouter manuellement les utilisateurs aux rôles.

Conditions préalables pour les IDP externes

Les étapes suivantes doivent être effectuées dans l'IDP externe avant qu'il ne soit configuré dans le VMS.

- L'ID et le secret du client à utiliser avec le VMS XProtect doivent avoir été créés dans l'IDP externe. Pour plus d'informations, voir Noms d'utilisateurs uniques pour les utilisateurs d'IDP externes on page 75.
- L'autorité d'authentification de l'IDP externe doit être connue. Pour plus d'informations, consultez les informations relatives à l'autorité d'authentification pour l'IDP externe dans la boîte de dialogue **Options**. doit être connue.
- Les URI de redirection vers le VMS XProtect doivent avoir été configurés dans l'IDP. Pour plus d'informations, voir Ajouter des URI de redirection pour les clients Web on page 426.
- Facultativement, les revendications liées au VMS doivent avoir été configurées pour les utilisateurs ou les groupes dans l'IDP.
- Le VMS XProtect doit être entièrement configuré avec des certificats pour garantir que toutes les communications sont effectuées via https crypté. Dans le cas contraire, la plupart des IDP externes n'accepteront pas les demandes du VMS XProtect et de ses clients, ou une partie du flux de communication et de l'échange de jetons de sécurité échouera.
- Le VMS XProtect et tous les ordinateurs ou téléphones intelligents clients qui doivent utiliser l'IDP externe doivent pouvoir contacter l'adresse de connexion de l'IDP externe.

Autorisez les utilisateurs à se connecter au VMS XProtect à partir d'un IDP externe

- À partir de l'IDP externe, créez les utilisateurs et les revendications pour identifier les utilisateurs en tant qu'utilisateurs de l'IDP externe dans le VMS XProtect. La création de revendications n'est pas une étape obligatoire, mais c'est ainsi que vous pouvez relier automatiquement les utilisateurs aux rôles. Pour plus d'informations, voir Revendications on page 74.
- À partir du VMS XProtect, créez une configuration qui permette à Identity Provider, intégré au VMS, de contacter l'IDP externe. Pour plus d'informations sur la création d'une configuration pour un IDP externe, voir Ajouter et configurer un IDP externe.
- À partir du VMS XProtect, établissez l'authentification des utilisateurs en mappant les revendications utilisateur depuis l'IDP externe à des rôles XProtect. Pour de plus amples informations sur la procédure de mappage des revendications à des rôles, consultez Mapper des revendications d'un IDP externe à des rôles dans XProtect.
- Connectez-vous à un client XProtect en utilisant un IDP externe pour l'authentification de l'utilisateur, voir Connexion via un IDP externe on page 308.

Rediriger URI

Le URI redirigé indique la page vers laquelle l'utilisateur est envoyé après une authentification réussie. Dans votre IDP externe, vous devez ajouter l'adresse du serveur de gestion suivie du **Chemin de rappel** que vous avez défini dans XProtect Management Client. Par exemple, https://management-server-computer.company.com/idp/signin-oidc

Selon le mode d'accès au VMS XProtect, la configuration du réseau, des serveurs et de Microsoft Active Directory, plusieurs URI de redirection peuvent être nécessaires, dont vous trouverez quelques exemples ci-dessous :

Exemples

Serveur de gestion avec ou sans domaine dans l'URL :

- « https://[nom_du_serveur]/idp/signin-oidc »
- « https://[nom_du_serveur].[nom_du_domaine]/idp/signin-oidc »

Serveur mobile avec ou sans le domaine dans l'URL :

- « https://[nom_du_serveur]:[port_mobile]/idp/signin-oidc »
- « https://[nom_du_serveur].[nom_du_domaine]:[port_mobile]/idp/signin-oidc »

Si le serveur mobile est configuré pour être accessible via Internet, vous devez également ajouter l'adresse publique et les ports.

Noms d'utilisateurs uniques pour les utilisateurs d'IDP externes

Les noms d'utilisateurs sont créés automatiquement pour les utilisateurs qui se connectent à Milestone XProtect via un IDP externe.

L'IDP externe fournit un ensemble de revendications pour créer automatiquement un nom pour l'utilisateur dans XProtect, et dans XProtect un algorithme est utilisé pour choisir un nom à partir de l'IDP externe qui est unique dans la base de données VMS.

Exemples de revendications d'un IDP externe

Les demandes se composent d'un nom de demande et d'une valeur de demande. Par exemple :

Nom de la revendication	Valeur de la revendication
nom	Raz Van
e-mail	123@domain.com
amr	pwd
idp	00o2ghkgazGgi9BIE5d7
preferred_ username	321@domain.com
vmsRole	Opérateur
paramètres régionaux	fr-FR
given_name	Raz
family_name	Lindberg
zoneinfo	Amérique/Los_Angeles
email_verified	Vrai

Utilisation d'un numéro de séquence de demande pour créer des noms d'utilisateur dans XProtect

Dans XProtect, la priorité de recherche lors de la création d'un utilisateur dans le VMS XProtect est déterminée par le numéro de séquence des demandes dans le tableau ci-dessous. Le premier nom de demande disponible sera utilisé dans le VMS XProtect :

Nom de la revendication	Numéro de séquence	Description
UserNameClaimType	1	Mappage configuré avec une demande pour définir le nom d'utilisateur. La revendication est définie dans le champ **Revendication à utiliser pour créer un nom d'utilisateur** dans l'onglet **IDP externe** sous **Outils** > **Options**.
preferred_username	2	Une revendication pouvant provenir d'un IDP externe. Une revendication standard qui est normalement utilisée pour ceci dans Oidc (OpenID Connect).
name	3	
given_name family_ name	4	Nom et nom de famille donnés dans une combinaison telle que Bob Johnson.
e-mail	5	
Première demande disponible + #(premier numéro disponible)	6	Par exemple, Bob#1

Définition de demandes spécifiques pour créer des noms d'utilisateur dans XProtect

Les administrateurs XProtect peuvent définir une revendication spécifique à partir de l'IDP externe qui doit être utilisé pour créer un nom d'utilisateur dans le VMS XProtect. Lorsqu'un administrateur définit une revendication à utiliser pour la création du nom d'utilisateur dans le VMS XProtect, le nom de la revendication doit être écrit exactement de la même manière que le nom de la revendication provenant de l'IDP externe.

- La revendication à utiliser pour créer un nom d'utilisateur est définie dans le champ **Revendication à utiliser pour créer un nom d'utilisateur** dans l'onglet **IDP externe** sous **Outils** > **Options**.

Supprimer des utilisateurs d'un IDP externe

Les utilisateurs créés dans XProtect par une connexion IDP externe sont supprimés de la même façon qu'un utilisateur basique et l'utilisateur peut être supprimé à n'importe quel moment après que l'utilisateur a été créé.

Si un utilisateur est supprimé dans XProtect et que l'utilisateur se connecte à nouveau à partir d'un IDP externe, un nouvel utilisateur sera créé dans XProtect. Cependant, les données associées à l'utilisateur dans XProtect comme les vues et les rôles privés sont perdues et ces informations doivent être recréées pour l'utilisateur dans XProtect.

Si un IDP externe est supprimé dans le/la Management Client, tous les utilisateurs connectés au VMS via l'IDP externe sont aussi supprimés.

Sécurité

Rôles et autorisations d'un rôle (explications)

Tous les utilisateurs dans Milestone XProtect VMS appartiennent à un rôle.

Les rôles définissent les autorisations des utilisateurs, y compris les périphériques auxquels les utilisateurs peuvent accéder. Les rôles déterminent également les autorisations d'accès et de sécurité au sein du système de gestion vidéo.

Le système est fourni avec un rôle **Administrateurs** par défaut avec un accès complet à toutes les fonctionnalités du système, mais dans la plupart des cas, vous avez besoin de plusieurs rôles pour différencier les utilisateurs et l'accès dont ils devraient disposer dans votre système. Vous pouvez ajouter autant de rôles que vous le souhaitez. Voir Assigner et supprimer des utilisateurs et groupes aux/des rôles on page 310.

Vous devrez peut-être configurer différents types de rôles pour les utilisateurs de XProtect Smart Client, selon les périphériques auxquels vous souhaitez qu'ils aient accès, ou des types de restrictions similaires qui nécessitent une différenciation entre les utilisateurs.

Pour créer une différenciation entre les utilisateurs, vous devez :

- Créer et configurer les rôles dont vous avez besoin pour répondre aux besoins commerciaux de votre organisation
- Ajouter des utilisateurs et des groupes d'utilisateurs que vous affectez aux rôles auxquels ils doivent appartenir
- Créez des profils Smart Client et des profils Management Client pour définir ce que les utilisateurs peuvent voir dans XProtect Smart Client et l'interface utilisateur Management Client.

  Les rôles contrôlent uniquement vos autorisations d'accès, et non ce que les utilisateurs peuvent voir dans l'interface utilisateur dans XProtect Smart Client ou le Management Client. Vous n'avez pas besoin de créer un profil spécifique Management Client pour les utilisateurs qui n'utiliseront jamais le Management Client.

Pour la meilleure expérience utilisateur possible des utilisateurs XProtect Smart Client ou des utilisateurs Management Client ayant un accès limité aux fonctionnalités Management Client, vous devez vous assurer que les autorisations fournies par le rôle et les éléments de l'interface utilisateur fournis par le profil Smart Client ou Management Client soient cohérentes.

> Pour avoir accès au Management Server, il est important que tous les rôles aient l'autorisation de sécurité **Connexion** activée. L'autorisation se trouve dans **Paramètres de rôle** > **Management Server** > Onglet Sécurité globale (rôles) on page 555.

Pour configurer les rôles dans votre système, développez le menu **Sécurité** > **Rôles**.

Autorisations d'un rôle

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Lorsque vous créez un rôle dans votre système, vous pouvez assigner ce rôle à un certain nombre d'autorisations concernant les 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 autorisations relatives aux fonctions d'accès dans XProtect Smart Client ou d'autres clients d'affichage Milestone, avec les autorisations nécessaires pour ne voir que certaines caméras. Si vous créez de tels rôles, ces rôles ne doivent pas avoir d'autorisations 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 répondre à ce besoin de différenciation, vous pouvez ensuite configurer un rôle disposant de certaines des autorisations d'administrateur les plus courantes, comme, par exemple, les autorisations pour ajouter ou supprimer des caméras, des serveurs et autres fonctions similaires. Vous pouvez créer des rôles qui disposent d'une partie ou de l'intégralité des autorisations d'un administrateur système. Par exemple, ceci peut s'avérer pertinent si votre institution souhaite faire la distinction entre les personnes pouvant gérer un sous-ensemble du système et les personnes qui peuvent gérer l'ensemble du système.

Les rôles vous offrent la possibilité de fournir des autorisations d'administrateur différenciées pour accéder, modifier ou modifier un grand nombre de fonctions système. Par exemple, l'autorisation de modifier les paramètres des serveurs ou des caméras de votre système. Vous précisez ces autorisations dans l'onglet **Sécurité générale** (voir Onglet Sécurité globale (rôles) on page 555). 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.

> Pour avoir accès au Management Server, il est important que tous les rôles aient l'autorisation de sécurité **Connexion** activée. L'autorisation se trouve dans **Paramètres de rôle** > **Management Server** > Onglet Sécurité globale (rôles) on page 555.

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 Profils Management Client (explications) on page 82 pour plus d'informations.

Pour doter un rôle de telles autorisations d'administrateur différenciées, la personne détentrice du rôle d'administrateur complet par défaut doit installer le rôle **Sécurité** > **Rôles > onglet Infos > 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 plus d'informations, voir Ajouter et gérer un rôle on page 309.

Lorsque vous avez spécifié les profils à associer au rôle, accédez à l'onglet **Sécurité globale** pour spécifier les autorisations du rôle.

> Les autorisations que vous pouvez définir pour un rôle sont différentes entre vos produits. Vous ne pouvez accorder toutes les autorisations disponibles à un rôle que dans XProtect Corporate.

Masquage de confidentialité (explications)

Masquage de confidentialité (explications)

Avec le masquage de confidentialité, vous pouvez définir les zones de la vidéo d'une caméra que vous souhaitez couvrir avec les masques de confidentialité lorsqu'elles s'affichent dans les clients. Par exemple, si une caméra de surveillance filme une rue, vous pouvez couvrir certaines zones d'un bâtiment (peut-être les fenêtres et les portes) à l'aide du masque de confidentialité pour protéger la confidentialité des résidents. Dans certains pays, il s'agit d'une exigence légale.

Vous pouvez indiquer les masques de confidentialité comme étant pleins ou flous. Les masques aussi bien la vidéo enregistrée, en direct que la vidéo exportée.

Les masques de confidentialité s'appliquent et sont verrouillés sur une zone de l'image de la caméra, donc la zone convertie ne suit pas les mouvements pan-til-zoom, mais couvre constamment la même zone de l'image de la caméra. Sur certaines caméras PTZ, vous pouvez activer une position en fonction du masquage de confidentialité sur la caméra elle-même.

Il existe deux types de masques de confidentialité :

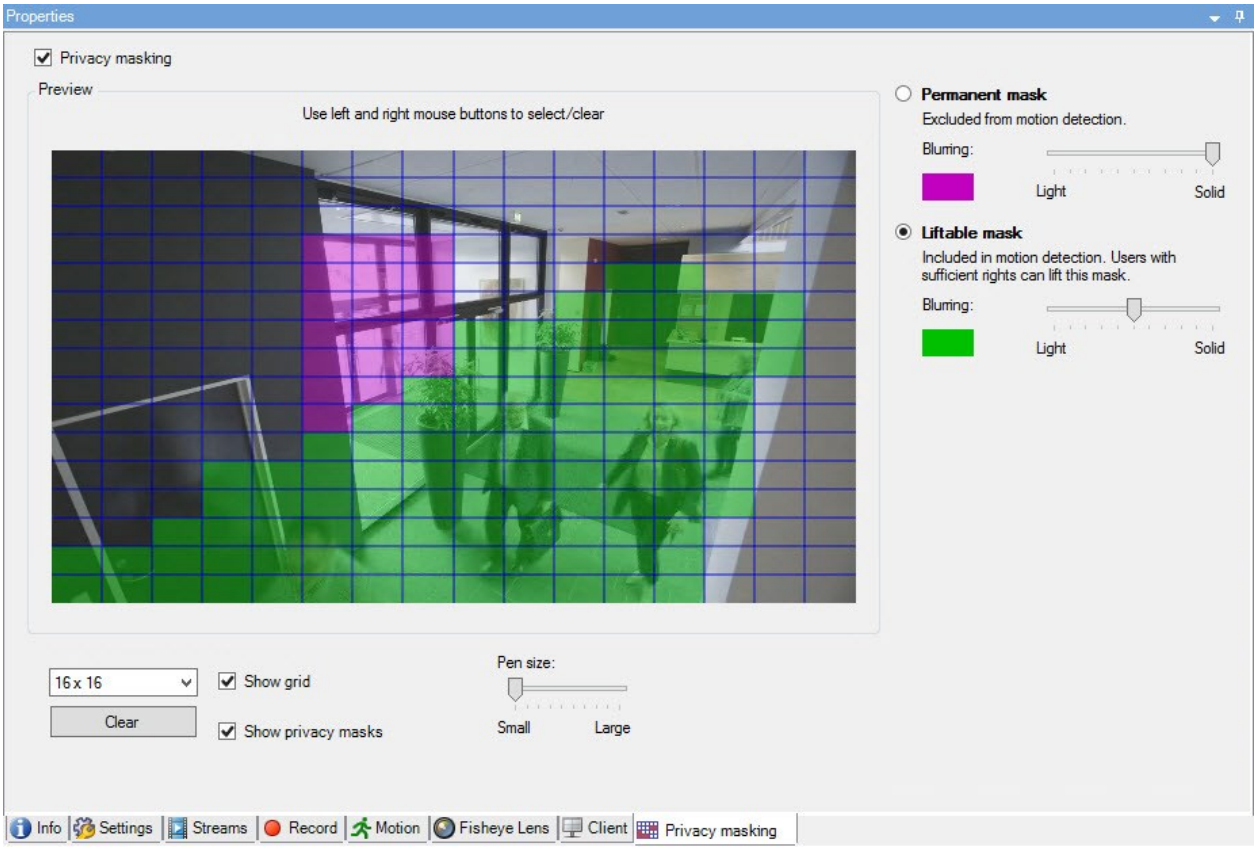
- **Masque de confidentialité permanent** : Les zones comportant ce type de maque sont toujours couvertes dans les clients. Peuvent servir à couvrir les zones de la vidéo qui ne requièrent jamais de surveillance, comme les zones publiques ou les zones où la surveillance n'est pas autorisée. La détection du mouvement est exclue des zones comprenant des masques de confidentialité permanents
- **Masque de confidentialité amovible** : La couverture des zones comprenant ce type de masque peut être temporairement suspendue dans XProtect Smart Client par les utilisateurs ayant l'autorisation de relever les masques de confidentialité. Si l'utilisateur de XProtect Smart Client connecté n'est pas autorisé à lever les masques de confidentialité, le système demandera un utilisateur autorisé pour approuver le levage.
  Les masques de confidentialité sont levés jusqu'à un délai d'expiration ou jusqu'à ce que l'utilisateur les applique à nouveau. N'oubliez pas que les masques de confidentialité sont relevés de toutes les caméras auxquelles l'utilisateur a accès

Si vous effectuez une mise à niveau à partir d'un système 2017 R3 ou plus ancien où des masques de confidentialité sont utilisés, les masques seront convertis en masques relevables.

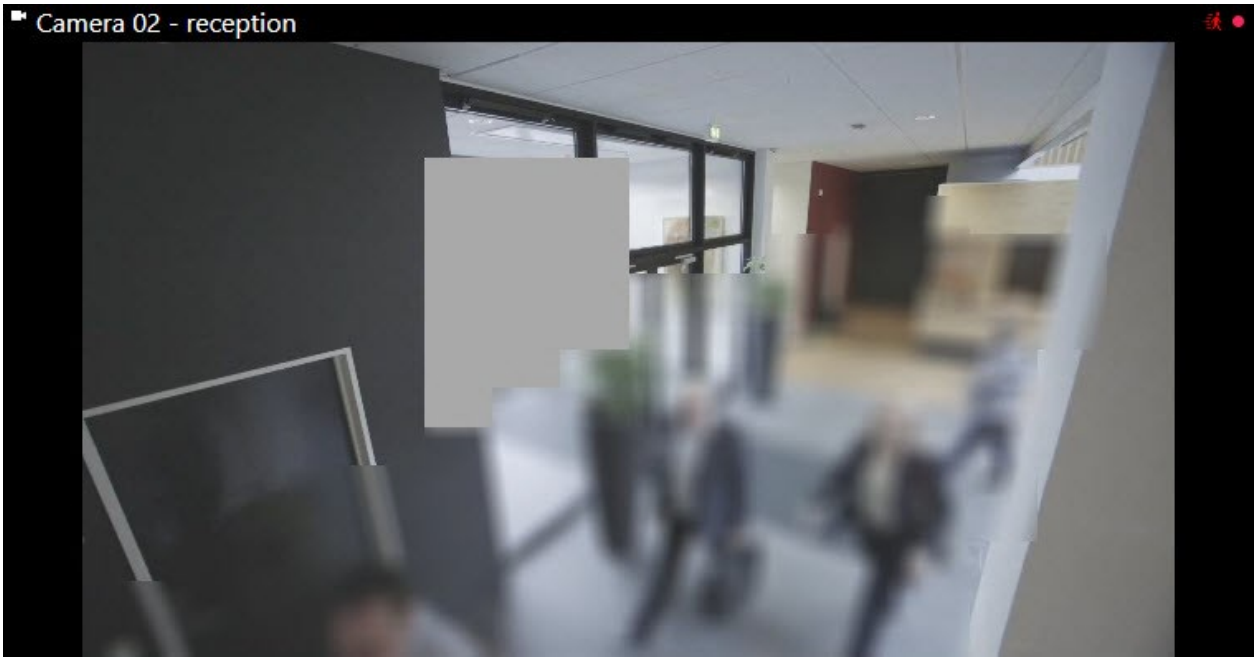
Lorsqu'un utilisateur exporte ou lit une vidéo enregistrée à partir d'un client, la vidéo comprend les masques de confidentialité configurés au moment de l'enregistrement même si vous avez modifié ou supprimé les masques de confidentialité par la suite. Si la protection de confidentialité est levée lors de l'exportation, la vidéo exportée **n'inclura pas** les masques de confidentialité relevables.

Si vous modifiez les paramètres de masquage de confidentialité très souvent, par exemple, une fois par semaine, votre système peut éventuellement être surchargé.

Exemple d'onglet de **masquage de confidentialité** avec configuration des masques de confidentialité :



Et voici comment ils s'affichent dans les clients :



Vous pouvez informer les utilisateurs du client des paramètres de masques de confidentialité permanents et relevables.

Profils Management Client (explications)

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.

Les profils Management Client ne traitent que la représentation visuelle des fonctions du système, et non l'accès à celles-ci. L'accès global aux fonctions du système est donné via le rôle auquel sont associés les utilisateurs individuels. Pour plus d'informations sur la gestion de l'accès global d'un rôle aux fonctions du système, voir Gérer la visibilité des fonctions pour un profil Management Client.

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.

Profils Smart Client (explications)

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Tous les utilisateurs de Milestone XProtect VMS appartiennent à un rôle auquel un profil Smart Client est connecté.

Les rôles définissent les autorisations des utilisateurs et les profils Smart Client définissent ce que les utilisateurs peuvent voir dans l'interface utilisateur XProtect Smart Client.

Toutes les installations Milestone XProtect VMS incluent un profil Smart Client par défaut qui est configuré avec une configuration par défaut pour afficher la majorité de la configuration disponible dans le système de votre organisation. Certains paramètres sont toujours désactivés par défaut.

Dans les cas où vous avez différents rôles dans une organisation, vous pouvez désactiver les fonctionnalités auxquelles un rôle particulier n'a pas/ne devrait pas avoir accès dans XProtect Smart Client.

Vous pouvez, par exemple, avoir un rôle dont le travail quotidien ne nécessite aucune lecture de vidéo. À cette fin, vous pouvez créer un nouveau profil Smart Client pour ce rôle pour lequel vous désactivez le mode **Lecture**. Lorsque vous désactivez ce paramètre dans le profil Smart Client, les utilisateurs XProtect Smart Client dont le rôle utilise ce Smart Client ne peuvent plus voir le mode **Lecture** dans leur interface utilisateur XProtect Smart Client.

Il est important de noter que les profils Smart Client contrôlent principalement ce que les utilisateurs peuvent voir dans l'interface utilisateur XProtect Smart Client et non les autorisations d'accès réelles du rôle. Ces autorisations d'accès, comme l'accès à la lecture, à la modification ou à la suppression, sont contrôlées par les paramètres de rôle. Les utilisateurs XProtect Smart Client peuvent donc avoir des autorisations sur les fonctionnalités via leur rôle qu'ils ne peuvent pas voir dans l'interface utilisateur, car il est désactivé dans le profil Smart Client.

Pour la meilleure expérience utilisateur possible des utilisateurs XProtect Smart Client, vous devez vous assurer que les autorisations fournies par le rôle et les éléments de l'interface utilisateur fournis par le profil Smart Client.

Pour créer ou modifier des profils Smart Client, développez **Client** et 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, ainsi que sur la manière de les utiliser ensemble (voir Créer et configurer des profils Smart Client, rôles et profils de temps on page 285).

Protection des preuves (explications)

> Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

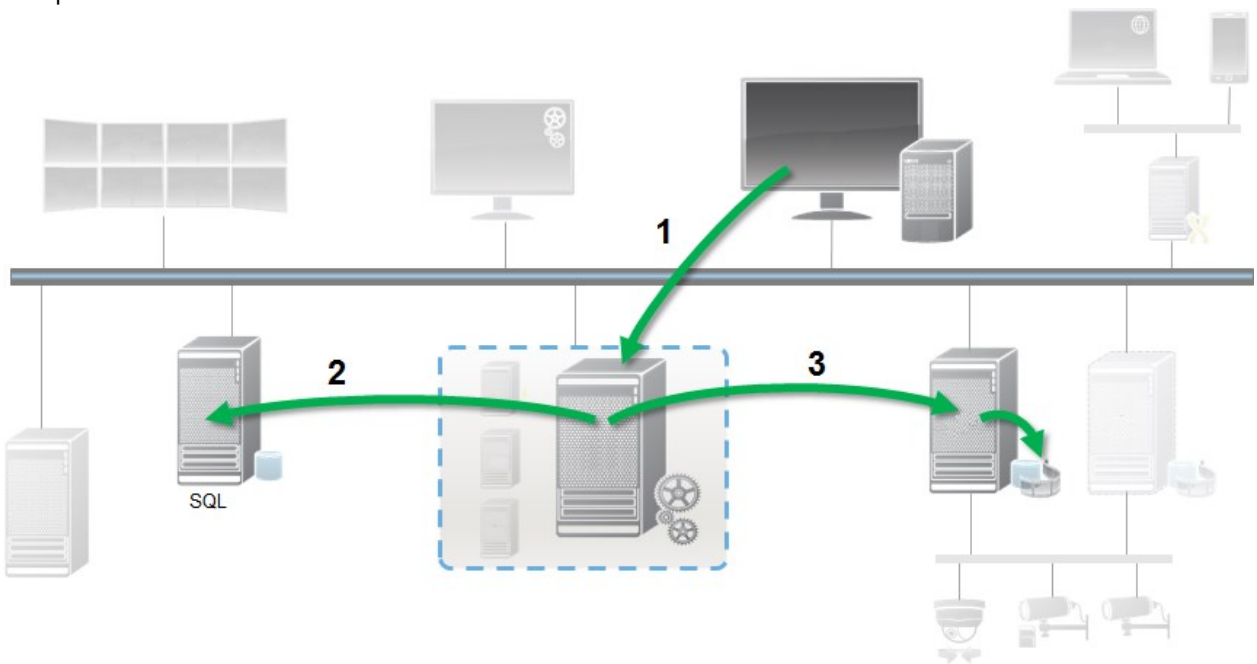
À partir de la version 2020 R2 du VMS XProtect, lorsque vous mettez à niveau le serveur de gestion vers une version plus récente, celui-ci ne pourra plus créer ou modifier la protection des preuves associées aux serveurs d'enregistrement de la version 2020 R1 ou une version antérieure, jusqu'à leur mise à niveau.
En d'autres termes, si le matériel a été déplacé d'un serveur d'enregistrement (à partir de la version 2020 R1 ou une version plus récente) vers un autre serveur d'enregistrement, et qu'il a toujours des enregistrements, il sera impossible de créer ou modifier les protections de preuves.

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, voir le manuel de l'utilisateur pour 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 autorisations utilisateur suffisantes ne déverrouille pas la protection de la preuve.

Organigramme pour la protection des preuves :

Composants



1. Un utilisateur XProtect Smart Client crée une protection des preuves. Des informations sont envoyées au serveur de gestion.
2. Management Server stocke les informations au sujet de la protection des preuves sur la base de données SQL Server.
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 dans le Management Client, vous pouvez voir lorsque un utilisateur crée, modifie ou supprime la protection des preuves.

Lorsqu'un disque est à court d'espace libre, cela n'affecte aucunement les données protégées. Au contraire, les anciennes données non-protégées seront 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 un matériel (voir Déplacer du matériel on page 367) vers un autre serveur d'enregistrement :

- Les enregistrements protégées par la protection des preuves seront conservées dans l'ancien serveur d'enregistrement selon une durée de rétention définie au préalable lors de la création de la protection des preuves.
- L'utilisateur XProtect Smart Client peut continuer de 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 par défaut un profil de protection des preuves qui leur est assigné, mais pas d'autorisations d'accès utilisateur à cette fonctionnalité. Pour spécifier les autorisations d'accès à la protection des preuves d'un rôle, reportez-vous à l'onglet Périphérique (rôles) pour les paramètres des rôles. Pour indiquer le profil de protection des preuves d'un rôle, voir l'onglet Info (rôles) 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.

Règles et événements

Règles (explications)

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.

> 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.

Complexité des règles

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, Caméra 1 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	Lorsqu'un mouvement est détecté (condition d'événement) sur la caméra 1, que

Exemple	Explication
durée, les événements et les périphériques	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 signifie que vous avez plus de règles dans votre système, cela offre un moyen simple de conserver un aperçu des actions de vos règles. Le fait de ne pas compliquer les règles veut également dire que vous avez plus de flexibilité lorsqu'il s'agit de désactiver/activer des éléments de règle individuels. Avec des règles simples, vous pouvez désactiver/activer des règles complètes le cas échéant.

Règles et événements (explications)

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.

Ces 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 ou que le système reçoit une entrée de détecteurs externes.
Intervalle de temps	Lorsque vous entrez des durées spécifiques, par exemple : `Thursday 16th August 2007 from 07.00 to 07.59` ou `every Saturday and Sunday`
Intervalle du temps de basculement	Période de temps au cours de laquelle le basculement est activé ou désactivé.
Temps récurrent	Lorsque vous configurez une action pour qu'elle soit exécutée sur un calendrier détaillé et périodique. Par exemple : • Chaque semaine, le mardi, à chaque heure entre 15h00 et 15h30 • Le 15 du mois tous les 3 mois à 11h45 • Chaque jour, chaque heure entre 15h00 et 19h00 L'heure est configurée en fonction des paramètres de l'heure locale du serveur sur lequel Management Client est installé.

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 d'analyse 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 dévénements XProtect en envoyant des chaînes simples via le réseau IP à votre système.

Profils de temps (explications)

> Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

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 joint n'ont aucune limite de temps sur leurs autorisations utilisateur 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. Beaucoup d'utilisateur peuvent maîtriser les concepts des périodes de temps uniques et récurrentes des applications du calendrier, comme celle dans Outlook de Microsoft®.

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 8h30 à 9h30, toutes les actions associées à un serveur d'enregistrement à New York sont exécutées entre 8h30 et 9h30 heure de New York, tandis que les mêmes actions sur un serveur placé à Los Angeles ont lieu plus tard, lorsqu'il est entre 8h30 et 9h30 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. Exemple seulement :

Pour voir une alternative aux profils de temps, reportez-vous aux Profils de temps journaliers (explications).

Profils de temps journalier (explications)

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 durée du jour en lieu et place afin de définir le lever et le coucher de soleil dans une zone géographique spécifique. Au travers des coordonnées géographiques, 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 durée du jour quand vous créez des règles, mais également des rôles.

Profils de notification (explications)

Les profils de notification permettent de configurer les notifications par e-mail préétablies. Les notifications peuvent être automatiquement déclenchées par une règle, par exemple lorsqu'un événement particulier se produit.

Lorsque vous créez le profil de notification, vous spécifiez le texte du message et décidez si vous souhaitez inclure des images et des vidéos AVI dans les notifications par e-mail.

> ⚠ Vous devrez peut-être désactiver tous les logiciels d'analyse de messagerie qui peuvent bloquer l'envoi des notifications par e-mail par l'application.

Conditions préalables à la création des profils de notification

Avant de pouvoir créer des profils de notification, vous devez préciser les paramètres du serveur de messagerie pour les notifications par e-mail.

Vous pouvez sécuriser la communication vers le serveur de messagerie, si vous installez les certificats de sécurité nécessaires dans le serveur de messagerie.

Si vous souhaitez que les notifications par e-mail soient en mesure de contenir des séquences vidéo au format AVI, vous devez tout d'abord préciser les paramètres de compression :

1. Rendez-vous sur **Outils** > **Options**. Cela ouvre la fenêtre **Options**.
2. Configurez le serveur de messagerie dans l'onglet **Serveur de messagerie** (Onglet Serveur de messagerie (options) on page 420) et les paramètres de compression dans l'onglet **Génération AVI** Onglet Génération AVI (options) on page 421.

Événements définis par l'utilisateur (explications)

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.
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	Description
	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.

Événements analytiques (explications)

Les événements d'analyse sont généralement des données reçues de la part d'un fournisseur d'analyse de contenu vidéo (VCA) tiers externe.

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 expliqué dans la Documentation de MIP SDK sur des événements analytiques.

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.

Événements génériques (explications)

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**.

Webhooks (expliqués)

Les webhooks sont des requêtes HTTP qui permettent aux applications Web de communiquer entre elles et facilitent l'envoi de données en temps réel d'une application à une autre lorsqu'un événement prédéfini se produit, par exemple l'envoi de données d'événement à un point de terminaison webhook prédéfini lorsqu'un utilisateur se connecte au système ou lorsqu'une caméra signale une erreur.

Un point de terminaison webhook (webhook URL) est l'adresse prédéfinie à laquelle les données d'événement doivent être envoyées, un peu comme un numéro de téléphone unidirectionnel.

Vous pouvez utiliser des webhooks pour créer des intégrations qui s'abonnent à des événements sélectionnés dans XProtect. Lorsqu'un événement est déclenché, un POST HTTP est envoyé au point de terminaison webhook que vous avez défini pour cet événement. Le corps POST HTTP contient des données d'événement au format JSON.

Les webhooks n'interrogent pas le système à la recherche de données ou d'événements déclenchés ; au lieu de cela, le système transmet les données d'événement au point de terminaison du webhook lorsqu'un événement se produit, ce qui rend les webhooks moins gourmands en ressources et plus rapides à configurer par rapport aux solutions d'interrogation.

Les webhooks peuvent être configurés pour s'intégrer avec ou sans scripts.

> Vous devez vérifier que les données d'événement envoyées par XProtect sont conformes à la législation existante sur la protection des données et de la vie privée de votre pays.

La fonctionnalité Webhooks est installée par défaut et prête à être utilisée sur XProtect 2023R1 ou version ultérieure et affiche l'action **Webhooks** dans l'onglet **Règles** dans Management Client.

Alarmes

Alarmes (explications)

> Cette fonctionnalité ne prend effet que si vous avez installé le XProtect Event Server.

Cet article décrit comment configurer des alarmes pour qu'elles apparaissent dans le système, déclenchées par des événements.

Basée sur les fonctions gérées par un serveur d'événements, la fonction des alarmes offre la visualisation centralisée, 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**

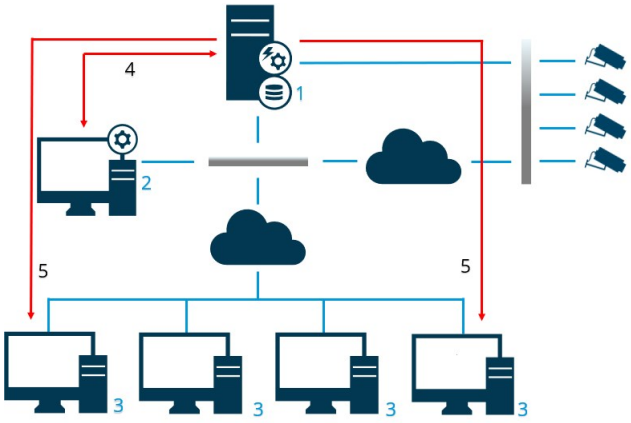
  Ce groupe se compose de plusieurs types d'événements externes :

  - **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 MIP SDK, un vendeur tiers peut développer des modules d'extension personnalisés (par exemple, l'intégration à des systèmes de contrôle d'accès externes ou 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 smart map et de plan de XProtect Smart Client.

Configuration de l'alarme

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	Cette autorisation 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 autorisations des utilisateurs relatives 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 **Alarmes et événements** vous permet de spécifier dans **Options** les paramètres des alarmes, des événements et des journaux.

Smart Map

Smart map (explications)

Dans la XProtect® Smart Client et dans la XProtect Mobile, la fonctionnalité de smart map vous permet de visualiser et d'accéder à des périphériques situés dans différentes localisations à travers le monde, et ce de manière géographiquement correcte. Contrairement aux plans avec lesquels vous avez un plan différent pour chaque emplacement, la smart map vous donne une vue d'ensemble dans une seule vue.

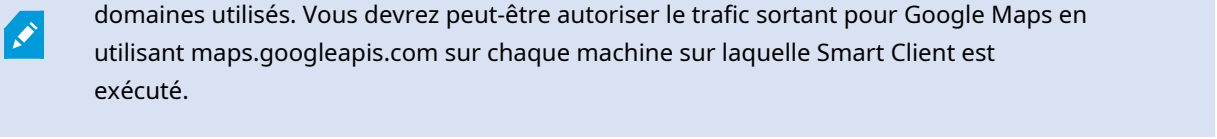
La configuration suivante des fonctionnalités de smart map se fait dans Management Client :

- Configurer l'arrière-plan géographique choisi pour votre smart map. Cette option inclut l'intégration de votre smart map à l'un des services suivants :
  - Bing Maps
  - Google Maps
  - Milestone Map Service
  - OpenStreetMap
- Activer Bing Maps ou Google Maps dans XProtect Management Client ou dans XProtect Smart Client
- Activer l'édition des smart map, y compris les périphériques, dans XProtect Smart Client
- Positionne géographiquement vos périphériques dans XProtect Management Client
- Configurer votre smart map avec Milestone Federated Architecture

Intégration de smart map avec Google Maps (explications)

Pour intégrer Google Maps à votre smart map, vous avez besoin d'une clé API Maps Static de Google. Pour obtenir une clé API, vous devez d'abord créer un compte de facturation Google Cloud. Vous serez facturé selon le volume du chargement des plans par mois.

Une fois que vous avez la clé API, vous devez l'entrer dans le XProtect Management Client. Voir également Activer Bing Maps ou Google Maps dans Management Client on page 345.



Si vous êtes protégé par un pare-feu restrictif, il est important d'autoriser l'accès aux domaines utilisés. Vous devrez peut-être autoriser le trafic sortant pour Google Maps en utilisant maps.googleapis.com sur chaque machine sur laquelle Smart Client est exécuté.

Pour plus d'informations, voir :

- Google Maps Platform - démarrer : https://cloud.google.com/maps-platform/
- Guide de la plate-forme de facturation Google Maps Platform :https://developers.google.com/maps/billing/gmp-billing
- Guide du développeur de Maps Static API :https://developers.google.com/maps/documentation/maps-static/dev-guide

Ajouter une signature numérique à la clé Maps Static API

Si vous vous attendez à ce que les opérateurs XProtect Smart Client fassent plus de 25 000 demandes de plan par jour, vous avez besoin d'une signature numérique pour votre clé Maps Static API. La signature numérique permet aux serveurs de Google de vérifier qu'un site générant des demandes avec votre clé API soit autorisé à le faire. Cependant, quelles que soient les exigences d'utilisation, Google recommande d'utiliser une signature numérique comme filtre de sécurité supplémentaire. Vous devez récupérer une signature secrète d'URL pour obtenir une signature numérique. Pour plus d'informations, voir https://developers.google.com/maps/documentation/maps-static/get-api-key#dig-sig-manual.

Intégration de smart map avec Bing Maps (explications)

Pour intégrer Bing Maps à votre smart map, vous avez besoin d'une clé basique ou d'une clé d'entreprise. La différence repose sur le fait que les clés basiques sont gratuites, mais fournissent un nombre limité de transactions avant que les transactions deviennent facturables ou que l'accès au service de plan soit refusé. La clé d'entreprise n'est pas gratuite, mais permet un nombre illimité de transactions.

Pour plus d'informations sur Bing Maps, voir https://www.microsoft.com/en-us/maps/licensing/.

Une fois que vous avez la clé API, vous devez l'entrer dans le XProtect Management Client. Voir Activer Bing Maps ou Google Maps dans Management Client on page 345.

Si vous êtes protégé par un pare-feu restrictif, il est important d'autoriser l'accès aux domaines utilisés. Vous devrez peut-être autoriser le trafic sortant pour les cartes Bing en utilisant *.virtualearth.net sur chaque machine sur laquelle Smart Client est exécuté.

Fichiers smart map en cache supprimés (explications)

Si vous utilisez Google Maps en tant qu'arrière-plan géographique, les fichiers ne sont pas mis en cache.

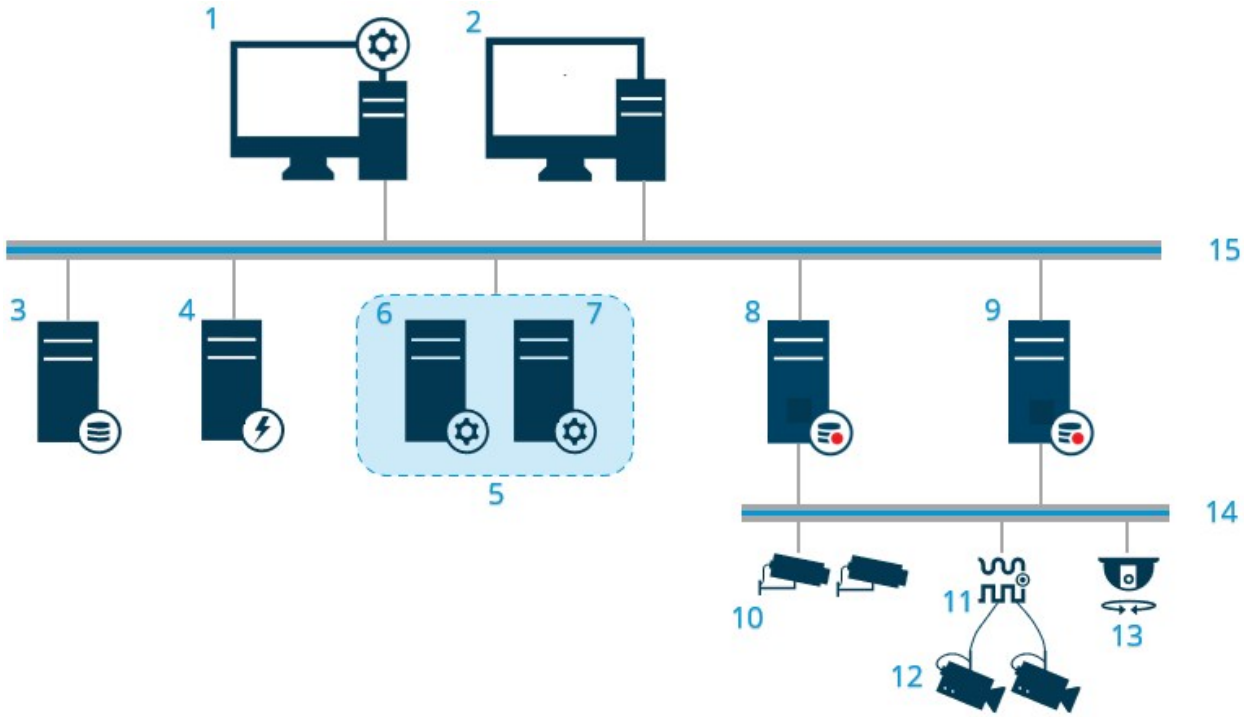
Les fichiers que vous utilisez pour votre arrière-plan géographique sont récupérés à partir d'un serveur de tuile. La durée de conservation des fichiers dans le répertoire de cache dépend des valeurs sélectionnées dans la liste **Fichiers Smart Map en cache supprimés** de la boîte de dialogue **Paramètres** dans XProtect Smart Client. Les fichiers sont stockés :

- Soit indéfiniment (**Jamais**)
- Soit pendant 30 jours si le fichier n'est pas utilisé (**Si inutilisé pendant 30 jours**)
- Lorsque l'opérateur quitte XProtect Smart Client (**À la sortie**)

Lorsque vous modifiez l'adresse du serveur de tuile, un nouveau répertoire de cache est automatiquement créé. Les fichiers des plans précédents sont conservés dans le répertoire de cache correspondant sur votre ordinateur local.

Architecture

Une configuration distribuée du système



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

Tous les ordinateurs d'une configuration distribuée doivent être dans un domaine ou dans un groupe de travail.

Légende :

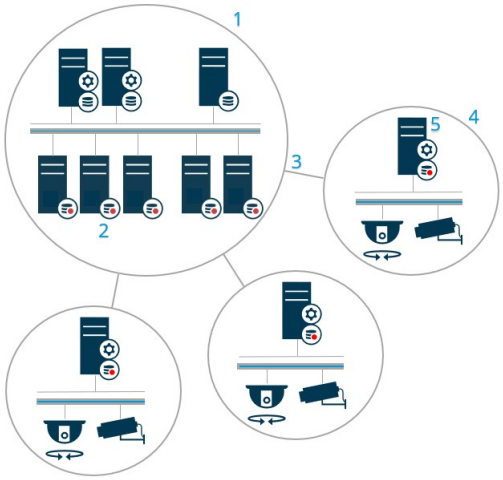
1. Management Client(s)
2. XProtect Smart Client(s)
3. Serveur avec SQL Server
4. Serveur d'événements
5. Cluster Microsoft
6. Serveur de gestion
7. Serveur de gestion de basculement
8. Serveur d'enregistrement de basculement
9. Serveur(s) d'enregistrement
10. Caméras vidéo IP
11. Encodeur vidéo
12.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

Milestone Interconnect (explications)

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Milestone Interconnect™ vous permet d'intégrer un nombre d'installations plus petites, physiquement fragmentées et des installations XProtect distantes avec un 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.

L'illustration suivante vous montre comment configurer Milestone Interconnect sur votre système :



1. Site Milestone Interconnect central XProtect Corporate
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 à distance par le biais de l'assistant **Ajouter du 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)

Vous ajoutez des sites distants à votre 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 on page 340).

Chaque site distant fonctionne indépendamment et peut effectuer n'importe quelle tâche de surveillance normale. Selon les connexions réseau et les autorisations utilisateur appropriées (voir Affecter des autorisations utilisateur on page 341), Milestone Interconnect vous offre la possibilité de visualiser en direct les caméras des sites distants et de lire les 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 on page 343).

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 informations sur la façon dont des produits XProtect spécifiques communiquent dans une configuration Milestone Interconnect, rendez-vous sur le site Web Milestone Interconnect (https://www.milestonesys.com/products/expand-your-solution/milestone-extensions/interconnect/).

Sélectionner Milestone Interconnect ou Milestone Federated Architecture (explications)

Dans un système à distribution physique où les utilisateurs d'un site central doivent pouvoir accéder à la vidéo 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 centraux et fédérés est stable
- Le réseau utilise le même domaine
- Il y a très peu de sites importants
- La bande passante est suffisante pour l'utilisation requise

Milestone recommande Milestone Interconnect lorsque :

- La connexion réseau entre les sites centraux et distants est instable
- Vous ou votre institution 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 taille

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. Le nombre de licences de caméra Milestone Interconnect requises dépend de l'activité de streaming sur les sites à distance dont vous souhaitez récupérer les données. Il ne peut pas y avoir plus d'une licence par flux. 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** du site central.

Configurations Milestone Interconnect (explications)

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. Cela nécessite l'utilisation de l'option **Lire les enregistrements à partir du système à distance** (voir Activer la lecture directe à partir de la caméra du site distant on page 341).

Récupération 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 limitations affectant le réseau. Vous pouvez configurer les paramètres de récupération d'enregistrements à distance sur l'onglet **Récupération à distance** (voir Onglet Rappel à distance on page 467).

La récupération des enregistrements à distance peut être déclenchée 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 une récupération automatique ou une demande de récupération à partir du XProtect Smart Client en-dehors de l'intervalle de temps que vous avez spécifié dans l'onglet **Récupération à distance**, elle est acceptée, mais n'est pas commencée 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 récupérés par défaut à partir des sites distants

Utilise des sites distants comme un serveur d'enregistrement utilise le stockage de bord 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 aux 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 **Récupérer automatiquement les enregistrements à distance lorsque la connexion est rétablie** (voir Rappeler les enregistrements à distance de la caméra du site distant on page 342) 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 institution.

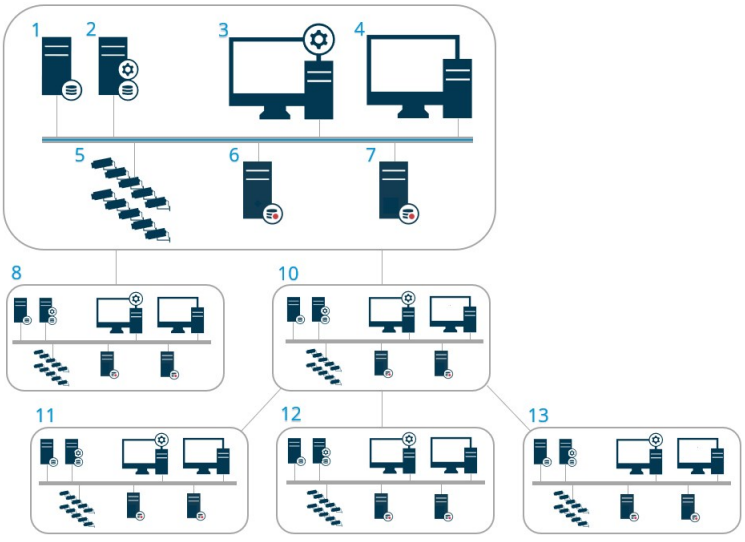
Configuration de Milestone Federated Architecture

XProtect Expert ne peuvent être 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 client disposant d'autorisations suffisantes peuvent accéder directement à la vidéo, l'audio et à d'autres ressources via les sites individuels. Les administrateurs peuvent gérer de façon centralisée tous les sites de la version 2018 R1 et plus récente dans la hiérarchie fédérée, en fonction des autorisations administrateur pour les sites individuels.

Les utilisateurs basiques ne sont pas pris en charge dans les systèmes Milestone Federated Architecture, vous devez donc ajouter les utilisateurs en tant qu'utilisateurs Windows via le service Active Directory.

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 on page 334). 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 on page 336). 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.



Composants d'une configuration Milestone Federated Architecture :

1. Serveur avec SQL Server
2. Serveur de gestion
3. Management Client

4. XProtect Smart Client
5. Caméras
6. Serveur d’enregistrement
7. Serveur d’enregistrement de basculement
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 par l’administrateur système. 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 exigences produits et système

- L’ouverture de Management Client dans un Milestone Federated Architecture est prise en charge par trois grands lancements, dont celui-ci. Pour les autres configurations de Milestone Federated Architecture, vous avez besoin d’un Management Client distinct qui soit compatible avec la version du serveur.
- Si le site central utilise XProtect Smart Wall, vous pouvez également utiliser les fonctionnalités XProtect Smart Wall dans la hiérarchie des sites fédérés.
- Si le site central utilise XProtect Access et qu’un utilisateur XProtect Smart Client se connecte à un site dans une hiérarchie des sites fédérés, les notifications de demande d’accès envoyées par les sites fédérés apparaissent également dans XProtect Smart Client
- Vous pouvez ajouter des systèmes XProtect Expert 2013 (ou des versions plus récentes) à la hiérarchie des sites fédérés en tant que sites enfants, et non en tant que sites parents
- Milestone Federated Architecture ne nécessite aucune licence supplémentaire
- Pour plus d’informations sur les applications et les avantages de ce système, voir le livre blanc sur Milestone Federated Architecture.

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 fédére en tant que système autonome normal avec des composants système, des paramètres, des règles, des calendriers, des administrateurs, des utilisateurs et des autorisations utilisateur standard. 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.

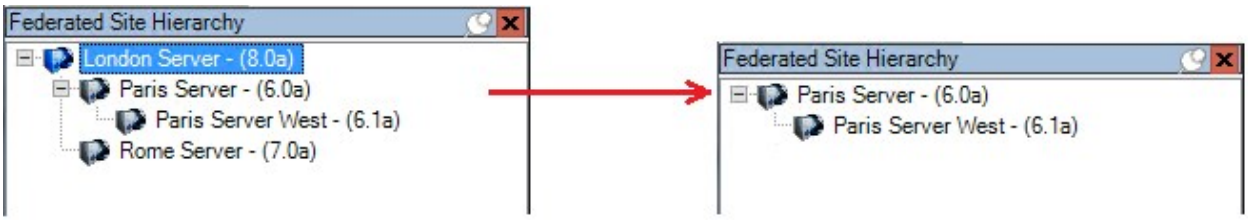
Une fois les sites individuels installés, vous devez les configurer afin qu'ils fonctionnent en tant que sites fédérés (voir Configurer votre système pour exécuter des sites fédérés on page 334).

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 on page 336) 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 des sites fédérés, 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 autorisations 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.

Vous trouverez ci-dessous un exemple de site fédéré dans le Management Client. À gauche, l'utilisateur s'est connecté au premier site. À droite, l'utilisateur s'est connecté à l'un des sites enfants, le serveur de Paris, qui est donc le site d'accueil.



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 pas encore opérationnel.	

Ports utilisés par le système

Tous les composants XProtect et les ports qu'ils requièrent sont répertoriés ci-dessous. Par exemple, pour vous assurer que le pare-feu bloque uniquement le trafic indésirable, vous devez spécifier les ports utilisés par le système. Vous devriez activer uniquement ces ports. Les listes incluent également les ports utilisés par les processus locaux.

Ceux-ci sont classés en deux groupes :

- Les **Composants du serveur** (services) offrent leur service sur des ports particulier. C'est pourquoi ils doivent rester à l'écoute des demandes du client sur ces ports. Ainsi, ces ports doivent être ouverts dans le pare-feu Windows pour les connexions entrantes et sortantes
- Les **Composants du client** (clients) initient les connexions vers des ports particuliers sur les composants du serveur. Ainsi, ces ports doivent être ouverts pour les connexions sortantes. Les connexions sortantes sont généralement ouvertes par défaut dans le pare-feu Windows

Si rien d'autre n'est mentionné, les ports des composants du serveur doivent être ouverts pour les connexions entrantes et les ports des composants du client doivent être ouverts pour les connexions sortantes.

N'oubliez pas que les composants du serveur peuvent également agir en tant que clients pour d'autres composants du serveur. Le présent document n'énumèrent pas explicitement ces derniers.

Les numéros de port sont les numéros par défaut, mais ceux-ci peuvent être modifiés. Contactez l'assistance Milestone si vous avez besoin de modifier des ports ne pouvant pas être configurés par le biais du Management Client.

Composants du serveur (connexions entrantes)

Chacune des rubriques suivantes affiche les ports qui doivent être ouverts pour un service particulier. Afin de savoir quels ports doivent être ouverts sur un ordinateur particulier, vous devez prendre en compte tous les services exécutés sur cet ordinateur.

Service Management Server et processus connexes

Numéro de port	Protocole	Processus	Connexions de...	Objectif
80	HTTP	IIS	Tous les serveurs et le XProtect Smart Client et le Management Client	L'objectif des ports 80 et 443 est le même. Cependant, le port utilisé par le VMS dépendra de si vous avez utilisé des certificats pour sécuriser la communication. • Lorsque vous n'avez pas sécurisé la communication avec des certificats, le VMS utilise le port 80. • Lorsque vous avez sécurisé la communication avec les certificats, le VMS utilise le port 443, sauf dans le cadre de la communication entre le serveur d'événements et le serveur de gestion. La communication entre le serveur d'événements et le serveur de gestion utilise le cadre sécurisé Windows (WCF) et l'authentification Windows sur le port 80.
443	HTTPS	IIS		
445	TCP	Service Management Server	Management Server Manager.	Permettre aux utilisateurs Windows Active Directory d'être ajoutés aux rôles.

Numéro de port	Protocole	Processus	Connexions de...	Objectif
6473	TCP	Service Management Server	Icône de la barre d'état Management Server Manager, connexion locale uniquement.	Affichage de l'état et gestion du service.
8080	TCP	Serveur de gestion	Connexion locale uniquement.	La communication entre les processus internes du serveur.
9000	HTTP	Serveur de gestion	Services Recording Server	Service Web pour une communication interne entre les serveurs.
12345	TCP	Service Management Server	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.
12974	TCP	Service Management Server	Service SNMP Windows	Communication avec l'agent d'extension SNMP. N'utilisez pas le port à d'autres fins, même si votre système n'applique pas SNMP. Dans les systèmes XProtect 2014 ou plus anciens, le numéro de port était 6475. Dans les système XProtect 2019 R2 et plus anciens, le numéro de port était 7475.

SQL ServerService

Numéro de port	Protocole	Processus	Connexions de...	Objectif
1433	TCP	SQL Server	Service Management Server	Enregistrement et récupération des configurations via le Identity Provider.
1433	TCP	SQL Server	Service Event Server	Enregistrement et récupération des événements via le Identity Provider.
1433	TCP	SQL Server	Service Log Server	Enregistrement et récupération des entrées de journal via le Identity Provider.

Data CollectorService

Numéro de port	Protocole	Processus	Connexions de...	Objectif
7609	HTTP	IIS	Sur l'ordinateur du serveur de gestion : Services Data Collector sur tous les autres serveurs. Sur d'autres ordinateurs : Service Data Collector sur le serveur de gestion.	Moniteur système.

Event ServerService

Numéro de port	Protocole	Processus	Connexions de...	Objectif
1234	TCP/UDP	Service Event	Tout serveur	Écouter des événements

Numéro de port	Protocole	Processus	Connexions de…	Objectif
		Server	envoyant des événements génériques à votre système XProtect.	génériques de systèmes ou de périphériques externes. Uniquement si la source de données pertinente est activée.
1235	TCP	Service Event Server	Tout serveur envoyant des événements génériques à votre système XProtect.	Écouter des événements génériques de systèmes ou de périphériques externes. Uniquement si la source de données pertinente est activée.
9090	TCP	Service Event Server	Tout système ou périphérique envoyant des événements analytiques à votre système XProtect.	Écouter les événements analytiques des systèmes ou des dispositifs externes. Pertinent uniquement si la fonction Événements analytiques est activée.
22331	TCP	Service Event Server	XProtect Smart Client et les Management Client	Configuration, événements, alarmes, et données de plan.
22332	WS/WSS HTTP/HTTPS*	Service Event Server	API Gateway et les Management Client	Abonnement aux événements/états, API REST des événements, API de messagerie Websockets et API REST des alarmes.
22333	TCP	Service Event Server	Modules d’extension et applications MIP.	Messagerie MIP.

***** Une erreur 403 sera renvoyée lors de l’accès à HTTP pour accéder à un point de terminaison HTTPS uniquement.

Recording ServerService

Numéro de port	Protocole	Processus	Connexions de...	Objectif
5210	TCP	Service Recording Server	Serveurs d'enregistrement de basculement.	Fusion des bases de données après l'exécution d'un serveur d'enregistrement de basculement.
7563	TCP	Service Recording Server	XProtect Smart Client, Management Client	Récupération des flux vidéo et audio, commandes PTZ.
8966	TCP	Service Recording Server	Icône de la barre d'état Recording Server Manager, connexion locale uniquement.	Affichage de l'état et gestion du service.
9001	HTTP	Service Recording Server	Serveur de gestion	Service Web pour une communication interne entre les serveurs. Si plusieurs instances du serveur d'enregistrement sont en cours d'utilisation, chaque instance doit avoir son propre port. Les ports supplémentaires seront 9002, 9003, etc.
11000	TCP	Service Recording Server	Serveurs d'enregistrement de basculement	Interrogation de l'état des serveurs d'enregistrement.
12975	TCP	Service Recording Server	Service SNMP Windows	Communication avec l'agent d'extension SNMP. N'utilisez pas le port à d'autres fins, même si votre système n'applique pas SNMP. Dans les systèmes XProtect

Numéro de port	Protocole	Processus	Connexions de...	Objectif
				2014 ou plus anciens, le numéro de port était 6474. Dans les système XProtect 2019 R2 et plus anciens, le numéro de port était 7474.
65101	UDP	Service Recording Server	Connexion locale uniquement	Écouter des notifications d'événements des pilotes.

Outre les connexions entrantes vers le service Recording Server susmentionné, le service Recording Server établit des connexions sortantes vers :

- Caméras
- Des NVR
- Des sites interconnectés à distance (Interconnect ICP Milestone)

Service Failover Server et service Failover Recording Server

Numéro de port	Protocole	Processus	Connexions de...	Objectif
5210	TCP	Service Failover Recording Server	Serveurs d'enregistrement de basculement	Fusion des bases de données après l'exécution d'un serveur d'enregistrement de basculement.
7474	TCP	Service Failover Recording	Service SNMP Windows	Communication avec l'agent d'extension SNMP.

Numéro de port	Protocole	Processus	Connexions de...	Objectif
		Server		N'utilisez pas le port à d'autres fins, même si votre système n'applique pas SNMP.
7563	TCP	Service Failover Recording Server	XProtect Smart Client	Récupération des flux vidéo et audio, commandes PTZ.
8844	UDP	Service Failover Recording Server	Communication entre services Failover Recording Server.	La communication entre les serveurs.
8966	TCP	Service Failover Recording Server	Icône de la barre d'état Failover Recording Server Manager, connexion locale uniquement.	Affichage de l'état et gestion du service.
8967	TCP	Service Failover Server	Icône de la barre d'état Failover Server Manager, connexion locale uniquement.	Affichage de l'état et gestion du service.
8990	HTTP	Service Failover Server	Service Management Server	Suivi de l'état du service Failover Server.
9001	HTTP	Service Failover Server	Serveur de gestion	Service Web pour une communication interne entre les serveurs.

Outre les connexions entrantes vers le service Failover Server/Failover Recording Server susmentionné, le service Failover Server/Failover Recording Server établit des connexions sortantes vers les autres enregistreurs et caméras et pour la vidéo push.

Log ServerService

Numéro de port	Protocole	Processus	Connexions de...	Objectif
22337	HTTP	Service Log Server	Tous les composants XProtect à l'exception du serveur d'enregistrement.	Écrire dans, lire et configurer le serveur de journaux.

Ce port utilise HTTP, mais la communication est cryptée avec la sécurité des messages qui utilise la spécification WS-Security pour sécuriser les messages. Pour plus d'informations, voir Sécurité des messages dans WCF.

Mobile ServerService

Numéro de port	Protocole	Processus	Connexions de...	Objectif
8000	TCP	Service Mobile Server	Icône de la barre d'état Mobile Server Manager, connexion locale uniquement.	Application SysTray.
8081	HTTP	Service Mobile Server	Clients mobiles, clients Web, et Management Client.	Envoi de flux de données, vidéo et audio.
8082	HTTPS	Service Mobile Server	Clients mobiles et clients Web.	Envoi de flux de données, vidéo et audio.
40001 - 40099	HTTP	Service Mobile Server	Service Recording Server	Mobile Server Vidéo Push. Cette plage de port est désactivée par défaut.

LPR ServerService

Numéro de port	Protocole	Processus	Connexions de...	Objectif
22334	TCP	Service LPR Server	Serveur d'événements	Récupération des plaques d'immatriculation reconnues et de l'état du serveur. Afin de se connecter, le module d'extension LPR doit être installé sur le serveur d'événements.
22334	TCP	Service LPR Server	Icône de la barre d'état LPR Server Manager, connexion locale uniquement.	Application SysTray

Milestone Open Network BridgeService

Numéro de port	Protocole	Processus	Connexions de...	Objectif
580	TCP	Service Milestone Open Network Bridge	Clients ONVIF	Authentification et requêtes de configuration du flux vidéo.
554	RTSP	Service RTSP	Clients ONVIF	Diffusion de vidéo demandée sur les clients ONVIF.

XProtect DLNA ServerService

Numéro de port	Protocole	Processus	Connexions de...	Objectif
9100	HTTP	Service DLNA Server	Périphérique DLNA	Découverte de périphérique et possibilité de configuration de canaux DLNA. Requêtes de flux vidéo.
9200	HTTP	Service DLNA Server	Périphérique DLNA	Diffusion de vidéo demandée sur les périphériques DLNA.

XProtect Screen RecorderService

Numéro de port	Protocole	Processus	Connexions de...	Objectif
52111	TCP	XProtect Screen Recorder	Service Recording Server	Fournit la vidéo à partir d'un moniteur. Il apparaît et agit de la même façon qu'une caméra sur le serveur d'enregistrement. En cas de besoin, vous pouvez modifier le numéro de port dans le Management Client.

Service XProtect Incident Manager

Numéro de port	Protocole	Processus	Connexions de...	Objectif
80	HTTP	IIS	XProtect Smart Client et les Management Client	L'objectif des ports 80 et 443 est le même. Cependant, le port utilisé par le VMS dépendra de si vous avez utilisé des certificats pour sécuriser la communication. • Lorsque vous n'avez pas sécurisé la communication avec des certificats, le VMS utilise le port 80. • Lorsque vous avez sécurisé la communication avec des certificats, le VMS utilise le port 443.
443	HTTPS	IIS		

Composants du serveur (connexions sortantes)

Management ServerService

Numéro de port	Protocole	Connexions à...	Objectif
443	HTTPS	Le serveur de licence qui héberge le service de gestion des licences. Communiquer via https://www.milestonesys.com/OnlineActivation/LicenseManagementService.asmx	Activation de licences.

Recording ServerService

Numéro de port	Protocole	Connexions à...	Objectif
80	HTTP	Caméras, NVR, encodeurs Sites interconnectés	Authentification, configuration, flux de données, vidéo et audio. Connexion
443	HTTPS	Caméras, NVR, encodeurs	Authentification, configuration, flux de données, vidéo et audio.
554	RTSP	Caméras, NVR, encodeurs	Flux de données, vidéo et audio.
7563	TCP	Sites interconnectés	Flux de données et événements.
11000	TCP	Serveurs d'enregistrement de basculement	Interrogation de l'état des serveurs d'enregistrement.
40001 – 40099	HTTP	Service Mobile Server	Vidéo push sur le serveur mobile. Cette plage de port est désactivée par défaut.

Service Failover Server et service Failover Recording Server

Numéro de port	Protocole	Connexions à...	Objectif
11000	TCP	Serveurs d'enregistrement de basculement	Interrogation de l'état des serveurs d'enregistrement.

Event ServerService

Numéro de port	Protocole	Connexions à...	Objectif
80	HTTP	API Gateway et les Management Server	Accéder à l'API de configuration à partir de API Gateway
443	HTTPS	API Gateway et les Management Server	Accéder à l'API de configuration à partir de API Gateway
443	HTTPS	Milestone Customer Dashboard par https://service.milestonesys.com/	Envoyer l'état, les événements et les messages d'erreur depuis le système XProtect vers Milestone Customer Dashboard.

Log ServerService

Numéro de port	Protocole	Connexions à...	Objectif
443	HTTP	Serveur de journaux	Transmettre les messages au serveur de journaux.

API Gateway

Numéro de port	Protocole	Connexions à...	Objectif
443	HTTPS	Management Server	API RESTful
22332	WS/WSS HTTP/HTTPS*	Management Client	Abonnement aux événements/états, API REST des événements, API de messagerie Websockets et API REST des alarmes.

Caméras, encodeurs et périphériques E/S (connexions entrantes)

Numéro de port	Protocole	Connexions de...	Objectif
80	TCP	Serveurs d'enregistrement et serveurs d'enregistrement de basculement	Authentification, configuration et flux de données, vidéo et audio.
443	HTTPS	Serveurs d'enregistrement et serveurs d'enregistrement de basculement	Authentification, configuration et flux de données, vidéo et audio.
554	RTSP	Serveurs d'enregistrement et serveurs d'enregistrement de basculement	Flux de données, vidéo et audio.

Caméras, encodeurs et périphériques E/S (connexions sortantes)

Numéro de port	Protocole	Connexions à...	Objectif
22337	HTTP	Serveur de journaux	Transmettre les messages au serveur de journaux.

Seuls quelques modèles de caméras sont capables d'établir des connexions sortantes.

Composants du client (connexions sortantes)

XProtect Smart Client, XProtect Management Client, serveur XProtect Mobile

Numéro de port	Protocole	Connexions à...	Objectif
80	HTTP	API Gateway et service Management Server	Authentication et autres API dans API Gateway.
443	HTTPS	API Gateway et service Management Server	Authentification des utilisateurs basiques quand le cryptage est activé et autres API dans API Gateway.
443	HTTPS	Milestone Systems A/S (doc.milestonesys.com au 52.178.114.226)	Management Client et Smart Client vérifient de temps en temps si l'aide en ligne est disponible en accédant à l'URL de l'aide.
7563	TCP	Service Recording Server	Récupération des flux vidéo et audio, commandes PTZ.
22331	TCP	Service Event Server	Alarmes.

XProtect Web Client, client XProtect Mobile

Numéro de port	Protocole	Connexions à...	Objectif
8081	HTTP	Serveur XProtect Mobile	Récupération des flux vidéo et audio.
8082	HTTPS	Serveur XProtect Mobile	Récupération des flux vidéo et audio.

API Gateway

Numéro de port	Protocole	Connexions à...	Objectif
80	HTTP	Management Server	API RESTful
443	HTTPS	Management Server	API RESTful

Les pools d'applications

Le VMS contient des pools d'applications standard, tels que .NET v4.5, .NET v4.5 Classic et le DefaultAppPool. Les pools d'applications disponibles sur votre système apparaissent dans le gestionnaire des services d'information Internet (IIS). En plus des pools d'applications standard mentionnés ci-dessus, un ensemble de pools d'applications VideoOS est fourni avec le Milestone XProtect VMS.

Les pools d'applications dans Milestone XProtect

Dans le tableau ci-dessous, vous pouvez obtenir un aperçu des pools d'applications VideoOS livrés avec Milestone XProtect.

Nom	Identité	Objectif
.NET v4.5	ApplicationPoolId	Fonctionnalité de IIS standard
.NET v4.5 Classic	ApplicationPoolId	Fonctionnalité de IIS standard
DefaultAppPool	ApplicationPoolId	Fonctionnalité de IIS standard
VideoOS ApiGateway	NetworkService	Héberge la passerelle API XProtect qui est l'API publique future et la passerelle vers le VMS.
VideoOS Classic	NetworkService	Héberge les composants hérités, tels que l'aide locale principalement pour se conformer à la rétrocompatibilité.
VideoOS IDP	NetworkService	Héberge l'API Identity Provider. Le Identity Provider crée, maintient et gère les informations d'identité pour les utilisateurs basiques et fournit des services d'authentification et d'enregistrement aux applications ou services dépendants.
VideoOS IM	NetworkService	Héberge l'API XProtect Incident Manager. Le XProtect Incident Manager documente les incidents et les combine avec des preuves

Nom	Identité	Objectif
		séquentielles (vidéo et, potentiellement, audio) de leur VMS XProtect.
VideoOS Management Server	NetworkService	Héberge l'API de configuration, les API des composants du serveur et d'autres services Management Server, et gère les autorisations des utilisateurs.
VideoOS ReportServer	NetworkService	Héberge l'application web chargée de collecter et de créer des rapports sur les alarmes et les événements.
VideoOS ShareService	NetworkService	Héberge le service qui facilite les signets et le partage de vidéos en direct entre les utilisateurs du client XProtect Mobile.

Utiliser des pools d'applications

À partir de la page **Pools d'applications** de la fenêtre **Services d'informations Internet (IIS)**, vous pouvez ajouter des pools d'applications ou définir les paramètres par défaut du pool d'applications et afficher les applications hébergées par chaque pool d'applications.

Ouvrir la page Pools d'applications

1. Dans le menu **Démarrer** de Windows, ouvrez le **gestionnaire de services d'information Internet (IIS)**.
2. Dans le volet **Connexions**, cliquez sur le nom de votre environnement, puis sur **Pools d'applications**.
3. Sous **Actions**, cliquez sur **Ajouter un pool d'applications** ou **Définir les valeurs par défaut du pool d'applications** pour effectuer l'une de ces tâches.
4. Sélectionnez un pool d'applications sur la page **Pools d'applications** pour afficher d'autres options sous **Actions** pour chaque pool d'applications.

Comparaison des produits

Le VMS XProtect comprend les produits suivants :

- XProtect Corporate
- XProtect Expert
- XProtect Professional+
- XProtect Express+

Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

XProtect Remote Manager

XProtect Remote Manager est un outil en ligne permettant aux fournisseurs de services et aux utilisateurs finaux de gérer et de surveiller une ou plusieurs installations XProtect. Il permet aux responsables informatiques et aux administrateurs de VMS XProtect de gérer efficacement des systèmes de grande taille et distribués depuis n'importe où et d'obtenir une vue instantanée de l'état du système VMS.

XProtect Remote Manager comprend les éléments suivants :

- Un aperçu instantané de toutes les installations VMS détenues par un compte d'entreprise
- La possibilité d'accorder aux fournisseurs de services un accès pour surveiller des installations VMS spécifiques à partir de XProtect Remote Manager

Pour plus d'informations, rendez-vous sur https://doc.milestonesys.com/xrm/latest/en-US/index.htm

Licence

Licences (explications)

Licences pour les produits VMS XProtect

Fichier de licence logicielle et SLC

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

- Une confirmation de commande et un fichier de licence logicielle doté de l'extension .lic et nommé en fonction de votre SLC (code de licence du logiciel) par e-mail
- Une couverture Milestone Care

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

- 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, produits VMS et extensions XProtect. 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 pour une utilisation ultérieure. Vous pouvez également afficher votre SLC dans la fenêtre **Informations sur les licences** dans Management Client. Vous pouvez ouvrir la fenêtre **Informations sur les licences** dans le volet **Navigation du site** -> noeud **Basiques** -> **Informations sur les licences**.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 pour obtenir de l'aide ou pour apporter des modifications à votre système.

Processus général pour le processus d'installation et de licence

Pour commencer, téléchargez le logiciel sur notre site Internet (https://www.milestonesys.com/download/). Pendant l'installation du logiciel (voir Installer un nouveau système XProtect on page 160), vous êtes invité à fournir le fichier de licence logicielle. Vous ne pouvez pas effectuer l'installation sans un fichier de licence logicielle.

Une fois l'installation effectuée et que vous avez ajouté quelques caméras, vous devez activer vos licences (voir Activation des licences (explications) on page 129. Vous activez vos licences depuis la fenêtre **Informations sur les licences** dans Management Client. Vous pouvez y afficher un aperçu de vos licences pour toutes les installations sous le même SLC. Vous pouvez ouvrir la fenêtre **Informations sur les licences** dans le volet **Navigation du site** -> noeud **Basiques** -> **Informations sur les licences**.

Types de licences

Il existe plusieurs types de licences dans le système de licences XProtect.

Licences de base

Vous disposez au moins d'une licence de base pour l'un des produits de logiciel de gestion des vidéos XProtect. Vous pouvez également disposer d'une ou plusieurs licences de base pour les extensions XProtect.

Licences de périphériques

Vous disposez d'au moins plusieurs licences de périphériques. Généralement, vous avez besoin d'une licence de périphérique par périphérique avec une caméra que vous souhaitez ajouter à votre système. Cependant, cela peut varier d'un périphérique à un autre si le périphérique est un périphérique Milestone pris en charge ou non. Pour plus d'informations, voir Périphériques pris en charge on page 128 et Périphériques non pris en charge on page 128.

Si vous souhaitez utiliser la fonction vidéo push dans XProtect Mobile, vous aurez besoin d'une licence de périphérique pour chaque périphérique mobile ou tablette pouvant utiliser cette fonction dans votre système.

Les licences de périphérique ne sont pas requises pour les haut-parleurs, microphones ni pour les périphériques d'entrée et de sortie connectés à votre caméra.

Périphériques pris en charge

Généralement, vous avez besoin d'une licence de périphérique par périphérique avec une caméra que vous souhaitez ajouter à votre système. Cependant, quelques périphériques pris en charge requièrent plus d'une licence de périphérique. Vous pouvez voir le nombre de licences de périphériques requis par votre périphérique dans la liste des périphériques pris en charge sur le site Internet Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

Pour les encodeurs vidéo qui ont jusqu'à 16 canaux, seule une licence de périphérique par adresse IP de l'encodeur vidéo est nécessaire. Un encodeur vidéo peut avoir une ou plusieurs adresses IP.

Cependant, si l'encodeur vidéo a plus de 16 canaux, une licence de périphérique par caméra activée sur l'encodeur vidéo est requise. De même pour les premières 16 caméras activées.

Périphériques non pris en charge

Un périphérique non pris en charge requiert une licence de périphérique par caméra activée utilisant un canal vidéo.

Les périphériques non pris en charge ne figurent pas dans la liste des périphériques pris en charge sur le site Web de Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

Licences de caméras pour Milestone Interconnect™

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. Le nombre de licences de caméra Milestone Interconnect requises dépend de l'activité de streaming sur les sites à distance dont vous souhaitez récupérer les données. Il ne peut pas y avoir plus d'une licence par flux. Seul XProtect Corporate peut servir de site central.

Licences pour les extensions XProtect

La plupart des extensions XProtect nécessitent des types de licences supplémentaires. Le fichier de licence logicielle contient également des informations sur les licences de vos extensions. Certaines extensions possèdent leurs propres fichiers de licence logicielle.

Licenses de test

Les licences test du VMS XProtect sont utilisées à des fins de démonstration et de formation. Elles peuvent être obtenues de différentes manières :

- À partir de Milestone Customer Dashboard
- Auprès de votre revendeur
- Auprès de votre représentant local Milestone

Les licences test prennent en charge un nombre limité de caméras. Leur durée de validité est de 365 jours pour le VMS XProtect et de six mois pour XProtect Remote Manager.

Activation des licences (explications)

Votre SLC doit être enregistré avant l'installation (voir Enregistrer le code de licence du logiciel on page 157). Vos différentes licences connectées avec vos SLC doivent être activées pour que le logiciel de gestion des vidéos XProtect et les extensions XProtect fonctionnent et que les périphériques puissent envoyer des données au système. Pour une vue d'ensemble de tous vos types de licences XProtect, voir Types de licences on page 128.

Il existe plusieurs manières d'activer les licences. Toutes sont disponibles dans la fenêtre **Informations sur les licences**. La meilleure activation varie en fonction des politiques de votre entreprise et si votre serveur de gestion a accès à Internet ou non. Pour découvrir comment activer des licences, voir Activer vos licences on page 134.

Après la première activation des licences de votre logiciel de gestion des vidéos XProtect, vous n'avez plus à activer les licences périphériques à chaque fois que vous ajoutez un périphérique avec une caméra grâce à la flexibilité intégrée au système de licences XProtect. Pour plus d'informations sur ces flexibilités, voir Période d'évaluation pour l'activation des licences (explications) on page 130 et Changements apportés aux périphériques sans activation (explications) on page 131.

Activation automatique des licences (explications)

Pour une maintenance et une flexibilité facilitées, et lorsque les politiques de votre entreprise le permettent, Milestone recommande d'activer l'activation automatique des licences. L'activation automatique des licences requiert la mise en ligne du serveur de gestion. Pour découvrir comment activer l'activation automatique des licences, voir Activer l'activation automatique des licences on page 135.

Avantages de l'activation automatique des licences

- Le système active vos périphériques quelques minutes après avoir ajouté, supprimé ou remplacé des périphériques ou effectué d'autres changements qui affectent l'utilisation de vos licences. Par conséquent, vous devez démarrer une activation des licences manuelle dans de très rares cas uniquement. Consultez lesdites exceptions dans Cas où une activation manuelle des licences est tout de même requise on page 130.
- Le nombre de changements apportés aux périphériques sans activation est toujours à zéro.
- Aucun périphérique n'est compris dans la période d'évaluation et n'est sous 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.

Cas où une activation manuelle des licences est tout de même requise

L'activation manuelle des licences est requise si vous effectuez les changements suivants à votre système.

- Achat de licences supplémentaires (voir Obtenir des licences supplémentaires on page 137)
- Mise à niveau vers une nouvelle version ou un vers un système de logiciel de gestion des vidéos plus avancé (voir Conditions préalables de mise à niveau on page 403)
- Achat ou renouvellement d'un abonnement Milestone Care
- Réception d'une indemnité pour davantage de changements apportés aux périphériques sans activation (voir Changements apportés aux périphériques sans activation (explications) on page 131)

Période d'évaluation pour l'activation des licences (explications)

Lorsque vous avez installé votre logiciel de gestion des vidéos et ajouté des périphériques (périphériques, caméras Milestone Interconnect ou licence de contrôle d'accès pour une porte), les périphériques fonctionnent dans le cadre d'une période d'évaluation de 30 jours si vous avez décidé de ne pas activer l'activation automatique des licences. Vous devez activer vos licences avant la fin de la période d'évaluation de 30 jours et si vous n'avez plus de changements apportés aux périphériques sans activation à effectuer. Sinon, vos périphériques arrêteront d'envoyer la vidéo à votre système de surveillance.

Changements apportés aux périphériques sans activation (explications)

La fonctionnalité de changements apportés aux périphériques sans activation permet une flexibilité intégrée au système de licence XProtect. Donc même si vous avez décidé d'activer manuellement les licences, vous n'avez pas forcément besoin d'activer les licences chaque fois que vous ajoutez ou supprimez des périphériques.

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 détaillée, voir Calcul du nombre de changements apportés aux périphériques sans activation disponible (explications) on page 131.

Un an après votre dernière activation des licences, votre 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.

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 disponible (explications)

Le nombre de changements apportés aux périphériques sans activation est calculé 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.

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

Vous achetez 100 licences de périphériques. Vous ajoutez ensuite 100 caméras à votre système. À moins que vous n'activiez l'activation automatique des licences, vous ne disposez d'aucun changement sans activation. Vous activez vos licences et vous avez maintenant 15 changements apportés aux périphériques sans activation.

Vous achetez 100 licences de périphériques. Vous ajoutez ensuite 100 caméras au système et activez les licences. Votre nombre de changements apportés aux périphériques sans activation s'élève désormais à 15. Vous décidez alors de supprimer un périphérique du système. Vous avez maintenant 99 périphériques activés et le nombre de changements apportés aux périphériques sans activation est descendu à 14.

Vous achetez 1000 licences de périphériques. Vous ajoutez ensuite 1000 caméras et activez les licences. Vos changements apportés aux périphériques sans activation s'élèvent désormais à 100. Selon la variable **C%**, vous devriez maintenant avoir 150 changements apportés aux périphériques sans activation, mais la variable **Cmax** vous permet d'avoir uniquement 100 changements apportés aux périphériques sans activation.

Vous achetez 10 licences de périphériques. Vous ajoutez ensuite 10 caméras au système et activez les licences. Votre nombre de changements apportés aux périphériques sans activation s'élève désormais à 10 étant donné la variable **Cmin**. Si le nombre était calculé uniquement en fonction de la variable **C%**, vous n'auriez que 1 (15 % de 10 = 1.5 arrondi à 1).

Vous achetez 115 licences de périphériques. Vous ajoutez ensuite 100 caméras au système et activez les licences. Vos changements apportés aux périphériques sans activation s'élèvent désormais à 15. Vous ajoutez 15 autres caméras, utilisant ainsi 15 changements apportés aux périphériques sans activation sur les 15. Vous supprimez maintenant 50 des caméras du système et le nombre de changements apportés aux périphériques sans activation baisse à 7. Cela signifie que 8 des caméras précédemment ajoutées au sein des 15 changements apportés aux périphériques sans activation passent en période d'évaluation. Vous ajoutez maintenant 50 nouvelles caméras. Vu que vous aviez ajouté 100 caméras sur le système lors de l'activation des licences, le nombre de changements apportés aux périphériques sans activation repasse à 15 et les 8 caméras en période d'évaluation sont à nouveau considérées comme des changements apportés aux périphériques sans activation. Les 50 nouvelles caméras passent en période d'évaluation.

Milestone Care™ (explications)

Milestone Care est le nom du service complet et du programme d'assistance pour les produits XProtect tout au long de leur durée de vie.

Milestone Care qui vous donne accès à différents types de documents, tels que des articles, guides et tutoriels de notre base de connaissances (Knowledge Base) sur notre site Internet d'assistance (https://www.milestonesys.com/support/).

Pour bénéficier d'avantages supplémentaires, vous pouvez acheter des abonnements Milestone Care plus avancés.

Milestone Care Plus

Si vous disposez d'un abonnement Milestone Care Plus, vous avez également accès à des mises à jour gratuites de votre produit VMS XProtect actuel et pouvez mettre à niveau vers des produits VMS XProtect plus avancés à un prix avantageux. Milestone Care Plus offre également des fonctionnalités supplémentaires :

- Le service Tableau de bord client
- La fonctionnalité Smart Connect
- La fonctionnalité de notification push complète

Milestone Care Premium

Si vous disposez d'un abonnement Milestone Care Premium, vous pouvez également contacter l'assistance Milestone directement. Lorsque vous contactez l'assistance Milestone Care, n'oubliez pas de préciser les informations concernant votre identifiant Milestone.

Expiration, renouvellement et achat d'abonnements avancés Milestone Care

La date d'expiration de votre Milestone Care Plus le plus avancé et des types d'abonnements Milestone Care Premium est visible dans la fenêtre **Informations sur les licences** dans le tableau **Produits installés**. Voir Produits installés on page 139.

Si vous décidez d'acheter ou de renouveler un abonnement Milestone Care après avoir installé votre système, vous devez activer manuellement vos licences avant que n'apparaissent les informations Milestone Care correctes. Voir Activation des licences en ligne on page 136 ou Activation des licences hors ligne on page 136.

Remplacement des licences et des matériels (explications)

Si une caméra du système est défectueuse ou que, pour toute autre raison, vous souhaitez la remplacer par une nouvelle, il existe des meilleures pratiques pour ce faire.

Si vous retirez une caméra d'un serveur d'enregistrement, vous libérez par la même occasion une licence de périphérique, mais vous permet l'accès à toutes les bases de données (caméras, microphones, entrées, sorties) et les paramètres de l'ancienne caméra. Utilisez l'option la plus pertinente ci-dessous pour conserver l'accès à vos bases de données de l'ancienne caméra et réutiliser ses paramètres lors du remplacement de la nouvelle caméra.

Remplacer une caméra par une caméra similaire

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 l'ancienne caméra. La nouvelle caméra continue d'utiliser les mêmes bases de données ainsi que les paramètres de l'ancienne caméra. Dans ce cas, vous transférez le câble de réseau de l'ancienne caméra à la nouvelle sans changer les paramètres du Management Client.

Remplacer une caméra par une caméra différente

Si vous remplacez une caméra par une caméra différente (fabricant, marque et modèle), vous devez utiliser l'assistant **Remplacer le matériel** (voir Remplacer le matériel on page 371) pour cartographier toutes les bases de données pertinentes des caméras, microphones, entrées, sorties et paramètres.

Activation de la licence après le remplacement du matériel

Si vous avez activé l'activation automatique des licences (voir Activer l'activation automatique des licences on page 135), la nouvelle caméra sera automatiquement activée.

Si l'activation automatique des licences, et si tous les changements apportés aux périphériques sans activation ont été utilisés (voir Changements apportés aux périphériques sans activation (explications) on page 131), vous devez activer manuellement vos licences. Pour plus d'informations sur l'activation des licences manuelle, voir Activation des licences en ligne on page 136 ou Activation des licences hors ligne on page 136.

Obtenir une vue d'ensemble de vos licences

Il existe plusieurs raisons pour lesquelles vous souhaitez obtenir une vue d'ensemble de vos SLC et votre nombre de licences achetées ainsi que leurs états. En voici quelques-unes :

- Vous souhaitez ajouter un ou plusieurs nouveaux périphériques, mais vous avez des licences périphériques inutilisées, ou vous souhaitez savoir si vous devez en acheter des nouvelles.
- Vous souhaitez savoir si la période d'évaluation de vos périphériques prend bientôt fin. Vous devez alors les activer avant qu'ils ne cessent d'envoyer des données vers le logiciel de gestion des vidéos.
- L'assistance a besoin d'informations concernant votre SLC et votre ID Milestone Care pour vous aider. Vous souhaitez donc savoir lesquelles.
- Vous avez plusieurs installations de XProtect et vous utilisez le même SLC pour toutes ces installations, et vous souhaitez savoir où les licences sont utilisées et quels sont leurs états.

Vous pouvez trouver toutes les informations mentionnées ci-dessus et bien d'autres dans la fenêtre **Informations sur les licences**.

Vous pouvez ouvrir la fenêtre **Informations sur les licences** dans le volet **Navigation du site** -> noeud **Basiques** -> **Informations sur les licences**.

Pour en savoir plus sur les différentes informations et fonctionnalités disponibles dans la fenêtre **Informations sur les licences**, voir Fenêtre Informations sur les licences on page 139.

Activer vos licences

Il existe plusieurs manières d'activer les licences. Toutes sont disponibles dans la fenêtre **Informations sur les licences**. La meilleure activation varie en fonction des politiques de votre entreprise et si votre serveur de gestion a accès à Internet ou non.

Vous pouvez ouvrir la fenêtre **Informations sur les licences** dans le volet **Navigation du site** -> noeud **Basiques** -> **Informations sur les licences**.

Pour en savoir plus sur les différentes informations et fonctionnalités disponibles dans la fenêtre **Informations sur les licences**, voir Fenêtre Informations sur les licences on page 139.

Activer l'activation automatique des licences

Pour une maintenance et une flexibilité facilitées, et lorsque les politiques de votre entreprise le permettent, Milestone recommande d'activer l'activation automatique des licences. L'activation automatique des licences requiert la mise en ligne du serveur de gestion.

Si vous souhaitez connaître tous les avantages de l'activation de l'activation automatique des licences, voir Activation automatique des licences (explications) on page 130.

1. Depuis le volet **Navigation du site** -> noeud **Basiques** -> **Informations 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 :
   - 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

   Les identifiants sont enregistrés dans un fichier sur le serveur de gestion.
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

Si votre entreprise n'autorise pas l'activation automatique des licences ou si vous avez changé d'avis, vous pouvez désactiver l'activation automatique des licences.

Le type de désactivation dépend de si vous souhaitez réutiliser plus tard l'activation automatique des licences ou non.

Désactiver tout en conservant le mot de passe pour une utilisation ultérieure :

1. Depuis le volet **Navigation du site** -> noeud **Basiques** -> **Informations sur la licence**, décochez la case **Activer l'activation automatique des licences**. Les mot de passe et nom d'utilisateur sont toujours enregistrés sur le serveur de gestion.

Désactiver et supprimer le mot de passe :

1. Depuis le volet **Navigation du site** -> noeud **Basiques** -> **Informations sur la licence**, cliquez sur **Modifier les identifiants d'activation**.
2. Cliquez sur **Supprimer le mot de passe**.
3. Confirmez la suppression du mot de passe et du nom d'utilisateur sur le serveur de gestion.

Activation des licences en ligne

Si le serveur de gestion a accès à Internet, mais que vous préférez démarrer manuellement le processus d'activation, voici une option d'activation de la licence simplifiée pour vous.

1. Depuis le volet **Navigation du site** -> noeud **Basiques** -> **Informations sur la licence**, sélectionnez **Activer la 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 ou contactez l'assistance Milestone.

Activation des licences hors ligne

Si votre entreprise n'autorise pas l'accès à Internet du serveur de gestion, vous devez activer les licences manuellement et hors ligne.

1. Depuis le volet **Navigation du site** -> noeud **Basiques** -> **Informations sur la licence**, sélectionnez **Activer la licence manuellement** > **Hors ligne** > **Exporter la licence pour l'activation** pour exporter un fichier de demande de licence (.lrq) contenant les informations sur vos périphériques ajoutés et les autres éléments qui requièrent une licence.

2. Le fichier de demande de licence (.lrq) reçoit automatiquement le même nom que votre SLC. Si vous possédez plusieurs sites, n'oubliez pas de renommer les fichiers afin de facilement identifier quel fichier correspond à quel site.
3. Copiez le fichier de demande de licence sur un ordinateur avec connexion Internet et connectez-vous à notre site Internet (https://online.milestonesys.com/) pour obtenir le fichier de licence logicielle activé (.lic).
4. Copiez le fichier .lic que vous recevez sur votre ordinateur avec Management Client. Le fichier comporte le même nom que celui de votre fichier de demande de licence.
5. Depuis le volet **Navigation du site** noeud -> **Basiques** -> **Informations sur la licence**, sélectionnez **Activer la licence manuellement** > **Importer une licence activée**, puis sélectionnez le fichier de licence logicielle activée pour l'importer et activer vos licences.
6. Cliquez sur **Terminer** pour conclure le processus d'activation.

Activer des licences après la période d'évaluation

Si vous avez opté pour l'activation manuelle des licences et que vous avez omis d'activer une licence dans la période d'évaluation (périphérique, caméra Milestone Interconnect, licence de contrôle d'accès pour une porte ou autres), le périphérique qui utilise cette licence n'est plus disponible et ne peut envoyer de données au système de surveillance

Peu importe si la période d'évaluation a expiré : la configuration de vos périphériques et vos paramètres est enregistrée et utilisée lorsqu'une licence est activée.

Pour réactiver les périphériques indisponibles, vous activez les licences manuellement selon la méthode souhaitée. Pour plus d'informations, voir Activation des licences hors ligne on page 136 et Activation des licences en ligne on page 136.

Obtenir des licences supplémentaires

Si vous souhaitez ajouter ou si vous avez déjà ajouté plus de périphériques, systèmes Milestone Interconnect, portes ou autres éléments pour lesquels vous avez actuellement des licences, vous devez ajouter des licences supplémentaires pour les permettre d'envoyer des données à votre système :

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

Si vous avez acheté de nouvelles licences à 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 Activation des licences en ligne on page 136 et Activation des licences hors ligne on page 136.

Si vous avez acheté de nouvelles licences et une version de système de surveillance mise à jour :

- Vous recevrez un nouveau fichier de licence logicielle (.lic) avec de nouvelles licences et une nouvelle version. Vous devez utiliser le nouveau fichier de licence logicielle au cours de l'installation de la nouvelle version. Pour plus d'informations, voir Conditions préalables de mise à niveau on page 403

Changer le code de licence du logiciel

Si vous exécutez une installation sur un code de licence logicielle (SLC) temporaire ou si vous avez effectué une mise à niveau vers un produit XProtect plus avancé, vous pouvez remplacer votre SLC par un SLC permanent ou plus avancé sans devoir effectuer une désinstallation ou une réinstallation lorsque vous recevez votre nouveau fichier de licence logicielle.

Vous pouvez effectuer cette opération localement sur le serveur de gestion ou à distance à partir du Management Client.

À partir de l'icône de barre d'état du serveur de gestion

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** et vous êtes maintenant prêt à enregistrer le SLC. Voir Enregistrer le code de licence du logiciel on page 157.

À partir de Management Client

1. Copiez le fichier .lic que vous recevez sur votre ordinateur avec Management Client.
2. À partir du volet **Navigation du site** -> Noeud **Basiques** -> **Informations sur la licence**, sélectionnez **Activer la licence manuellement** > **Importer une licence activée**, puis sélectionnez le fichier de licence logicielle à importer.
3. Lorsqu'il est ouvert, acceptez que le fichier de licence logicielle soit différent de celui qui est actuellement utilisé.
4. Vous êtes maintenant prêt à enregistrer le SLC. Voir Enregistrer le code de licence du logiciel on page 157.

Le fichier de licence logicielle est uniquement importé et modifié, mais pas activé. Rappelez-vous d'activer votre licence. Pour plus d'informations, voir Activer vos licences on page 134.

Fenêtre Informations sur les licences

Dans la fenêtre **Informations sur les licences**, vous pouvez suivre les licences qui partagent les mêmes fichiers de licence du logiciel sur ce site et tous les autres sites, faire un suivi de vos abonnements Milestone Care et décider comment activer vos licences.

Vous pouvez ouvrir la fenêtre **Informations sur les licences** dans le volet **Navigation du site** -> noeud **Basiques** -> **Informations sur les licences**.

Si vous souhaitez obtenir une compréhension globale de comment le système de licence XProtect fonctionne, voir Licences (explications) on page 127.

Licence accordée à

Cette zone de la fenêtre **Informations sur la licence**, répertorie les coordonnées du propriétaire de la licence qui ont été saisies au cours de l'enregistrement du logiciel.

Si la zone **Licence attribuée à** n'est pas visible, cliquez sur le bouton **Actualiser** dans le coin inférieur droit de la fenêtre.

Cliquez sur **Modifier les détails** pour modifier les informations relatives au propriétaire de la licence. Cliquez sur **CLUF** pour consulter le CLUF que vous avez accepté avant l'installation.

Milestone Care

Vous y trouverez des informations relatives à votre abonnement Milestone Care™ actuel. Les dates d'expiration de vos abonnements sont indiquées dans le tableau **Produits installés** ci-dessous.

Pour plus d'informations sur Milestone Care, utiliser les liens ou voir Milestone Care™ (explications) on page 132.

Produits installés

Liste les informations suivantes relatives à toutes vos licences de base installées pour le VMS XProtect et les produits complémentaires qui partagent le même fichier de licence logicielle :XProtect

- Produits et versions
- Le code de licence du logiciel (SLC) des produits
- La date d'expiration de votre SLC. Généralement sans limite
- 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 20 R	M01-C01-211-01-	Unlimited	16-11-20	16-11-20
Milestone XProtect Smart Wall	M01-P03-100-01-	Unlimited	Unlimited	
Milestone XProtect Access	M01-P01-011-01-	Unlimited	Unlimited	
Milestone XProtect Transact	M01-P08-100-01-	Unlimited	Unlimited	

Vue d'ensemble des licences - Tous les sites

Répertorie le nombre des licences de périphériques activées ou autres licences dans le fichier de licence de votre logiciel et le 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**. Voir la section **Détails de la licence - Site actuel** ci-dessous pour consulter les informations disponibles affichées.

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

License Type	Activated
Device Licenses	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**.XProtectXProtect

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 utilisés (voir Changements apportés aux périphériques sans activation (explications) on page 131) et combien vous en possédez par an dans la colonne **Changements apportés aux périphériques sans activation**.

Si vous disposez de licences que vous n'avez pas encore activées et qui sont dans la période d'évaluation, elles s'afficheront dans la colonne **En période d'évaluation**. 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 d'évaluation, vous ne recevrez plus de vidéo dans le système. Ces licences s'affichent dans la colonne **Période d'évaluation expirée**. Pour plus d'informations, voir Activer des licences après la période d'évaluation on page 137.

Si vous utilisez plus de licences que vous n'en possédez, elles s'afficheront dans la colonne **Sans licence** et vous ne pourrez pas les utiliser dans votre système. Pour plus d'informations, voir Obtenir des licences supplémentaires on page 137.

Si vous avez des produits en période d'évaluation, en fin de période d'évaluation ou sans licence, un message de rappel apparaîtra à chaque connexion sur votre Management Client.

License Details - Current Site: [redacted]

License Type	Activated	Changes without activation	In Grace Period	Grace Period Expired	Without License
Device Licenses	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

Si vous avez des périphériques qui utilisent plus d'une licence, le lien **Cliquer ici pour ouvrir le rapport complet des licences de périphériques** apparaît sous le tableau **Détails de la licence - Site actuel**. Lorsque vous cliquez sur le lien, vous pouvez voir le nombre de licences de périphériques requis par chacun des périphériques.

Les périphériques sans licence sont identifiés par un point d'exclamation dans le Management Client. 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 Activation automatique des licences (explications) on page 130 et Activer l'activation automatique des licences on page 135.
  Si l'activation automatique échoue, un message apparaitra en rouge. Pour plus d'informations, cliquez sur le lien **Détails**.
  Certaines licences sont installées au moyen d'une activation automatique et il est impossible de désactiver ce paramètre.
- Liste déroulante pour activer manuellement les licences en ligne ou hors ligne. Pour plus d'informations, voir Activation des licences en ligne on page 136 et Activation des licences hors ligne on page 136.
- Dans le coin inférieur droit de la fenêtre, vous pouvez voir la date de la dernière activation de vos licences (automatique ou manuelle) et la date d'actualisation des informations de la fenêtre. Les données d'horodatage proviennent du serveur et non pas de l'ordinateur local

Exigences et considérations

Heure d'été (explications)

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.

> ⚠ Ne modifiez pas les paramètres de l'heure d'été alors que vous êtes déjà passé à l'heure d'été ou si vous disposez d'enregistrements réalisés à 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 01h00 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.

Serveurs de temps (explications)

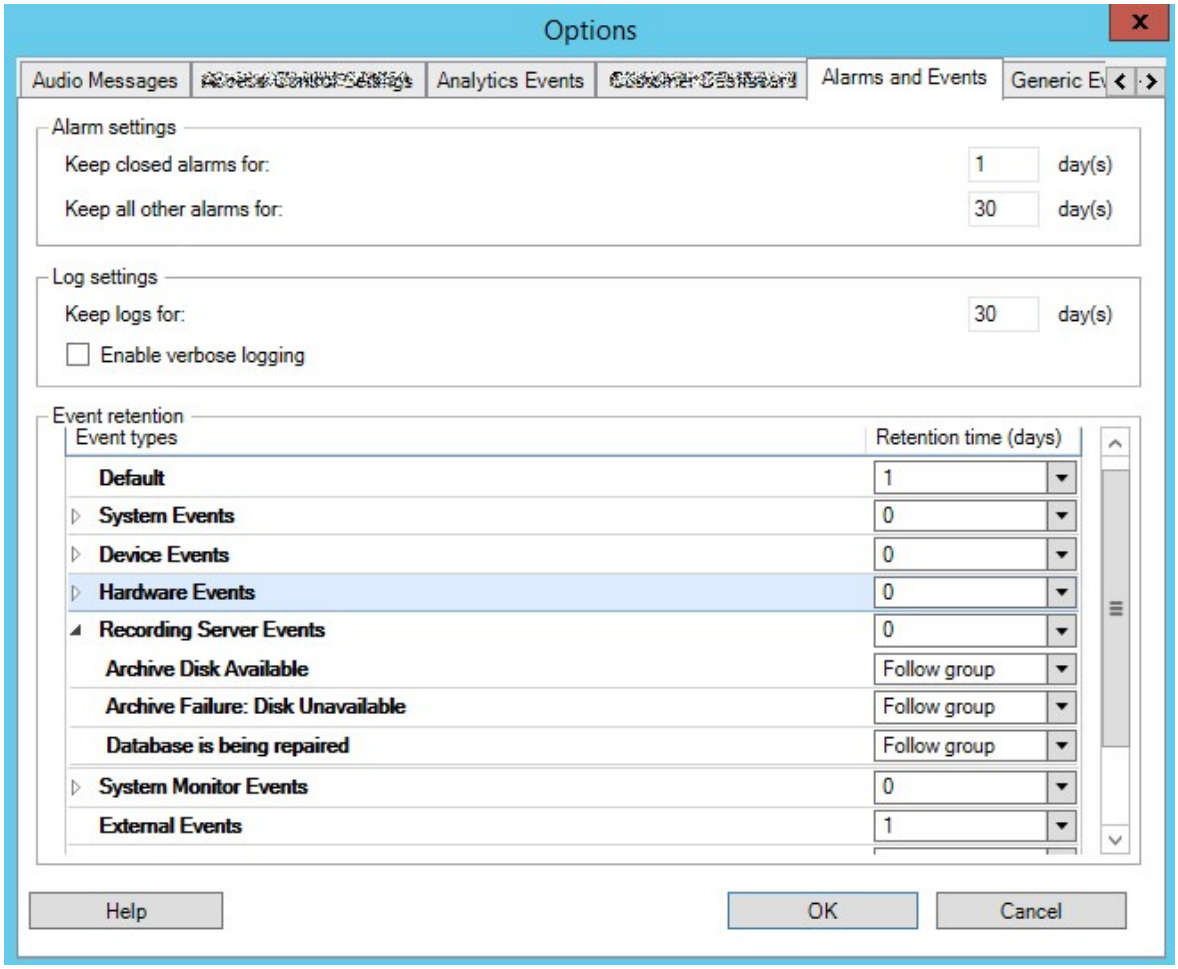
Dès que votre système reçoit les images, elles sont immédiatement horodatées. Les caméras sont des unités distinctes qui peuvent avoir des périphériques de réglage de l'heure distincts. L'heure de la caméra et l'heure de votre système peuvent par conséquent ne pas correspondre exactement. Cela peut parfois 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 le site Internet de Microsoft (https://www.microsoft.com/) en saisissant les mots-clés « **serveur de temps** », « **service de temps** » ou d'autres termes similaires.

Taille limite de la base de données

Pour éviter que la base de données SQL Server (voir SQL Server installations et bases de données (explications) on page 37) n'atteigne une taille qui affecte les performances du système, vous pouvez spécifier le temps de stockage en jours des différents types d'événements et d'alarmes dans celle-ci.

1. Ouvrez le menu **Outils**.
2. Cliquezsurl'onglet**Options**>**Alarmesetévénements**.



3. Appliquez les paramètres nécessaires. Pour plus d'informations, voir Onglet Alarmes et événements (Options) on page 431.

IPv6 et IPv4 (explications)

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'institutions 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.

Utilisation du système avec IPv6 (explications)

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 IP.

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.

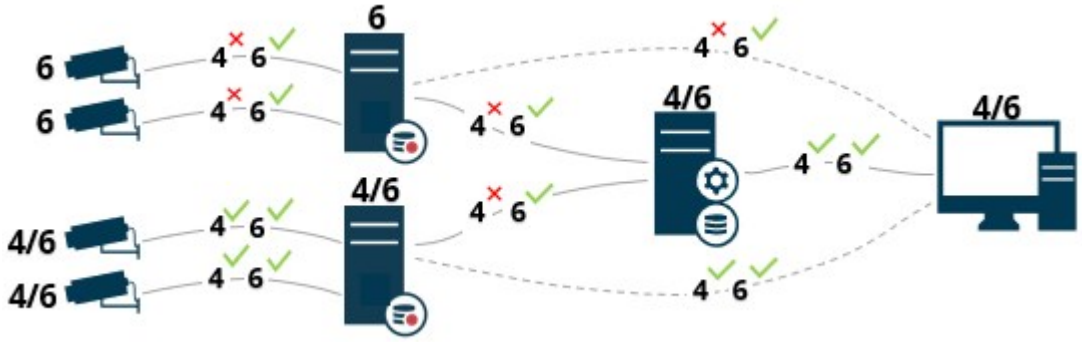
Clients

Si votre système utilise IPv6, les utilisateurs doivent se connecter avec le XProtect Smart Client. Le XProtect Smart Client prend en charge IPv6 et 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 les installations XProtect Smart Client se connectent techniquement 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 ***Ipv6 install***, 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.

Écriture des adresses IPv6 (explications)

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]:1234, qui peut être évidemment abrégé, par exemple, *http://[2001:B80::F80:3FA8:18AB]:1234*

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

Serveurs virtuels

Vous pouvez exécuter tous les composants du système dans des serveurs Windows® virtuels, tels que 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 le nombre d'images configuré.

Protection des bases de données d'enregistrement contre la corruption

Les bases de données des caméras peuvent devenir corrompues. Plusieurs options de réparation des bases de données existent pour résoudre un tel problème. Mais Milestone vous recommande de prendre des mesures pour vous assurer que les bases de données de votre caméra ne deviennent 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)
- Feu, eau, et autre (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 service système en cliquant sur **Fermer le processus** dans le Gestionnaire des tâches Windows, 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.

La sélection du type d'onduleur adéquat 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.

Journal des transactions de la base de données SQL Server (explications)

Chaque fois qu'un changement est écrit dans une base de données SQL Server, la base de données SQL Server enregistre ce changement dans son journal de transaction.

Avec le journal de transaction, vous pouvez revenir à la version précédente et annuler des modifications apportées à la base de données SQL Server par le biais de Microsoft® SQL Server Management Studio. Par défaut, la base de données SQL Server stocke son journal de transaction indéfiniment, ce qui signifie qu'au fil du temps, le journal de transaction accumule de plus en plus d'entrées. Le journal de transaction est situé par défaut sur le lecteur système et, s'il continue de croître, il peut empêcher le bon fonctionnement de Windows.

Pour éviter un tel scénario, il est recommandé de purger régulièrement le journal de transaction. La purge en elle-même ne diminue pas la taille du journal de transaction, mais elle efface son contenu et l'empêche ainsi de croître et devenir hors de contrôle. Votre système VMS ne purge pas les journaux de transaction. Dans SQL Server, il existe des manières de purger le journal de transaction. Rendez-vous sur la page d'assistance de Microsoft https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017 et cherchez *Troncation du journal de transactions*.

Configuration système minimum

Pour de plus amples informations sur la configuration système des divers éléments de votre système et applications VMS, allez sur le site Web de Milestone (https://www.milestonesys.com/systemrequirements/).

Avant de commencer l'installation

Milestone vous recommande de parcourir les conditions préalables décrites au fil des prochaines sections avant de débuter l'installation réelle.

Préparation de vos serveurs et du réseau

Système d’exploitation

Assurez-vous que tous les serveurs disposent d’une installation propre d’un système d’exploitation Microsoft Windows et de la mettre à jour en appliquant toutes les mises à jour les plus récentes de Windows.

Pour de plus amples informations sur la configuration système des divers éléments de votre système et applications VMS, allez sur le site Web de Milestone (https://www.milestonesys.com/systemrequirements/).

Microsoft® .NET Framework

Vérifiez que Microsoft® .NET 4.7.2 Framework et Microsoft® .NET 6 Runtime sont installés sur tous les serveurs.

Réseau

Assignation d’adresses IP statiques ou réservations DHCP sur tous les composants et caméras du système. Pour vous assurer de disposer d’une bande passante suffisante sur votre réseau, vous devez comprendre comment et quand le système consomme de la bande passante. La charge principale de votre réseau est composée de trois éléments :

- Flux vidéo des caméras
- Clients affichant la vidéo
- Archivage des vidéos enregistrées

Le serveur d’enregistrement récupère les flux vidéo à partir des caméras, ce qui constitue une charge constante sur le réseau. Les clients affichant la vidéo consomment la bande passante du réseau. Si aucune modification n’est apportée au contenu des vues des clients, la charge est constante. Les changements de contenus des vues, les recherches de vidéos ou la lecture font varier la charge.

L’archivage de vidéos enregistrées représente une fonctionnalité facultative qui permet au système de déplacer les enregistrements vers un emplacement de stockage sur le réseau si l’espace du système de stockage interne de l’ordinateur est insuffisant. Il s’agit d’une tâche programmée que vous devez définir. Généralement, vous archivez les vidéos vers un disque réseau, ce qui entraîne une variation programmée de la charge sur le réseau.

Votre réseau doit disposer de suffisamment de bande passante en réserve pour prendre en charge ces pics de trafic. Ceci améliore la réactivité du système et, de façon plus générale, l’expérience des utilisateurs.

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 de votre système, vous devrez réinstaller le serveur de gestion et remplacer des utilisateurs par de nouveaux utilisateurs Windows définis dans Active Directory.

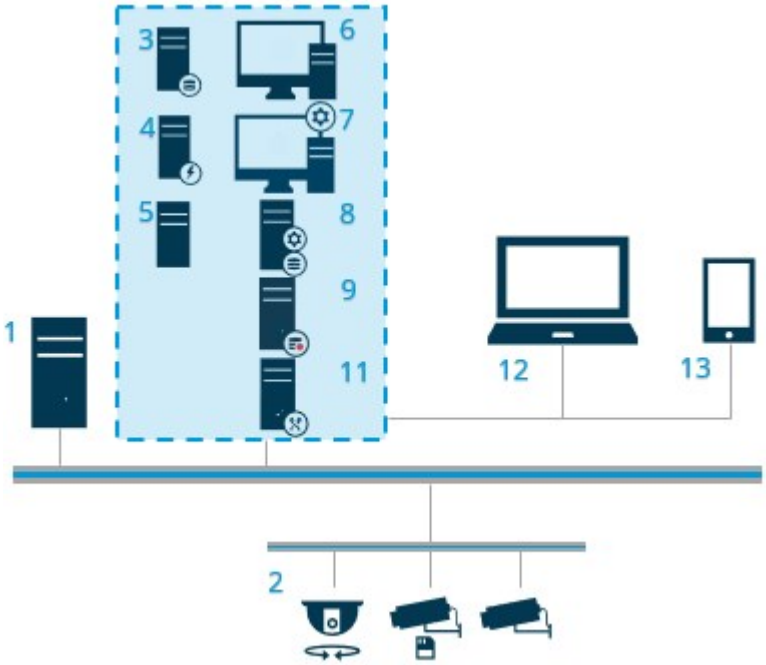
Les utilisateurs basiques ne sont pas pris en charge dans les systèmes Milestone Federated Architecture, donc si vous pensez utiliser Milestone Federated Architecture, vous devez ajouter les utilisateurs en tant qu'utilisateurs de Windows via le service Active Directory. Si vous n'installez pas Active Directory, suivez les étapes dans Installation pour les groupes de travail on page 198 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 institution, mais il est très probable que vous ayez déjà décidé de la méthode à adopter au moment de l'achat du système.

Options	Description
Ordinateur unique	Installe l'ensemble des composants liés au serveur et au client, ainsi que SQL Server sur l'ordinateur actuel. Une fois terminée l'installation, vous obtenez la possibilité de configurer votre système par le biais d'un assistant. Si vous acceptez de continuer, le serveur d'enregistrement analyse le réseau pour trouver des périphériques et vous pouvez sélectionner quels périphériques à ajouter à votre système. Le numéro maximal de périphériques pouvant être ajoutés dans l'assistant de configuration dépend de votre licence de base. Les caméras sont également préconfigurées dans des vues et un rôle d'opérateur est créé par défaut. Après l'installation, XProtect Smart Client s'ouvre et vous pouvez utiliser le système.
Personnalisé	Le serveur de gestion est toujours sélectionné dans la liste de composants du système et il est toujours installé, mais vous pouvez choisir librement les éléments à installer sur l'ordinateur actuel, parmi les autres composants du serveur et du client. Par défaut, la case du serveur d'enregistrement est décochée dans la liste de composants, mais vous pouvez modifier cette configuration. Vous pouvez installer les composants non sélectionnés sur d'autres ordinateurs par la suite.

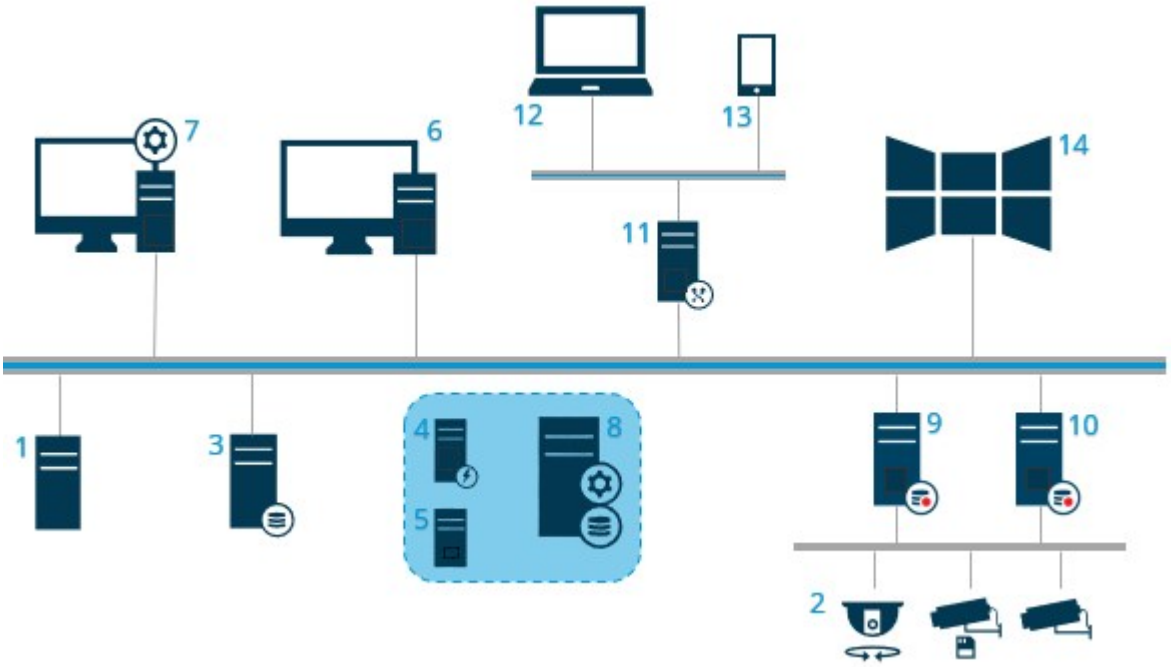
Installation sur un seul ordinateur



Composants typiques d’un système :

1. **Active Directory**
2. **Périphériques**
3. **Serveur avec SQL Server**
4. **Serveur d’événements**
5. **Serveur de journaux**
6. **XProtect Smart Client**
7. **Management Client**
8. **Serveur de gestion**
9. **Serveur d’enregistrement**
10. **Serveur d’enregistrement de basculement**
11. **XProtect MobileServeur**
12. **XProtect Web Client**
13. **XProtect MobileClient**
14. **XProtect Smart Client avec XProtect Smart Wall**

Installation personnalisée - exemple des composants du système distribués



Décider d'une édition de SQL Server

Microsoft® SQL Server® Express est une édition gratuite de SQL Server et est facile à installer et prête à l'utilisation en comparaison des autres éditions de SQL Server.

L'assistant d'installation installe Microsoft SQL Server Express 2022 à moins que SQL Server ne soit déjà installé sur l'ordinateur. Lorsque vous installez le VMS XProtect en tant que mise à niveau, l'assistant conserve l'installation SQL Server précédente.

Pour vérifier si votre système répond aux exigences des éditions SQL Server, voir https://www.milestonesys.com/systemrequirements/.

Pour de très grands systèmes ou des systèmes avec beaucoup de transactions provenant de bases de données et allant vers des bases de données SQL Server, Milestone vous recommande d'utiliser l'édition Microsoft® SQL Server® Standard ou Microsoft® SQL Server® Enterprise de SQL Server sur un ordinateur dédié sur le réseau et sur un disque dur dédié qui n'est pas utilisé à d'autres fins. L'installation de SQL Server sur ses propres périphériques améliore la performance de l'intégralité du système.

Sélectionner un compte de service

Dans le cadre de l'installation, il vous est demandé de préciser un compte pour exécuter les services de Milestone sur cet ordinateur. Les services fonctionnent toujours sur ce compte, quel que soit l'utilisateur connecté. Assurez-vous que le compte dispose de toutes les autorisations utilisateur nécessaires, par exemple, les autorisations adéquates pour effectuer des tâches, le réseau et l'accès aux fichiers appropriés, et l'accès aux dossiers partagés sur le réseau.

Vous pouvez sélectionner un compte prédéfini ou un compte utilisateur. Basez votre décision 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 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 vous recommande d'utiliser le compte d'utilisateur local qui dispose de toutes les autorisations nécessaires. Ceci est souvent le compte administrateur.

> Si vous avez installé vos composants système sur plusieurs ordinateurs, le compte d'utilisateur sélectionné doit être configuré sur tous les ordinateurs de vos installations avec les mêmes noms, mot de passe et autorisations d'accès.

Authentification Kerberos (explications)

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 mutuelle dans votre XProtect VMS, 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 services Milestone ainsi que les numéros de port correspondants que vous devez inscrire :

Service	Numéro de port
Management Server - IIS	80 - Configurable
Management Server - Interne	8080
Recording Server - Data Collector	7609
Failover Server	8990
Event Server	22331
LPR Server	22334

Le nombre de services que vous devez inscrire dans le répertoire actif dépend de votre installation actuelle. Data Collector s'installe de manière automatique lorsque vous installez le service Management Server, Recording Server, Event Server ou Failover Server.

Vous devez enregistrer deux SPN pour que l'utilisateur puisse exécuter ce service : un avec le nom d'hôte et l'autre avec le nom du domaine complet.

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.

Il s'agit de la convention de nomination SPN Milestone :

```
VideoOS/[DNS Host Name]:[Port]
VideoOS/[Fully qualified domain name]:[Port]
```

Voici un exemple de SPN pour le service Recording Server fonctionnant sur un ordinateur avec les détails ci-dessous :

```
Hostname: Record-Server1
Domain: Surveillance.com
```

SPN à enregistrer :

```
VideoOS/Record-Server1:7609
VideoOS/Record-Server1.Surveillance.com:7609
```

Exclusions scan antivirus (explications)

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 que certains trafics du réseau. Sans appliquer ces exceptions, la détection de virus utilise une quantité considérable de ressources système. De plus, le processus de numérisation peut verrouiller temporairement des fichiers, ce qui peut engendrer une interruption du processus d'enregistrement et même la corruption des bases de données.

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

Créer les exclusions supplémentaires suivantes :

- Types de fichiers : .blk, .idx, .pic
- Dossiers et sous-dossiers :
  - `C:\Program Files\Milestone` ou `C:\Program Files (x86)\Milestone`
  - `C:\ProgramData\Milestone\IDP\Logs`
  - `C:\ProgramData\Milestone\KeyManagement\Logs`
  - `C:\ProgramData\Milestone\ MilestoneMIPSDK`
  - `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 Mobile Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Recording Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Report Web Server\Logs`
  - `C:\ProgramData\Milestone\XProtect Recording Server\Secure\TablesDb`

- Exclure l'analyse en réseau sur les ports TCP suivants :

Produit	Ports TCP
XProtectVMS	80, 8080, 7563, 25, 21, 9000
XProtect Mobile	8081

ou

- Exclure l'analyse en réseau des processus suivants :

Produit	Processus :
XProtectVMS	VideoOS.Recorder.Service.exe, VideoOS.Server.Service.exe, VideoOS.Administration.exe
XProtect Mobile	VideoOS.MobileServer.Service.exe

Votre entreprise emploie peut-être des directives strictes concernant les analyses antivirus, mais il est important d'exclure les dossiers et les fichiers mentionnés de l'analyse antivirus.

Comment configurer le VMS XProtect pour qu'il s'exécute au mode FIPS 140-2 ?

Pour exécuter XProtect VMS en mode FIPS 140-2, vous devez :

- Exécuter le système d'exploitation de Windows en mode FIPS 140-2. Voir le site de Microsoft pour plus d'informations sur l'activation du mode FIPS.
- Vous assurer que les intégrations autonomes tierces peuvent s'exécuter dans un système d'exploitation Windows où est activé le mode FIPS.
- Vous connecter aux périphériques tout en garantissant que leur exécution est conforme aux normes FIPS 140-2

- Vous assurer que les données des bases de données multimédia sont cryptées avec un cryptage conforme aux normes FIPS 140-2

  Pour ce faire, exécutez l'outil de mise à niveau de la base de données médias. Pour de plus amples informations sur comment configurer votre XProtect VMS pour qu'il s'exécute conformément au mode FIPS 140-2, voir la section de conformité aux normes FIPS 140-2 dans le guide de durcissement.

Avant d'installer le VMS XProtect sur un système où est activé le mode FIPS

Vous pouvez effectuer les nouvelles installations du VMS XProtect sur des ordinateurs où est activé le mode FIPS, mais vous ne pouvez pas mettre à niveau le VMS XProtect si le mode FIPS est activé sur le système d'exploitation Windows.

Lorsque vous effectuez la mise à niveau, avant de procéder à l'installation, veuillez désactiver la politique de sécurité du mode FIPS sur Windows sur tous les composants faisant partie du VMS, y compris l'ordinateur qui héberge SQL Server.

Le programme d'installation du VMS XProtect vérifie la politique de sécurité du mode FIPS et empêche le démarrage de l'installation si le mode FIPS est activé.

Mais si vous effectuez la mise à niveau depuis la version VMS XProtect 2020 R3 ou une version ultérieure, vous n'avez pas besoin de désactiver le mode FIPS.

Vous pouvez réactiver la police de sécurité du mode FIPS sur Windows sur tous les ordinateurs de votre VMS après avoir installé les composants du VMS XProtect sur tous les ordinateurs et avoir préparé le système au mode FIPS.

Pour de plus amples informations sur comment configurer votre XProtect VMS pour qu'il s'exécute conformément au mode FIPS 140-2, voir la section de conformité aux normes FIPS 140-2 dans le guide de durcissement.

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 logicielle 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 logicielle est lié à votre SCL.

Milestone vous recommande d'enregistrer votre SLC sur notre site Internet (https://online.milestonesys.com/) avant l'installation. Votre revendeur a peut-être déjà effectué cette action.

Pilotes de périphériques (explications)

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 périphériques sur chaque serveur d'enregistrement de votre système.

À partir de la version 2018 R1, les pilotes de périphériques sont répartis en deux packs de pilotes de périphériques : le pack de pilotes de périphériques régulier équipé des pilotes plus récents et un pack de pilotes de périphériques hérités doté de pilotes plus anciens.

Le pack de pilotes de périphériques régulier est installé automatiquement au moment où vous installez le serveur d'enregistrement. Par la suite, vous pouvez mettre à jour les pilotes en téléchargeant et en installant une version plus récente du pack de pilotes de périphériques. Milestone publie régulièrement de nouvelles versions des pilotes de périphériques et les met à disposition sur la page de téléchargement (https://www.milestonesys.com/download/) de notre site web sous forme de packs de pilotes de périphériques. Lorsque vous mettez à jour un pack de pilotes de périphériques, vous pouvez installer la dernière version en plus de toute version que vous avez déjà installée.

Le pack de pilotes de périphériques hérités ne peut être installé que si un pack de pilotes de périphériques régulier est installé dans le système. Les pilotes relevant du pack de pilotes de périphériques hérités sont installés automatiquement si une version précédente est déjà installée sur votre système. Ils sont disponibles au téléchargement manuel et à l'installation sur la page de téléchargement du logiciel (https://www.milestonesys.com/download/).

Arrêtez le service 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 périphériques pour garantir des performances optimales.

Conditions préalables de l'installation hors ligne

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

- Le fichier `Milestone XProtect VMS Products 2025 R2 System Installer.exe`
- Le fichier de licence logicielle (SLC) de votre système XProtect
- Média d'installation du système d'exploitation incluant la version .NET requise (https://www.milestonesys.com/systemrequirements/)

Communication sécurisée (explications)

Hypertext Transfer Protocol Secure (HTTPS) est une extension de Hypertext Transfer Protocol (HTTP) pour une communication sécurisée sur un réseau informatique. Sur HTTPS, le protocole de communication est crypté en utilisant Sécurité de la couche transport (TLS), ou son prédécesseur, Couche de sockets sécurisés (SSL).

Dans XProtect VMS, la communication sécurisée est obtenue en utilisant TLS/SSL avec un chiffrement asymétrique (RSA).

TLS/SSL utilise une paire de clés (une privée, une publique) pour authentifier, sécuriser et gérer les connexions sécurisées.

Une autorité de certification (AC) est toute personne capable d'émettre des certificats racine. Il peut s'agir d'un service Internet qui émet des certificats racine ou de toute personne qui génère manuellement et distribue un certificat. Une AC peut émettre des certificats aux services Web, c'est-à-dire à tout logiciel utilisant la

communication https. Ce certificat contient deux clés, une clé privée et une clé publique. La clé publique est installée sur les clients d'un service Web (clients de service) en installant un certificat public. La clé privée est utilisée pour la signature des certificats de serveur qui doivent être installés sur le serveur. Lorsqu'un client de service appelle le service Web, le service Web envoie le certificat du serveur incluant la clé publique au client. Le client de service peut valider le certificat de serveur utilisant le certificat public de l'AC déjà installé. Le client et le serveur peuvent maintenant utiliser les certificats de serveur publics et privés pour échanger une clé secrète et par conséquent, établir une connexion TLS/SSL sécurisée.

Pour les certificats distribués manuellement, les certificats doivent être installés avant que le client ne puisse effectuer cette vérification.

Reportez-vous à la section Transport Layer Security pour plus d'informations concernant TLS.

Les certificats possèdent une date d'expiration. XProtect VMS ne vous préviendra pas lorsqu'un certificat est sur le point d'expirer. Si un certificat expire :
• Les clients ne feront plus confiance au serveur d'enregistrement dû au certificat expiré et ils ne pourront donc plus communiquer avec lui
• Les serveurs d'enregistrement ne feront plus confiance au serveur de gestion dû au certificat expiré et ne pourront donc plus communiquer avec lui
• Les périphériques mobiles ne feront plus confiance au serveur mobile dû au certificat expiré et ils ne pourront donc plus communiquer avec lui

Pour renouveler les certificats, suivez les étapes figurant dans ce guide que vous avez suivies lors de la création des lesdits certificats.

Pour plus d'informations, voir le guide des certificats sur comment sécuriser votre installation de XProtect VMS.

Installation

Installer un nouveau système XProtect

La manière dont vous l'installez dépend de la taille de votre système :

Taille	Processus d'installation
Petite	Installer votre système - option sur ordinateur unique on page 160
Grande	Installer votre système - option personnalisée on page 166

Installer votre système - option sur ordinateur unique

L'option **Ordinateur unique** installe l'ensemble des composants liés au serveur et au client sur l'ordinateur actuel.

Milestone vous recommande de lire avec attention la section suivante avant de procéder à l'installation : Avant de commencer l'installation on page 148.

En ce qui concerne les installations conformes aux normes FIPS, vous ne pouvez pas mettre à jour XProtect VMS si le mode FIPS est activé sur le système d'exploitation Windows. Avant l'installation, désactivez la politique de sécurité Windows FIPS sur tous les ordinateurs qui font partie du VMS, y compris l'ordinateur qui héberge SQL Server. Mais si vous effectuez la mise à niveau depuis la version VMS XProtect 2020 R3 ou une version ultérieure, vous n'avez pas besoin de désactiver le mode FIPS. Pour de plus amples informations sur comment configurer votre XProtect VMS pour qu'il s'exécute conformément au mode FIPS 140-2, voir la section de conformité aux normes FIPS 140-2 dans le guide de durcissement.

Après l'installation initiale, vous pouvez continuer avec l'assistant configuration. Selon votre matériel et votre configuration, le serveur d'enregistrement analyse votre réseau à la recherche de périphériques. Vous pouvez ensuite sélectionner les périphériques à ajouter à votre système. Les caméras sont préconfigurées dans les vues et vous avez la possibilité d'activer les autres périphériques, tels que les microphones et les haut-parleurs. Vous avez également la possibilité d'ajouter au système un rôle d'opérateur ou un rôle d'administrateur. Après l'installation, XProtect Smart Client s'ouvre et vous pouvez utiliser le système.

Dans le cas contraire, si vous fermez l'assistant d'installation, le XProtect Management Client s'ouvre et vous permet d'effectuer des configurations manuelles, telles que l'ajout de matériel et d'utilisateurs au système.

> Si vous réalisez une mise à niveau à partir d'une version précédente du produit, le système n'effectue pas de scan à la recherche de matériels et ne crée pas de nouveaux profils utilisateur.

1. Téléchargez le fichier .iso avec le logiciel depuis Internet (https://www.milestonesys.com/download/). Lorsque vous téléchargez le fichier .iso, il sera chargé en tant que lecteur de DVD appelé « XProtect VMS Installer ».
2. Exécutez le fichier `Milestone XProtect VMS Products 2025 R2 System Installer.exe`.
3. La décompression des fichiers d'installation débute. Un ou plusieurs messages d'avertissement Windows® s'afficheront en fonction des paramètres de sécurités. Acceptez-les afin de poursuivre la décompression.
4. Lorsque vous avez terminé, l'assistant d'installation **Milestone XProtect VMS** s'affiche.
    1. 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**.
    2. Lisez le *MilestoneContrat de licence utilisateur final*. Cochez la case **J'accepte les termes du contrat de licence**, puis cliquez sur **Continuer**.
    3. Sur la page **Paramètres de confidentialité**, sélectionnez si vous souhaitez partager les données d'utilisation et cliquez sur **Continuer**.

        > Vous devez activer la collecte des données si vous souhaitez que le système possède une installation conforme au RGPD de l'UE. Pour plus d'informations sur la protection des données et la collecte des données d'utilisation, voir le Guide de confidentialité du RGPD.

        > Vous pouvez toujours modifier vos paramètres de confidentialité plus tard. Voir également Paramètres du système (boîte de dialogue Options).

5. Sélectionnez **Ordinateur unique**.

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

6. Sur la page **Assigner un mot de passe de configuration système**, saisissez un mot de passe qui protégera votre configuration système. Vous en aurez besoin lorsque vous souhaiterez restaurer votre système ou bien l'étendre, par exemple, avec l'ajout de grappes.

   Il est important que vous enregistriez ce mot de passe dans un emplacement sécurisé. La perte du mot de passe pourrait vous empêcher de restaurer votre configuration système.

   Si vous ne souhaitez pas protéger votre configuration système avec un mot de passe, sélectionnez **Je choisis de ne pas utiliser de mot de passe de configuration système et je comprends que la configuration système ne sera pas cryptée**.

   Cliquez sur **Continuer**.

7. Sur la page **Assigner un mot de passe de protection des données au serveur mobile**, saisissez un mot de passe pour crypter vos enquêtes. En tant qu'administrateur de système, vous devrez saisir ce mot de passe pour accéder aux données du serveur mobile en cas de restauration du système ou en cas d'ajout de serveurs mobiles supplémentaires au système.

   Vous devez enregistrer ce mot de passe dans un emplacement sécurisé. Dans le cas contraire, vous pourriez rencontrer des difficultés pour restaurer les données du serveur mobile.

   Si vous ne souhaitez pas protéger vos enquêtes avec un mot de passe, sélectionnez **Je choisis de ne pas utiliser de mot de passe de protection pour les données du serveur mobile et je comprends que les enquêtes ne seront pas cryptées**.

   Cliquez sur **Continuer**.

8. Sur la page **Spécifier les paramètres du serveur d'enregistrement**, spécifiez les paramètres du serveur d'enregistrement :
    1. Dans le champ **Nom du serveur d'enregistrement**, saisissez le nom du serveur d'enregistrement. Le nom par défaut est celui de l'ordinateur.
    2. Le champ **Adresse du serveur de gestion** indique l'adresse et le numéro du port du serveur de gestion : localhost:80.
    3. Dans le champ **Sélectionner l'emplacement de votre base de données médias**, sélectionnez l'emplacement où vous voulez sauvegarder votre enregistrement vidéo. Milestone vous recommande de sauvegarder vos enregistrements vidéo dans un emplacement différent de celui où vous avez installé le logiciel, et non sur le lecteur système. L'emplacement par défaut est le lecteur qui dispose du plus grand espace disponible.
    4. Dans le champ **Durée de rétention des enregistrements vidéo**, définissez la durée pendant laquelle vous souhaitez sauvegarder les enregistrements. Vous pouvez saisir une valeur comprise entre 1 et 365 000 jours, où 7 jours correspond à la durée de rétention par défaut.
    5. Cliquez sur **Continuer**.

9. Vous pouvez sécuriser les flux de communication sur la page **Choisir le cryptage** :

   - Entre les serveurs d'enregistrement, les collecteurs de données et le serveur de gestion

     Choisissez un certificat dans la rubrique **Certificat du serveur** pour activer le cryptage des flux de communication internes.

     > ⚠ Si vous cryptez la connexion du serveur d'enregistrement vers le serveur de gestion, le système exige le cryptage de la connexion du serveur de gestion aux serveurs d'enregistrement.

   - Entre les serveurs d'enregistrement et les clients

     Choisissez un certificat dans la rubrique **Certificat de flux de multimédia** pour activer le cryptage entre les serveurs d'enregistrement et les composants des clients récoltant des flux de données.

   - Entre le serveur mobile et les clients

     Choisissez un certificat dans la rubrique **Certificat des flux de média mobiles** pour activer le cryptage entre les composants des clients récoltant des flux de données depuis le serveur mobile.

   - Entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements

     Pour activer le chiffrement entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements, y compris le LPR Server, dans la section **Serveur d'événements et extensions**, sélectionnez un certificat.

   Vous pouvez utiliser le même fichier de certificat pour tous les composants du système ou utiliser différents fichiers de certificat en fonction des composants du système.

   Pour plus d'informations sur la préparation de votre système pour des communications sécurisées, voir :

   - Communication sécurisée (explications) on page 158
   - Le guide de certificats Milestone

   Vous pouvez également activer le cryptage après l'installation depuis l'icône de la barre des tâches de Server Configurator dans la zone de notification de Management Server Manager.

10. Sur la page **Sélectionner l'emplacement du fichier et la langue du produit**, procédez comme suit :

    1. Dans le champ **Emplacement du fichier**, sélectionnez l'emplacement où vous souhaitez installer le logiciel.

       > Si un produit Milestone XProtect VMS est déjà installé sur l'ordinateur, ce champ est désactivé. Le champ affiche l'emplacement où sera installé le composant.

    2. Dans **Langue du produit**, sélectionnez la langue dans laquelle votre produit XProtect doit être installé.
    3. Cliquez sur **Installer**.

    Le logiciel procède maintenant à l'installation. Si Microsoft® SQL Server® Express et Microsoft IIS ne sont pas installés sur l'ordinateur, ils le seront automatiquement lors de l'installation.

11. Vous serez invité à redémarrer votre ordinateur. Après avoir redémarré votre ordinateur, un ou plusieurs messages d'avertissement Windows s'afficheront en fonction des paramètres de sécurités. Acceptez-les afin de terminer l'installation.

12. Une fois l'installation terminée, une liste s'affiche pour indiquer les composants installés sur l'ordinateur.

    Cliquez sur **Continuer** pour ajouter un matériel et des utilisateurs au système.

    > Si vous cliquez sur **Fermer** maintenant, vous passez outre l'assistant de configuration et le XProtect Management Client s'ouvre. Vous pouvez configurer le système, par exemple, ajouter du matériel informatique et des clients aux système, dans Management Client.

13. Sur la page **Saisir les noms d'utilisateur et les mots de passe du matériel**, saisissez les noms d'utilisateur et les mots de passe du matériel modifié à partir des paramètres par défaut du fabricant.

    L'assistant d'installation analysera le réseau pour ce matériel, ainsi que les identifiants spécifiques et le matériel doté des identifiants de connexion par défaut du fabricant.

    Cliquez sur **Continuer** et patientez pendant que le système analyse le matériel.

14. Sur la page **Sélectionner le matériel à ajouter au système**, sélectionnez le matériel que vous souhaitez ajouter au système. Cliquez sur **Continuer** et patientez pendant que le système ajoute le matériel.

15. Sur la page **Configurer les périphériques**, vous pouvez attribuer des noms descriptifs au matériel en cliquant sur l'icône Modifier située en regard du nom du matériel. Ce nom est ensuite préfixé aux périphériques.

    Développez les nœuds pour activer ou désactiver les appareils, tels que les caméras, les haut-parleurs et les microphones.

    > Les caméras sont activées par défaut, tandis que les haut-parleurs et les microphones sont désactivés par défaut.

    Cliquez sur **Continuer** et patientez pendant que le système configure le matériel.

16. Sur la page **Ajouter des utilisateurs**, vous pouvez ajouter des utilisateurs au système en tant qu'utilisateurs Windows ou utilisateurs de base. Les utilisateurs peuvent avoir le rôle d'administrateur ou le rôle d'opérateur.

    Définissez l'utilisateur et cliquez sur **Ajouter**.

    Lorsque vous avez fini d'ajouter les utilisateurs, cliquez sur **Continuer**.

17. Lorsque l'installation et la configuration initiale sont terminées, la page **La configuration est terminée** s'ouvre et affiche :

    - Une liste de périphériques qui sont ajoutés au système
    - Une liste d'utilisateurs qui sont ajoutés au système
    - Les adresses vers le XProtect Web Client et le client XProtect Mobile que vous pouvez partager avec vos utilisateurs

    Lorsque vous cliquez sur **Fermer**, XProtect Smart Client s'ouvre et est prêt à l'emploi.

Installer votre système - option personnalisée

L'option **Personnalisée** installe le serveur de gestion, mais vous pouvez sélectionner quels autres composants du client et du serveur vous souhaitez installer sur l'ordinateur actuel. Par défaut, la case du serveur d'enregistrement est décochée dans la liste de composants. En fonction de vos choix, vous pouvez installer les composants du système non sélectionnés sur d'autres ordinateurs par la suite. Pour plus d'informations sur chaque composant du système et leur rôle, voir Présentation générale du produit on page 36. L'installation sur les autres ordinateurs se fait via la page Internet de téléchargement du serveur de gestion intitulée Download Manager. Pour plus d'informations sur l'installation via le Download Manager, voir Download Manager/page web de téléchargement. on page 200.

> Milestone vous recommande de lire avec attention la section suivante avant de procéder à l'installation : Avant de commencer l'installation on page 148.

> En ce qui concerne les installations conformes aux normes FIPS, vous ne pouvez pas mettre à jour XProtect VMS si le mode FIPS est activé sur le système d'exploitation Windows. Avant l'installation, désactivez la politique de sécurité Windows FIPS sur tous les ordinateurs qui font partie du VMS, y compris l'ordinateur qui héberge SQL Server. Mais si vous effectuez la mise à niveau depuis la version VMS XProtect 2020 R3 ou une version ultérieure, vous n'avez pas besoin de désactiver le mode FIPS. Pour de plus amples informations sur comment configurer votre XProtect VMS pour qu'il s'exécute conformément au mode FIPS 140-2, voir la section de conformité aux normes FIPS 140-2 dans le guide de durcissement.

1. Téléchargez le fichier .iso avec le logiciel depuis Internet (https://www.milestonesys.com/download/). Lorsque vous téléchargez le fichier .iso, il sera chargé en tant que lecteur de DVD appelé « XProtect VMS Installer ».
2. Exécutez le fichier `Milestone XProtect VMS Products 2025 R2 System Installer.exe`.
3. La décompression des fichiers d'installation débute. Un ou plusieurs messages d'avertissement Windows® s'afficheront en fonction des paramètres de sécurités. Acceptez-les afin de poursuivre la décompression.
4. Lorsque vous avez terminé, l'assistant d'installation **Milestone XProtect VMS** s'affiche.
    1. 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**.
    2. Lisez le *MilestoneContrat de licence utilisateur final*. Cochez la case **J'accepte les termes du contrat de licence**, puis cliquez sur **Continuer**.
    3. Sur la page **Paramètres de confidentialité**, sélectionnez si vous souhaitez partager les données d'utilisation et cliquez sur **Continuer**.

        > Vous devez activer la collecte des données si vous souhaitez que le système possède une installation conforme au RGPD de l'UE. Pour plus d'informations sur la protection des données et la collecte des données d'utilisation, voir le Guide de confidentialité du RGPD.

        > Vous pouvez toujours modifier vos paramètres de confidentialité plus tard. Voir également Paramètres du système (boîte de dialogue Options).

5. Sélectionnez **Personnaliser**. Une liste de composants à installer apparaît. Hormis le serveur de gestion, tous les composants de la liste sont facultatifs. Le serveur d'enregistrement et le serveur mobile ne sont par défaut pas sélectionnés. Sélectionnez les composants du système que vous souhaitez installer et cliquez sur **Continuer**.

   Pour que votre système fonctionne correctement, vous devez installer au moins une instance de XProtect API Gateway.

   Dans les étapes ci-dessous, tous les composants du système sont installés. Pour un système plus distribué, n'installez que quelques composants du système sur cet ordinateur et les autres composants de système sur d'autres ordinateurs. Si vous ne reconnaissez pas une étape de l'installation, c'est sûrement dû au fait que vous n'avez pas choisi d'installer le composant du système auquel appartient cette page. Dans ce cas, passez à l'étape suivante. Voir également Installation via Download Manager (explications) on page 174, Installer le serveur d'enregistrement via Download Manager on page 175, et Installation silencieuse via un interpréteur de ligne de commande (explications) on page 187.

6. La page **Sélectionnez un site Web IIS à utiliser avec le système XProtect** ne s'affiche que si vous avez plus d'un site Web IIS disponibles sur cet ordinateur. Vous devez sélectionner le site Web à utiliser avec votre système XProtect. Sélectionnez un site Web avec un lien HTTPS. Cliquez sur **Continuer**.

   Si Microsoft® IIS n'est pas installé sur l'ordinateur, il s'installe.

7. Sur la page **Sélectionner Microsoft SQL Server**, sélectionnez le SQL Server que vous souhaitez utiliser. Voir également SQL Server options lors de l'installation personnalisée on page 173. Cliquez sur **Continuer**.

   Si SQL Server n'est pas présent sur votre ordinateur local, vous pouvez installer Microsoft SQL Server Express, mais sur un système distribué plus grand, vous utiliseriez typiquement un SQL Server dédié sur votre réseau.

8. Sur **Sélectionner une base de données** (ne s'affiche que si vous avez sélectionné un SQL Server existant), sélectionnez ou créez une base de données SQL Server pour y stocker votre configuration système. Si vous choisissez une base de données SQL Server existante, choisissez **Conserver** ou **Remplacer** les données existantes. Si vous procédez à une mise à niveau, choisissez de conserver les données existantes afin de ne pas perdre votre configuration système. Voir également SQL Server options lors de l'installation personnalisée on page 173. Cliquez sur **Continuer**.

9. Sur la page **Paramètres de la base de données**, sélectionnez soit **Laisser le programme d'installation créer ou recréer une base de données**, soit **Utiliser une base de données pré-créée**.

10. Pour que vos bases de données soient créées ou recréées automatiquement, sélectionnez **Laisser le programme d'installation créer ou recréer une base de données**, puis cliquez sur **Continuer**.
11. Pour utiliser des bases de données que vous avez configurées à cet effet ou des bases de données qui ont déjà été créées, sélectionnez **Utiliser une base de données pré-créée**. Vous verrez alors la page **Configuration avancée de la base de données**.
12. Sur la page **Configuration avancée de la base de données**, entrez le serveur et le nom de la base de données pour les composants XProtect.
13. Sélectionnez **Authentification Windows, ne pas faire confiance au certificat du serveur (recommandé)** ou **Authentification Windows, faire confiance au certificat du serveur** ou sélectionnez **Microsoft Entra Integrated, ne pas faire confiance au certificat du serveur (recommandé)**.

    Le compte à utiliser pour l'installation doit être créé dans Microsoft Entra ID ou Windows AD en fonction du type d'authentification que vous souhaitez utiliser. L'authentification multifacteur (AMF) n'est pas prise en charge pour les comptes.

    L'option **(ne pas faire confiance au certificat du serveur)** est recommandée pour l'Authentification Windows et obligatoire pour Microsoft Entra Integrated. Cela permet de s'assurer que les certificats du serveur sont validés et vérifiés avant l'installation. De plus amples informations sur les certificats de serveur non valides sont disponibles dans le fichier journal de l'installation. L'option **Authentification Windows, faire confiance au certificat du serveur** permet d'ignorer la validation des certificats du serveur.

14. Cliquez sur l'icône pour vérifier la connexion. En cliquant sur l'icône, vous validez également les certificats des serveurs.
15. Cliquez sur **Continuer**

16. Sur la page **Assigner un mot de passe de configuration système**, saisissez un mot de passe qui protégera votre configuration système. Vous en aurez besoin lorsque vous souhaiterez restaurer votre système ou bien l'étendre, par exemple, avec l'ajout de grappes.

    Il est important que vous enregistriez ce mot de passe dans un emplacement sécurisé. La perte du mot de passe pourrait vous empêcher de restaurer votre configuration système.

    Si vous ne souhaitez pas protéger votre configuration système avec un mot de passe, sélectionnez **Je choisis de ne pas utiliser de mot de passe de configuration système et je comprends que la configuration système ne sera pas cryptée**.

    Cliquez sur **Continuer**.

17. Sur la page **Assigner un mot de passe de protection des données au serveur mobile**, saisissez un mot de passe pour crypter vos enquêtes. En tant qu'administrateur de système, vous devrez saisir ce mot de passe pour accéder aux données du serveur mobile en cas de restauration du système ou en cas d'ajout de serveurs mobiles supplémentaires au système.

    Vous devez enregistrer ce mot de passe dans un emplacement sécurisé. Dans le cas contraire, vous pourriez rencontrer des difficultés pour restaurer les données du serveur mobile.

    Si vous ne souhaitez pas protéger vos enquêtes avec un mot de passe, sélectionnez **Je choisis de ne pas utiliser de mot de passe de protection pour les données du serveur mobile et je comprends que les enquêtes ne seront pas cryptées**.

    Cliquez sur **Continuer**.

18. Dans la fenêtre **Sélectionner le compte de service pour le serveur d'enregistrement**, sélectionnez soit **Ce compte prédéfini**, soit **Ce compte** pour sélectionner le compte de service pour le serveur d'enregistrement.

    Si nécessaire, saisissez un mot de passe.

    Le nom d'utilisateur du compte doit se composer d'un seul mot. Les espaces ne sont pas acceptés.

    Cliquer sur **Continuer**.

19. Sur la page **Spécifier les paramètres du serveur d’enregistrement**, spécifiez les paramètres du serveur d’enregistrement :
    1. Dans le champ **Nom du serveur d’enregistrement**, saisissez le nom du serveur d’enregistrement. Le nom par défaut est celui de l’ordinateur.
    2. Le champ **Adresse du serveur de gestion** indique l’adresse et le numéro du port du serveur de gestion : localhost:80.
    3. Dans le champ **Sélectionner l’emplacement de votre base de données médias**, sélectionnez l’emplacement où vous voulez sauvegarder votre enregistrement vidéo. Milestone vous recommande de sauvegarder vos enregistrements vidéo dans un emplacement différent de celui où vous avez installé le logiciel, et non sur le lecteur système. L’emplacement par défaut est le lecteur qui dispose du plus grand espace disponible.
    4. Dans le champ **Durée de rétention des enregistrements vidéo**, définissez la durée pendant laquelle vous souhaitez sauvegarder les enregistrements. Vous pouvez saisir une valeur comprise entre 1 et 365 000 jours, où 7 jours correspond à la durée de rétention par défaut.
    5. Cliquez sur **Continuer**.

20. Vous pouvez sécuriser les flux de communication sur la page **Choisir le cryptage** :

    - Entre les serveurs d'enregistrement, les collecteurs de données et le serveur de gestion

      Choisissez un certificat dans la rubrique **Certificat du serveur** pour activer le cryptage des flux de communication internes.

      > ⚠ Si vous cryptez la connexion du serveur d'enregistrement vers le serveur de gestion, le système exige le cryptage de la connexion du serveur de gestion aux serveurs d'enregistrement.

    - Entre les serveurs d'enregistrement et les clients

      Choisissez un certificat dans la rubrique **Certificat de flux de multimédia** pour activer le cryptage entre les serveurs d'enregistrement et les composants des clients récoltant des flux de données.

    - Entre le serveur mobile et les clients

      Choisissez un certificat dans la rubrique **Certificat des flux de média mobiles** pour activer le cryptage entre les composants des clients récoltant des flux de données depuis le serveur mobile.

    - Entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements

      Pour activer le chiffrement entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements, y compris le LPR Server, dans la section **Serveur d'événements et extensions**, sélectionnez un certificat.

    Vous pouvez utiliser le même fichier de certificat pour tous les composants du système ou utiliser différents fichiers de certificat en fonction des composants du système.

    Pour plus d'informations sur la préparation de votre système pour des communications sécurisées, voir :

    - Communication sécurisée (explications) on page 158
    - Le guide de certificats Milestone

    Vous pouvez également activer le cryptage après l'installation depuis l'icône de la barre des tâches de Server Configurator dans la zone de notification de Management Server Manager.

21. Sur la page **Sélectionnez l'emplacement du fichier et la langue du produit**, sélectionnez l'**Emplacement des fichiers** pour le fichier du programme.

    > Si un produit Milestone XProtect VMS est déjà installé sur l'ordinateur, ce champ est désactivé. Le champ affiche l'emplacement où sera installé le composant.

22. Dans le champ, **Langue du produit**, sélectionnez la langue dans laquelle votre produit XProtect doit être installé. Cliquez sur **Installer**.

    Le logiciel procède maintenant à l'installation. Au terme de l'installation, une liste des composants du système correctement installés s'affiche. Cliquez sur **Fermer**.

23. Vous serez invité à redémarrer votre ordinateur. Après avoir redémarré votre ordinateur, un ou plusieurs messages d'avertissement Windows s'afficheront en fonction des paramètres de sécurités. Acceptez-les afin de terminer l'installation.

24. Configuration de votre système dans Management Client. Voir Liste des tâches initiales de configuration on page 208.

25. En fonction de vos choix, installez les composants du système restants sur les autres ordinateurs par le biais du Download Manager. Voir Installation via Download Manager (explications) on page 174.

SQL Server options lors de l'installation personnalisée

Décider quel SQL Server et quelle base de données utiliser avec les options suivantes.

SQL Server options :

- **Installer Microsoft® SQL Server® Express sur cet ordinateur** : cette option n'est affichée que si SQL Server n'est pas installé sur l'ordinateur.
- **Utiliser le SQL Server sur cet ordinateur** : cette option n'est affichée que si SQL Server est déjà installé sur l'ordinateur
- **Sélectionner un SQL Server sur votre réseau par le biais de la recherche** : permet de rechercher toutes les installations SQL Server qui peuvent être découvertes sur le sous-réseau de votre réseau.
- **Sélectionner un SQL Server sur votre réseau** : permet de saisir l'adresse (nom d'hôte ou adresse IP) de SQL Server que la recherche ne permet pas de trouver

Options de la base de données SQL Server :

- **Créer une nouvelle base de données** : Principalement pour les nouvelles installations
- **Utiliser une base de données existante** : Principalement pour les mises à niveau des installations existantes. Milestone vous recommande de réutiliser la base de données SQL Server préexistante et d'y maintenir la base de données existante pour ne pas perdre la configuration de votre système. Vous pouvez également choisir de remplacer les données de la base de données SQL Server

Installer les nouveaux composants XProtect

Installation via Download Manager (explications)

Si vous souhaitez installer les composants du système sur d'autres ordinateurs que celui du serveur de gestion, vous devez installer ces composants du système par le biais du site Web de téléchargement de Management Server Download Manager.

1. Depuis l'ordinateur où est installé Management Server, allez sur la page Web de téléchargement Management Server. Dans le menu **Démarrer** de Windows, sélectionnez **Milestone** > **Page d'installation administrative** et notez ou copiez l'adresse Internet à des fins d'utilisation ultérieures lors de l'installation des composants du système sur les autres ordinateurs. L'adresse est généralement la suivante : *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Connexion à tous les ordinateurs pour installer un ou plusieurs autres composants du système :
   - Recording Server (Pour de plus amples informations, voir Installer le serveur d'enregistrement via Download Manager on page 175 ou Installation silencieuse d'un serveur d'enregistrement on page 188)
   - Management Client (Pour de plus amples informations, voir Installer un Management Client via Download Manager on page 175)
   - Smart Client
   - Event Server N'oubliez pas de redémarrer la passerelle API après l'installation. Si vous renommez l'ordinateur ultérieurement, vous devrez également redémarrer la passerelle API.

     > ⚠ Si vous installez Event Server dans un environnement conforme aux normes FIPS, vous devez d'abord désactivez le mode FIPS 140-2 sur Windows avant d'effectuer l'installation.

   - Log Server (Pour de plus amples informations, voir Installation silencieuse d'un serveur de journaux on page 193)
   - Mobile Server (Pour plus d'informations, voir le manuel pour XProtect Mobilele serveur)
3. Ouvrez un navigateur Internet, saisissez l'adresse de la page Web de téléchargement du Management Server dans le champ d'adresse et téléchargez l'assistant d'installation en question.
4. Exécutez l'installateur.

Voir Installer votre système - option personnalisée on page 166 en cas de doute quant aux sélections et paramètres dans les différentes étapes de l'installation.

Installer un Management Client via Download Manager

S'il existe plusieurs administrateurs du système XProtect ou si vous souhaitez simplement gérer le système XProtect à partir de plusieurs ordinateurs, vous pouvez installer le Management Client en suivant les instructions ci-dessous.

Le Management Client est toujours installé sur le serveur de gestion.

1. Depuis l'ordinateur où est installé Management Server, allez sur la page Web de téléchargement Management Server. Dans le menu **Démarrer** de Windows, sélectionnez **Milestone** > **Page d'installation administrative** et notez ou copiez l'adresse Internet à des fins d'utilisation ultérieures lors de l'installation des composants du système sur les autres ordinateurs. L'adresse est généralement la suivante : *http://[management server address]/installation/Admin/default-en-US.htm*.

   Connectez-vous à l'ordinateur où vous souhaitez installer le composant du système.
2.

1. Ouvrez un navigateur Internet et saisissez l'adresse de la page Web de téléchargement du Management Server dans le champ d'adresse et appuyez sur Entrée.
3. Cliquez sur **Toutes les langues** pour le programme d'installation Management Client. Lancez le fichier téléchargé.
4. Cliquez sur **Oui** pour tous les avertissements. La procédure de décompression commence.
5. Choisissez la langue du programme d'installation. Cliquez sur **Continuer**.
6. Lisez et acceptez le contrat de licence. Cliquez sur **Continuer**.
7. Choisissez l'emplacement du fichier et la langue du produit. Cliquez sur **Installer**.
8. L'installation est terminée. Une liste de composants correctement installés s'affiche. Cliquez sur **Fermer**.
9. Cliquez l'icône du bureau pour ouvrir le Management Client.
10. La page de connexion au Management Client s'affiche.
11. Spécifiez le nom d'hôte ou l'adresse IP de votre serveur de gestion dans le champ **Ordinateur**.
12. Sélectionnez Authentification, saisissez votre identifiant et votre mot de passe. Cliquez sur **Connexion**. Le Management Client démarre.

    Pour plus de détails sur les fonctionnalités de Management Client et sur les actions possibles avec votre système, cliquez sur **Aide** dans le menu Outils.

Installer le serveur d'enregistrement via Download Manager

Si vos composants système sont répartis sur plusieurs ordinateurs, vous pouvez installer les serveurs d'enregistrement en suivant les instructions ci-dessous.

Le serveur d'enregistrement est déjà installé si vous avez effectué une installation **Ordinateur unique**, mais vous pouvez utiliser les mêmes instructions pour ajouter de nouveaux serveurs d'enregistrement si vous avez besoin de plus de capacité.

Si vous avez besoin d'installer un serveur d'enregistrement de basculement, voir Installer un serveur d'enregistrement de basculement via Download Manager on page 183.

1. Depuis l'ordinateur où est installé Management Server, allez sur la page Web de téléchargement Management Server. Dans le menu **Démarrer** de Windows, sélectionnez **Milestone** > **Page d'installation administrative** et notez ou copiez l'adresse Internet à des fins d'utilisation ultérieures lors de l'installation des composants du système sur les autres ordinateurs. L'adresse est généralement la suivante : *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Connectez-vous à l'ordinateur où vous souhaitez installer le composant du système.
3. Ouvrez un navigateur Internet et saisissez l'adresse de la page Web de téléchargement du Management Server dans le champ d'adresse et appuyez sur Entrée.
4. Télécharger l'assistant d'installation du serveur d'enregistrement en sélectionnant **Toutes les langues** sous l'**Assistant d'installation du serveur d'enregistrement**. Sauvegardez l'installateur ou exécutez-le directement à partir de la page Web.
5. Sélectionnez la **Langue** que vous souhaitez utiliser pendant l'installation. Cliquez sur **Continuer**.
6. Sur la page **Sélectionner un type d'installation**, sélectionnez :

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

   Personnalisé : pour installer un serveur d'enregistrement avec des valeurs personnalisées.

7. Sur la page **Spécifier les paramètres du serveur d'enregistrement**, spécifiez les paramètres du serveur d'enregistrement :
    1. Dans le champ **Nom du serveur d'enregistrement**, saisissez le nom du serveur d'enregistrement. Le nom par défaut est celui de l'ordinateur.
    2. Le champ **Adresse du serveur de gestion** indique l'adresse et le numéro du port du serveur de gestion : localhost:80.
    3. Dans le champ **Sélectionner l'emplacement de votre base de données médias**, sélectionnez l'emplacement où vous voulez sauvegarder votre enregistrement vidéo. Milestone vous recommande de sauvegarder vos enregistrements vidéo dans un emplacement différent de celui où vous avez installé le logiciel, et non sur le lecteur système. L'emplacement par défaut est le lecteur qui dispose du plus grand espace disponible.
    4. Dans le champ **Durée de rétention des enregistrements vidéo**, définissez la durée pendant laquelle vous souhaitez sauvegarder les enregistrements. Vous pouvez saisir une valeur comprise entre 1 et 365 000 jours, où 7 jours correspond à la durée de rétention par défaut.
    5. Cliquez sur **Continuer**.
8. La page **Adresse IP des serveurs d'enregistrement** ne s'affiche que si vous choisissez **Personnalisée**. Précisez le nombre de serveurs d'enregistrement que vous souhaitez installer sur cet ordinateur. Cliquez sur **Continuer**.
9. Dans la fenêtre **Sélectionner le compte de service pour le serveur d'enregistrement**, sélectionnez soit **Ce compte prédéfini**, soit **Ce compte** pour sélectionner le compte de service pour le serveur d'enregistrement.

    Si nécessaire, saisissez un mot de passe.

    > Le nom d'utilisateur du compte doit se composer d'un seul mot. Les espaces ne sont pas acceptés.

    Cliquer sur **Continuer**.

10. Vous pouvez sécuriser les flux de communication sur la page **Choisir le cryptage** :

    - Entre les serveurs d'enregistrement, les collecteurs de données et le serveur de gestion

      Choisissez un certificat dans la rubrique **Certificat du serveur** pour activer le cryptage des flux de communication internes.

      > ⚠ Si vous cryptez la connexion du serveur d'enregistrement vers le serveur de gestion, le système exige le cryptage de la connexion du serveur de gestion aux serveurs d'enregistrement.

    - Entre les serveurs d'enregistrement et les clients

      Choisissez un certificat dans la rubrique **Certificat de flux de multimédia** pour activer le cryptage entre les serveurs d'enregistrement et les composants des clients récoltant des flux de données.

    - Entre le serveur mobile et les clients

      Choisissez un certificat dans la rubrique **Certificat des flux de média mobiles** pour activer le cryptage entre les composants des clients récoltant des flux de données depuis le serveur mobile.

    - Entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements

      Pour activer le chiffrement entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements, y compris le LPR Server, dans la section **Serveur d'événements et extensions**, sélectionnez un certificat.

    Vous pouvez utiliser le même fichier de certificat pour tous les composants du système ou utiliser différents fichiers de certificat en fonction des composants du système.

    Pour plus d'informations sur la préparation de votre système pour des communications sécurisées, voir :

    - Communication sécurisée (explications) on page 158
    - Le guide de certificats Milestone

    Vous pouvez également activer le cryptage après l'installation depuis l'icône de la barre des tâches de Server Configurator dans la zone de notification de Management Server Manager.

11. Sur la page **Sélectionnez l'emplacement du fichier et la langue du produit**, sélectionnez l'**Emplacement des fichiers** pour le fichier du programme.

    > Si un produit Milestone XProtect VMS est déjà installé sur l'ordinateur, ce champ est désactivé. Le champ affiche l'emplacement où sera installé le composant.

12. Dans le champ, **Langue du produit**, sélectionnez la langue dans laquelle votre produit XProtect doit être installé. Cliquez sur **Installer**.

    Le logiciel procède maintenant à l'installation. Au terme de l'installation, une liste des composants du système correctement installés s'affiche. Cliquez sur **Fermer**.

13. Une fois que vous avez installé le serveur d'enregistrement, vous pouvez vérifier son état à partir de l'icône de Recording Server Manager et le configurer dans Management Client. Pour plus d'informations, voir Liste des tâches initiales de configuration on page 208.

Installer un Management Client via Download Manager

S'il existe plusieurs administrateurs du système XProtect ou si vous souhaitez simplement gérer le système XProtect à partir de plusieurs ordinateurs, vous pouvez installer le Management Client en suivant les instructions ci-dessous.

> Le Management Client est toujours installé sur le serveur de gestion.

1. Depuis l'ordinateur où est installé Management Server, allez sur la page Web de téléchargement Management Server. Dans le menu **Démarrer** de Windows, sélectionnez **Milestone** > **Page d'installation administrative** et notez ou copiez l'adresse Internet à des fins d'utilisation ultérieures lors de l'installation des composants du système sur les autres ordinateurs. L'adresse est généralement la suivante : *http://[management server address]/installation/Admin/default-en-US.htm*.

   Connectez-vous à l'ordinateur où vous souhaitez installer le composant du système.

2.

1. Ouvrez un navigateur Internet et saisissez l'adresse de la page Web de téléchargement du Management Server dans le champ d'adresse et appuyez sur Entrée.
3. Cliquez sur **Toutes les langues** pour le programme d'installation Management Client. Lancez le fichier téléchargé.
4. Cliquez sur **Oui** pour tous les avertissements. La procédure de décompression commence.
5. Choisissez la langue du programme d'installation. Cliquez sur **Continuer**.
6. Lisez et acceptez le contrat de licence. Cliquez sur **Continuer**.
7. Choisissez l'emplacement du fichier et la langue du produit. Cliquez sur **Installer**.
8. L'installation est terminée. Une liste de composants correctement installés s'affiche. Cliquez sur **Fermer**.

9. Cliquez l'icône du bureau pour ouvrir le Management Client.
10. La page de connexion au Management Client s'affiche.
11. Spécifiez le nom d'hôte ou l'adresse IP de votre serveur de gestion dans le champ **Ordinateur**.
12. Sélectionnez Authentification, saisissez votre identifiant et votre mot de passe. Cliquez sur **Connexion**. Le Management Client démarre.

    Pour plus de détails sur les fonctionnalités de Management Client et sur les actions possibles avec votre système, cliquez sur **Aide** dans le menu Outils.

Installer le serveur d'enregistrement via Download Manager

Si vos composants système sont répartis sur plusieurs ordinateurs, vous pouvez installer les serveurs d'enregistrement en suivant les instructions ci-dessous.

Le serveur d'enregistrement est déjà installé si vous avez effectué une installation **Ordinateur unique**, mais vous pouvez utiliser les mêmes instructions pour ajouter de nouveaux serveurs d'enregistrement si vous avez besoin de plus de capacité.

Si vous avez besoin d'installer un serveur d'enregistrement de basculement, voir ????.

1. Depuis l'ordinateur où est installé Management Server, allez sur la page Web de téléchargement Management Server. Dans le menu **Démarrer** de Windows, sélectionnez **Milestone** > **Page d'installation administrative** et notez ou copiez l'adresse Internet à des fins d'utilisation ultérieures lors de l'installation des composants du système sur les autres ordinateurs. L'adresse est généralement la suivante : *http://[management server address]/installation/Admin/default-en-US.htm*.
2. Connectez-vous à l'ordinateur où vous souhaitez installer le composant du système.
3. Ouvrez un navigateur Internet et saisissez l'adresse de la page Web de téléchargement du Management Server dans le champ d'adresse et appuyez sur Entrée.
4. Télécharger l'assistant d'installation du serveur d'enregistrement en sélectionnant **Toutes les langues** sous l'**Assistant d'installation du serveur d'enregistrement**. Sauvegardez l'installateur ou exécutez-le directement à partir de la page Web.
5. Sélectionnez la **Langue** que vous souhaitez utiliser pendant l'installation. Cliquez sur **Continuer**.
6. Sur la page **Sélectionner un type d'installation**, sélectionnez :

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

   Personnalisé : pour installer un serveur d'enregistrement avec des valeurs personnalisées.

7. Sur la page **Spécifier les paramètres du serveur d'enregistrement**, spécifiez les paramètres du serveur d'enregistrement :
    1. Dans le champ **Nom du serveur d'enregistrement**, saisissez le nom du serveur d'enregistrement. Le nom par défaut est celui de l'ordinateur.
    2. Le champ **Adresse du serveur de gestion** indique l'adresse et le numéro du port du serveur de gestion : localhost:80.
    3. Dans le champ **Sélectionner l'emplacement de votre base de données médias**, sélectionnez l'emplacement où vous voulez sauvegarder votre enregistrement vidéo. Milestone vous recommande de sauvegarder vos enregistrements vidéo dans un emplacement différent de celui où vous avez installé le logiciel, et non sur le lecteur système. L'emplacement par défaut est le lecteur qui dispose du plus grand espace disponible.
    4. Dans le champ **Durée de rétention des enregistrements vidéo**, définissez la durée pendant laquelle vous souhaitez sauvegarder les enregistrements. Vous pouvez saisir une valeur comprise entre 1 et 365 000 jours, où 7 jours correspond à la durée de rétention par défaut.
    5. Cliquez sur **Continuer**.
8. La page **Adresse IP des serveurs d'enregistrement** ne s'affiche que si vous choisissez **Personnalisée**. Précisez le nombre de serveurs d'enregistrement que vous souhaitez installer sur cet ordinateur. Cliquez sur **Continuer**.
9. Dans la fenêtre **Sélectionner le compte de service pour le serveur d'enregistrement**, sélectionnez soit **Ce compte prédéfini**, soit **Ce compte** pour sélectionner le compte de service pour le serveur d'enregistrement.

    Si nécessaire, saisissez un mot de passe.

    > Le nom d'utilisateur du compte doit se composer d'un seul mot. Les espaces ne sont pas acceptés.

    Cliquer sur **Continuer**.

10. Vous pouvez sécuriser les flux de communication sur la page **Choisir le cryptage** :

    - Entre les serveurs d'enregistrement, les collecteurs de données et le serveur de gestion

      Choisissez un certificat dans la rubrique **Certificat du serveur** pour activer le cryptage des flux de communication internes.

      > ⚠ Si vous cryptez la connexion du serveur d'enregistrement vers le serveur de gestion, le système exige le cryptage de la connexion du serveur de gestion aux serveurs d'enregistrement.

    - Entre les serveurs d'enregistrement et les clients

      Choisissez un certificat dans la rubrique **Certificat de flux de multimédia** pour activer le cryptage entre les serveurs d'enregistrement et les composants des clients récoltant des flux de données.

    - Entre le serveur mobile et les clients

      Choisissez un certificat dans la rubrique **Certificat des flux de média mobiles** pour activer le cryptage entre les composants des clients récoltant des flux de données depuis le serveur mobile.

    - Entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements

      Pour activer le chiffrement entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements, y compris le LPR Server, dans la section **Serveur d'événements et extensions**, sélectionnez un certificat.

    Vous pouvez utiliser le même fichier de certificat pour tous les composants du système ou utiliser différents fichiers de certificat en fonction des composants du système.

    Pour plus d'informations sur la préparation de votre système pour des communications sécurisées, voir :

    - Communication sécurisée (explications) on page 158
    - Le guide de certificats Milestone

    Vous pouvez également activer le cryptage après l'installation depuis l'icône de la barre des tâches de Server Configurator dans la zone de notification de Management Server Manager.

11. Sur la page **Sélectionnez l'emplacement du fichier et la langue du produit**, sélectionnez l'**Emplacement des fichiers** pour le fichier du programme.

    Si un produit Milestone XProtect VMS est déjà installé sur l'ordinateur, ce champ est désactivé. Le champ affiche l'emplacement où sera installé le composant.

12. Dans le champ, **Langue du produit**, sélectionnez la langue dans laquelle votre produit XProtect doit être installé. Cliquez sur **Installer**.

    Le logiciel procède maintenant à l'installation. Au terme de l'installation, une liste des composants du système correctement installés s'affiche. Cliquez sur **Fermer**.

13. Une fois que vous avez installé le serveur d'enregistrement, vous pouvez vérifier son état à partir de l'icône de Recording Server Manager et le configurer dans Management Client. Pour plus d'informations, voir Liste des tâches initiales de configuration on page 208

Installer un serveur d'enregistrement de basculement via Download Manager

Si vous exécutez des groupes de travail, vous devez utiliser une méthode d'installation alternative pour les serveurs d'enregistrement de basculement (voir Installation pour les groupes de travail on page 198).

1. Depuis l'ordinateur où est installé Management Server, allez sur la page Web de téléchargement Management Server. Dans le menu **Démarrer** de Windows, sélectionnez **Milestone** > **Page d'installation administrative** et notez ou copiez l'adresse Internet à des fins d'utilisation ultérieures lors de l'installation des composants du système sur les autres ordinateurs. L'adresse est généralement la suivante : *http://[management server address]/installation/Admin/default-en-US.htm*.

   Connectez-vous à l'ordinateur où vous souhaitez installer le composant du système.

2. Ouvrez un navigateur Internet et saisissez l'adresse de la page Web de téléchargement du Management Server dans le champ d'adresse et appuyez sur Entrée.

3. Télécharger l'assistant d'installation du serveur d'enregistrement en sélectionnant **Toutes les langues** sous l'**Assistant d'installation du serveur d'enregistrement**. Sauvegardez l'installateur ou exécutez-le directement à partir de la page Web.
4. Sélectionnez la **Langue** que vous souhaitez utiliser pendant l'installation. Cliquez sur **Continuer**.
5. Sur la page **Sélectionner un type d'installation**, sélectionnez **Basculement** pour installer un serveur d'enregistrement en tant que serveur d'enregistrement de basculement.

6. Sur la page **Spécifier les paramètres du serveur d'enregistrement**, spécifiez les paramètres du serveur d'enregistrement. Le nom du serveur d'enregistrement de basculement, l'adresse du serveur de gestion et le chemin vers la base de données multimédia. Cliquez sur **Continuer**.
7. Sur la page **Sélectionner un compte de service pour le serveur d'enregistrement** et lors de l'installation d'un serveur d'enregistrement de basculement, vous devez utiliser le compte d'utilisateur particulier appelé **Ce compte**. Cela crée le compte d'utilisateur de basculement. Si nécessaire, saisissez un mot de passe et confirmez-le. Cliquez sur **Continuer**.

8. Vous pouvez sécuriser les flux de communication sur la page **Choisir le cryptage** :

   - Entre les serveurs d'enregistrement, les collecteurs de données et le serveur de gestion

     Choisissez un certificat dans la rubrique **Certificat du serveur** pour activer le cryptage des flux de communication internes.

     > ⚠ Si vous cryptez la connexion du serveur d'enregistrement vers le serveur de gestion, le système exige le cryptage de la connexion du serveur de gestion aux serveurs d'enregistrement.

   - Entre les serveurs d'enregistrement et les clients

     Choisissez un certificat dans la rubrique **Certificat de flux de multimédia** pour activer le cryptage entre les serveurs d'enregistrement et les composants des clients récoltant des flux de données.

   - Entre le serveur mobile et les clients

     Choisissez un certificat dans la rubrique **Certificat des flux de média mobiles** pour activer le cryptage entre les composants des clients récoltant des flux de données depuis le serveur mobile.

   - Entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements

     Pour activer le chiffrement entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements, y compris le LPR Server, dans la section **Serveur d'événements et extensions**, sélectionnez un certificat.

   Vous pouvez utiliser le même fichier de certificat pour tous les composants du système ou utiliser différents fichiers de certificat en fonction des composants du système.

   Pour plus d'informations sur la préparation de votre système pour des communications sécurisées, voir :

   - Communication sécurisée (explications) on page 158
   - Le guide de certificats Milestone

   Vous pouvez également activer le cryptage après l'installation depuis l'icône de la barre des tâches de Server Configurator dans la zone de notification de Management Server Manager.

9. Sur la page **Sélectionnez l'emplacement du fichier et la langue du produit**, sélectionnez l'**Emplacement des fichiers** pour le fichier du programme.

   Si un produit Milestone XProtect VMS est déjà installé sur l'ordinateur, ce champ est désactivé. Le champ affiche l'emplacement où sera installé le composant.

10. Dans le champ, **Langue du produit**, sélectionnez la langue dans laquelle votre produit XProtect doit être installé. Cliquez sur **Installer**.

    Le logiciel procède maintenant à l'installation. Au terme de l'installation, une liste des composants du système correctement installés s'affiche. Cliquez sur **Fermer**.

11. Une fois que vous avez installé le serveur d'enregistrement de basculement, vous pouvez vérifier son état à partir de l'icône Service de Failover Server et le configurer dans Management Client. Pour plus d'informations, voir Liste des tâches initiales de configuration on page 208.

Installer le VMS XProtect en utilisant des ports non définis par défaut

L'installation du VMS XProtect requiert l'utilisation de ports spécifiques. En particulier, le Management Server et API Gateway fonctionnent dans le/la IIS, et certains ports doivent être disponibles. Cette partie décrit comment installer le VMS XProtect et utiliser des ports non définis par défaut sur IIS. Ceci s'applique aussi lors de l'installation de API Gateway seulement.

Pour un aperçu de tous les ports utilisés pas le VMS voir le manuel de l'administrateur XProtect VMS (https://doc.milestonesys.com/fr-FR/csh?context=1111040).

Si IIS n'est pas encore installé sur le système, l'installateur du VMS XProtect installe IIS et utilise le site Web par défaut avec les ports par défaut.

Afin d'éviter le VMS XProtect par défaut, installez le IIS par défaut. En option, ajoutez un nouveau site Web ou poursuivez en utilisant le site Web par défaut.

Ajoutez un lien pour HTTPS, s'il n'existe pas déjà, et sélectionnez un certificat valide sur l'ordinateur (vous devrez le sélectionner durant l'installation du VMS XProtect). Modifiez les numéros de port sur les liens HTTP et HTTPS vers les ports de votre choix.

Lancez l'installateur du VMS XProtect et sélectionnez une installation **Personnalisée**.

Durant l'installation, la page **Sélectionner un site Web sur le/la IIS à utiliser avec votre système XProtect** apparaît s'il y a plus d'un site Web disponible. Vous devez sélectionner le site Web à utiliser avec votre système XProtect. L'installateur utilise les numéros de port changés.

Installation silencieuse via un interpréteur de ligne de commande (explications)

Avec l'installation silencieuse, les administrateurs de système peuvent installer et mettre à jour le VMS XProtect et le logiciel Smart Client sur un large réseau sans interaction de la part des utilisateurs et avec le moins de perturbations possibles pour les utilisateurs finaux.

Les installateurs du VMS XProtect et Smart Client (fichiers .exe) disposent d'arguments de ligne de commande différents. Ils ont chacun leur propre ensemble de paramètres de ligne de commande, lesquels peuvent être invoqués directement dans un interpréteur de ligne de commande ou par le biais d'un ficher Arguments. Vous pouvez également utiliser les options de ligne de commande avec les programmes d'installation dans l'interpréteur de ligne de commande.

Vous pouvez combiner les programmes d'installation de XProtect, les paramètres de ligne de commande et les options de ligne de commande avec les outils pour une distribution et une installation silencieuses de logiciel, tel que Microsoft System Center Configuration Manager (SCCM, également connu sous ConfigMgr). Pour plus d'informations concernant ces outils, rendez-vous sur le site Web du fabricant. Vous pouvez également utiliser Milestone Software Manager pour installer et mettre à jour à distance le VMS XProtect, les packs de pilotes de périphériques et Smart Client. Pour plus d'informations, voir le manuel de l'administrateur pour Milestone Software Manager.

Paramètres de ligne de commande et fichiers d'arguments

Lors de l'installation silencieuse, vous pouvez préciser les paramètres qui sont étroitement liés aux différents composants du système VMS, ainsi que leur communication interne avec les paramètres de la ligne de commande et des fichiers d'arguments. Les paramètres de la ligne de commande et les fichiers d'arguments doivent uniquement être utilisés pour les nouvelles installations car vous ne pouvez pas modifier les paramètres que les paramètres de la ligne de commande représentent lors d'une mise à jour.

Rendez-vous dans le répertoire où se trouve le programme d'installation et saisissez la commande suivante pour voir les paramètres de ligne de commande disponibles et pour générer un fichier Arguments pour un programme d'installation, dans l'interpréteur de ligne de commande :

```
[NameOfExeFile].exe --generateargsfile=[path]
```

Exemple :

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=c:\temp
```

Dans le fichier des arguments enregistrés (Arguments.xml), chaque paramètre de ligne de commande est accompagné d'une description indiquant son but. Vous pouvez modifier et enregistrer le fichier d'arguments pour que les valeurs des paramètres de la ligne de commande conviennent aux besoins de votre installation.

Lorsque vous souhaitez utiliser un fichier d'arguments, ainsi que son programme d'installation, utilisez l'option de ligne de commande `--arguments` en saisissant la commande suivante :

```
[NameOfExeFile].exe --quiet --arguments=[path]\[filename]
```

Exemple :

```
Milestone XProtect VMS Products 2025 R2 System Installer.exe --quiet
--arguments=C:\temp\arguments.xml
```

Options de ligne de commande

Vous pouvez également combiner les programmes d'installation aux options de ligne de commande dans l'interpréteur de ligne de commande. En général, les options de ligne de commande modifient le comportement d'une commande.

Rendez-vous au répertoire où se situe le programme d'installation et saisissez `[NameOfExeFile].exe --help` dans l'interpréteur de ligne de commande pour afficher la liste complète des options de la ligne de commande. Vous devez préciser une valeur pour les options de ligne de commande nécessitant une valeur afin de réussir l'installation.

Vous pouvez utiliser à la fois les paramètres de ligne de commande et les options de ligne de commande au sein d'une même commande. Utilisez l'option de ligne de commande `--parameters` et divisez chaque paramètre de ligne de commande avec deux-points (:). Dans l'exemple ci-dessous, `--quiet`, `--showconsole` et `--parameters` représentent les options de ligne de commande, et `ISFAILOVER` et `RECORDERNAME` sont les paramètres de ligne de commande :

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --showconsole
--parameters=ISFAILOVER:true:RECORDERNAME:Failover1
```

Installation silencieuse d'un serveur d'enregistrement

Lors d'une installation silencieuse, vous ne recevez pas de notifications une fois l'installation terminée. Pour recevoir des notifications, incluez l'option de ligne de commande `--showconsole` dans la commande. L'icône de la barre d'état Milestone XProtect Recording Server apparaît une fois l'installation terminée.

Dans les exemples de commandes ci-dessous, le texte figurant entre les crochets ([ ]) et les crochets eux-mêmes doivent être remplacés par des valeurs réelles. Exemple : au lieu de « [path] », `d:\record\`vous pourriez saisir `d:\program files\`, ou `\\network-storage-02\surveillance`. Utilisez l'option de ligne de commande `--help` pour en lire plus sur les formats légaux de chaque valeur d'option de ligne de commande.

1. Connectez-vous sur l'ordinateur où vous souhaitez installer le composant Recording Server.
2. Ouvrez un navigateur Internet, saisissez l'adresse de la page Web de téléchargement du Management Server destinée aux administrateurs dans le champ d'adresse et appuyez sur Entrée.

L'adresse est généralement la suivante : `http://[adresse du serveur de gestion]:[port]/installation/Admin/default-en-US.htm`.

3. Téléchargez l'assistant d'installation du serveur d'enregistrement en sélectionnant **Toutes les langues** sous **Assistant d'installation du Recording Server**.
4. Ouvrez votre interpréteur de ligne de commande préféré. Pour ouvrir Invite de commande Windows, ouvrez le menu Démarrer de Windows et saisissez **cmd**.
5. Naviguez jusqu'au répertoire contenant le ficher d'installation téléchargé.
6. Poursuivez l'installation selon l'un des deux scénarios ci-dessous :

Scénario 1 : Mettre à jour une installation existante ou en installer une sur un serveur avec le composant Management Server avec des valeurs par défaut

- Saisissez la commande suivante pour démarrer l'installation.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
```

Scénario 2 : Installer dans un système distribué

1. Saisissez la commande suivante pour générer un fichier d'arguments avec des paramètres de ligne de commande.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=[path]
```

2. Ouvrez le fichier d'arguments (Arguments.xml) à partir du chemin spécifié et modifiez les valeurs des paramètres de la ligne de commande si nécessaire.

Assurez-vous de donner aux paramètres de ligne de commande SERVERHOSTNAME et SERVERPORTdes valeurs valides. Sinon, l'installation ne peut pas se terminer.

4. Enregistrez le fichier Arguments.
5. Retournez à l'interpréteur de ligne de commande et entrez la commande ci-dessous pour installer les valeurs de paramétrage de la ligne de commande spécifiées dans le fichier Arguments.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
--arguments=[path]\[filename]
```

Installer XProtect Smart Client silencieusement

Lors d'une installation silencieuse, vous ne recevez pas de notifications une fois l'installation terminée. Pour recevoir des notifications, incluez l'option de ligne de commande `--showconsole` dans la commande. Un raccourci vers XProtect Smart Client apparaît sur le bureau une fois l'installation terminée.

Dans les exemples de commandes ci-dessous, le texte figurant entre les crochets ([ ]) et les crochets eux-mêmes doivent être remplacés par des valeurs réelles. Exemple : au lieu de « [path] », `d:\record\`vous pourriez saisir `d:\program files\`, ou `\\network-storage-02\surveillance`. Utilisez l'option de ligne de commande `--help` pour en lire plus sur les formats légaux de chaque valeur d'option de ligne de commande.

1. Ouvrez un navigateur Internet, saisissez l'adresse de la page Web de téléchargement du Management Serverdestinée aux utilisateurs finaux dans le champ d'adresse et appuyez sur Entrée.

   L'adresse est généralement la suivante : `http://[adresse du serveur de gestion]:[port]/installation/default-en-US.htm`.

2. Téléchargez le programme d'installation XProtect Smart Client en sélectionnant **Toutes les langues** sous **Programme d'installation XProtect Smart Client**.
3. Ouvrez votre interpréteur de ligne de commande préféré. Pour ouvrir Invite de commande Windows, ouvrez le menu Démarrer de Windows et saisissez **cmd**.
4. Naviguez jusqu'au répertoire contenant le ficher d'installation téléchargé.
5. Poursuivez l'installation selon l'un des deux scénarios ci-dessous :

   Scénario 1 : Mettre à jour une installation existante ou en installer une avec des valeurs de paramètres de ligne de commande par défaut

   - Saisissez la commande suivante pour démarrer l'installation.

     ```
     "Milestone XProtect Smart Client 2025 R2 Installer.exe" --quiet
     ```

   Scénario 2 : Installer des valeurs de paramètres de ligne de commande personnalisées à l'aide d'un fichier d'arguments xml comme entrée

   1. Saisissez la commande suivante pour générer un fichier d'arguments xml avec des paramètres de ligne de commande.

      ```
      "Milestone XProtect Smart Client 2025 R2 Installer.exe"
      --generateargsfile=[path]
      ```

   2. Ouvrez le fichier d'arguments (Arguments.xml) à partir du chemin spécifié et modifiez les valeurs des paramètres de la ligne de commande si nécessaire.
   3. Enregistrez le fichier Arguments.

4. Retournez à l'interpréteur de ligne de commande et entrez la commande ci-dessous pour installer les valeurs de paramétrage de la ligne de commande spécifiées dans le fichier Arguments.

```
"Milestone XProtect Smart Client 2025 R2 Installer.exe" --quiet
--arguments=[path]\[filename]
```

Installation silencieuse d'un serveur de journaux

Lors d'une installation silencieuse, vous ne recevez pas de notifications une fois l'installation terminée. Pour recevoir des notifications, incluez l'option de ligne de commande `--showconsole` dans la commande.

Dans les exemples de commandes ci-dessous, le texte figurant entre les crochets ([ ]) et les crochets eux-mêmes doivent être remplacés par des valeurs réelles. Exemple : au lieu de « [path] », `d:\record\` vous pourriez saisir `d:\program files\`, ou `\\network-storage-02\surveillance`. Utilisez l'option de ligne de commande `--help` pour en lire plus sur les formats légaux de chaque valeur d'option de ligne de commande.

1. Connectez-vous sur l'ordinateur où vous souhaitez installer le composant Log Server.
2. Ouvrez un navigateur Internet, saisissez l'adresse de la page Web de téléchargement du Management Server destinée aux administrateurs dans le champ d'adresse et appuyez sur Entrée.

   L'adresse est généralement la suivante : `http://[adresse du serveur de gestion]:[port]/installation/Admin/default-en-US.htm`.
3. Téléchargez l'assistant d'installation du serveur de journaux en sélectionnant **Toutes les langues** sous **Assistant d'installation du serveur de journaux**.
4. Ouvrez votre interpréteur de ligne de commande préféré. Pour ouvrir Invite de commande Windows, ouvrez le menu Démarrer de Windows et saisissez **cmd**.
5. Naviguez jusqu'au répertoire contenant le ficher d'installation téléchargé.
6. Poursuivez l'installation selon l'un des deux scénarios ci-dessous :

Scénario 1 : Mettre à jour une installation existante ou en installer une avec des valeurs de paramètres de ligne de commande par défaut

- Saisissez la commande suivante pour démarrer l'installation.

```
"Milestone XProtect Log Server 2025 R2 Installer.exe" --quiet
--showconsole
```

Scénario 2 : Installer des valeurs de paramètres de ligne de commande personnalisées à l'aide d'un fichier d'arguments XML comme entrée

1. Saisissez la commande suivante pour générer un fichier d'arguments xml avec des paramètres de ligne de commande.

```
"Milestone XProtect Log Server 2025 R2 Installer.exe"
--generateargsfile=[path]
```

2. Ouvrez le fichier d'arguments (Arguments.xml) à partir du chemin spécifié et modifiez les valeurs des paramètres de la ligne de commande si nécessaire.
3. Enregistrez le fichier Arguments.
4. Retournez à l'interpréteur de ligne de commande et entrez la commande ci-dessous pour installer les valeurs de paramétrage de la ligne de commande spécifiées dans le fichier Arguments.

```
"Milestone XProtect Log Server 2025 R2 Installer.exe" --quiet
--arguments=[path]\[filename] --showconsole
```

Procéder à une installation silencieuse de XProtect Smart Client

Lors d'une installation silencieuse, vous ne recevez pas de notifications une fois l'installation terminée. Pour recevoir des notifications, incluez l'option de ligne de commande `--showconsole` dans la commande. Un raccourci vers XProtect Smart Client apparaît sur le bureau une fois l'installation terminée.

Dans les exemples de commandes ci-dessous, le texte figurant entre les crochets ([ ]) et les crochets eux-mêmes doivent être remplacés par des valeurs réelles. Exemple : au lieu de « [path] », `d:\record\`vous pourriez saisir `d:\program files\`, ou `\\network-storage-02\surveillance`. Utilisez l'option de ligne de commande `--help` pour en lire plus sur les formats légaux de chaque valeur d'option de ligne de commande.

1. Ouvrez un navigateur Internet, saisissez l'adresse de la page Web de téléchargement du Management Serverdestinée aux utilisateurs finaux dans le champ d'adresse et appuyez sur Entrée.

   L'adresse est généralement la suivante : `http://[adresse du serveur de gestion]:[port]/installation/default-en-US.htm`.

2. Téléchargez le programme d'installation XProtect Smart Client en sélectionnant **Toutes les langues** sous **Programme d'installation XProtect Smart Client**.
3. Ouvrez votre interpréteur de ligne de commande préféré. Pour ouvrir Invite de commande Windows,

ouvrez le menu Démarrer de Windows et saisissez **cmd**.

4. Naviguez jusqu'au répertoire contenant le ficher d'installation téléchargé.
5. Poursuivez l'installation selon l'un des deux scénarios ci-dessous :

Scénario 1 : Mettre à jour une installation existante ou en installer une avec des valeurs de paramètres de ligne de commande par défaut

- Saisissez la commande suivante pour démarrer l'installation.

```
"Milestone XProtect Smart Client 2025 R2 Installer.exe" --quiet
```

Scénario 2 : Installer des valeurs de paramètres de ligne de commande personnalisées à l'aide d'un fichier d'arguments xml comme entrée

1. Saisissez la commande suivante pour générer un fichier d'arguments xml avec des paramètres de ligne de commande.

```
"Milestone XProtect Smart Client 2025 R2 Installer.exe"
--generateargsfile=[path]
```

2. Ouvrez le fichier d'arguments (Arguments.xml) à partir du chemin spécifié et modifiez les valeurs des paramètres de la ligne de commande si nécessaire.
3. Enregistrez le fichier Arguments.
4. Retournez à l'interpréteur de ligne de commande et entrez la commande ci-dessous pour installer les valeurs de paramétrage de la ligne de commande spécifiées dans le fichier Arguments.

```
"Milestone XProtect Smart Client 2025 R2 Installer.exe" --quiet
--arguments=[path]\[filename]
```

Installation silencieuse d'un serveur de journaux

Lors d'une installation silencieuse, vous ne recevez pas de notifications une fois l'installation terminée. Pour recevoir des notifications, incluez l'option de ligne de commande `--showconsole` dans la commande.

Dans les exemples de commandes ci-dessous, le texte figurant entre les crochets ([ ]) et les crochets eux-mêmes doivent être remplacés par des valeurs réelles. Exemple : au lieu de « [path] », `d:\record\` vous pourriez saisir `d:\program files\`, ou `\\network-storage-02\surveillance`. Utilisez l'option de ligne de commande `--help` pour en lire plus sur les formats légaux de chaque valeur d'option de ligne de commande.

1. Connectez-vous sur l'ordinateur où vous souhaitez installer le composant Log Server.
2. Ouvrez un navigateur Internet, saisissez l'adresse de la page Web de téléchargement du Management Server destinée aux administrateurs dans le champ d'adresse et appuyez sur Entrée.

   L'adresse est généralement la suivante : `http://[adresse du serveur de gestion]:[port]/installation/Admin/default-en-US.htm`.
3. Téléchargez l'assistant d'installation du serveur de journaux en sélectionnant **Toutes les langues** sous **Assistant d'installation du serveur de journaux**.
4. Ouvrez votre interpréteur de ligne de commande préféré. Pour ouvrir Invite de commande Windows, ouvrez le menu Démarrer de Windows et saisissez **cmd**.
5. Naviguez jusqu'au répertoire contenant le ficher d'installation téléchargé.
6. Poursuivez l'installation selon l'un des deux scénarios ci-dessous :

Scénario 1 : Mettre à jour une installation existante ou en installer une avec des valeurs de paramètres de ligne de commande par défaut

- Saisissez la commande suivante pour démarrer l'installation.

```
"Milestone XProtect Log Server 2025 R2 Installer.exe" --quiet
--showconsole
```

Scénario 2 : Installer des valeurs de paramètres de ligne de commande personnalisées à l'aide d'un fichier d'arguments XML comme entrée

1. Saisissez la commande suivante pour générer un fichier d'arguments xml avec des paramètres de ligne de commande.

```
"Milestone XProtect Log Server 2025 R2 Installer.exe"
--generateargsfile=[path]
```

2. Ouvrez le fichier d'arguments (Arguments.xml) à partir du chemin spécifié et modifiez les valeurs des paramètres de la ligne de commande si nécessaire.
3. Enregistrez le fichier Arguments.
4. Retournez à l'interpréteur de ligne de commande et entrez la commande ci-dessous pour installer les valeurs de paramétrage de la ligne de commande spécifiées dans le fichier Arguments.

```
"Milestone XProtect Log Server 2025 R2 Installer.exe" --quiet
--arguments=[path]\[filename] --showconsole
```

Effectuer une installation silencieuse à l'aide d'un compte de service réservé

Si vous souhaitez installer le VMS XProtect sans assistance, vous devez lancer le programme d'installation avec les arguments indiqués dans le tableau ci-dessous. Les arguments doivent être créés et enregistrés dans un fichier XML d'arguments qui sera généré avant l'installation.

Argument	Description
`--quiet`	Force une installation silencieuse.
`--arguments`	Chemin d'accès au fichier XML des arguments contenant la configuration complète. Le chemin d'accès peut être : `C:\Arguments.xml« »`.
`--license`	Chemin d'accès au fichier de licence.

Utilisation d'un compte de service réservé

Cette description est basée sur l'utilisation d'un compte de service réservé à la sécurité intégrée. Les services s'exécutent toujours sur le compte réservé, quel que soit l'utilisateur connecté, et vous devez vous assurer que ce compte dispose de toutes les autorisations nécessaires pour, par exemple, exécuter des tâches et accéder au réseau, aux fichiers et aux répertoires partagés.

Le compte de service doit être spécifié dans un fichier XML d'arguments pour les clés suivantes :

`SERVICEACCOUNT`
`SERVICEACCOUNT_NONLOC`

Le mot de passe du compte de service doit être spécifié en texte clair dans la valeur de la clé suivante :

`ENCRYPTEDPASSWORD`

Exemple : ligne de commande pour démarrer une installation en mode silencieux

```
"Milestone XProtect VMS Products 2023 R2 System Installer.exe" --quiet --
arguments=C:\Arguments.xml --license=C:\M01-C01-231-01-ABCDEF.lic
```

Exemple : fichier d'arguments basé sur l'utilisation d'un compte de service réservé

```
<?xml version="1.0" encoding="utf-8"?>
<CommandLineArguments xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="urn:milestone-systems">
  <InstallEnvironment>
    <Parameters>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>USERACCOUNT</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>domain\sampleaccount</Value>
        <Key>SERVICEACCOUNT</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>domain\sampleaccount</Value>
        <Key>SERVICEACCOUNT_NONLOC</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>sampleaccountpasswordplaintext</Value>
        <Key>ENCRYPTEDPASSWORD</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>%PROGRAMFILES%\Milestone</Value>
        <Key>TARGETDIR</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>IsXPCO</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>true</Value>
        <Key>IsDPInstaller</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>false</Value>
        <Key>LEGACY</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>yes</Value>
        <Key>SQL-KEEP-DATA</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>no</Value>
        <Key>SQL-CREATE-DATABASE</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>True</Value>
        <Key>IS_EXTERNALLY_MANAGED</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_MS</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
```

```
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_IDP;Persist
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_IDP</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_IM;Persist
Security Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_IM</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated</Value>
        <Key>SQL_CONNECTION_STRING_ES</Key>
      </KeyValueParametersOfStringString>
      <KeyValueParametersOfStringString>
        <Value>Data Source=server.database.windows.net;Initial Catalog=Surveillance_
LogServerV2;Persist Security
Info=True;TrustServerCertificate=True;Authentication=ActiveDirectoryIntegrated;Application
Name=Surveillance_LogServerV2</Value>
        <Key>SQL_CONNECTION_STRING_LOG</Key>
      </KeyValueParametersOfStringString>
    </Parameters>
  </InstallEnvironment>
</CommandLineArguments>
```

Conditions à remplir avant de procéder à l'installation :

- Le compte de service ainsi que le compte utilisé pour effectuer l'installation doivent être créés.
- Le compte de service doit être autorisé à se connecter en tant que service sur l'ordinateur où l'installation est effectuée. Voir Se connecter en tant que service.
- Les bases de données à utiliser par XProtect doivent être créées et nommées dans le fichier XML des arguments, par exemple :

Nom de la base de données
Surveillance
Surveillance_IDP
Surveillance_IM
Surveillance_LogServerV2

- Les bases de données doivent être configurées selon la liste suivante :

Configuration de la base de données
Le collationnement par défaut doit être réglé sur « `SQL_Latin1_General_CP1_CI_AS` »
`ALLOW_SNAPSHOT_ISOLATION` doit être réglé sur `ON`
`READ_COMMITTED_SNAPSHOT` doit être réglé sur `ON`

- Une connexion au serveur SQL doit être créée pour le compte de service et pour le compte utilisé pour effectuer l'installation dans chacune des bases de données. Un utilisateur de base de données doit être créé dans chacune des bases de données, et l'utilisateur doit être membre du rôle db_owner sur chaque base de données.

Installation pour les groupes de travail

Si vous utilisez une configuration de groupe de travail au lieu d'une configuration de domaine avec un serveur Active Directory, effectuez les étapes suivantes lors de l'installation.

> Tous les ordinateurs d'une configuration distribuée doivent être dans un domaine ou dans un groupe de travail.

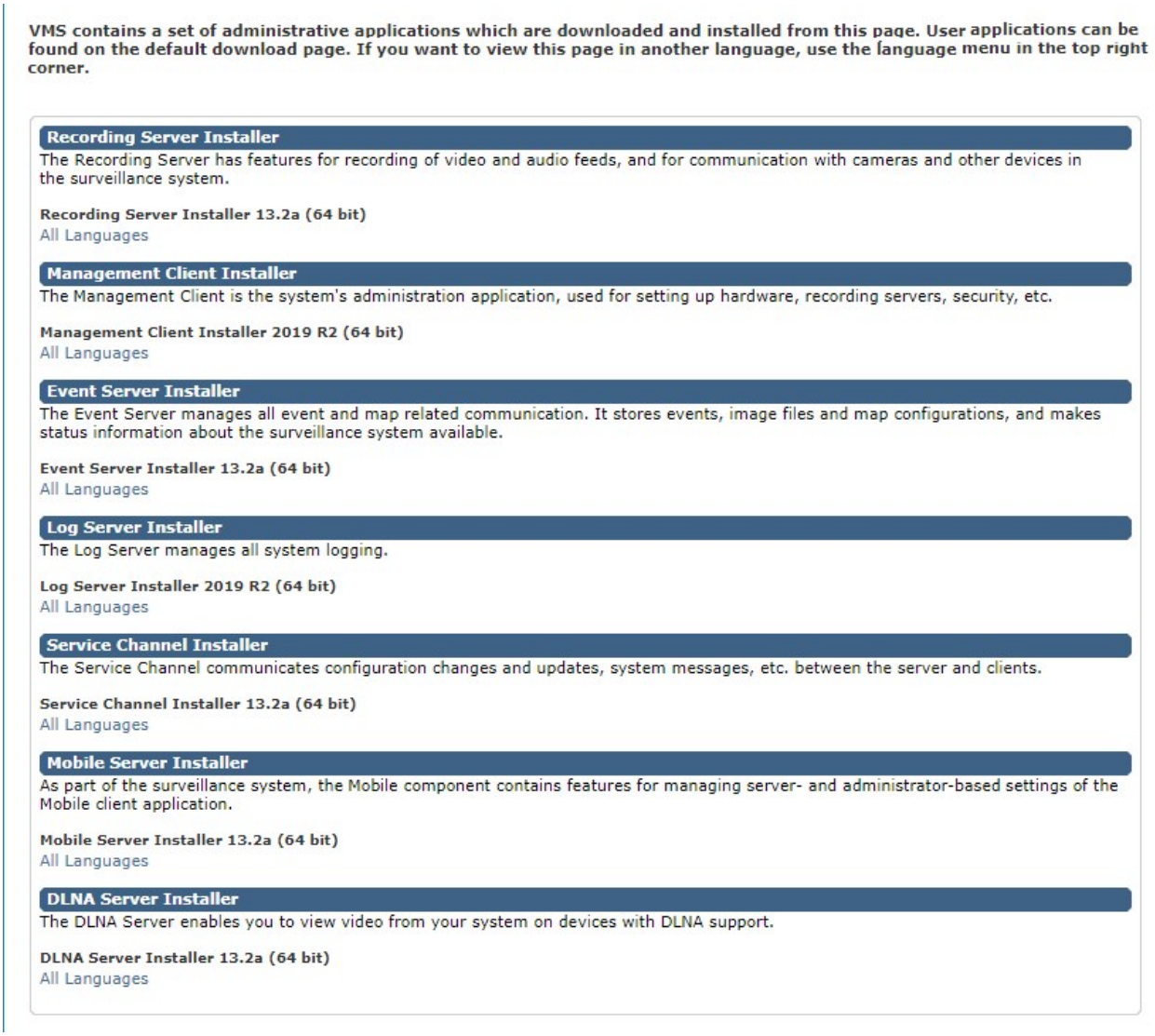
1. Connectez-vous à Windows. Le compte utilisateur que vous utilisez ici sera ajouté au rôle d'administrateur XProtect pendant l'installation.

   > 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 2e étape, choisissez d'installer le service Management Server ou Recording Server à l'aide d'un compte 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 à l'aide du même compte système.

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 par défaut dans une version de langue correspondant 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/

  L'[adresse du 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.

- 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/

  L'[adresse du 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.

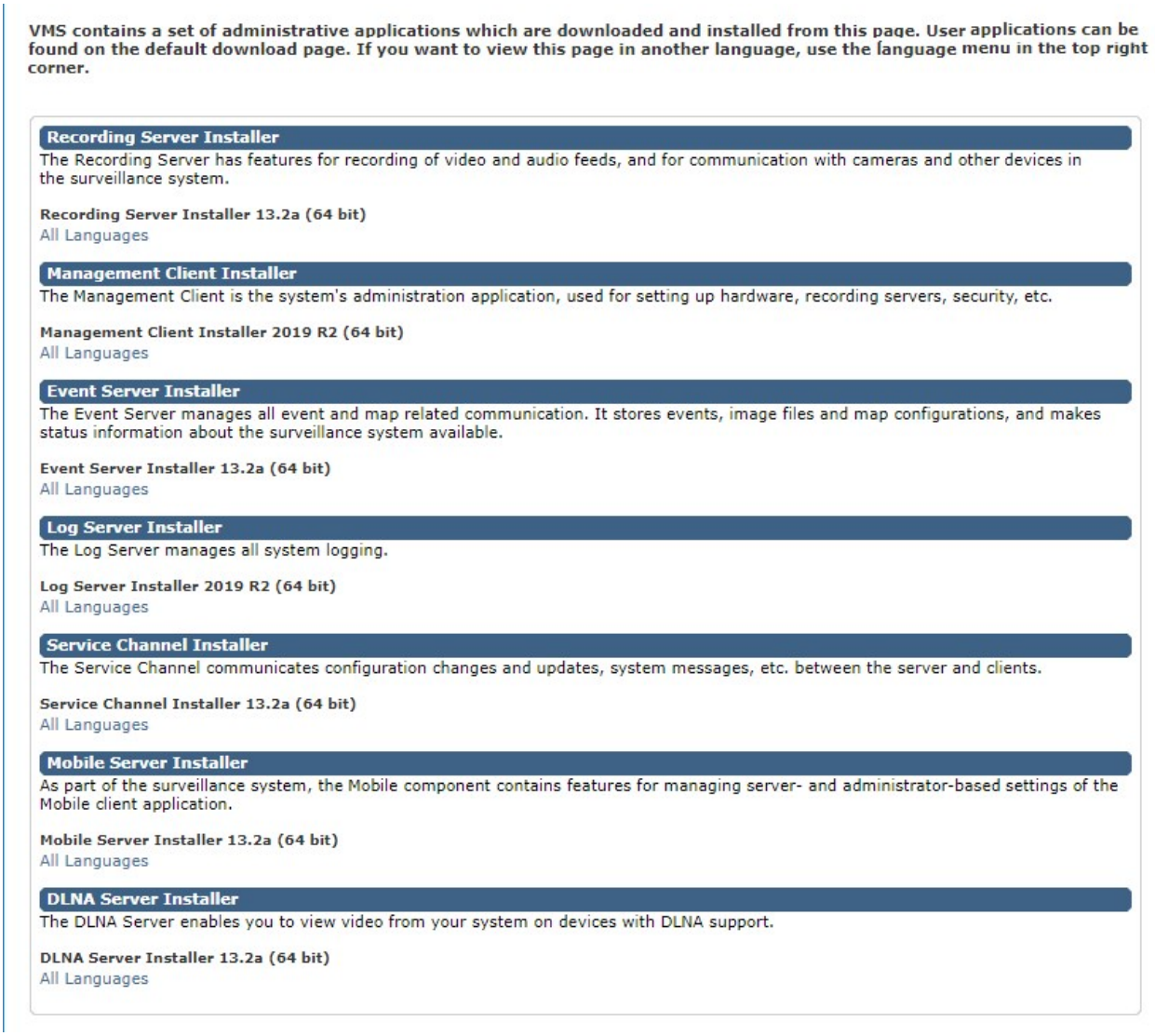
Les deux pages Web contiennent des contenus par défaut et peuvent ainsi être utilisées immédiatement après l'installation. Cependant, en tant qu'administrateur, vous pouvez personnaliser les éléments apparaissant sur les pages Web à l'aide du Download Manager. Vous pouvez également déplacer des composants 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 Download Manager vous permet de contrôler les composants que les utilisateurs peuvent télécharger et installer, il n'est pas possible de l'utiliser comme outil de gestion des autorisations des utilisateurs. Ces autorisations sont déterminées par les rôles définis dans le Management Client.

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

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 par défaut dans une version de langue correspondant 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/

  L'[adresse du 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.

- 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/

  L'[adresse du 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 contiennent des contenus par défaut et peuvent ainsi être utilisées immédiatement après l'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.

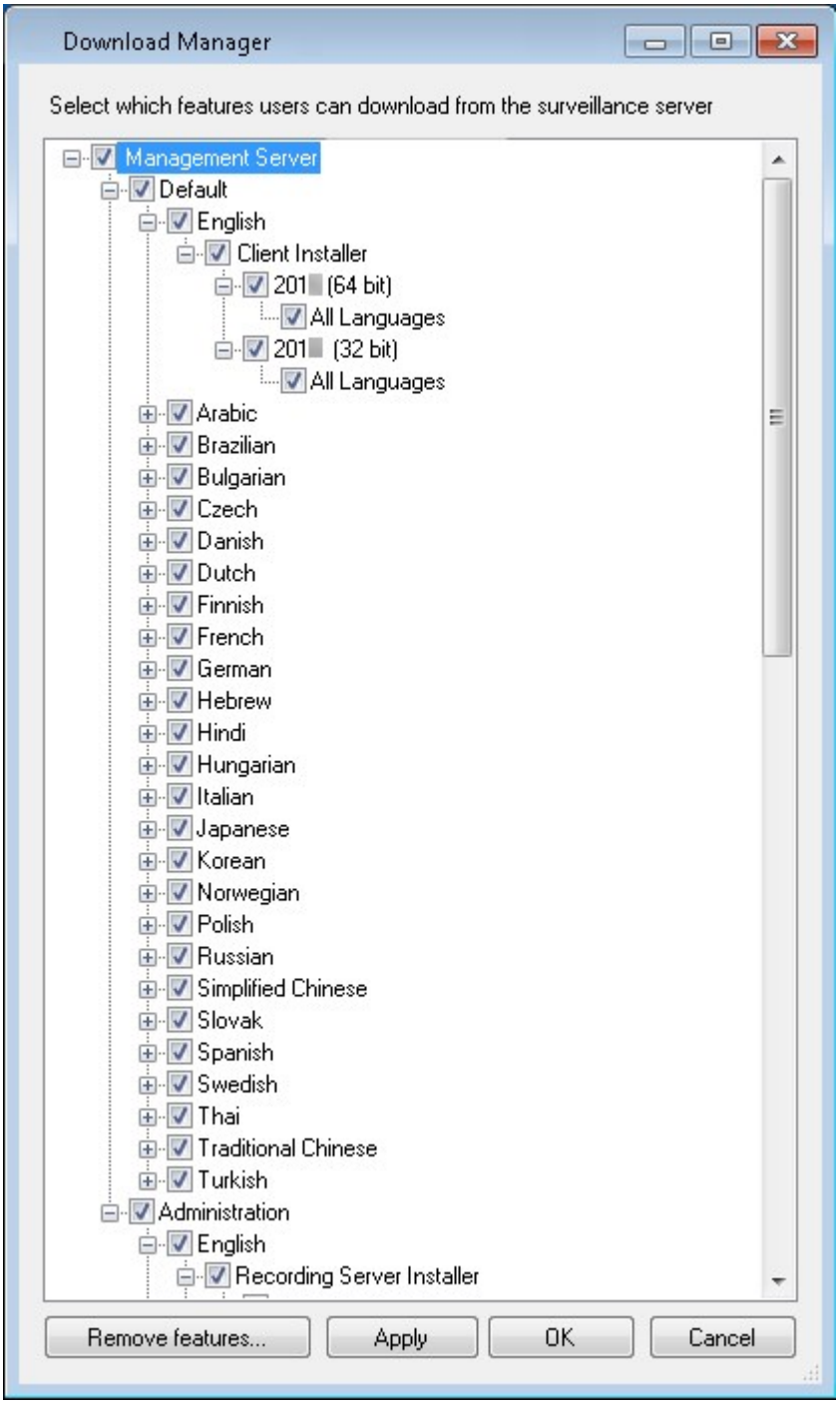
Même si Download Manager vous permet de contrôler les composants que les utilisateurs peuvent télécharger et installer, il n'est pas possible de l'utiliser comme outil de gestion des autorisations des utilisateurs. Ces autorisations sont déterminées par les rôles définis dans le Management Client.

Sur le serveur de gestion, vous pouvez accéder à la 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 institution 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 basculement. Les serveurs d'enregistrement de basculement 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 basculement.
- 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
- Serveur XProtect Mobile
- De plus amples options peuvent être disponibles pour votre entreprise.

Pour l'installation des packs de pilotes de périphériques, voir Installateur de pack de pilotes de périphériques - doit être téléchargé on page 206.

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.

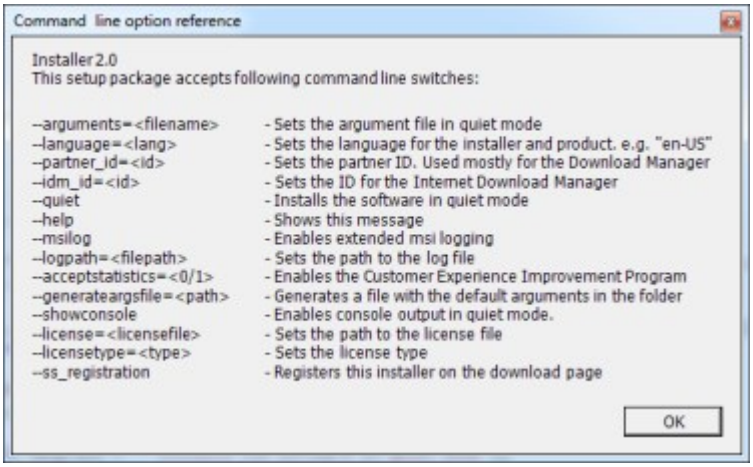
Ajouter de nouveaux fichiers/des fichiers non standard sur le Download Manager :

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

   Exemple : *MilestoneXProtectRecordingServerInstaller_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]*--help* 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.

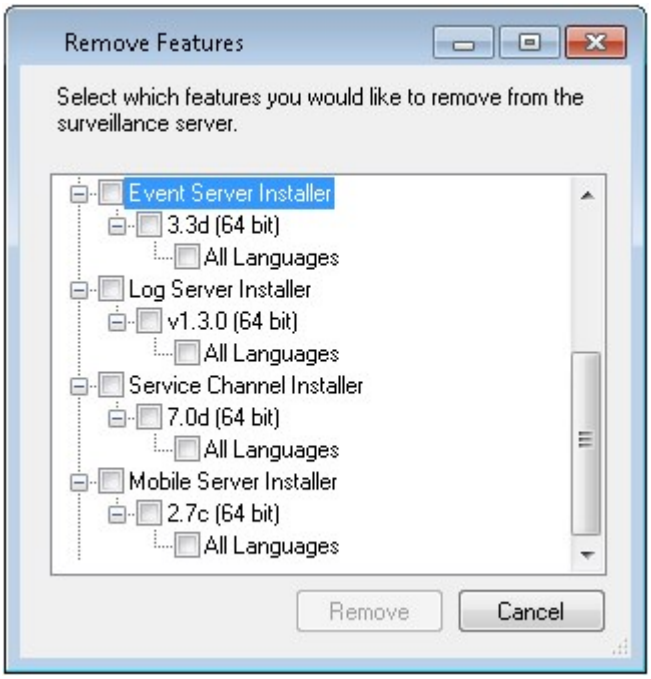
Masquer/supprimer les composants de l'installateur Download Manager

Trois options s'offrent à vous :

- **Masquer des composants** depuis la page Web en décochant des cases de l'arborescence de 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 des fonctionnalités**.
    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 pack de pilotes de périphériques - doit être téléchargé

Le pack de pilotes de périphériques inclus dans votre installation d'origine n'est pas inclus sur le Download Manager. Ainsi, si vous devez réinstaller le pack de pilotes de périphériques ou mettre l'installateur de pack de pilotes de périphériques à disposition, vous devez tout d'abord ajouter ou publier le tout dernier installateur de pack de pilotes de périphériques sur le Download Manager en procédant comme suit :

1. Profitez des tout dernier pack de pilotes de périphériques régulier sur la page de téléchargement du site Internet Milestone(https://www.milestonesys.com/download/).
2. Vous pourrez également y télécharger le pack de pilotes de périphériques hérités avec des pilotes plus anciens. Pour vérifier si vos caméras utilisent des pilotes du pack de pilotes de périphériques hérités, rendez-vous sur ce site Internet (https://www.milestonesys.com/support/software/device-packs/).
3. 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 pack de pilotes de périphériques.

Fichiers journaux de l'installation et dépannage

Lors d'une installation, mise à jour ou désinstallation, les entrées de journal sont écrites dans plusieurs fichiers journaux de l'installation : Dans le fichier journal de l'installation principal `installer.log` et dans les fichiers journaux appartenant aux différents composants du système que vous installez. Toutes les entrées de journal ont un horodatage et les entrées de journal les plus récentes se situent à la fin des fichiers journaux.

Vous pouvez localiser toutes les entrées des journaux de l'installation dans le dossier `C:\ProgramData\Milestone\Installer\`. Les fichiers journaux nommées *I.log ou *I[integer].log concernent les nouvelles installations ou mises à jour, alors que les fichiers journaux nommés *U.log ou *U[integer].log portent sur les installations. Si vous avez acheté un serveur avec un système XProtect déjà installé via un partenaire Milestone, il se peut qu'il en contienne aucun fichier journal de l'installation.

Les fichiers journaux contiennent des informations concernant les paramètres de ligne de commande et les options de ligne de commande, ainsi que leurs valeurs utilisées lors d'une installation, mise à jour ou désinstallation. Pour localiser les paramètres de ligne de commande figurant dans les fichiers journaux, recherchez **Command Line:** ou **Parameter '** selon le fichier journal.

Pour le dépannage, le fichier journal d'installation principal installer.log est le premier endroit où chercher. Les exceptions, erreurs ou avertissements survenant au cours de l'installation sont journalisées. Essayez de rechercher une **exception**, **error**, ou un **warning**. « Code de sortie : 0 » signifie que l'installation a réussi et Code de sortie : 1 », son échec. Vos conclusions dans les fichiers journaux peuvent vous permettre de trouver une solution dans la Milestone Base de connaissances. Sinon, contactez votre partenaire Milestone et partagez-lui les fichiers journaux de l'installation concernés.

Configuration

Liste des tâches initiales de configuration

La liste de contrôle ci-dessous répertorie les tâches initiales pour la configuration de votre système. Vous pouvez avoir déjà terminé certaines d'entre elles lors de l'installation.

Effectuer tous ces contrôles ne garantit pas en soi que le système soit parfaitement adapté aux besoins de votre institution. Pour que le système soit adapté aux besoins de votre institution, 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.

Étape	Description
☑	Vous avez terminé l'installation initiale de votre système. Voir Installer un nouveau système XProtect on page 160.
☑	Changer le SLC d'essai au profit d'un SLC permanent (si nécessaire). Voir Changer le code de licence du logiciel on page 138.
☑	Connectez-vous au Management Client. Voir Se connecter (explications) on page 32.
☐	Vérifier que les paramètres de stockage de chaque serveur d'enregistrement répondent à vos besoins. Voir Stockage et archivage (explications) on page 64.
☐	Vérifier que les paramètres d'archivage de chaque serveur d'enregistrement répondent à vos besoins. Voir Propriétés des paramètres de stockage et d'enregistrement on page 451.

Étape	Description
☐	Détecter les périphériques, caméras et encodeurs vidéo, qui peuvent être ajoutés à chaque serveur d'enregistrement. Voir Ajouter un matériel on page 231.
☐	Configurer les caméras individuelles de chaque serveur d'enregistrement. Voir Caméras (noeud Périphériques) on page 472.
☐	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 on page 215.
☐	Activer et configurer des périphériques. Voir Périphériques (noeud Périphériques) on page 468.
☐	Les règles déterminent largement le comportement du système. Vous créez des règles pour définir à quel moment les caméras doivent enregistrer, à quel moment les caméras PTZ (pan-tilt-zoom) doivent patrouiller et à quel moment les notifications doivent être envoyées. Créer des règles. Voir Règles et événements (explications) on page 88.
☐	Ajouter des rôles au système. Voir Rôles et autorisations d'un rôle (explications) on page 78.
☐	Ajouter des utilisateurs ou des groupes d'utilisateurs à chacun des rôles. Voir Assigner et supprimer des utilisateurs et groupes aux/des rôles on page 310.
☐	Activer des licences. Voir Activation des licences en ligne on page 136 ou Activation des licences hors ligne on page 136.

Pour plus d'informations sur comment configurer le système dans le volet **Navigation du site**, voir Volet Navigation du site on page 413.

Serveurs d'enregistrement

Changer ou vérifier la configuration de base du 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 ou changez, par exemple, les paramètres suivants :
   - **Serveur de gestion** : **Adresse** : Spécifiez l'adresse IP ou le nom d'hôte du serveur de gestion auquel le serveur d'enregistrement devrait être connecté.
   - **Serveur de gestion** : **Port** : Spécifiez le numéro de port à utiliser lors de la communication avec le serveur de gestion. Vous pouvez le modifier si nécessaire, mais le numéro de port doit toujours correspondre au numéro de port configuré sur le serveur de gestion. Voir Ports utilisés par le système on page 108.
   - **Serveur d'enregistrement** : **Port du serveur Web** : Spécifiez le numéro de port à utiliser lors de la communication avec le serveur Web du serveur d'enregistrement. Voir Ports utilisés par le système on page 108.
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**.

> ⚠ 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.

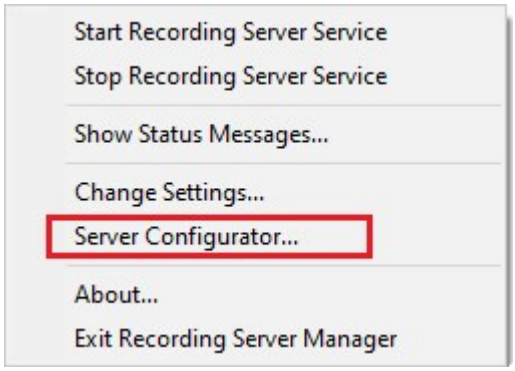
Enregistrer un serveur d'enregistrement

Lors de l'installation d'un serveur d'enregistrement, cet enregistrement est automatiquement accordé la plupart du temps. Toutefois, vous avez besoin de procéder à l'enregistrement manuellement, si :

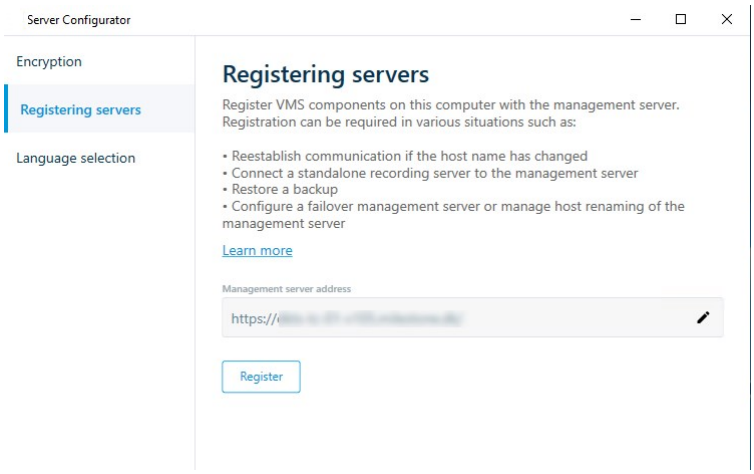
- Vous avez remplacé un serveur d'enregistrement
- Le serveur d'enregistrement a été installé hors ligne, puis ajouté par la suite au serveur de gestion
- Votre serveur de gestion n'utilise pas les ports par défaut. Les numéros de ports dépendent de la configuration du cryptage. Pour plus d'informations, voir Ports utilisés par le système on page 108
- Un enregistrement automatique a échoué, par exemple, après avoir changé l'adresse du serveur de gestion, après avoir modifié le nom de l'ordinateur du serveur d'enregistrement ou bien après avoir activé ou désactivé les paramètres du cryptage des communications. Pour plus d'informations sur le changement de l'adresse du serveur de gestion, voir Changer le nom d'hôte sur l'ordinateur du serveur de gestion.

Lorsque vous enregistrez un serveur d'enregistrement, vous le configurez pour qu'il se connecte à votre serveur de gestion. La partie du serveur de gestion qui gère les enregistrements est le service Authorization Server.

1. Ouvrez le Server Configurator depuis le menu Démarrer de Windows ou depuis l'icône de la barre des tâches du serveur d'enregistrement.



2. Dans le Server Configurator, sélectionnez **Enregistrement des serveurs**.



3. Vérifiez l'adresse du serveur de gestion et le modèle (http ou https) que vous souhaitez connecter aux serveurs de l'ordinateur, puis cliquez sur **Enregistrer**.

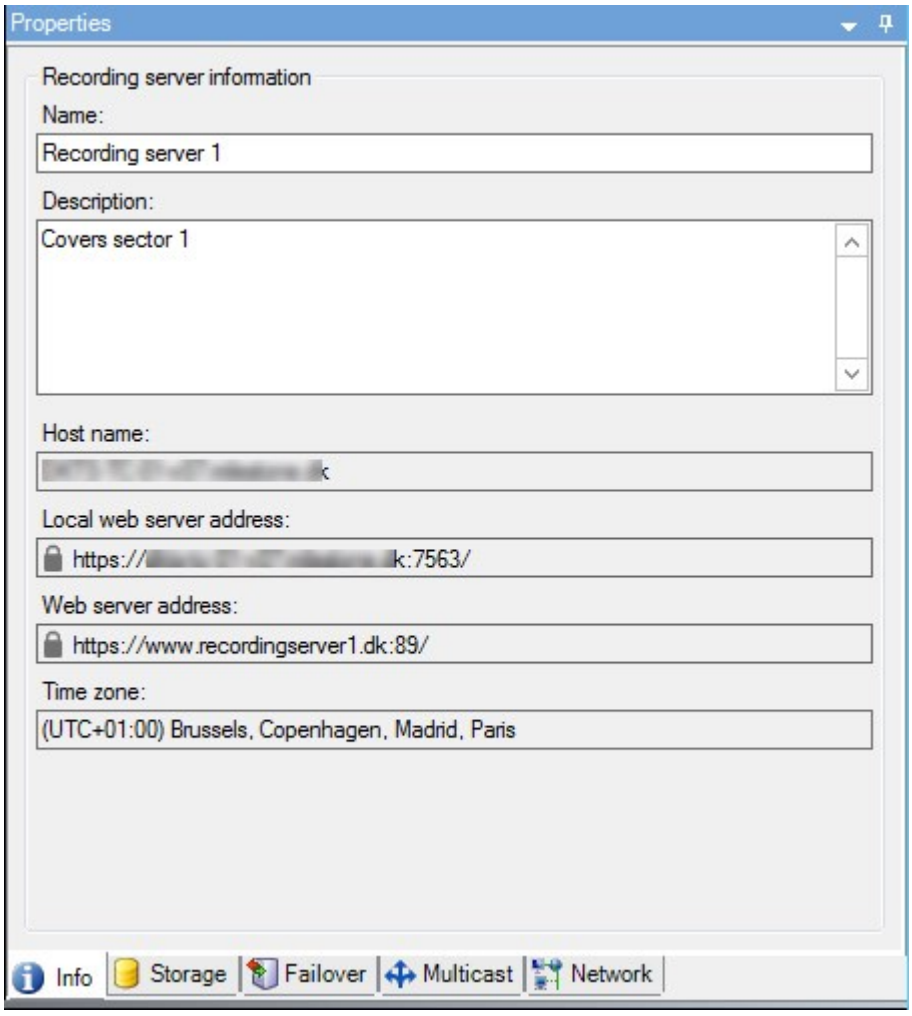
Un message de confirmation s'affiche, indiquant le succès de l'enregistrement sur le serveur de gestion.

Voir également Remplacer un serveur d'enregistrement on page 366.

Voir le status du cryptage vers les clients

Pour vérifier si votre serveur d'enregistrement crypte les connexions :

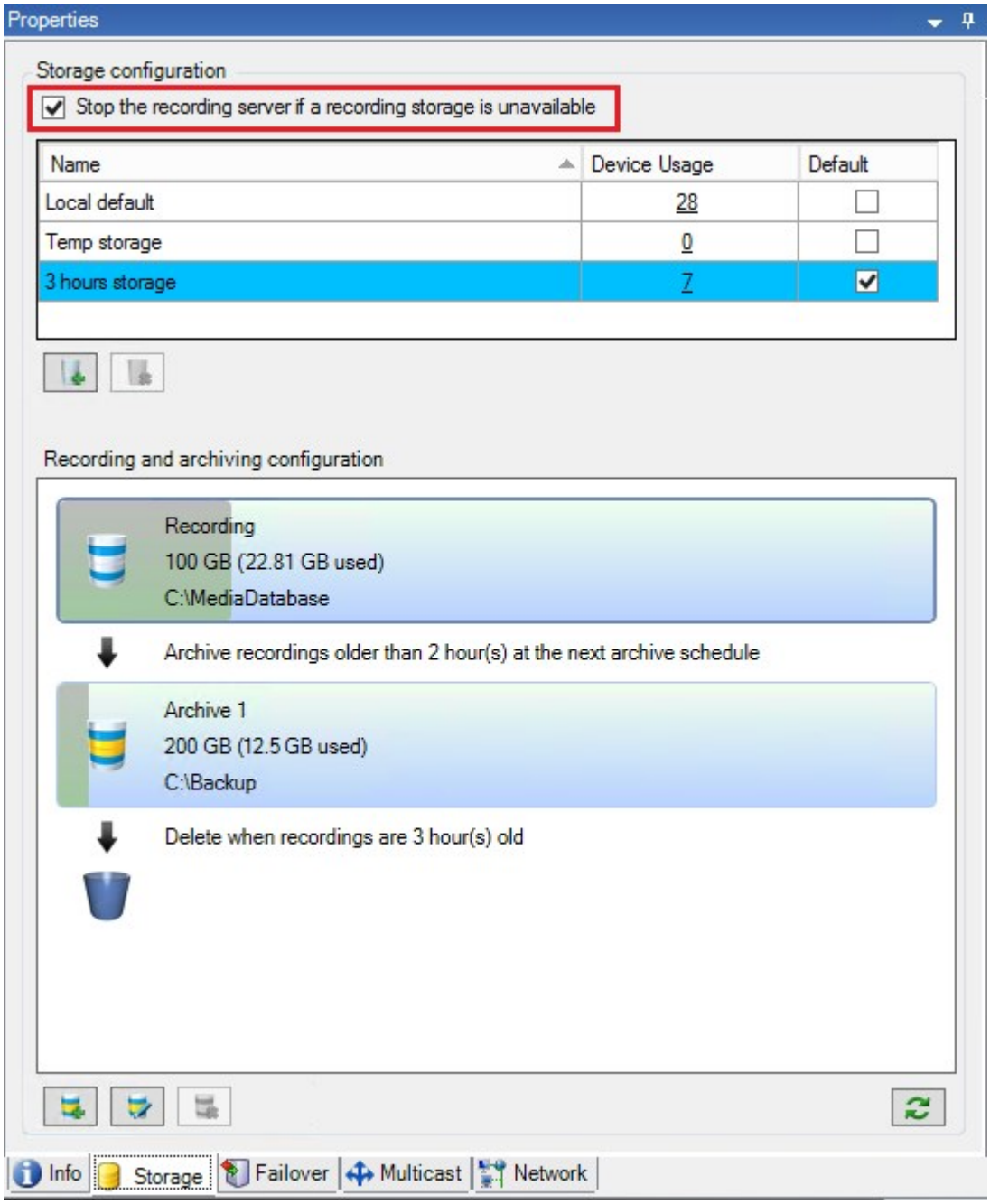
1. Ouvrez le Management Client.
2. Dans le panneau **Navigation du site**, sélectionnez **Serveurs** > **Serveurs d'enregistrement**. Cette commande ouvre une liste de serveurs d'enregistrement.
3. Dans le volet **Vue d'ensemble**, sélectionnez le serveur d'enregistrement concerné, puis allez sur l'onglet **Info**.
   Si le cryptage est activé vers les clients et serveurs récupérant des flux de données depuis le serveur d'enregistrement, une icône représentant un cadenas apparaîtra devant l'adresse du serveur Web local et l'adresse du serveur Web optionnel.



Spécifier le comportement lorsque le stockage des enregistrements n’est pas disponible

Par défaut, le serveur d’enregistrement continue de fonctionner si le stockage des enregistrements n’est plus disponible. Si votre système est configuré avec des serveurs d’enregistrement de basculement, vous pouvez spécifier le serveur d’enregistrement pour arrêter l’exécution, pour que les serveurs de basculement prennent le relais :

1. Sur le serveur d’enregistrement concerné, allez sur l’onglet **Stockage**.
2. Sélectionnez l’option **Arrêter le serveur d’enregistrement en cas d’indisponibilité d’un stockage d’enregistrement**.



Ajouter un nouvel emplacement de stockage

Lorsque vous ajoutez un nouveau stockage, vous créez toujours un stockage d'enregistrement avec une base de données d'enregistrement prédéfinie appelée **Enregistrement**. Vous ne pouvez pas renommer la base de données. Hormis le stockage d'enregistrement, un 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 concernés (voir Propriétés des paramètres de stockage et d'enregistrement on page 451).
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.

Créer une archive dans un emplacement de stockage

Un emplacement de stockage n'a pas d'archive(s) par défaut, mais vous pouvez les créer.

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 on page 453).
4. Cliquez sur **OK**.

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

Une fois qu'un stockage est configuré pour un serveur d'enregistrement, vous pouvez l'activer pour des périphériques individuels tels que des caméras, microphones 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.

Périphériques désactivés

Tous les périphériques, y compris les périphériques désactivés, sont affichés par défaut dans le volet **Vue d'ensemble**.

Pour masquer les périphériques désactivés, en haut du panneau **Vue d'ensemble**, cliquez sur **Filtrer** pour ouvrir l'onglet **Filtrer** et sélectionnez **Masquer les périphériques désactivés**.

Pour afficher à nouveau les périphériques désactivés, désactivez l'option **Masquer les périphériques désactivés**.

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.

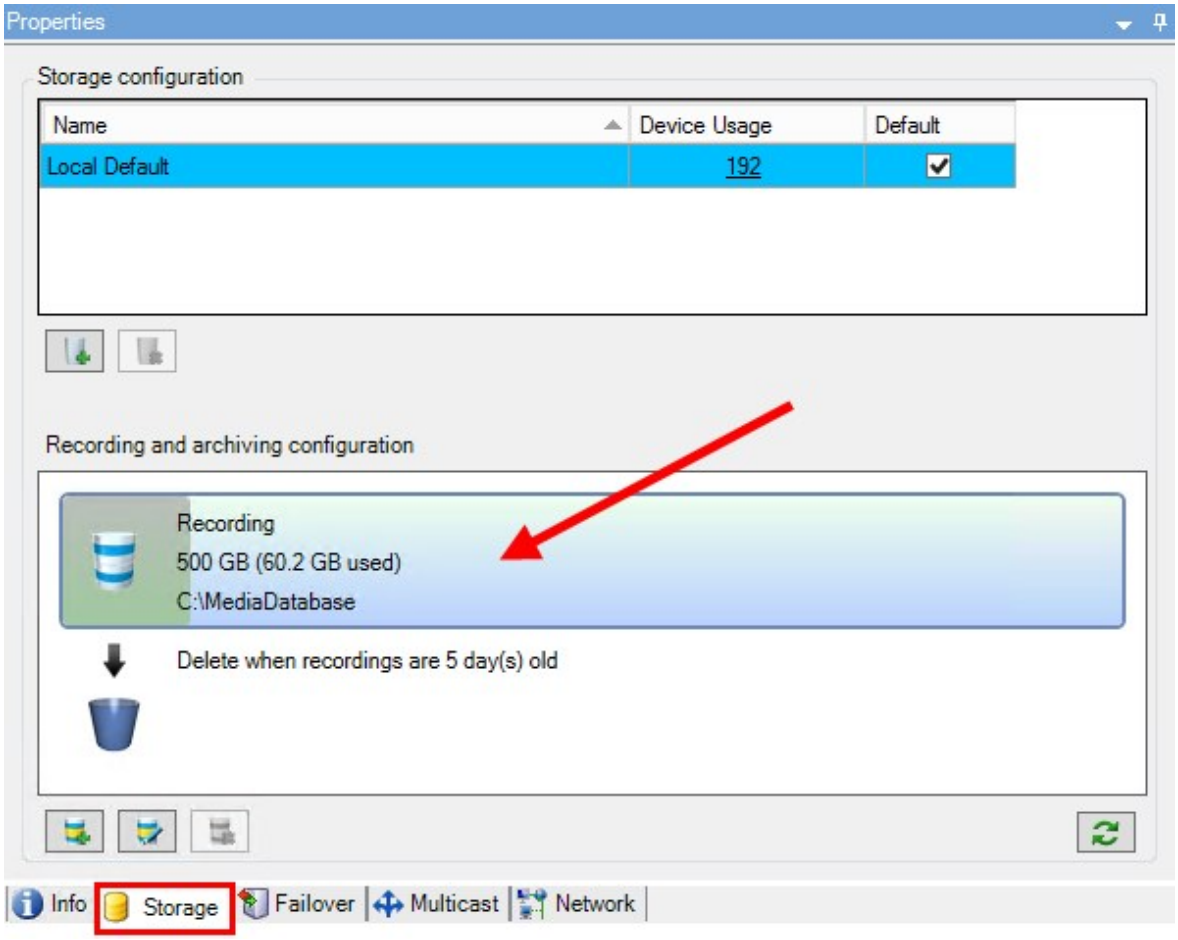
Activer la signature numérique à des fins d'export

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Vous pouvez activer la signature numérique pour la vidéo enregistrée, de sorte que les utilisateurs du client puissent vérifier que la vidéo enregistrée n'a pas été falsifiée depuis son enregistrement. La vérification de l'authenticité de la vidéo est une tâche que l'utilisateur peut effectuer dans XProtect Smart Client – Player une fois que la vidéo a été exportée.

La signature doit également être activée dans l'onglet XProtect Smart Client > **Exportations** > **Paramètres d'exportation** > **Format de XProtect** > **Inclure la signature numérique**. Autrement, le bouton **Vérifier les signatures** dans XProtect Smart Client – Player ne s'affiche pas.

1. Dans le panneau **Navigation du site**, développez le nœud **Serveurs**.
2. Cliquez sur **Serveurs d'enregistrement**.
3. Dans le volet de vue d'ensemble, cliquez sur le serveur d'enregistrement sur lequel vous souhaitez activer la signature.
4. En bas du panneau **Propriétés**, cliquez sur l'onglet **Stockage**.



5. Dans la rubrique **Configuration de l'enregistrement et de l'archivage**, double-cliquez sur la barre horizontale représentant la base de données d'enregistrement. La fenêtre **Paramètres de stockage et d'enregistrement** apparaît.
6. Cochez la case **Signature**.
7. Cliquez sur **OK**.

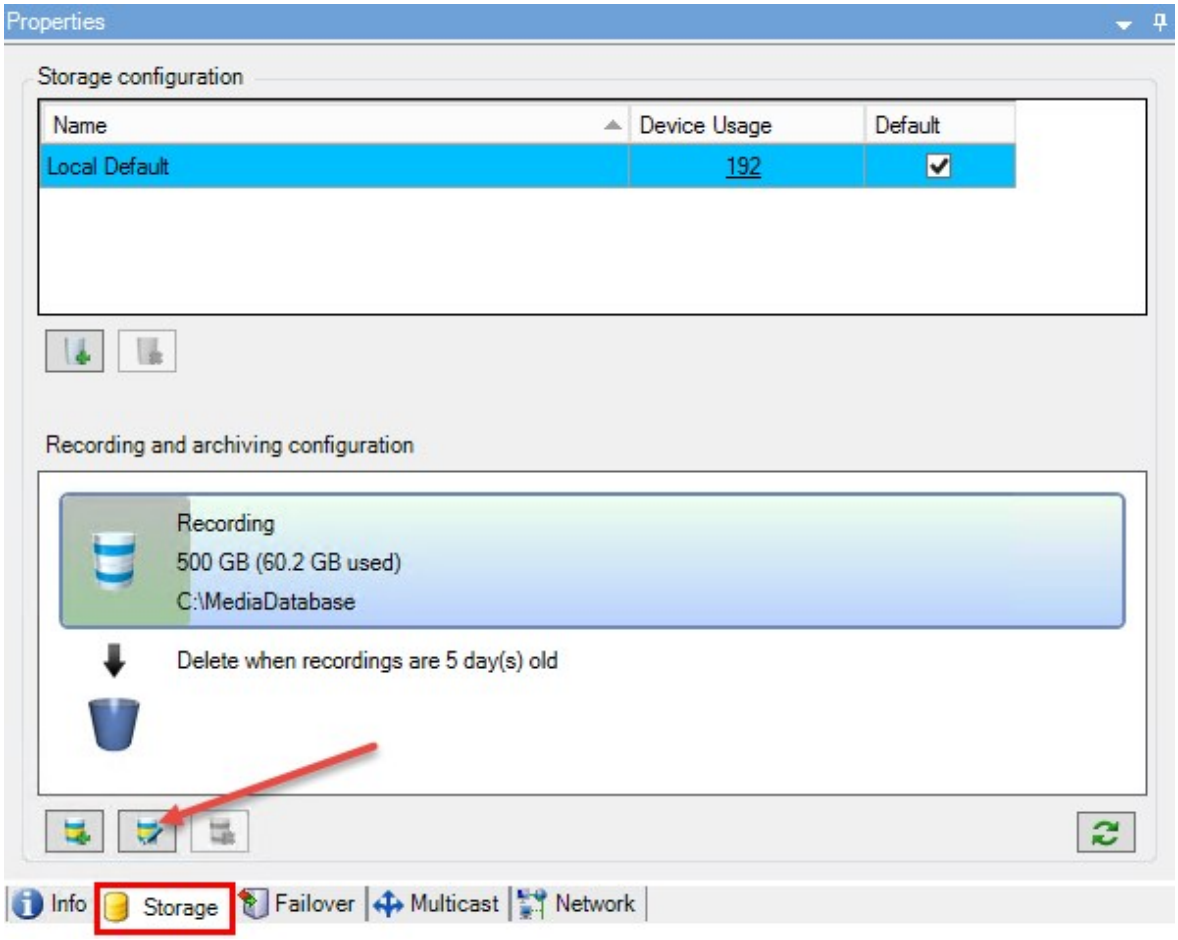
Cryptez vos enregistrements

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

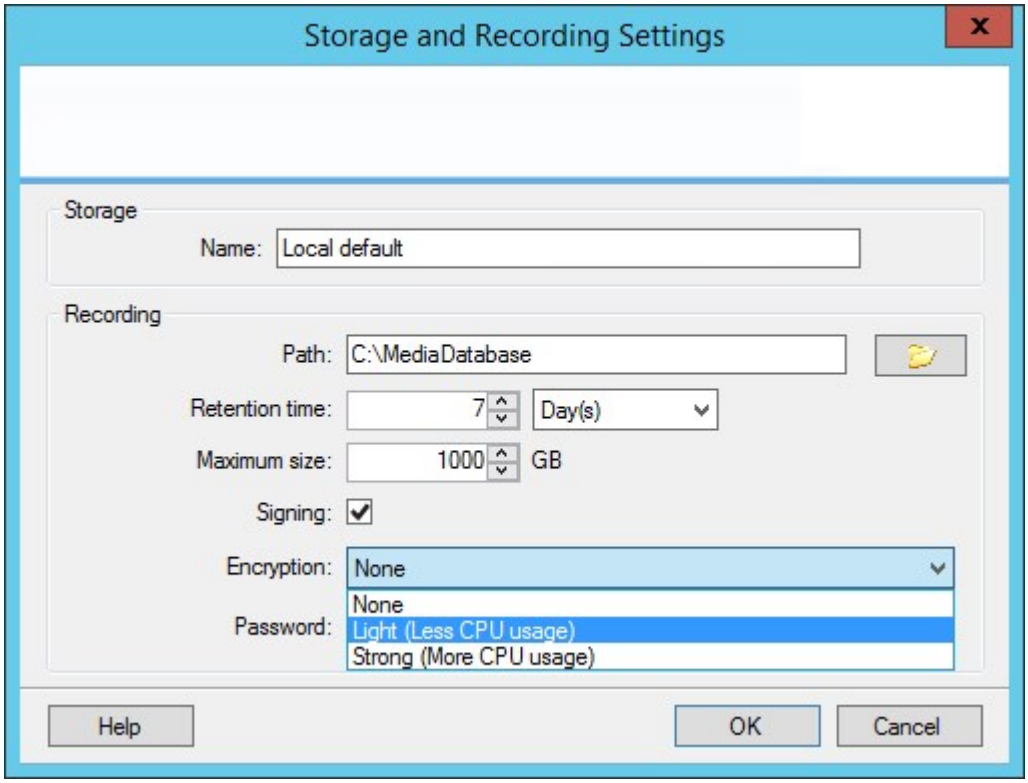
Vous avez la possibilité de sécuriser vos enregistrements en activant le cryptage dans l'option stockage et archives de vos serveurs d'enregistrement. Vous pouvez choisir entre un cryptage faible et un cryptage fort. En activant le cryptage, vous devez également spécifier un mot de passe ci-dessous.

Le fait d'activer ou de modifier les paramètres de cryptage ou le mot de passe peut éventuellement prendre du temps, en fonction de la taille de la base de données et de la performance du lecteur. Vous pouvez suivre la progression dans **Tâches en cours**. **N'arrêtez pas** l'enregistrement du serveur d'enregistrement lorsque cette tâche est en cours.

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



2. Dans la fenêtre de dialogue qui s'affiche, indiquez le niveau de cryptage.



3. Vous êtes automatiquement redirigé vers la boîte de dialogue **Définir un mot de passe**. Saisissez un mot de passe et cliquez sur **OK**.

Sauvegarde des enregistrements archivés

De nombreuses institutions 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**.

Pour vous assurer que l'archivage ne se produit pas pendant la sauvegarde, vous pouvez démonter l'archive, effectuer la sauvegarde, puis remonter l'archive. Le montage et le démontage des archives s'effectuent via le API Gateway.

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 important de connaître votre structure de sous-répertoires (voir Structure des archives (explication) on page 69 si vous souhaitez sauvegarder vos enregistrements archivés (voir Sauvegarde et restauration de la configuration système on page 354).

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**.

   > Pour les archives non disponibles, par exemple les archives hors ligne, il n'est pas possible de vérifier si l'archive contient des médias avec protection des preuves, mais l'archive peut être supprimée sur confirmation de l'utilisateur.

   > Les archives (archives en ligne) qui contiennent des médias avec protection des preuves ne peuvent pas être supprimées.

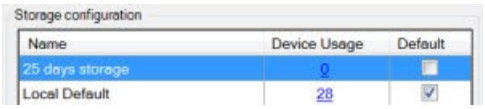
Suppression d'un espace de stockage

Vous ne pouvez pas supprimer le ou les stockages par défaut utilisés par les dispositifs comme stockage des enregistrements pour les enregistrements en direct.
Cela signifie que vous pourriez avoir besoin de déplacer des périphériques (voir Déplacer du matériel on page 367) et tout autre enregistrements non archivé vers un autre stockage avant de supprimer le stockage.

1. Pour consulter la liste des périphériques qui utilisent cet emplacement 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 dans Déplacer les enregistrements non archivés d'un espace de stockage à un autre on page 222.
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**.

Assigner des serveurs d'enregistrement de basculement

Dans l'onglet **Basculement** d'un serveur d'enregistrement, vous pouvez choisir parmi trois types de configurations de basculement :

- Pas de configuration de basculement
- Une configuration de basculement primaire/secondaire (veille à froid)
- 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 basculement secondaire. En cas d'indisponibilité du serveur d'enregistrement, un serveur d'enregistrement de basculement du groupe de basculement primaire prend le relais. Si vous avez également sélectionné un groupe de basculement secondaire, un serveur d'enregistrement de basculement du groupe secondaire prend le relais si tous les serveurs d'enregistrement de basculement du groupe de basculement 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 basculement des groupes de basculement primaire et secondaire sont occupés.

1. Dans le panneau **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 **Basculement**.
3. Pour choisir le type de configuration de basculement, faites votre choix parmi :
   - **Aucun**
   - **Groupe de serveurs de basculement primaire / Groupe de serveurs de basculement secondaire**
   - **Serveur de basculement à affectation unique**

   Vous ne pouvez pas choisir le même groupe de basculement comme groupe de basculement primaire et secondaire ni sélectionner des serveurs de basculement ordinaires qui font déjà partie d'un groupe de basculement en tant que serveurs de basculement à affectation unique.
4. Ensuite, cliquez sur **Paramètres de basculement avancés**. Ceci ouvre la fenêtre **Paramètres de basculement avancés**, qui répertorie tous les périphériques rattachés au serveur d'enregistrement sélectionné. Si vous avez sélectionné **Aucun**, les Paramètres de basculement avancés sont disponibles. Toute sélection est conservée pour toute configuration de basculement ultérieure.
5. Afin de spécifier le niveau d'assistance de basculement, sélectionnez **Basculement complet**, **Uniquement en direct** ou **Désactivé** pour chaque périphérique de la liste. Cliquez sur **OK**.
6. Dans le champ **Port de communication du service de basculement (TCP)**, modifiez le numéro de port si nécessaire.

Si vous activez l'assistance de basculement et que le serveur est configuré pour continuer à fonctionner en cas d'indisponibilité d'un stockage d'enregistrement, le serveur d'enregistrement de basculement ne prendra pas le relais. Pour que l'assistance de basculement fonctionne, vous devez sélectionner l'option **Arrêter le serveur d'enregistrement en cas d'indisponibilité d'un stockage d'enregistrement** sous l'onglet **Stockage**.

Activez le multicast pour le serveur d'enregistrement

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.

Les flux de multidiffusion ne sont pas cryptés, même si le serveur d'enregistrement utilise le cryptage.

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.

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 dadresses IP complète pour le multicast est déjà en cours dutilisation sur un ou plusieurs serveurs denregistrement, vous devez libérer tout dabord certaines adresses IP multicast avant de pouvoir activer le multicast sur des serveurs denregistrement supplémentaires.

Les flux de multidiffusion ne sont pas cryptés, même si le serveur d'enregistrement utilise le cryptage.

Activation du multicast pour des caméras individuelles

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

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 ces étapes pour toutes les caméras pertinentes.

Les flux de multidiffusion ne sont pas cryptés, même si le serveur d'enregistrement utilise le cryptage.

Définition de l'adresse publique et du port

Si vous avez besoin d'accéder au VMS avec XProtect Smart Client sur un réseau public ou non approuvé, Milestone vous recommande d'utiliser une connexion sécurisée via le VPN. Ceci vous permet de vous assurer que la communication entre XProtect Smart Client et le serveur VMS est protégée.

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

Pourquoi utiliser une adresse publique ?

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 à Internet, le système de surveillance doit répondre avec l'adresse publique du serveur d'enregistrement. C'est l'adresse du pare-feu ou du routeur NAT (Network Address Translation), et souvent aussi un autre numéro de port. L'adresse et le port peuvent ensuite être redirigés à l'adresse locale et au port du serveur.

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**

Filtrer l'arborescence de périphériques

L'arborescence de périphériques dans le panneau **Vue d'ensemble** peut devenir extrêmement large si vous avez de nombreux périphériques enregistrés. Vous pouvez appliquer des filtres à l'arborescence de périphériques afin de localiser plus facilement les périphériques avec lesquels vous souhaitez travailler.

En fournissant des conditions de filtres qui sont uniques à quelques-uns des périphériques, vous pouvez choisir d'afficher uniquement les périphériques en question.

Filtrer l'arborescence de périphériques

- En haut du panneau **Vue d'ensemble**, cliquez sur **Filtres** pour ouvrir l'onglet de **Filtres**.
- Dans le champ **Saisir du texte ici pour trier vos périphériques**, saisissez un ou plusieurs critères de filtrage et cliquez sur **Appliquer les filtres** pour filtrer la liste de périphériques.

Caractéristiques des critères de filtrage

Les critères de filtrage sont appliqués au nom du périphérique, au nom raccourci du périphérique, à l'adresse du matériel (IP), à l'ID du périphérique et aux valeurs de champ de l'ID du matériel.

Les résultats de recherche partiels ne sont pas affichés lorsque vous filtrez par ID de matériel et de valeurs de champ d'identifiant de périphérique. En conséquence, vous devez définir le numéro d'identification complet et exact lorsque vous triez par ID de matériel et de périphérique.

Des résultats de recherche partiels sont affichés pour le nom du périphérique, le nom raccourci du périphérique et les valeurs des champs des adresses de matériel, alors le terme « camér » affichera tous les périphériques qui contiennent le mot « caméra » dans le nom du périphérique.

> Les critères de filtrage ne sont pas sensibles à la casse. L'utilisation de « caméra » ou « Caméra » en tant que critère de recherche produira les mêmes résultats.

Spécification de plusieurs critères de recherche

Vous pouvez spécifier plusieurs critères de recherche et affiner votre recherche dans l'arborescence des périphériques. Une fois le filtre appliqué, tous les critères de recherche sont considérés comme co-joints avec un ET, ce qui signifie qu'ils sont cumulatifs.

Par exemple, si vous avez saisi deux critères de recherche : « Caméra » et « Entrepôt », la liste affichera tous les périphériques qui contiennent les mots « Caméra » et « Entrepôt » dans le nom du périphérique, mais n'affichera pas les périphériques qui contiennent les mots « Caméra » et « Parking » dans le nom du périphérique et n'affichera pas non plus les périphériques qui contiennent uniquement le mot « Caméra » dans le nom du périphérique.

Supprimez chaque filtre individuel du champ des filtres pour élargir la recherche si vous avez spécifié un critère trop restreint. Le filtre est automatiquement appliqué à l'arborescence des périphériques lorsque vous supprimez certains critères de recherche.

Réinitialisation du filtre

Si vous supprimez le critère de recherche du champ des filtres, le panneau **Vue d'ensemble** sera réinitialisé et affichera tous les périphériques à nouveau.

> Si le Management Client est redémarré, les critères de filtrage seront également réinitialisés.

Périphériques désactivés

Tous les périphériques, y compris les périphériques désactivés, sont affichés par défaut dans le volet **Vue d'ensemble**.

Pour masquer les périphériques désactivés, en haut du panneau **Vue d'ensemble**, cliquez sur **Filtrer** pour ouvrir l'onglet **Filtrer** et sélectionnez **Masquer les périphériques désactivés**.

Pour afficher à nouveau les périphériques désactivés, désactivez l'option **Masquer les périphériques désactivés**.

Serveurs d'enregistrement de basculement

Configurer et activer des serveurs d'enregistrement de basculement

> ⚠ Si vous avez désactivé le serveur d'enregistrement de basculement, 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 basculement et modifier ses propriétés de base :

1. Dans le panneau **Navigation du site**, sélectionnez **Serveurs** > **Serveurs de basculement**. Ceci ouvre une liste des serveurs d'enregistrement de basculement et des groupes de basculement installés.
2. Dans le volet **Vue d'ensemble**, sélectionnez le serveur d'enregistrement de basculement requis.
3. Faites un clic droit et sélectionnez **Activé**. Le serveur d'enregistrement de basculement est maintenant activé.
4. Pour modifier les propriétés du serveur d'enregistrement de basculement, 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 basculement. 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.
6. Dans le panneau **Navigation du site**, sélectionnez **Serveurs** > **Serveurs d'enregistrement**. Sélectionnez le serveur d'enregistrement pour lequel vous voulez l'assistance de basculement et attribuez-lui les serveurs d'enregistrement de basculement (voir Onglet Basculement (serveur d'enregistrement) on page 455).

Pour voir l'état d'un serveur d'enregistrement de basculement, placez votre souris sur l'icône de la barre d'état du Failover Recording Server Manager dans la zone de notification. Une infobulle apparaît. Celle-ci contient le texte saisi dans le champ Description du serveur d'enregistrement de basculement. Cela peut vous aider à déterminer le serveur d'enregistrement duquel le serveur d'enregistrement de basculement est censé prendre le relais.

Serveurs d'enregistrement de basculement groupes pour une veille à froid

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

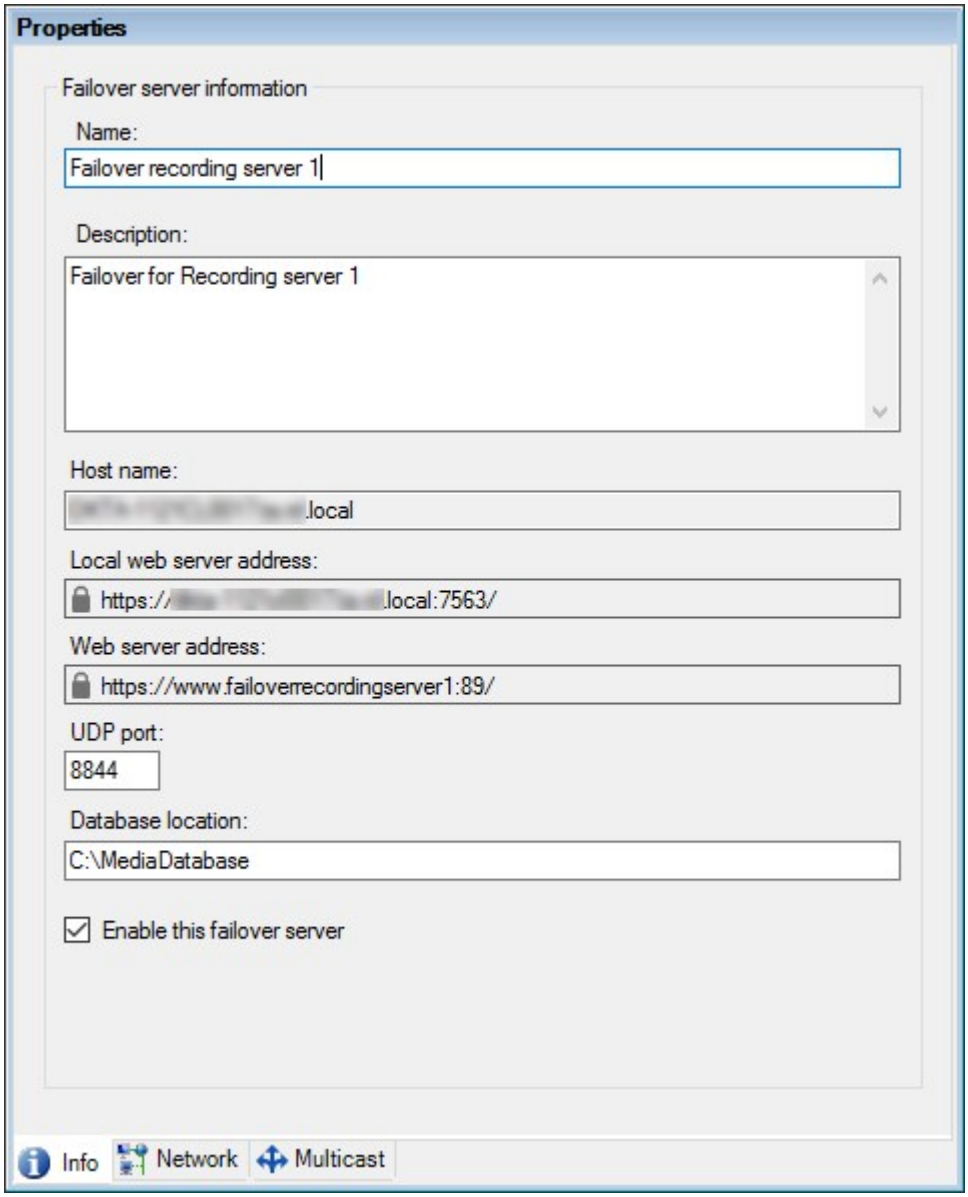
4. Faites un clic droit sur le groupe (*Groupe de basculement 1*) que vous venez de créer. Sélectionnez **Modifier les membres du groupe**. La fenêtre **Sélectionner les membres du groupe** s'ouvre.
5. Utilisez les boutons ou votre souris pour déplacer le(s) serveur(s) d'enregistrement de redondance du côté gauche au côté droit. Cliquez sur **OK**. Le(s) serveur(s) d'enregistrement de redondance appartiennent maintenant au groupe (*Groupe de basculement 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 basculement ordinaires dans le groupe.

Voir le cryptage sur un serveur d'enregistrement de basculement

Pour vérifier si votre serveur d'enregistrement de basculement utilise le cryptage, suivez les étapes suivantes :

1. Dans le panneau **Navigation du site**, sélectionnez **Serveurs** > **Serveurs de basculement**. Cette commande ouvre une liste de serveurs d'enregistrement.
2. Dans le volet **Vue d'ensemble**, sélectionnez le serveur d'enregistrement concerné, puis allez sur l'onglet **Info**.
   Si le cryptage est activé vers les clients et serveurs récupérant des flux de données depuis le serveur d'enregistrement, une icône représentant un cadenas apparaîtra devant l'adresse du serveur Web local

et l'adresse du serveur Web optionnel.



Voir les messages d'état

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

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 basculement, faites un clic droit sur l'icône **Service Milestone Failover Recording Server**.
2. Sélectionnez **À propos**.
3. Une petite boîte de dialogue s'ouvre. Elle affiche la version exacte de votre **Service Failover Recording Server**.

Matériel

Ajouter un matériel

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

> ⚠ 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 panneau **Vue d'ensemble**.

> ⚠ Certains matériels doivent être préconfigurés lorsque vous ajoutez le matériel pour la première fois. Un assistant **Préconfigurer les périphériques matériels** apparaîtra lorsque vous ajouterez ledit matériel. Voir Configuration matérielle (explications) on page 60 pour plus d'informations.

Ajouter un matériel (boîte de dialogue)

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 ou un module E/S.
- Un serveur d'enregistrement sur un site distant dans une configuration Milestone Interconnect

Pour plus d'informations sur comment ajouter un matériel à votre système, voir Ajouter un matériel on page 231.

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. Pour ajouter les matériels HTTP et HTTPS, exécutez la détection **Express** en ayant coché l'option **HTTPS (Sécurisé)**, puis en ayant coché l'option **HTTP (Non sécurisé)**.
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. Ceci n'est pas nécessaire si votre matériel utilise 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.
Manuel	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

Nom	Description
	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 un 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.

Modifier le matériel

Effectuez un clic droit sur le matériel ajouté et sélectionnez **Modifier le matériel** pour modifier la configuration du réseau et les paramètres d'authentification de l'utilisateur du matériel dans Management Client.

Modifier un matériel (boîte de dialogue)

Pour certains matériels, la boîte de dialogue **Modifier le matériel** vous permet également d'appliquer les paramètres directement sur le matériel.

Si le bouton radio **Modifier les paramètres de Management Client** est sélectionné, la boîte de dialogue **Modifier le matériel** affiche les paramètres qu'utilisent Management Client pour se connecter au matériel. Pour vous assurez que le matériel est correctement ajouté au système, entrez les paramètres que vous avez utilisés pour vous connecter à l'interface de configuration du matériel du fabriquant :

Nom	Description
Nom	Affiche le nom du matériel, ainsi que son adresse IP détectée (entre parenthèses).
URL du matériel	L'adresse Web de l'interface de configuration du matériel du fabriquant, contient en général l'adresse IP du matériel. Spécifiez une adresse valide dans votre réseau.
Nom d'utilisateur	Le nom d'utilisateur utilisé pour se connecter au matériel. ⚠ Le nom d'utilisateur saisi ici ne modifie pas le nom d'utilisateur sur le périphérique matériel actuel. Sélectionnez le bouton radio **Modifier les paramètres de Management Client et du matériel** pour modifier les paramètres des périphériques pris en charge.
Mot de passe	Le mot de passe utilisé pour se connecter au matériel. ⚠ Le mot de passe saisi ici ne modifie pas le mot de passe sur le périphérique matériel actuel. Sélectionnez le bouton radio **Modifier les paramètres de Management Client et du matériel** pour modifier les paramètres des périphériques pris en charge. ✓ Pour des informations sur comment modifier les mots de passe sur plusieurs périphériques matériels, voir Modifier les mots de passe sur les périphériques on page 239. En tant qu'administrateur du système, vous devez donner aux autres utilisateurs la permission de voir le mot de passe dans le Management Client. Pour plus d'informations, voir Paramètre des rôles sous Matériel.

Si le bouton radio **Modifier les paramètres du Management Client et du matériel** est sélectionné (pour le matériel pris en charge), la boîte de dialogue **Modifier le matériel** affiche les paramètres, qui sont également appliqués directement au matériel :

⚠ L'application des paramètres avec ce bouton radio sélectionné remplacera les paramètres actuels sur le matériel. Le matériel perdra momentanément sa connexion au serveur d'enregistrement lors de l'application des paramètres.

Nom	Description
Nom	Affiche le nom du matériel, ainsi que son adresse IP détectée (entre parenthèses).
Configuration du réseau	Les paramètres du réseau sur le matériel. Pour ajuster les paramètres réseau, sélectionnez Configuration on page 235.
Configuration	Spécifiez le protocole Internet (pour les périphériques matériels pris en charge) via la liste déroulante **Version IP**. • Pour IPv4, les valeurs doivent être au format : **(0-999).(0-999).(0-999).(0-999)** • Pour IPv6, les valeurs doivent être au format de huit groupes de chiffres hexadécimaux, chacun séparé d'une virgule. Le masque de sous-réseau doit être un numéro entre **0-128**. Le bouton **Vérifier** teste s'il existe actuellement un autre matériel dans le système qui utilise l'adresse IP saisie. La fonction **Vérifier** ne détecte pas les conflits avec des matériels éteints, en dehors du système VMS XProtect ou qui ne répondent pas momentanément.
Nom d'utilisateur	Le nom d'utilisateur et le niveau utilisés pour se connecter au matériel. Sélectionnez un autre utilisateur dans la liste déroulante et ajoutez un nouveau mot de passe dans le champ **Mot de passe** décrit ci-dessous. Ajouter ou supprimer des utilisateurs en utilisant les actions soulignées à la fin de la section **Authentification** (voir Ajouter un utilisateur on page 236 ou Supprimer des utilisateurs on page 236). La sélection d'un utilisateur n'ayant pas le niveau d'utilisateur le plus élevé spécifié par le fabricant pourrait rendre certaines fonctionnalités indisponibles.
Mot de passe	Le mot de passe utilisé pour se connecter au matériel. Afficher le texte actuellement saisi à l'aide de l'icône **Révéler**. Lorsque vous changez le mot de passe, consultez la documentation fournie par le fabriquant concernant les règles du mot de passe du matériel en question ou utilisez

Nom	Description
	l'icône **Générer un mot de passe** pour générer automatiquement un mot de passe qui répond aux exigences du fabriquant. Pour des informations sur comment modifier les mots de passe sur plusieurs périphériques matériels, voir Modifier les mots de passe sur les périphériques on page 239. En tant qu'administrateur du système, vous devez donner aux autres utilisateurs la permission de voir le mot de passe dans le Management Client. Pour plus d'informations, voir Paramètre des rôles sous Matériel.
Ajouter un utilisateur	Cliquez sur le lien souligné **Ajouter** pour ouvrir la boîte de dialogue **Ajouter un utilisateur** et ajouter un utilisateur au matériel. L'ajout d'un utilisateur le configurera automatiquement comme utilisateur actif actuel et remplacera les identifiants saisis auparavant. Lorsque vous créez le mot de passe, consultez la documentation fournie par le fabriquant concernant les règles du mot de passe du périphérique en question ou utilisez l'icône **Générer un mot de passe** pour générer automatiquement un mot de passe qui répond aux exigences du fabriquant. Le niveau d'utilisateur le plus élevé détecté sur le matériel sera automatiquement présélectionné. Il n'est pas conseillé de modifier la valeur par défaut du **Niveau d'utilisateur**. La sélection d'un **Niveau d'utilisateur** autre que le niveau d'utilisateur le plus élevé spécifié par le fabricant pourrait rendre certaines fonctionnalités indisponibles.
Supprimer des utilisateurs	Cliquez sur le lien souligné **Supprimer** pour ouvrir la boîte de dialogue **Supprimer des utilisateurs** et supprimer des utilisateurs du matériel.

Nom	Description
	Vous ne pouvez pas supprimer l'utilisateur actuellement actif. Pour configurer un nouvel utilisateur, utilisez la boîte de dialogue **Ajouter un utilisateur** décrite ci-dessus, puis supprimez l'ancien utilisateur à l'aide de l'interface.

Activer/désactiver des périphériques individuels

Les caméras sont **activées** par défaut.

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

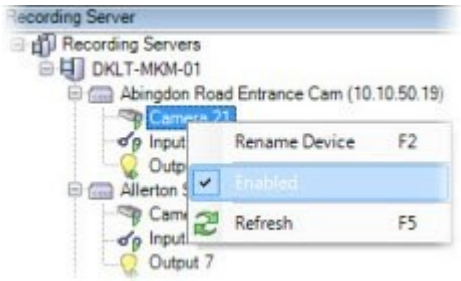
Cela signifie que les microphones, haut-parleurs, métadonnées, entrées et sorties doivent être activés individuellement avant de pouvoir être utilisés sur le système. Cela s'explique par le fait que les systèmes de surveillance reposent intrinsèquement sur les caméras, alors que l'utilisation de microphones,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

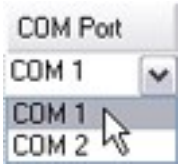
2. Dans l'onglet **Paramètres**, activez HTTPS. Cela n'est pas activé par défaut.
3. Saisissez le port du serveur d'enregistrement auquel la connexion HTTPS est raccordée. Le numéro du port doit correspondre au port configuré sur la page d'accueil du périphérique.
4. Apportez les changements nécessaires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

Activer PTZ sur un encodeur vidéo

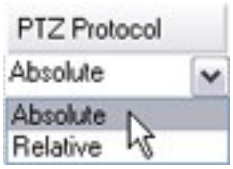
Pour activer l'utilisation de caméras PTZ sur un encodeur vidéo, procédez comme suit dans l'onglet **PTZ** :

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**.
6. Vous êtes maintenant prêt à configurer les positions prédéfinies et la patrouille de chaque caméra PTZ :
   - Ajouter une position prédéfinie (type 1)
   - Ajouter un profil de patrouille

Modifier les mots de passe sur les périphériques

> Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Vous pouvez modifier les mots de passe sur plusieurs périphériques matériels en une seule opération.

Initialement, les périphériques pris en charge sont les modèles des périphériques compatibles de Canon, Axis, Bosch, Hanwa, Panasonic, Sony, Hikvision et ONVIF, mais l'interface utilisateur vous affiche directement si un modèle est pris en charge ou non. Vous pouvez également vous rendre sur notre site Web pour vérifier si un modèle est pris en charge : https://www.milestonesys.com/community/business-partner-tools/supported-devices/

> Pour les périphériques ne prenant pas en charge la gestion des mots de passe périphériques, vous devez modifier le mot de passe d'un périphérique matériel depuis sa page Web, puis saisir manuellement le nouveau mot de passe dans Management Client. Pour plus d'informations, voir Modifier le matériel on page 233.

Vous pouvez choisir les approches suivantes :

- Laisser le système générer des mots de passe individuels pour chaque périphérique. Le système génère des mots de passe en fonction des exigences du fabricant des périphériques matériels.
- Utiliser un mot de passe unique défini par l'utilisateur pour tous les périphériques. Lorsque vous appliquez les nouveaux mots de passe, les périphériques matériels perdent momentanément leur connexion au serveur denregistrement. Après avoir appliqué les nouveaux mots de passe, le résultat de chaque périphérique matériel s'affiche à l'écran. En cas d'échec des modifications, la raison de l'échec s'affiche si le périphérique matériel prend en charge lesdites informations. Depuis l'assistant, vous pouvez créer un rapport sur la réussite ou l'échec des modifications de mot de passe. Les résultats sont tout de même enregistrés dans **Journaux de serveur**.

  > Pour les périphériques matériels dotés de pilotes ONVIF et de plusieurs comptes d'utilisateurs, seul un administrateur de XProtect disposant d'autorisations administratives du périphérique matériel peut modifier les mots de passe à partir du VMS.

Exigences :

- Le modèle de périphérique matériel prend en charge la gestion des mots de passe des périphériques par Milestone.

Étapes :

1. Dans le volet **Navigation du site** pane, sélectionnez le nœud **Serveurs d'enregistrement**.
2. Faites un clic droit sur le serveur d'enregistrement ou le matériel concerné dans le panneau Vue d'ensemble.
3. Sélectionnez **Modifier le mot de passe du matériel**. Un assistant apparaît.
4. Saisissez le mot de passe en utilisant des lettres minuscules et majuscules, des chiffres et les caractères suivants : **! ( ) * - .** _

   La longueur maximale du mot de passe est de 64 caractères.

   > La longueur maximale du mot de passe pour la caméra Bosch FLEXIDOME IP extérieure 5 000 MP NDN-50051 est de 19 caractères.

5. Suivez les instructions à l'écran pour achever les changements.

   > Le champ **Dernière modification du mot de passe** indique l'horodatage du dernier changement de mot de passe en fonction des paramètres de l'heure locale de l'ordinateur où a été modifié le mot de passe.

6. Le résultat s'affiche sur la dernière page. Si le système échoue lors de la mise à jour d'un mot de passe, cliquez sur **Échec** à côté du périphérique matériel pour en connaître la raison.
7. Vous pouvez également cliquer sur le bouton **Imprimer un rapport** pour afficher la liste complète des mises à jour réussies et infructueuses.
8. Si vous souhaitez modifier le mot de passe sur les périphériques matériels ayant échoué, cliquez sur **Réessayer** et l'assistant recommence l'opération sur lesdits périphériques matériels.

> Si vous sélectionnez **Réessayer**, vous perdez l'accès au rapport correspondant à votre première tentative avec l'assistant.

> En raison de limitations liées à la sécurité, certains périphériques matériels peuvent devenir indisponibles durant une période de temps si vous échouez à modifier le mot de passe plusieurs fois de suite. Les limitations strictions liées à la sécurité varient en fonctions des fabricants.

Mettre à jour le firmware sur les périphériques

> Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Management Client vous permet de mettre à jour le firmware du matériel ayant été ajouté à votre système VMS. Vous pouvez mettre à jour le firmware de plusieurs périphériques en même temps si ces derniers sont compatibles avec le même ficher du firmware.

L'interface utilisateur vous indique directement si un modèle prend en charge les mises à jour du firmware. Vous pouvez également vous rendre sur le site Web de Milestone pour vérifier si un modèle est pris en charge : https://www.milestonesys.com/community/business-partner-tools/supported-devices/

> Pour les périphériques qui ne prennent pas en charge les mises à jour du firmware, vous devez mettre à jour le firmware d'un périphérique depuis sa page Web.

Lorsque vous mettez à jour le firmware, les périphériques perdent momentanément leur connexion au serveur d'enregistrement.

Après avoir mise à jour le firmware, le résultat de chaque périphérique s'affiche à l'écran. En cas d'échec des modifications, la raison de l'échec s'affiche si le périphérique matériel prend en charge lesdites informations. Les résultats se trouvent sous **Journaux du serveur**.

Pour les périphériques matériels dotés de pilotes ONVIF et de plusieurs comptes utilisateurs, seul un administrateur de XProtect disposant des autorisations administratives du périphérique matériel peut mettre le firmware à jour à partir du VMS.

Exigences :

- Le modèle du périphérique doit prendre en charge les mises à jour du firmware par Milestone.

Étapes :

1. Dans le volet **Navigation du site** pane, sélectionnez le nœud **Serveurs d'enregistrement**.
2. Faites un clic droit sur le serveur d'enregistrement ou le matériel concerné dans le panneau Vue d'ensemble.
3. Sélectionnez **Mettre à jour le firmware du matériel**. Un assistant apparaît.
4. Suivez les instructions à l'écran pour achever les changements.

   Vous pourrez peut-être mettre à jour uniquement plusieurs périphériques étant compatibles avec le même fichier du firmware. Le matériel ajouté par le pilote ONVIF se trouve sous **autre**, et non sous le nom du fabricant.

6. Le résultat s'affiche sur la dernière page. Si le système échoue lors de la mise à jour du firmware, cliquez sur **Échec** à côté du périphérique pour en connaître la raison.

Milestone n'assume pas la responsabilité d'un dysfonctionnement du périphérique si un fichier firmware ou un périphérique incompatible est sélectionné.

Ajouter et configurer un IDP externe

1. Dans Management Client, sélectionnez **Outils** > **Options** et ouvrez l'onglet **IDP Externe**.
2. Dans la section **IDP Externe**, sélectionnez **Ajouter**. Notez qu'un seul IDP externe peut être ajouté.
3. Saisissez les informations relatives à l'IDP externe. Pour de plus amples informations sur les informations requises, consultez Onglet IDP externe (options) on page 423.

Pour des plus amples informations sur la procédure d'enregistrement des revendications à partir de l'IDP externe que vous souhaitez utiliser dans le VMS, consultez Enregistrer les demandes à partir d'un IDP externe.

Périphériques - Groupes

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 :

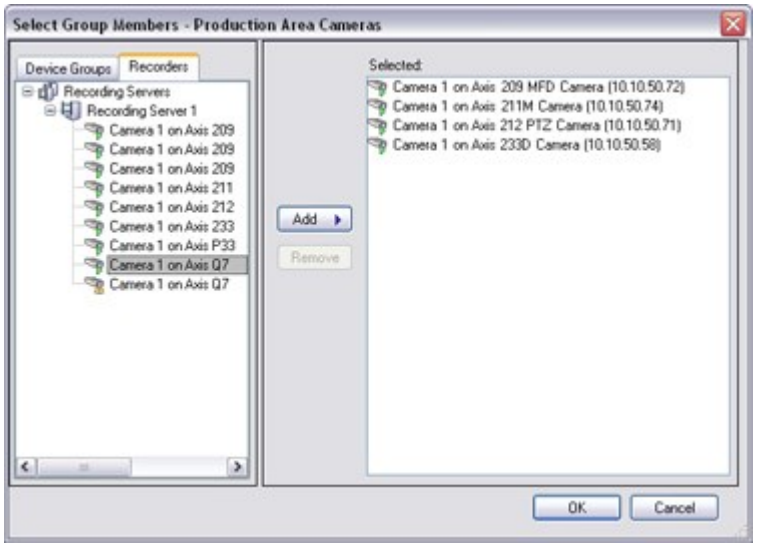
   La description s'affiche lorsque vous survolez le groupe de périphériques dans la liste des périphériques avec le curseur de la souris.
4. Cliquez sur **OK**. Un dossier représentant le nouveau groupe de périphériques apparaît dans la liste.
5. Continuez de spécifier les périphériques à inclure dans un groupe de périphériques (voir Spécifier les périphériques à inclure dans un groupe de périphériques on page 243).

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 :

Périphériques désactivés

Tous les périphériques, y compris les périphériques désactivés, sont affichés par défaut dans le volet **Vue d'ensemble**.

Pour masquer les périphériques désactivés, en haut du panneau **Vue d'ensemble**, cliquez sur **Filtrer** pour ouvrir l'onglet **Filtrer** et sélectionnez **Masquer les périphériques désactivés**.

Pour afficher à nouveau les périphériques désactivés, désactivez l'option **Masquer les périphériques désactivés**.

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.

Périphériques désactivés

Tous les périphériques, y compris les périphériques désactivés, sont affichés par défaut dans le volet **Vue d'ensemble**.

Pour masquer les périphériques désactivés, en haut du panneau **Vue d'ensemble**, cliquez sur **Filtrer** pour ouvrir l'onglet **Filtrer** et sélectionnez **Masquer les périphériques désactivés**.

Pour afficher à nouveau les périphériques désactivés, désactivez l'option **Masquer les périphériques désactivés**.

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.

Tous les périphériques, y compris les périphériques désactivés, sont affichés par défaut dans le volet **Vue d'ensemble**.

Pour masquer les périphériques désactivés, en haut du panneau **Vue d'ensemble**, cliquez sur **Filtrer** pour ouvrir l'onglet **Filtrer** et sélectionnez **Masquer les périphériques désactivés**.

Pour afficher à nouveau les périphériques désactivés, désactivez l'option **Masquer les périphériques désactivés**.

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**.

Périphériques - Paramètres des caméras

Voir ou modifier les paramètres de la caméra

1. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra requise dans le volet **Vue d'ensemble**.
3. Ouvrez l'onglet **Paramètres**.

Vous pouvez afficher ou modifier des paramètres tels que :

- Fluidité d'image par défaut
- Résolution
- Compression
- Le 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 qui prennent en charge plus d'un type de flux, par exemple, MJPEG et MPEG-4/H.264/H.265, vous pouvez utiliser la multi-diffusion, voir Gérer la multidiffusion on page 255.

Aperçu

Si vous modifiez un paramètre, vous pouvez rapidement vérifier les effets de votre modification si votre volet **Aperçu** est activé.

- Pour activer **Prévisualisation**, cliquez sur le menu **Vue**, puis sur **Fenêtre de prévisualisation**.

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**.

Performance

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. Ainsi, XProtect Smart Client une période plus longue entre les images-clés prolonge le démarrage de XProtect Smart Client.

Ajouter un matériel

Pour plus d'informations sur comment ajouter un matériel à votre système, voir Ajouter un matériel on page 231.

Activer et désactiver la prise en charge fisheye

La prise en charge fisheye est désactivée par défaut.

1. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra PTZ dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Objectif fisheye**, cochez ou décochez la case **Activer la prise en charge de l'objectif fisheye**.

Spécifier les paramètres de la lentille fisheye

1. Dans l'onglet **Objectif fisheye**, sélectionnez le type d'objectif.
2. Indiquez la position physique / l'orientation de la caméra dans la liste **Position/orientation de la caméra**.
3. Sélectionnez le nombre de Lentilles Panomorph Enregistrées (RPL) depuis la liste du numéros de RPL panomorph **ImmerVision Enables®**.

   Ceci permet d'identifier et de corriger la configuration de la lentille utilisée avec la caméra. Vous trouverez généralement le numéro RPL sur la lentille elle-même ou sur sa boîte d'origine. Pour plus d'informations sur ImmerVision, les objectifs panomorph, et les RPL, voir le site Internet d'ImmerVision (https://www.immervisionenables.com/).

   Si vous sélectionnez le profil de lentille **Suppression générique des déformations**, n'oubliez pas de configurer le **Champ de vue** souhaité.

Périphériques - Enregistrement

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, par exemple. Cela signifie que les périphériques connexes enregistrent lorsque la caméra enregistre.

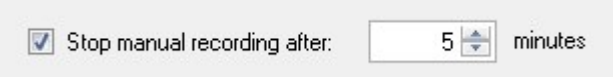
L'enregistrement sur les périphériques connexes est activé par défaut pour les nouvelles caméras, mais vous pouvez désactiver et activer cette fonction selon vos besoins. Pour les caméras existantes du système, la case est décochée par défaut.

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 les périphériques concernés**.
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.

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 de XProtect Smart Client.



1. Dans le volet **Navigation du site**, sélectionnez **Périphériques**.
2. Sélectionnez le périphérique requis dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Enregistrer**, cochez ou décochez la case **Arrêter l'enregistrement manuel après**.

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 l'autorisation de démarrer et d'arrêter l'enregistrement manuel aux utilisateurs du client sur chaque caméra dans **Rôles** de 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.

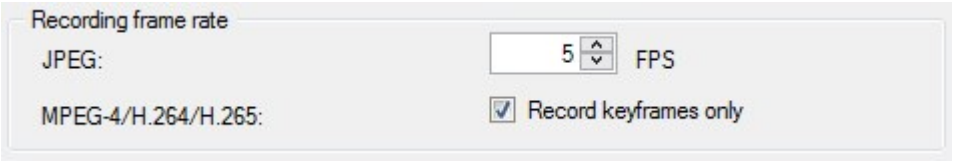
1. Dans le volet **Navigation du site**, sélectionnez **Périphériques**.
2. Sélectionnez le périphérique requis dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Enregistrer**, dans **Fluidité d'image à l'enregistrement : boîte de dialogue (JPEG)**, sélectionnez ou saisissez la fluidité d'image à l'enregistrement (dans FPS, images par seconde).

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. Dans le volet **Navigation du site**, sélectionnez **Périphériques**.
2. Sélectionnez le périphérique requis dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Enregistrer**, cochez la case **Enregistrer les images-clés uniquement**.



4. Configurez une règle qui active la fonction, voir Actions et actions d'arrêt.

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, 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 les périphériques concernés**.
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.

Enregistrer et rappeler l'enregistrement à distance

Pour garantir que tous les enregistrements à distance sont enregistrés en cas de problème de réseau, vous pouvez activer la récupération des enregistrements automatique une fois la connexion rétablie.

1. Dans le volet **Navigation du site**, sélectionnez **Périphériques**.
2. Sélectionnez le périphérique requis dans le volet **Vue d'ensemble**.
3. Sous **Enregistrements à distance**, sélectionnez **Récupérer les enregistrements à distance automatiquement lorsque la connexion est rétablie**. Cette option permet la récupération automatique des enregistrements une fois que la connexion est rétablie.

L'option d'enregistrement à distance n'est disponible que si la caméra sélectionnée prend en charge le stockage de bord ou s'il s'agit d'une caméra avec une configuration Milestone Interconnect.

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> à partir des <périphériques>**

Supprimer les enregistrements

1. Dans le volet **Navigation du site**, sélectionnez **Périphériques**.
2. Sélectionnez le périphérique requis dans le volet **Vue d'ensemble** puis sélectionnez l'onglet **Enregistrement**.
3. Cliquez sur le bouton **Supprimer tous les enregistrements** pour supprimer tous les enregistrements du périphérique ou du groupe de périphérique.

Vous pouvez utiliser cette méthode uniquement si vous avez ajouté tous les périphériques dans le groupe sur le même serveur. Les données protégées ne sont pas supprimées.

Périphériques - Flux

Flux adaptatif (explications)

Le flux adaptatif est une méthode de diffusion utilisée lorsque plusieurs flux vidéo en direct sont affichés dans la même vue. Cela permet aux clients de sélectionner automatiquement les flux vidéo en direct avec la meilleure correspondance de résolution pour les flux requis par les éléments de vue. Le flux adaptatif réduit la charge réseau et améliore la capacité de décodage et les performances de l'ordinateur client.

Vous pouvez configurer la correspondance la plus proche des flux vidéo disponibles pour la résolution demandée par un élément de vue lorsque vous activez le flux adaptatif dans XProtect Smart Client. Pour plus d'informations, voir Permettre le flux adaptatif on page 253.

Dans XProtect Smart Client, le flux adaptatif peut être appliqué en direct et en mode lecture. Pour les clients mobiles, il n'est disponible qu'en mode en direct.

Lorsqu'elle est appliquée en mode lecture, la méthode de diffusion est appelée lecture adaptative. Pour plus d'informations, voir Lecture adaptative (expliquée) on page 251

Lecture adaptative (expliquée)

La lecture adaptative est une configuration qui permet l'utilisation du flux adaptatif en mode lecture.

La lecture adaptative nécessite deux flux d'enregistrement, un flux principal et un flux secondaire. Si les deux flux sont activés dans le Management Client, les deux flux seront enregistrés.

- Si vous effectuez une lecture d'une vidéo d'une période antérieure à la configuration de l'enregistrement secondaire, seuls les enregistrements principaux seront lus.
- Si vous effectuez une lecture d'une vidéo qui a été enregistrée après la configuration de l'enregistrement secondaire, la vidéo est lue à partir de l'enregistrement principal ou secondaire en fonction de ce qui correspond le mieux à la taille de la vue du client.

Disponibilité

> Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Permettre le flux adaptatif

Vous pouvez activer la lecture adaptative avec le flux adaptatif dans l'onglet **Avancé** dans **Profils Smart Client** et elle doit également être activée dans XProtect Smart Client sous **Paramètres** > **Avancés** > **Flux adaptatif**. Pour plus d'informations sur l'activation du flux adaptatif dans XProtect Smart Client, consultez Permettre le flux adaptatif on page 253.

Enregistrements à distance

En option, vous pouvez utiliser des enregistrements décentralisés pour la lecture adaptative. Les enregistrements décentralisés vous permettent de visionner les séquences d'un flux avec une résolution différente, généralement plus élevée, que le reste du flux. Par exemple, vous pouvez enregistrer un flux principal avec une faible résolution et fusionner des enregistrements à partir d'une source haute résolution. Vous pouvez activer la fusion des enregistrements décentralisés lorsque vous parcourez les données.

Les enregistrements décentralisés sont stockés dans la base de données multimédia et la résolution de ces enregistrements est définie selon les caméras particulières.

Résolution de la lecture vidéo

Lors de l'utilisation de la lecture adaptative, la résolution de la vidéo lue est déterminée par les paramètres de résolution actuels pour l'enregistrement principal et le secondaire. En lecture, le choix du flux principal ou secondaire est basé sur la résolution qui est actuellement configurée pour les flux d'enregistrement respectifs.

Ajouter un flux

Les flux que vous ajoutez pour l'enregistrement peuvent être visionnés en direct et en mode lecture.

Vous pouvez également afficher la vidéo enregistrée dans votre élément de vue avec le flux adaptatif activé. Le flux adaptatif en mode lecture est appelé lecture adaptative.

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
   - **Lorsque cela est nécessaire** : le flux démarre à la demande d'un client ou si le flux est défini pour enregistrer
4. Dans la colonne **Flux en direct par défaut**, sélectionnez le flux par défaut et à utiliser si le client ne demande pas de flux spécifique et que le flux adaptatif est désactivé.
5. Dans la colonne **Enregistrement**, sélectionnez **Principal** ou **Secondaire**. Pour la lecture adaptative, vous devez créer un flux de chaque type. La vidéo lue provient du flux vidéo principal et le flux secondaire est inclus lorsque cela est nécessaire. Il doit toujours y avoir un enregistrement principal. En outre, le flux que vous configurez comme **Principal** est utilisé dans différents contextes, comme la détection du mouvement et pour l'exportation depuis XProtect Smart Client.
6. Dans **Lecture par défaut**, sélectionnez le flux par défaut. Le flux par défaut sera fourni au client si la lecture adaptative n'est pas configurée.
7. Dans la colonne **Utiliser les enregistrements décentralisés**, cochez la case si vous souhaitez utiliser les enregistrements décentralisés. Pour plus d'informations sur les enregistrements décentralisés, voir Enregistrements à distance on page 252.
8. Cliquez sur **Enregistrer**.

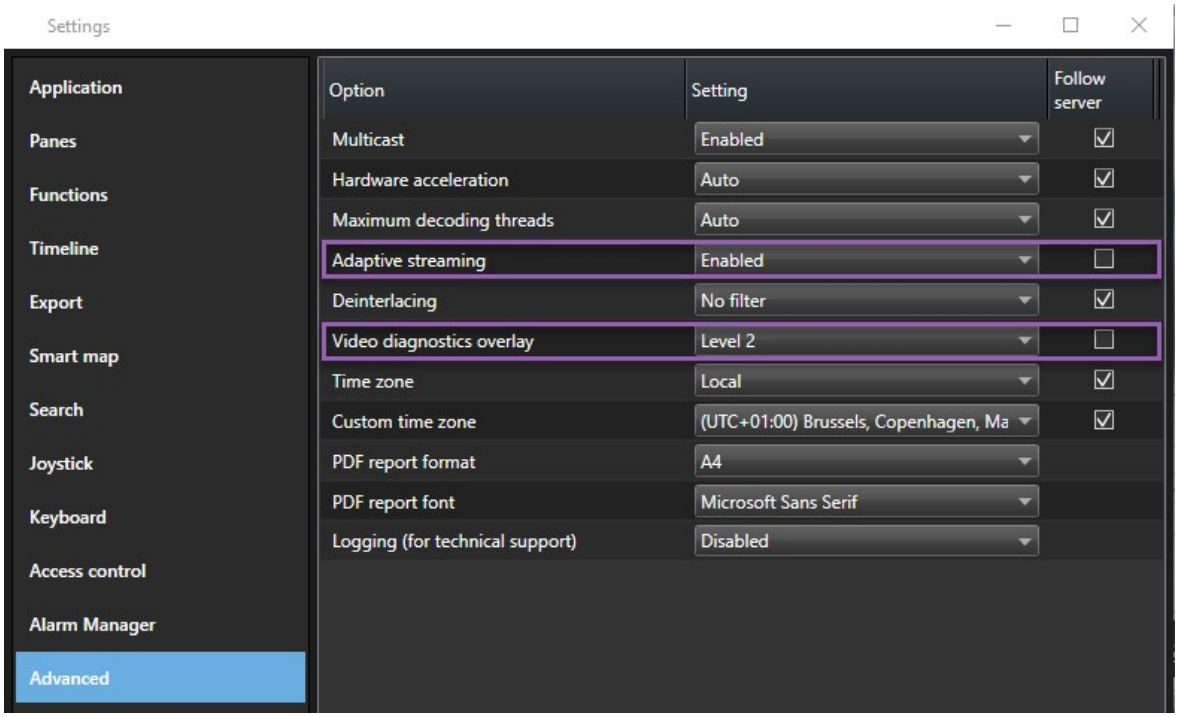
Si vous ne souhaitez pas que les flux fonctionnent du tout à moins que quelqu'un ne consulte la vidéo en direct, vous pouvez modifier la **Règle de démarrage des flux par défaut** pour les démarrer à la demande avec l'événement prédéfini **Flux client en direct requis**.

Permettre le flux adaptatif

Activez le flux adaptatif pour améliorer les performances des ordinateurs exécutant XProtect Smart Client.

1. Dans le menu **Paramètres et autres**, sélectionnez **Paramètres**.
2. Dans l'onglet **Avancé**, sélectionnez **Flux adaptatif**.
3. Il existe deux paramètres pour le flux adaptatif : **Désactivé** et **Activé**.

   Sélectionnez **Activé**.

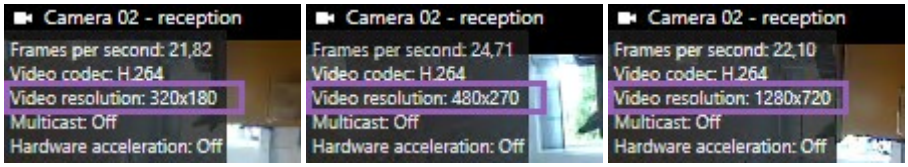


4. Allez dans **Recouvrement de diagnostic vidéo**.
5. Pour rendre visible la résolution du flux de la vidéo actuelle, sélectionnez **Niveau 2**.

> Ce paramètre s'applique à tous les éléments de vue. **Masquer** est le paramètre par défaut.

6. La superposition des diagnostics vidéo devrait désormais être **Activée**.

   Essayez de redimensionner la fenêtre d'affichage de petit à grand, de grand à petit, puis vérifiez si la valeur de la **Résolution de la vidéo** change.



   Si la valeur reste inchangée, poursuivez votre examen des flux vidéo en direct disponibles sur vos caméras afin d'activer le flux adaptatif, si possible.

Gérer la multidiffusion

Laffichage de la vidéo en direct ou la lecture dune vidéo enregistrée ou ne nécessite pas obligatoirement la même qualité vidéo et la même fluidité dimage.

Pour modifier le flux à utiliser lors de l'enregistrement

La lecture adaptative nécessite que deux flux soient définis pour l'enregistrement, un flux principal et un flux secondaire. Pour la diffusion en direct, vous pouvez configurer et utiliser autant de flux en direct que le nombre pris en charge par la caméra.

1. Dans le volet **Navigation du site**, sélectionnez **Périphériques**.
2. Sélectionnez la caméra requise dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Flux**, sélectionnez le flux que vous souhaitez utiliser pour l'enregistrement.
4. Sélectionnez l'option appropriée dans la liste **Mode en direct**. Les options **Lorsque cela est nécessaire**, **Toujours** et **Jamais** indiquent quand le flux doit être appliqué pour le client. Si rien n'est demandé par le client, l'enregistrement utilisera le flux où la case **Flux en direct** par défaut est cochée.
5. Pour enregistrer sur un flux, sélectionnez **Principal** ou **Secondaire** dans la liste **Enregistrements**.
6. Pour utiliser la lecture adaptative, configurez deux flux et définissez l'un des flux sur **Principal** et l'autre sur **Secondaire**.
7. Pour enregistrer sur un flux, sélectionnez le flux **Principal** ou le **Secondaire** dans la liste **Enregistrements**.

Limiter la transmission de données

Vous pouvez configurer un ensemble de conditions pour assurer que la diffusion vidéo s'exécutera uniquement lorsqu'un client la visualisera.

Pour gérer la diffusion et limiter la transmission de données inutiles, la diffusion ne commence pas si :

1. Dans le volet **Navigation du site**, sélectionnez **Périphériques**.
2. Sélectionnez la caméra requise dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Flux**, dans la liste du **Mode en direct**, sélectionnez **Si besoin**.
4. Dans l'onglet **Enregistrer**, décochez la case **Enregistrement**.
5. Dans l'onglet **Mouvement**, décochez la case **Détection du mouvement**.

Si ces conditions sont remplies, la diffusion vidéo s'exécutera uniquement lorsqu'un client la visualisera.

Exemples

Exemple 1, vidéo en direct et enregistrée :

- Pour le visionnage d'une vidéo **en direct**, votre société peut préférer le format H.264 avec une fluidité d'image élevée
- Pour la lecture d'une vidéo **enregistrée**, votre société peut préférer MJPEG avec une fluidité d'image inférieure pour préserver de l'espace disque

Exemple 2, vidéo en direct locale et à distance :

- Pour le visionnage d'une **vidéo en direct à partir d'un point de fonctionnement local**, votre société peut préférer le format H.264 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 MJPEG avec une fluidité d'image et une qualité inférieures afin de préserver la bande passante du réseau

Exemple 3, flux adaptatif :

- Pour le visionnage d'une **vidéo en direct et diminuer la charge sur le CPU et le GPU de l'ordinateur XProtect Smart Client**, votre société peut préférer le format H.264/H.265 avec une fluidité d'image élevée pour correspondre à la résolution requise par XProtect Smart Client lors de l'utilisation du flux adaptatif. Pour plus d'informations, voir Profils Smart Client (nœud client) on page 506.

> Si vous activez **Multicast en direct** dans l'onglet **Client** de la caméra (voir Onglet Client (périphériques)), cette option fonctionnera uniquement sur le flux vidéo par défaut.

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, voir **Onglet Paramètres (périphériques)**.

Périphériques - Stockage

Gérer la mise en mémoire-tampon préalable

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.

Pour utiliser la fonction de mémoire-tampon préalable, les périphériques doivent être activés et envoyer un flux au système.

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. Dans le volet **Navigation du site**, sélectionnez **Périphériques**.
2. Sélectionnez le périphérique requis dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Enregistrer**, cochez ou décochez la case **Pré-enregistrement**.
4. Dans l'onglet **Client**, spécifiez les périphériques associés à cette caméra.

Préciser 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. Dans le volet **Navigation du site**, sélectionnez **Périphériques**.
2. Sélectionnez le périphérique requis dans le volet **Vue d'ensemble** puis sélectionnez l'onglet **Enregistrer**.
3. Dans la liste **Localisation**, sélectionnez **Mémoire** ou **Disque**, et spécifiez le nombre de secondes.
4. Si vous avez besoin d'une durée de mise en mémoire-tampon supérieure à 15 secondes, sélectionnez **Disque**.

Le nombre de secondes saisi doit être suffisamment grand pour correspondre à vos exigences dans les différentes règles d'enregistrement définies.

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.

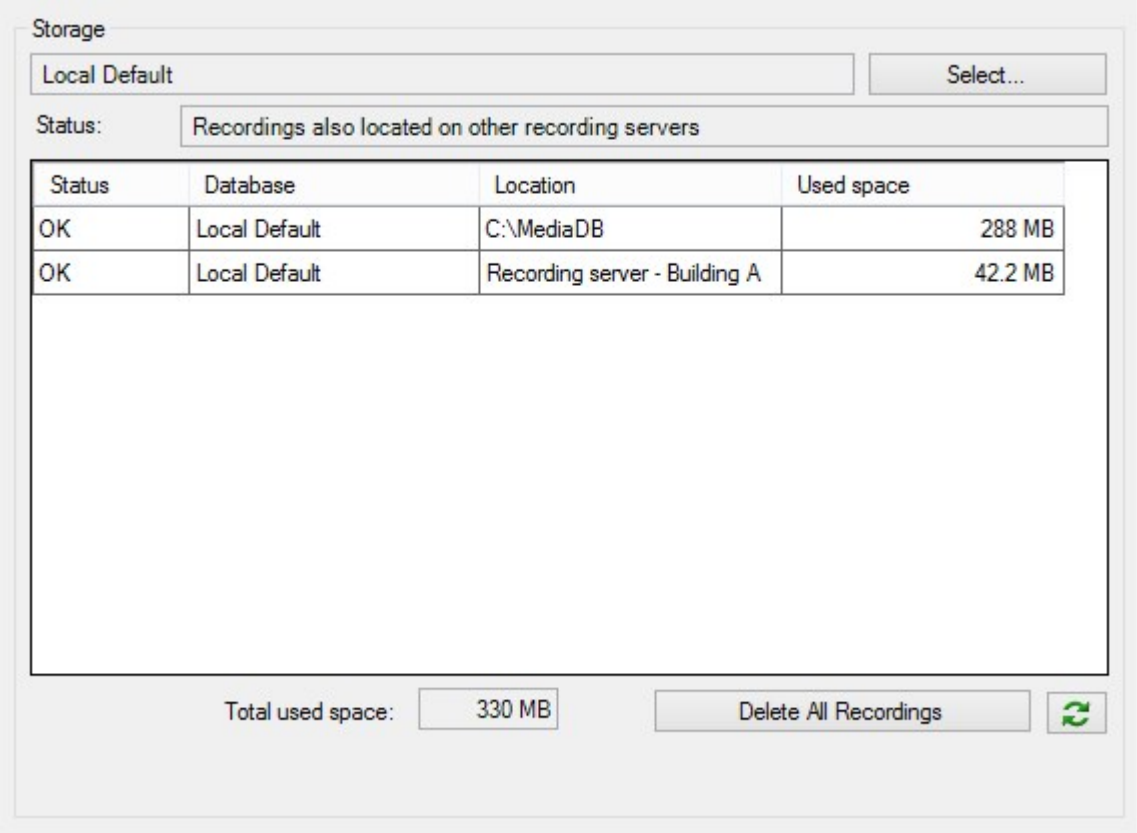
Pour utiliser la fonction d'enregistrement avec mise en mémoire-tampon préalable dans la règle, vous devez activer la mise en mémoire-tampon préalable sur le périphérique en cours d'enregistrement et définir la durée de la mise en mémoire-tampon préalable afin qu'elle soit au minimum égale à celle spécifiée dans la règle.

Surveiller l'état des bases de données pour les périphériques

1. Dans le volet **Navigation du site**, sélectionnez **Périphériques**.
2. Sélectionnez le périphérique requis dans le volet **Vue d'ensemble** puis sélectionnez l'onglet **Enregistrement**.

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, **Défaut local** 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.
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 de certains 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 de basculement	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 basculement.

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**.

Pour plus d'informations sur la configuration de stockage, voir Onglet Stockage (serveur d'enregistrement).

Plus de périphériques d'un stockage à un autre

La sélection d'un nouvel emplacement de stockage des enregistrements n'affecte pas les enregistrements actuels. Ces derniers resteront dans leur emplacement actuel et seront toujours soumis aux conditions définies par la configuration de stockage à laquelle ils appartiennent.

1. Dans le volet **Navigation du site**, sélectionnez **Périphériques**.
2. Sélectionnez le périphérique requis dans le volet **Vue d'ensemble** puis sélectionnez l'onglet **Enregistrement**.
3. Cliquez sur **Sélectionner** sous **Stockage** pour sélectionner un stockage d'enregistrement pour vos périphériques.

Les enregistrements seront archivés en fonction de la configuration de stockage que vous sélectionnez.

Périphériques - Détection des mouvements

Détection du mouvement (explications)

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 pour chaque caméra 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.

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. Par exemple, vous pouvez spécifier les intervalles entre l'analyse de la détection du mouvement et les zones d'une vue dans lesquelles le mouvement doit être ignoré. Vous pouvez également ajuster la précision de la détection du mouvement et donc la charge des ressources du système.

Qualité d'image

Avant de configurer la détection du mouvement pour une caméra, Milestone recommande d'avoir configuré les paramètres de qualité d'image de la caméra, par exemple, la résolution, le codec de la vidéo et les paramètres de diffusion. Pour ce faire, rendez-vous dans l'onglet **Paramètres** dans la fenêtre **Propriétés** du périphérique. Si vous changez plus tard les paramètres de qualité d'image, vous devez toujours tester la configuration de détection du mouvement par la suite.

Masques de confidentialité

Les zones couvertes par des masques de confidentialité permanents ne comporte aucune détection du mouvement.

Activer et désactiver la détection du mouvement

Spécifier le paramètre par défaut de la détection du mouvement pour les caméras

1. Dans le menu **Outils**, cliquez sur **Options**.
2. Dans l'onglet **Général**, sous **Lors de l'ajout de nouveaux périphériques de type caméra, activer automatiquement**, cochez la case **Détection du mouvement**.

Activer ou désactiver la détection du mouvement pour une caméra spécifique

1. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra requise dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Onglet Mouvement**, cochez ou décochez la case **Détection du mouvement**.

> Lorsque la détection du mouvement d'une caméra est désactivée, aucune des règles de la caméra associées à la détection du mouvement ne fonctionne.

Activer ou désactiver l'accélération du matériel

Le paramètre par défaut de la détection du mouvement lors de l'ajout d'une caméra est le décodage vidéo accéléré pour la détection du mouvement. Le serveur d'enregistrement utilise des ressources du GPU lorsqu'elles sont disponibles. Ceci réduira la charge du processus sur le serveur d'enregistrement au cours de l'analyse des mouvements sur la vidéo et améliorera la performance générale du serveur d'enregistrement.

Pour activer ou désactiver l'accélération du matériel

1. Dans le volet **Navigation du site**, sélectionnez **Périphériques**.
2. Sélectionnez la caméra requise dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Mouvement**, sous **Accélération du matériel**, sélectionnez **Automatique** pour activer l'accélération du matériel ou **Off** pour désactiver le paramètre.

Utiliser les ressources du GPU

Le décodage vidéo accéléré pour la détection du mouvement utilise des ressource du GPU dans :

- Les processeurs Intel prenant en charge Intel Quick Sync
- NVIDIA® affiche les adaptateurs connectés à votre serveur d'enregistrement

Répartition des tâches et performance

La répartition de la charge entre les différentes ressources se fait automatiquement. Dans le nœud **Moniteur système**, vous pouvez vériifier que la charge d'analyse des mouvements actuelle sur les ressources NVIDIA GPU est comprise dans les limites spécifiées dans le nœud **Seuils du moniteur système**. Les témoins de

charge NVIDIA GPU sont :

- Décodage NVIDIA
- Mémoire NVIDIA
- Rendu NVIDIA

Si la charge est trop élevée, vous pouvez ajouter des ressources GPU à votre PC en installant plusieurs adaptateurs graphiques NVIDIA. Milestone ne recommande pas l'utilisation de Scalable Link Interface (SLI) pour la configuration de vos adaptateurs graphiques NVIDIA.

Les produits NVIDIA possèdent différentes capacités de calcul.

Le décodage vidéo accéléré pour la détection du mouvement qui utilise les GPU NVIDIA requièrent une version de capacité de calcul 6.x (Pascal) ou plus récente.

- Pour trouver la version de capacité de calcul de votre produit NVIDIA, consultez le site Internet NVIDIA (https://developer.nvidia.com/cuda-gpus/).
- Pour vérifier si la détection du mouvement vidéo fait l'objet d'une accélération matérielle pour une caméra donnée, activez la connexion du fichier journal du serveur d'enregistrement. Définissez le niveau sur **Débogage** et diagnostics connecté sur DeviceHandling.log. Le journal suit le modèle : [heure] [274] DÉBOGAGE – [guide] [nom] Décodage configuré : Automatique : Décodage réel : Intel/NVIDIA

La version du système d'exploitation du serveur d'enregistrement et la génération du CPU peuvent avoir une incidence sur le niveau de performance de l'accélération matérielle de la détection des mouvements vidéo. L'affectation de la mémoire du GPU constitue souvent un goulot d'étranglement avec les versions plus anciennes (la limite typique se situe entre 0,5 Go et 1,7 Go).

Les systèmes basés sur Windows 10 / Server 2016 et les CPU de 6e génération (Skylake) ou plus récents allouent 50 % de la mémoire système au GPU, ce qui permet ainsi de supprimer ou de réduire ce goulot d'étranglement.

Les CPU Intel de 6e génération ne permettent pas le décodage de l'accélération matérielle de H.265, ainsi le niveau de performance est comparable avec le H.264 de ces versions du CPU.

Activer la sensibilité manuelle pour définir le mouvement

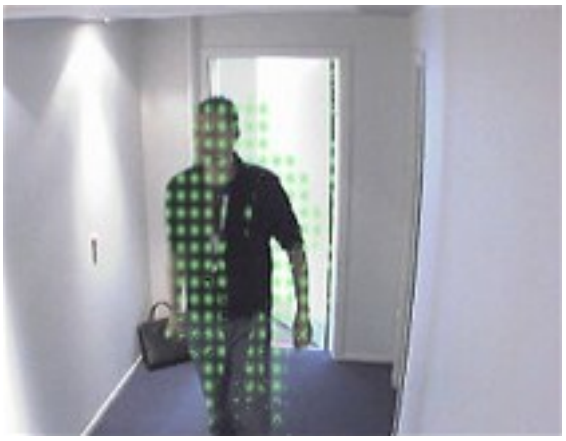
Le paramètre de sensibilité détermine **dans quelle mesure chaque pixel** de l'image doit changer avant que l'on considère qu'il y a mouvement.

1. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra requise dans le volet **Vue d'ensemble**.
3. Cochez la case **Sensibilité manuelle** dans l'onglet **Mouvement**.
4. 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.
5. Sélectionnez une position du curseur dans laquelle seuls les changements détectés que vous considérez comme des mouvements sont mis en surbrillance.



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 pour définir le mouvement

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.

Spécifier l’exclusion de régions pour la détection 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.

> Les zones caractérisées par des masques de confidentialité sont exclues de la détection du mouvement. Cochez la case **Afficher les masques de confidentialité** pour les afficher.

Le fait d’exclure la détection du mouvement 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.

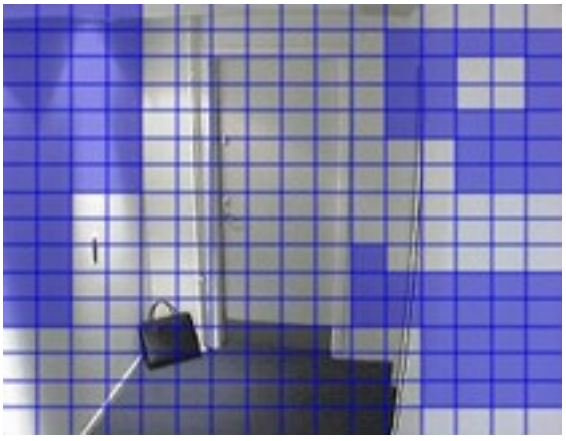
Lorsque vous utilisez l’exclusion de zones avec des caméras PTZ et que cette caméra peut être orientée, inclinée et agrandie, l’exclusion de zone **ne se déplace pas** car est verrouillée en fonction de l’image de la caméra et pas de l’objet.

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 tout en appuyant 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 :



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.

Périphériques - Position caméra prédéfinie

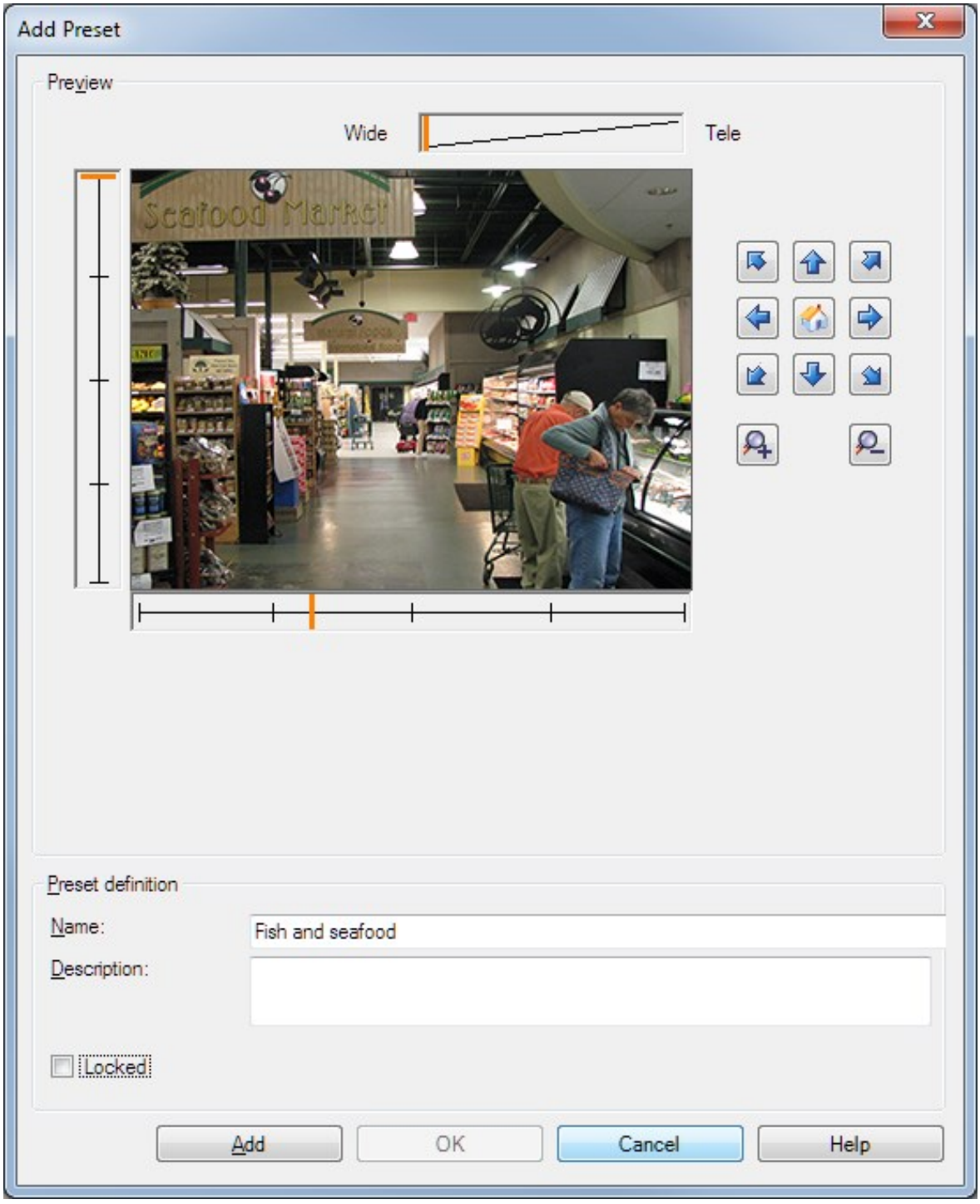
La position prédéfinie d’origine

Vous définissez la position prédéfinie **Origine** de la caméra PTZ sur la page d’accueil de la caméra. Les capacités PTZ disponibles sur la page d’accueil dépendent de la caméra.

Ajouter une position prédéfinie (type 1)

Pour ajouter une position prédéfinie pour la caméra :

1. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra PTZ dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Préréglages**, cliquez sur **Nouveau**. La fenêtre **Ajouter un préréglage** s'ouvre :



4. 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.
5. Précisez un nom en ce qui concerne la position prédéfinie, dans le champ **Nom**.
6. Facultativement, saisissez une description de la position prédéfinie dans le champ **Description**.
7. Sélectionnez **Verrouillé** si vous souhaitez verrouiller la position prédéfinie. Seuls les utilisateurs disposant des autorisations suffisantes peuvent déverrouiller la position ultérieurement.
8. Cliquez sur **Ajouter** pour spécifier des préréglages. Continuez à les ajouter jusqu'à ce que vous disposiez de tous les préréglages souhaités.
9. 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. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra PTZ dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Préréglages**, sélectionnez **Utiliser les préréglages du périphérique** pour importer les préréglages dans le système.

   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.
4. Cliquez sur **Supprimer** pour supprimer les préréglages dont vos utilisateurs n'ont pas besoin.
5. Cliquez sur **Modifier** si vous souhaitez modifier le nom affiché du préréglage (voir Renommer une position prédéfinie (type 2 uniquement)).
6. Si vous souhaitez ensuite modifier ces préréglages définis sur le périphérique, modifiez-les sur la caméra, puis réimportez-les.

Assigner une position prédéfinie de caméra 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. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra PTZ dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Préréglages**, sous **Positions prédéfinies**, sélectionnez le préréglage dans votre liste de positions prédéfinies.
4. Cochez la case **Préréglage par défaut** sous la liste.

Seule une position prédéfinie peut être définie comme position prédéfinie par défaut.

Si vous avez sélectionné **Utiliser le préréglage par défaut comme position d'origine de la caméra PTZ** dans **Options** > **Général**, la position prédéfinie par défaut sera utilisée au lieu de la position d'origine de la caméra PTZ définie.

Spécifier le préréglage par défaut comme position de base de la caméra PTZ

Les utilisateurs de Management Client et XProtect Smart Client disposant des autorisations utilisateurs nécessaires peuvent configurer le système pour utiliser la position prédéfinie par défaut au lieu de la position d'origine des caméras PTZ lorsque le bouton **Accueil** est activé dans un client.

Une position prédéfinie par défaut doit être définie pour la caméra. Si une position prédéfinie par défaut n'est pas définie, rien ne se passera lorsque le bouton **Accueil** est activé dans un client.

Activer le paramétrage de la position d'origine de la caméra PTZ

1. Sélectionnez **Outils** > **Options**.

2. Dans l'onglet **Général**, dans le groupe **Serveur d'enregistrement**, sélectionnez **Utiliser le préréglage par défaut comme position d'origine de la caméra PTZ**.

3. Assignez une position prédéfinie comme position prédéfinie par défaut pour la caméra.

Pour assigner une position prédéfinie par défaut, voir Assigner une position prédéfinie de caméra par défaut on page 267

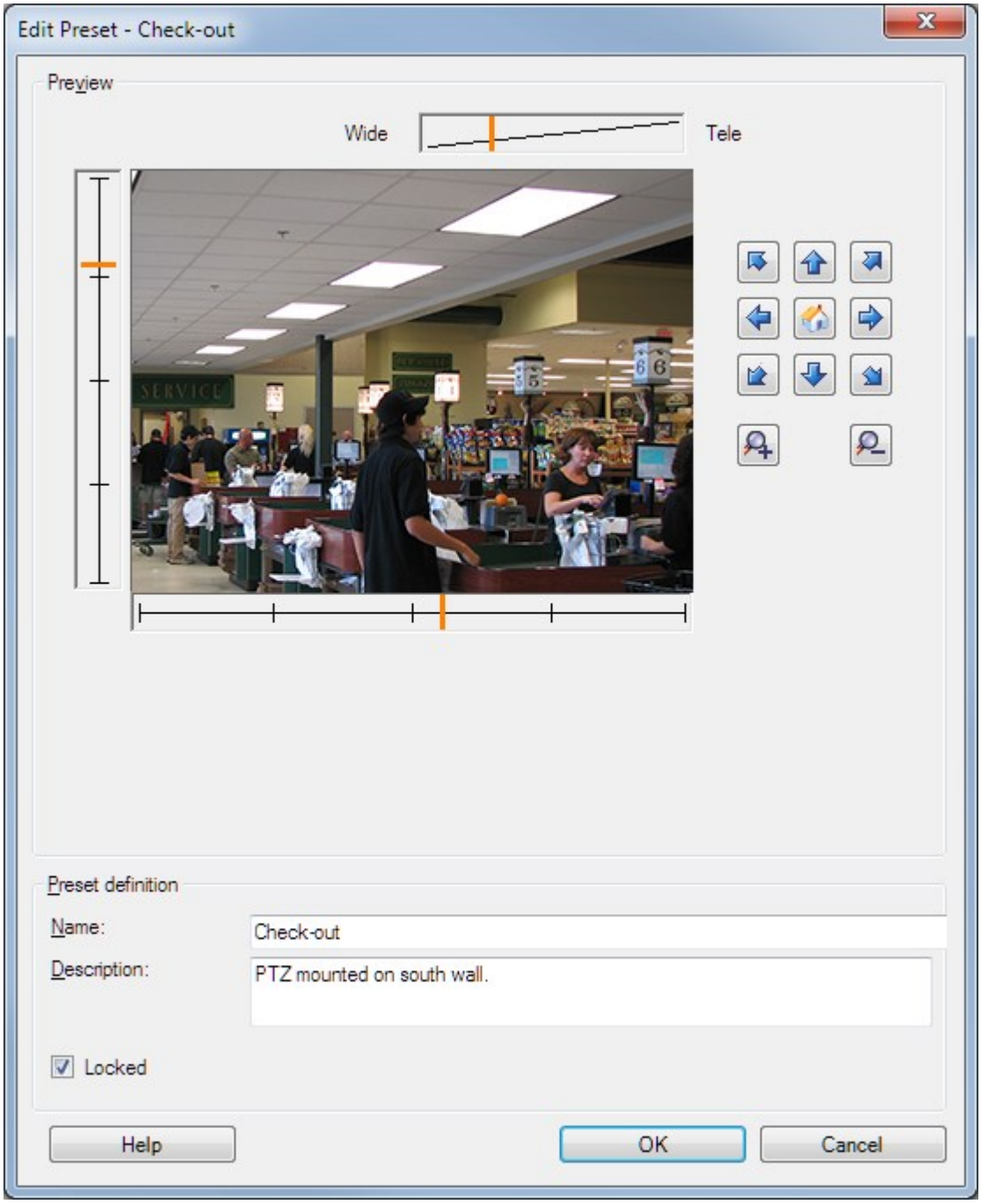
Voir également Paramètres du système (boîte de dialogue Options) on page 414

Modifier une position PTZ prédéfinie pour une caméra (type 1 uniquement)

Pour modifier une position prédéfinie existante, définie dans le système :

1. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra requise dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Préréglages**, sous Positions prédéfinies, sélectionnez la position prédéfinie dans la liste des positions prédéfinies à disposition pour la caméra.

4. Cliquez sur **Modifier**. Cela ouvre la fenêtre **Modifier un préréglage** :



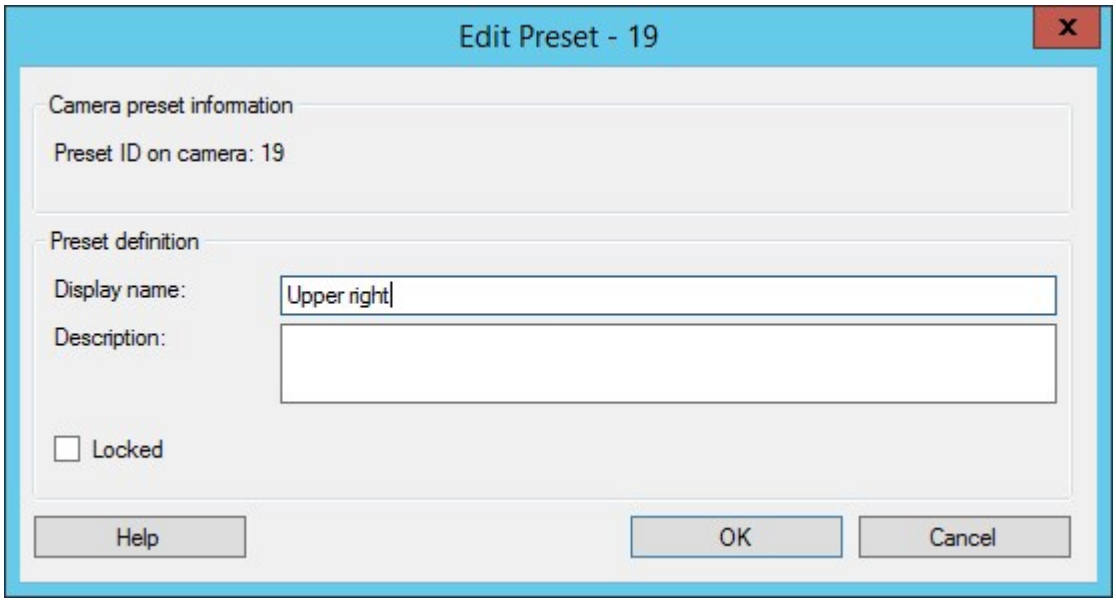
5. La fenêtre **Modifier un préréglage** affiche la vidéo en direct depuis la position prédéfinie. Utilisez les boutons de navigation et/ou les curseurs pour modifier la position prédéfinie en fonction de vos besoins.
6. Changez le nom/le numéro et la description de la position prédéfinie si nécessaire.

7. Sélectionnez **Verrouillé** si vous souhaitez verrouiller la position prédéfinie. Seuls les utilisateurs disposant des autorisations suffisantes peuvent déverrouiller la position ultérieurement.
8. Cliquez sur **OK**.

Renommer une position PTZ prédéfinie pour une caméra (type 2 uniquement)

Pour modifier le nom d'une position prédéfinie dans la caméra :

1. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra PTZ dans le volet **Vue d'ensemble**.
3. Sélectionnez la position prédéfinie requise dans la liste de l'onglet **Préréglages** des préréglages à disposition pour la caméra.
4. Cliquez sur **Modifier**. Cela ouvre la fenêtre **Modifier un préréglage** :



5. Modifiez le nom et ajoutez une description de la position prédéfinie si nécessaire.
6. 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 d'autorisations de sécurité limitées de mettre à jour le nom du préréglage ou de le supprimer. Les préréglages verrouillés sont indiqués par l'icône . Seuls les utilisateurs disposant d'autorisations suffisantes peuvent déverrouiller le nom du préréglage ultérieurement.
7. Cliquez sur **OK**.

Tester une position prédéfinie (type 1 seulement)

1. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra PTZ dans le volet **Vue d'ensemble**.
3. Sélectionnez la position prédéfinie requise dans la liste de l'onglet **Préréglages** des positions prédéfinies à disposition pour la caméra.
4. Cliquez sur **Activer**.
5. La caméra se déplace vers la position prédéfinie sélectionnée.

Périphériques - Patrouilles

Profils de patrouille et patrouille manuelle (explications)

Les profils de patrouille 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.

Patrouille manuelle

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.

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 stoppez la patrouille manuelle et que vous avez défini une position de fin pour votre profil de patrouille, la caméra revient à cette position.

Ajouter un profil de patrouille

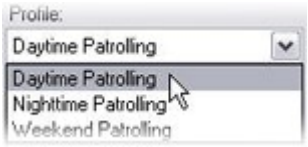
> Avant de pouvoir travailler avec la patrouille, vous devez spécifier au moins deux positions PTZ prédéfinies dans l'onglet **Préréglages**, voir Ajouter une positions PTZ prédéfinie (type 1).

1. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra PTZ dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Patrouille**, cliquez sur **Ajouter**. La boîte de dialogue **Ajouter profil** s'ouvre.
4. Dans la boîte de dialogue **Ajouter profil**, donnez un nom au profil de patrouille.
5. 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.

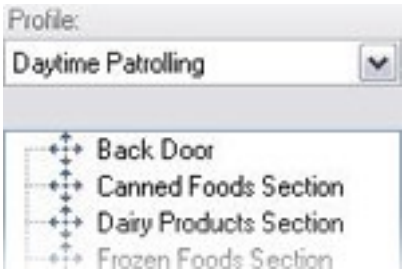
Spécifier des positions prédéfinies dans un profil de patrouille

1. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra PTZ dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Patrouille**, sélectionnez le profil de patrouille dans la liste **Profil** :



4. Cliquez sur **Ajouter**.
5. Dans la boîte de dialogue **Sélectionner la position PTZ prédéfinie**, sélectionnez les positions prédéfinies pour votre profil de patrouille :

6. Cliquez sur **OK**. Les positions prédéfinies sélectionnées sont ajoutées à la liste de positions prédéfinies du profil de patrouille :



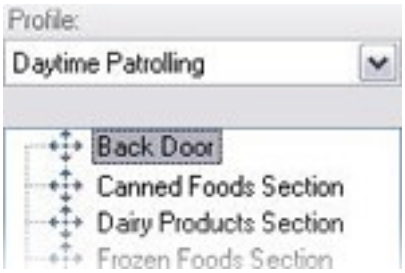
7. La caméra utilise la position prédéfinie la plus haute dans la liste comme premier arrêt lorsqu'elle patrouille en suivant le profil de patrouille. La position prédéfinie suivante depuis le haut constitue le second arrêt, et ainsi de suite.

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. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra PTZ dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Patrouille**, sélectionnez le profil de patrouille dans la liste **Profil**.
4. Sélectionnez la position prédéfinie pour laquelle vous souhaitez modifier la durée :



5. Indiquez la durée dans le champ **Durée en position (s)**.
6. Si nécessaire, recommencez pour d'autres positions prédéfinies.

Personnaliser les transitions (PTZ)

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. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra PTZ dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Patrouille**, dans la liste **Profil**, sélectionnez le profil de patrouille.
4. Cochez la case **Personnaliser transitions**.

   Les indications relatives à la transition sont ajoutées dans la liste des positions prédéfinies.
5. Dans la liste, sélectionnez la transition.

6. Indiquez la durée de transition estimée (en secondes) dans le champ **Temps escompté (sec.)**.

7. 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.
8. Répétez la procédure le cas échéant pour les autres transitions.

Spécifier une position de fin durant a patrouille

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. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra PTZ dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Patrouille**, dans la liste **Profil**, sélectionnez le profil de patrouille concerné.
4. Cochez la case **Atteindre une position spécifique à la fin**. Cela ouvre la boîte de dialogue **Sélectionner le préréglage**.
5. Sélectionnez la position de fin et 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.

6. 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.

Réserver et lancer des sessoins PTZ

En fonction de votre système de surveillance, vous pouvez réserver des sessions PTZ.

Les administrateurs dotés d'autorisations de sécurité suffisantes 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 à des opérations de maintenance urgentes sur une caméra PTZ ou sur ses préréglages sans être interrompu par d'autres utilisateurs.

Réserver une session PTZ

1. Dans le volet **Navigation sur le site**, sélectionnez **Périphériques** puis **Caméras**.
2. Sélectionnez la caméra PTZ dans le volet **Vue d'ensemble**.
3. Sélectionnez la session PTZ dans l'onglet **Préréglages**, et cliquez sur **Réservée**.

> Vous ne pouvez pas démarrer une session PTZ réservée si un utilisateur avec une priorité plus haute que la vôtre contrôle la caméra ou si un autre utilisateur a déjà réservé la caméra.

Libérer une session PTZ

Le bouton **Libére** 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.

Les administrateurs auxquels l'autorisation de sécurité **Lancer la session PTZ** a été affectée disposent des autorisations pour lancer une autre session PTZ réservée aux 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

Management Client et les utilisateurs de XProtect Smart Client disposant des autorisations utilisateur 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.

Périphériques - Événements pour les règles

Ajouter un événement pour un périphérique

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. Si vous souhaitez consulter la liste complète de tous les événements, ce qui vous permet d'ajouter des événements qui ont déjà été ajoutés, sélectionnez **Afficher les événements déjà ajoutés**.
5. Cliquez sur **OK**.
6. Dans la boîte à outils, cliquez sur **Enregistrer**.

Supprimer un événement pour un périphérique

Lorsque vous supprimez un événement, cela affecte toutes les règles qui utilisent l'événement.

1. Dans le volet **Vue d'ensemble**, sélectionnez un périphérique.
2. Sélectionnez l'onglet **Événements** et cliquez sur **Supprimer**.

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 l'onglet **[Événements]**.

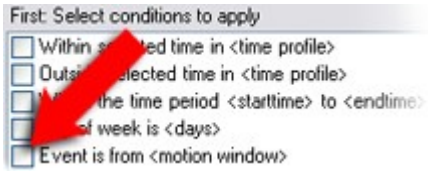
Utiliser plusieurs instances d'un événement

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 :



Périphériques - Masques de confidentialité

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 :

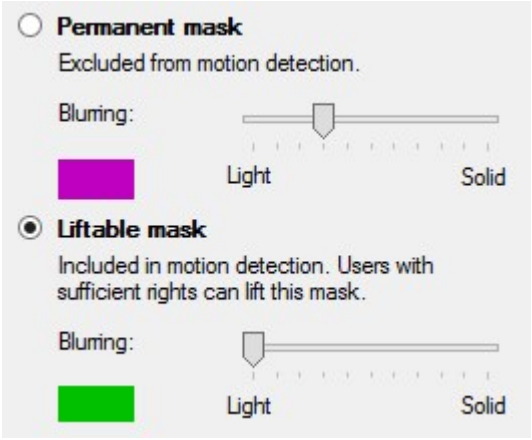
1. Dans le volet **Navigation du site**, sélectionnez **Périphériques**.
2. Sélectionnez le périphérique caméra requis dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Masquage de confidentialité**, cochez ou décochez la case **Masquage de confidentialité**.

> Dans une configuration Milestone Interconnect, le site central ignore les masques de confidentialité définis dans un site distant. Si vous souhaitez utiliser les mêmes masques de confidentialité, vous devez les redéfinir sur le site central.

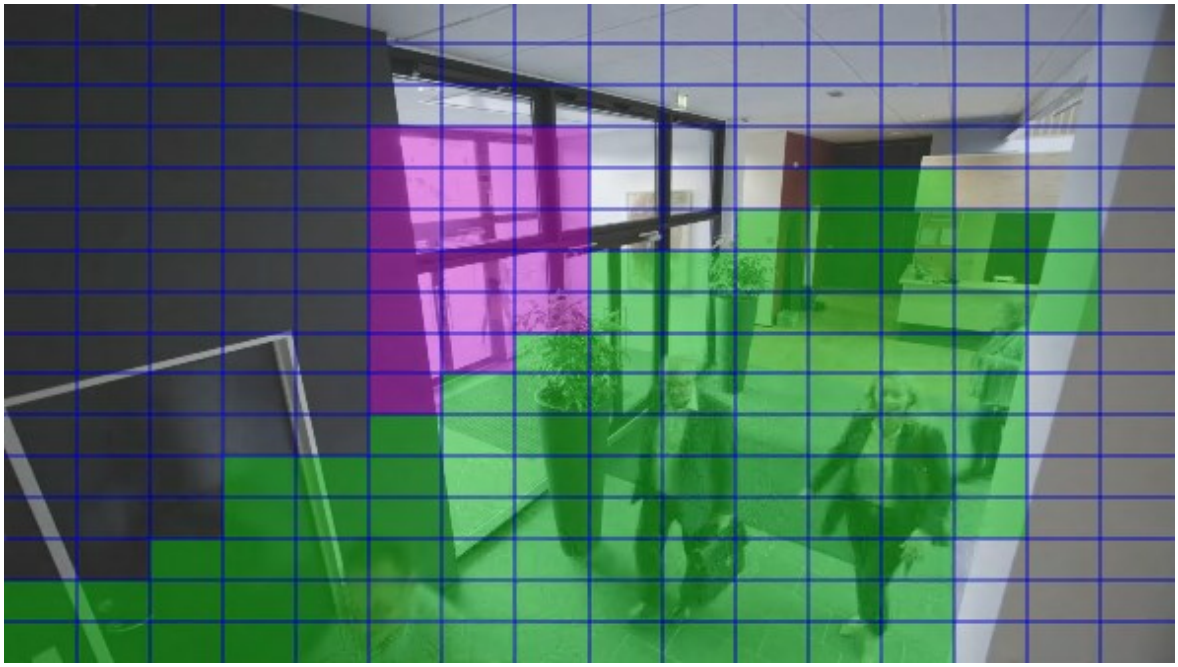
Définir les masques de confidentialité

Lorsque vous activez la fonction de masquage de confidentialité sur l'onglet **masquage de confidentialité**, une grille s'applique à l'aperçu de la caméra.

1. Dans le volet **Navigation du site**, sélectionnez **Périphériques**.
2. Sélectionnez la caméra requise dans le volet **Vue d'ensemble**.
3. Pour couvrir une zone avec un masque de confidentialité, sélectionnez d'abord **Masque permanent** ou **Masque amovible** dans l'onglet **Masquage de confidentialité** pour définir si vous souhaitez un masque de confidentialité permanent ou amovible.



4. Faites glisser le pointeur de souris sur l'aperçu. Cliquez avec le bouton gauche pour sélectionner une cellule de grille. Cliquez avec le bouton droit pour effacer une cellule de grille.
5. Vous pouvez définir autant de zones de masque de confidentialité que nécessaire. Les zones caractérisées par des masques de confidentialité s'affichent en violet et les zones se distinguant par des masques de confidentialité relevables sont en vert.



6. Définissez le mode de couverture des zones doit apparaître dans la vidéo lorsqu'elles s'affichent dans les clients. Utilisez des curseurs pour passer d'un masque de flou lumineux à un masque complètement opaque.

   > Les masques de confidentialité permanents se trouvent également sur l'onglet **Mouvement**.

7. Dans XProtect Smart Client, vérifiez que le masque de confidentialité apparaît tel que vous l'avez défini.

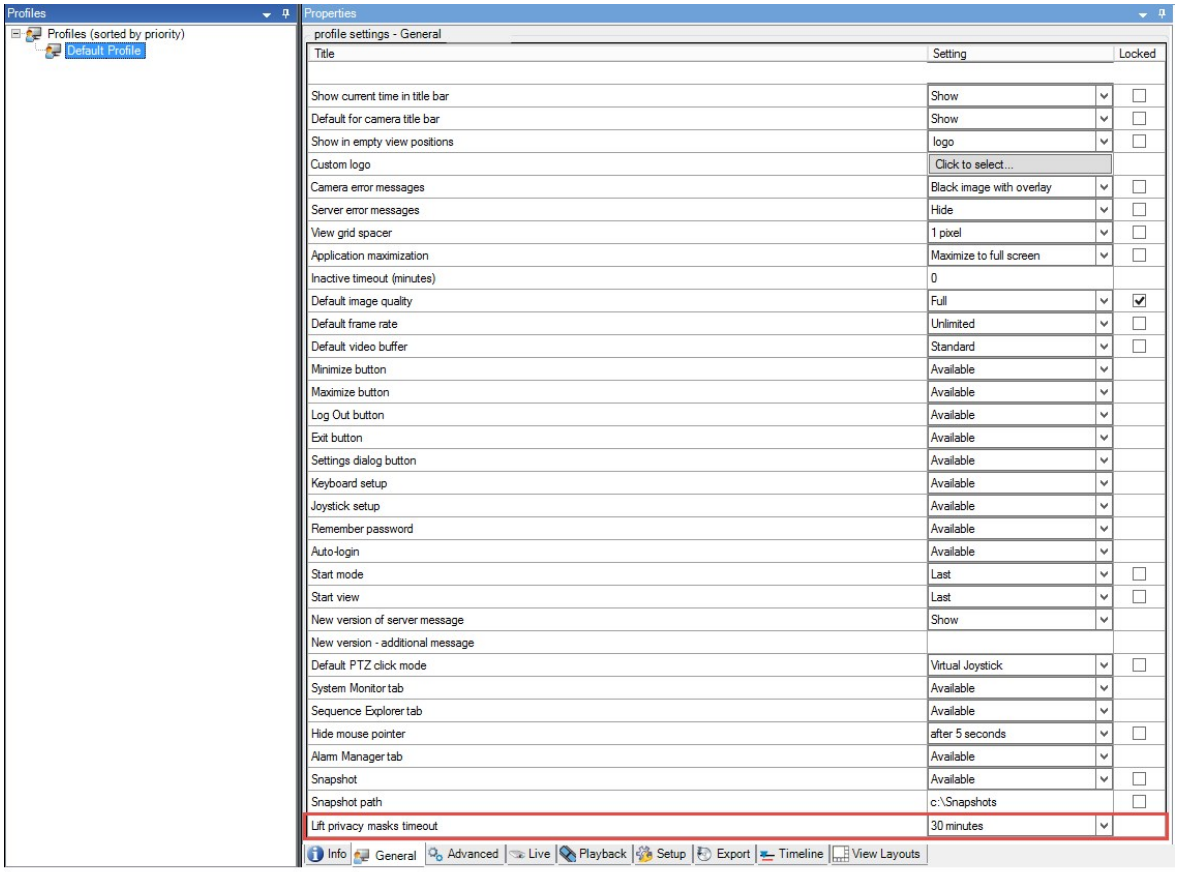
Changez le délai d'expiration des masques de confidentialité

Par défaut, les masques de confidentialité sont levés pendant 30 minutes dans XProtect Smart Client et utilisés par la suite automatiquement, mais vous pouvez modifier tout cela.

> Lorsque vous changez le délai d'expiration, n'oubliez pas de le faire pour le profil Smart Client associé au rôle qui a l'autorisation de lever les masques de confidentialité.

Pour changer le délai d'expiration :

1. Dans **Profils Smart Client**, sélectionnez le profil Smart Client concerné.
2. Sur l'onglet **Général**, repérez l'option **Délai d'expiration des masques de confidentialité**.



3. Sélectionnez parmi les valeurs :
   - **2 minutes**
   - **10 minutes**
   - **30 minutes**
   - **1 heure**
   - **2 heures**
   - **Jusqu'à la déconnexion**
4. Cliquez sur **Enregistrer**.

Donner aux utilisateurs l'autorisation d'enlever les masques de confidentialité

Par défaut, aucun utilisateur n'a l'autorisation de lever les masques de confidentialité dans XProtect Smart Client.

Pour activer/désactiver l'autorisation :

1. Dans le panneau **Navigation du site**, sélectionnez **Sécurité** puis **Rôles**.
2. Sélectionnez le rôle pour lequel vous souhaitez donner la permission aux masques de confidentialité.
3. Sélectionnez **Caméras**, sélectionnez l'onglet **Sécurité globale**.
4. Cochez la cas **Autoriser** de l'autorisation **Lever les masques de confidentialité**.

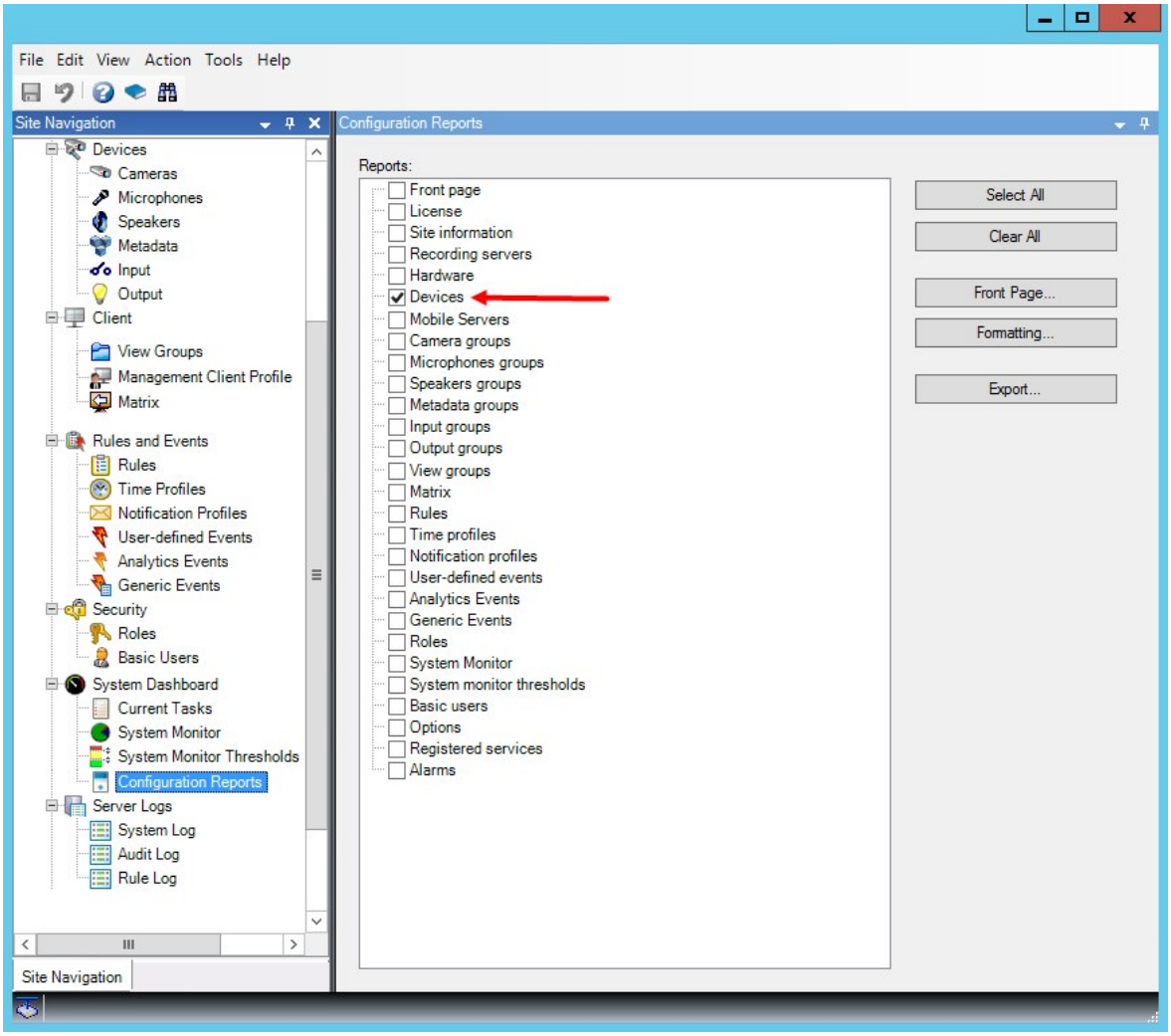
Les utilisateurs que vous affectez à ce rôle peuvent lever les masques de confidentialité configurés en tant que masques relevables pour lui-même et autoriser le levage pour les autres utilisateur de XProtect Smart Client.

Créez un rapport de configuration de votre configuration du masquage de confidentialité

Le rapport sur les périphériques comporte des informations relatives aux paramètres actuels de masquage de confidentialité de vos caméras.

Pour configurer un rapport :

1. Dans le volet **Navigation sur le site**, sélectionnez **Tableau de bord du système**.
2. Dans **Rapports de configuration**, sélectionnez le rapport **Périphériques**.



3. Si vous souhaitez modifier le rapport, vous pouvez modifier la page de couverture et la mise en forme.
4. Cliquez sur l'option **Exportation**, et le système crée le rapport au format de fichier PDF.

Pour plus d'informations sur les rapports, voir Imprimer un rapport avec votre configuration sytème on page 322.

Clients

Groupes de vues (explications)

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.

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 modifier ces autorisations du groupe de vues en configurant ceci dans 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 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

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**.

Aucun rôle ne peut utiliser le groupe de vues nouvellement ajouté tant que ces autorisations n'ont pas été spécifiées. Si vous avez spécifié les rôles qui doivent être capables d'utiliser le groupe de vues nouvellement ajouté, les utilisateurs clients qui sont déjà connectés et dotés des rôles pertinents doivent se déconnecter et se reconnecter avant de pouvoir afficher le groupe de vues.

Profils Smart Client

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 un profil Smart Client**.
3. Dans la fenêtre de dialogue **Ajouter un 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 présentant des paramètres ou des autorisations complexes et que vous avez besoin d'un profil similaire, il peut s'avérer plus simple de copier un profil déjà existant et d'apporter des ajustements mineurs 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 panneau **Vue d'ensemble**, sélectionnez **Copier un 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. Cette opération est effectuée en ajustant les paramètres sur 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 les profils Smart Client, les rôles et les profils de temps :

- Smart Client les profils concernent les paramètres d'autorisation 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.

Conjointement, ces trois fonctionnalités fournissent des possibilités de contrôle et de personnalisation uniques par rapport aux autorisations 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 à 16 h). Une manière de configurer pourrait être comme suit :

1. Créez un profil Smart Client et donnez-lui un nom, par exemple **En 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. Affectez le profil **En direct uniquement** Smart Client et le profil de temps **Journée uniquement** au rôle **Gardien (caméras sélectionnées)** pour connecter les trois éléments.

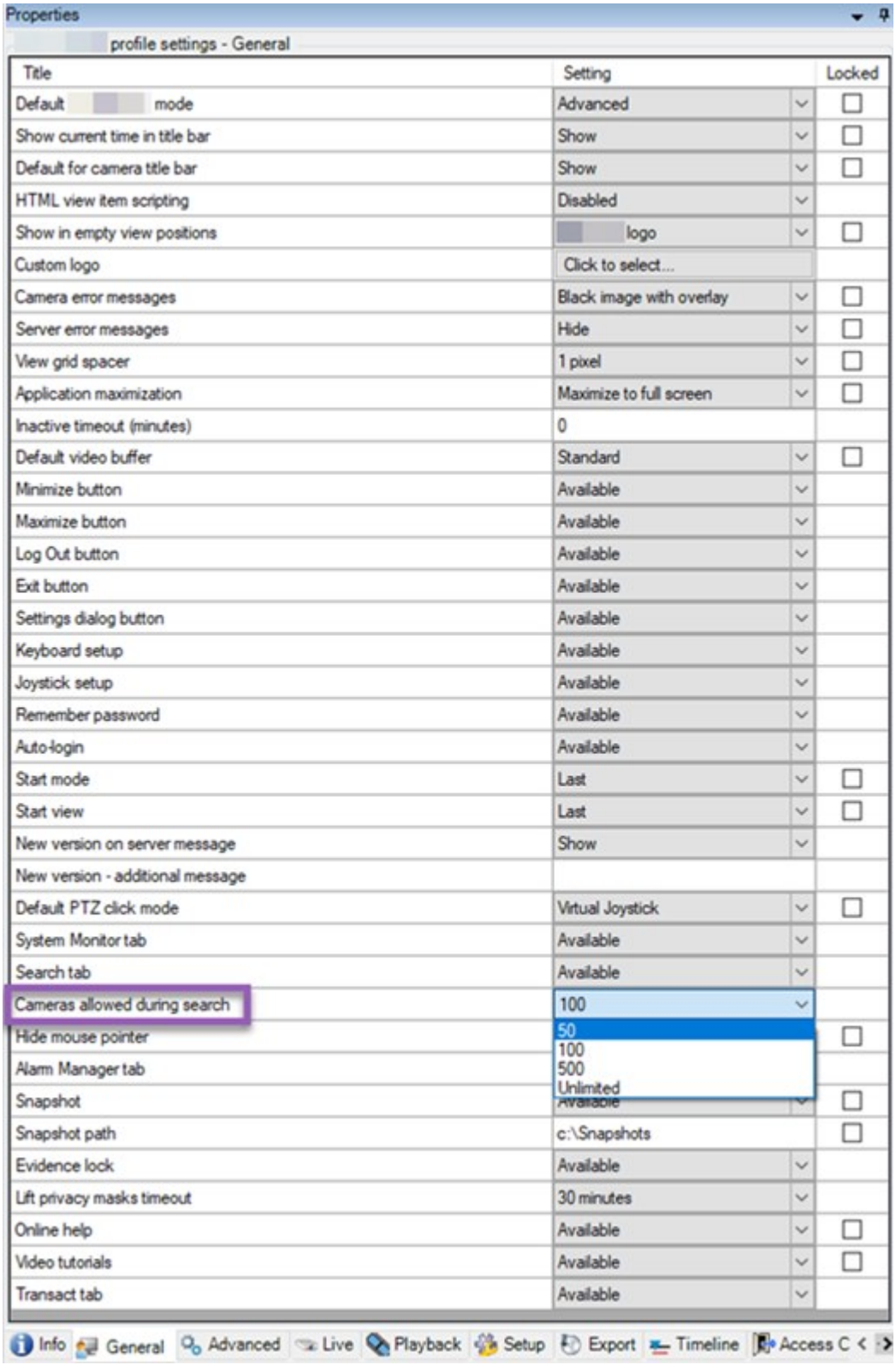
Vous disposez désormais d'une combinaison de trois fonctions créant le résultat souhaité et vous donnant la possibilité d'apporter des ajustements et de procéder à des réglages de précision. Vous pouvez effectuer la configuration dans un ordre différent, par exemple, en créant d'abord le rôle, puis le profil Smart Client et ensuite le profil de temps, ou dans un ordre différent.

Configurer un nombre de caméras autorisées lors de la recherche

Vous pouvez configurer combien de caméras l'opérateur peut-il ajouter à une recherche dans XProtect Smart Client. La valeur par défaut est de **100**. L'opérateur reçoit un avertissement en cas de dépassement de la limite.

1. Dans XProtect Management Client, développez **Client** > **Smart Client Profils**.
2. Sélectionnez le profil concerné.

3. Cliquez sur l'onglet **Général**.



4. Dans les **Caméras** autorisées lors de la recherche, sélectionnez l'une des valeurs suivantes :
    - **50**
    - **100**
    - **500**
    - **Sans restriction**
5. Sauvegardez vos modifications.

Modifier les paramètres d'exportation par défaut

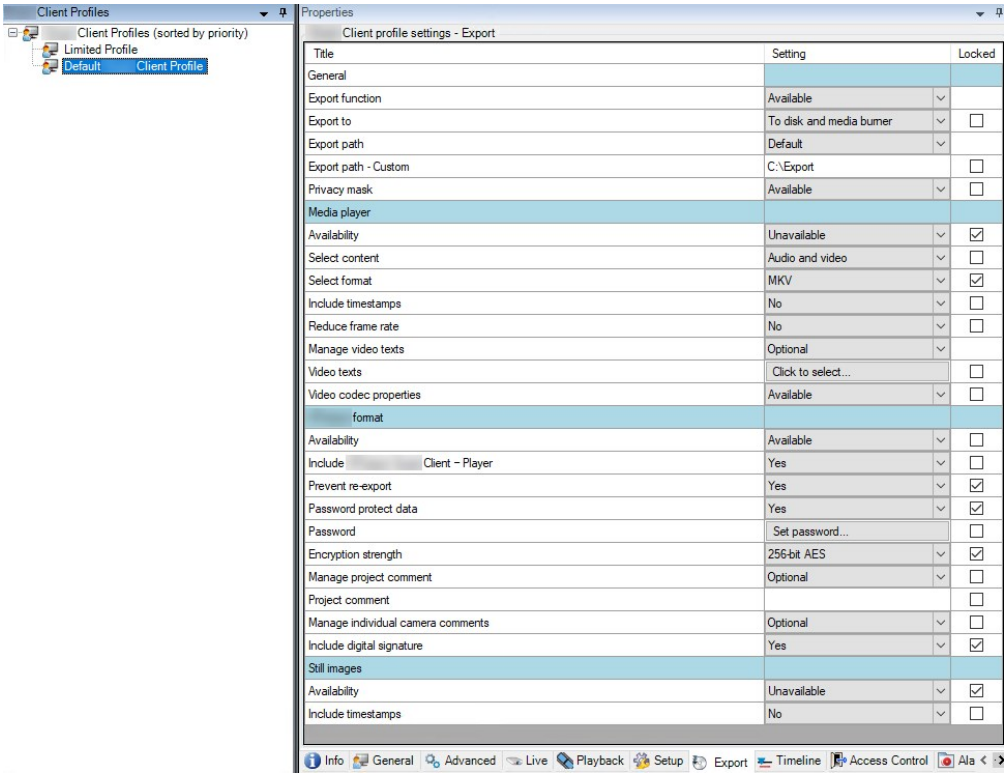
Lorsque vous installez votre système de logiciel de gestion des vidéos XProtect, les paramètres d'exportation par défaut qui définissent les options d'exportation dans XProtect Smart Client sont restreints afin de garantir le niveau de sécurité maximum. Vous pouvez modifier ces paramètres en vue de donner aux opérateurs plus d'options.

Paramètres par défaut

- Seul le format XProtect est disponible
    - La re-exportation est empêchée
    - Les exportations sont protégées par des mots de passe
    - Cryptage AES de 256 bits
    - Les signatures numériques sont ajoutées
- Impossible d'exporter au format MKV ou au format AVI
- Impossible d'exporter des images fixes

Étapes :

1. Dans XProtect Management Client, développez **Client** > **Smart Client Profils**.
2. Sélectionnez **Profil Smart Client par défaut**.
3. Dans le volet **Propriétés**, sélectionnez l'onglet **Exportation**.



4. Pour rendre disponible un format restreint dans XProtect Smart Client, trouvez le paramètre et sélectionnez **Disponible**.
5. Pour permettre aux opérateurs de modifier un paramètre dans XProtect Smart Client, décochez la case **Verrouillé** située à côté du paramètre concerné.
6. Le cas échéant, modifiez d'autres paramètres.
7. (optionnel) Connectez-vous à XProtect Smart Client pour vérifier que vos paramètres ont bien été appliqués.

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 un profil Management Client**.
3. Dans la fenêtre de dialogue **Ajouter un 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 panneau **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.

Gérer la visibilité des fonctions pour un profil Management Client

Associez des profils Management Client à des rôles pour limiter l'interface utilisateur afin de représenter les fonctions disponibles pour chaque rôle d'administrateur.

Associer un profil Management Client à un rôle

1. Développez le noeud **Sécurité** et cliquez sur **Rôles**.
2. Dans l'onglet **Info** dans la fenêtre **Paramètres des rôles**, associez un rôle à un profil. Pour plus d'informations, voir l'onglet Info (rôles).

Gérer l'accès global d'un rôle aux fonctionnalités du système

Les profils Management Client ne traitent que la représentation visuelle des fonctions du système, et non l'accès à celles-ci.

Pour gérer l'accès global d'un rôle aux fonctionnalités du système :

1. Développez le nœud **Sécurité** et cliquez sur **Rôles**.
2. Cliquez sur l'onglet **Sécurité globale** et cochez les cases appropriées. Pour plus d'informations, voir Onglet Sécurité globale (rôles) on page 555.

Dans l'onglet **Sécurité globale**, assurez-vous d'activer l'autorisation de sécurité **Connecter** afin d'octroyer l'accès de tous les rôles à Management Server.

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.

Limiter la visibilité des fonctions pour un profil

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.

1. Développez le noeud Client et cliquez sur Profils Management Client.
2. Sélectionnez un profil et cliquez sur l'onglet Profil.
3. 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.

Matrix

Destinataires Matrix et Matrix (explications)

Matrix est une fonctionnalité qui permet d'envoyer les vidéos à distance.

Un destinataire Matrix est un ordinateur avec XProtect Smart Client, qui est défini en tant que destinataire Matrix dans Management Client.

Si vous utilisez Matrix, vous pouvez envoyer les vidéos de n'importe quelle caméra sur le réseau de votre système vers n'importe quel destinataire Matrix en cours d'exécution.

Pour consulter la liste des destinataires Matrix ajouté dans le Management Client, développez **Client** dans la panneau **Navigation du site**, puis sélectionnez **Matrix**. Une liste des configurations Matrix est affichée dans le volet **Propriétés**.

Dans Management Client, vous devez ajouter chaque destinataire Matrix que vous souhaitez voir recevoir la vidéo déclenchée par Matrix.

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 l'action **Configurer Matrix pour consulter <périphériques>**.
3. Cliquez sur le lien Matrix dans la description initiale de règle.
4. Dans la boîte de dialogue **Sélectionner Matrix configuration**, 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.

Ajouter des destinataires Matrix

Pour ajouter un destinataire Matrix existant dans Management Client :

1. Agrandissez **Clients**, puis sélectionnez **Matrix**.
2. Faites un clic droit sur **Matrix Configurations** et sélectionnez **Ajouter Matrix**.
3. Remplissez les champs de la boîte de dialogue **Ajouter Matrix**.
    1. Dans le champ **Adresse**, saisissez l'adresse IP ou le nom d'hôte du destinataire Matrix souhaité.
    2. Dans le champ **Port**, saisissez le numéro du port utilisé par l'installation du destinataire Matrix.
4. Cliquez sur **OK**.

Vous pouvez maintenant utiliser le destinataire Matrix dans les règles.

> 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.

Envoyer la même vidéo à plusieurs vues XProtect Smart Client

Vous pouvez envoyer la même vidéo aux positions Matrix dans plusieurs des vues XProtect Smart Client, si les positions des vues Matrix partagent le même numéro de port et le même 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

Ajouter des règles

Lorsque vous ajoutez des règles, l'assistant **Gérer les règles** vous guide en affichant uniquement les options concernées.

Il s'assure que les éléments souhaités ne sont pas manquants dans une règle. 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.

Événements

Lorsque vous ajoutez une règle basée sur l'événement, vous pouvez sélectionner différents types d'événements.

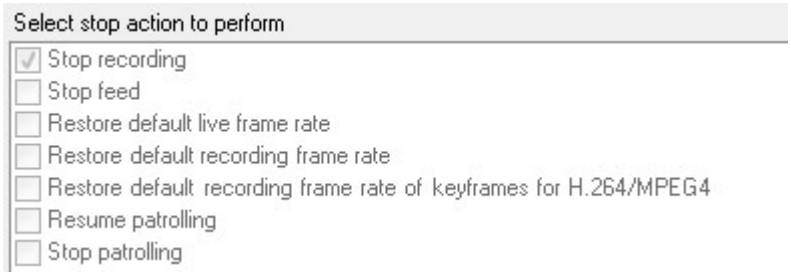
- Voir Vue d'ensemble des événements pour obtenir une vue d'ensemble et une description des types d'événements que vous pouvez sélectionner.

Actions et actions d'arrêt

Lorsque vous ajoutez des règles, vous pouvez sélectionner différentes actions.

Certaines actions exigent une action d'arrêt. Par 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).

- Voir Actions et options d'arrêt pour une vue d'ensemble des actions de démarrage et d'arrêt que vous pouvez sélectionner.

Créer une règle

1. Cliquez avec le bouton droit sur l'article **Règles** > **Ajouter une règle**. Cela ouvre l'assistant **Gestion des règles**. L'assistant vous guide dans la spécification du contenu de votre règle.
2. Spécifiez un nom et 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 seconde 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>** :

En fonction de vos sélections, modifiez la description de la règle dans la partie inférieure de la fenêtre de l'assistant :

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**.

Valider des règles

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 une règle** assure la validité de tous les éléments des règles.

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**.

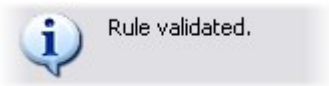
Valider une règle

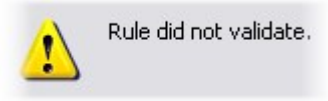
1. Cliquez sur **Règles** puis sélectionnez la règle que vous souhaitez valider.
2. Effectuez un clic droit sur la règle et cliquez sur **Valider la règle.**
3. Cliquez sur **OK**.

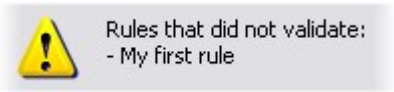
Valider toutes les règles

1. Effectuez un clic droit sur l'élément **Règles** puis cliquez sur **Valider toutes les règles**. .
2. Cliquez sur **OK**.

Une boîte de dialogue vous indique si la ou les règles ont été bien validées. Si vous choisissez de valider plus d'une règle et qu'une ou plusieurs règles n'ont pas été exécutées, la boîte de dialogue énumère les noms des règles affectées.







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 est validée 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.

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. Si vous sélectionnez **Copier la règle**, l'assistant ouvre un affichage d'une copie du règle sélectionnée. Cliquez sur **Finir** pour créer une copie.
4. Si vous sélectionnez **Modifier la règle**, l'assistant s'ouvre et vous pouvez saisir les changements. Cliquez sur **Terminer** pour accepter les changements.
5. Si vous sélectionnez **Renommer la règle**, vous pouvez renommer directement le texte du nom de la règle.

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** :

Activer une règle

Lorsque vous souhaitez réactiver la règle, sélectionnez la règle, cochez la case **Activer** et sauvegardez la configuration.

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**.

Ajouter un temps récurrent

Lorsque vous sélectionnez **Ajouter une période récurrente**, la fenêtre **Sélectionner la période récurrente** s'affiche :

1. Dans la fenêtre **Sélectionner la période**, indiquez la plage horaire, le schéma 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.

Temps récurrent

Lorsque vous configurez une action pour qu'elle soit exécutée sur un calendrier détaillé et périodique.

Par exemple :

- Chaque semaine, le mardi, à chaque heure entre 15h00 et 15h30
- Le 15 du mois tous les 3 mois à 11h45
- Chaque jour, chaque heure entre 15h00 et 19h00

> L'heure est configurée en fonction des paramètres de l'heure locale du serveur sur lequel Management Client est installé.

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**.

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.

Créer des profils de durée du jour

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 durée du jour**.
3. Dans la fenêtre **Profil de durée du jour**, référez-vous au tableau de propriétés ci-dessous pour remplir les informations demandées. 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 géographiques 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 durée du jour

Nom	Description
Nom	Le nom du profil.
Description	Une description du profil (facultatif).
Coordonnées géographiques	Coordonnées géographiques 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.

Ajouter des profils de notification

Avant de pouvoir créer des profils de notification, vous devez préciser les paramètres du serveur de messagerie pour les notifications par e-mail. Pour plus d'informations, voir Conditions préalables à la création des profils de notification.

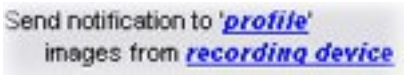
1. Développez **Règles et événements**, faites un clic droit sur **Profils de notification** > **Ajouter profil de notification**. Cela ouvre l'assistant **Ajouter profil de notification**.
2. Précisez le nom et une description. Cliquez sur **Suivant**.
3. Saisissez le destinataire, l'objet, le texte du message et la durée entre les messages.
4. Pour envoyer une notification par e-mail test aux destinataires indiqués, cliquez sur **Envoyer un courriel test**.
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.

> Les notifications contenant des vidéos encodées au format H.265 requièrent un ordinateur prenant en charge l'accélération du matériel.

7. Cliquez sur **Terminer**.

Déclencher les notifications par e-mail depuis les règles

1. Effectuez un clic droit sur l'article **Règles** puis cliquez sur > **Ajouter une règle** ou **Modifier une règle**.
2. Dans l'assistant **Gérer la règle**, cliquez sur **Suivant** pour accéder à la liste **Sélectionner des actions à exécuter**, puis sélectionnez **Envoyer une notification à <profil>**.
3. Sélectionnez le profil de notification concerné et sélectionnez les caméras depuis lesquelles doivent provenir les enregistrements à inclure dans les notifications par e-mail du profil de notification.



Vous ne pouvez pas inclure d'enregistrements dans les notifications par e-mai du profil de notification à moins que quelque chose soit déjà en cours d'enregistrement. 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** :

Ajouter un événement défini par l'utilisateur

> 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.

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**.

L'utilisateur peut maintenant déclencher l'événement défini par l'utilisateur manuellement dans XProtect Smart Client si l'utilisateur dispose des autorisations correspondantes.

> 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.

Renommer un événement défini par l'utilisateur

> 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.

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**.

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.

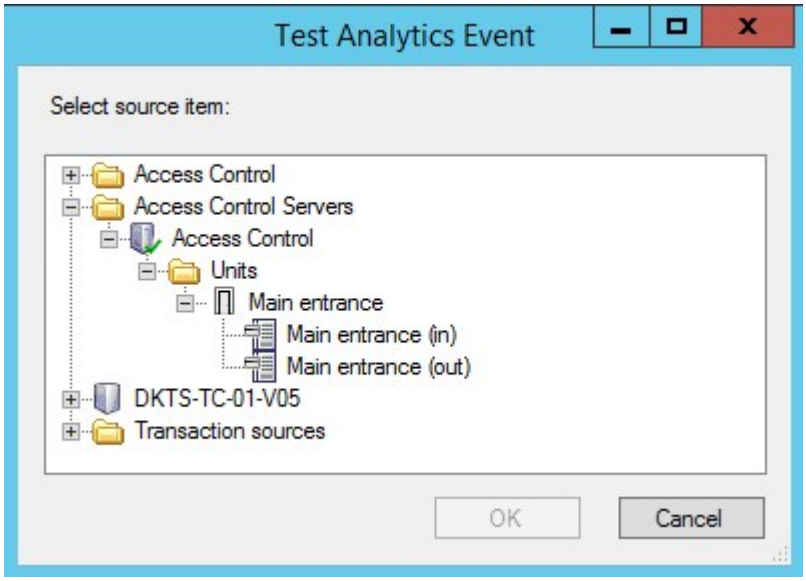
Modifier les paramètres des événements analytiques

Dans la barre d'outils, allez dans **Outils** > **Options** > **Événements analytiques** pour modifier les paramètres pertinents.

Tester un événement analytique

Après avoir créer un événement analytique, vous pouvez tester les exigences (voir Ajouter et modifier un événement analytique on page 303), par exemple, que la fonction d'événements analytiques a été établie 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, vous pouvez dans XProtect Smart Client 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 d'alarme**.

Ajouter un événement générique

Vous pouvez définir des événements génériques pour aider le VMS 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.

Configuration
Vous avez des événements génériques activés et avez précisé les destinations sources autorisées. Pour plus d'informations, voir Onglet Événements génériques (options) on page 433.

Pour ajouter un événement générique :

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 plus d'informations, voir Événements génériques et sources de données (propriétés) on page 550.
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**.

Authentification

Enregistrer les demandes à partir d'un IDP externe

1. Dans Management Client, sélectionnez **Outils** > **Options** et ouvrez l'onglet **IDP Externe**.
2. Dans la section **IDP Externe**, sélectionnez **Ajouter**.
3. Dans la section **Demandes enregistrées**, sélectionnez **Ajouter**.

4. Saisissez les informations sur la demande. Pour de plus amples informations, consultez Enregistrer des demandes.

Allocation automatique des utilisateurs avec un IDP externe

XProtect prend en charge la synchronisation d'identité entre votre fournisseur d'identité et le VMS via un système de gestion des identités inter-domaines (SCIM).

SCIM permet l'attribution automatique d'utilisateurs lors de l'accès au VMS à l'aide d'un IDP externe. Toutes les modifications apportées aux autorisations d'utilisateur sont instantanément répercutées dans le VMS sans nécessiter de nouvelle connexion.

Pour appliquer l'attribution automatique d'utilisateurs par SCIM avec un IDP externe, le fournisseur d'identité de votre système doit être configuré comme IDP externe. Pour plus d'informations, voir Ajouter et configurer un IDP externe on page 242.

Échange SCIM et identité utilisateur

Lors de l'échange SCIM, les utilisateurs configurés dans votre IDP externe sont mis en correspondance avec les utilisateurs de XProtect. La propriété d'ID de l'utilisateur est utilisée comme identifiant principal. Par défaut, la propriété a la valeur d'une sous-revendication, mais cela peut varier en fonction du fournisseur d'identité. Une non-concordance peut entraîner l'allocation de l'utilisateur deux fois lors du processus de connexion.

La sous-revendication n'est pas la même que la revendication utilisée comme source des noms d'utilisateur créés lors de la configuration de l'IDP externe.

Pour plus d'informations sur la configuration de l'identifiant principal, voir Présentation de SCIM.

Configuration d'un fournisseur d'identité (Identity Provider, IDP) pour SCIM

En général, pour configurer votre fournisseur d'identité (Identity Provider, IDP) pour SCIM, vous configurez un client avec les autorisations SCIM et l'associez à un fournisseur externe.

Si votre IDP externe est déployé sur votre réseau local, vous utilisez l'URL de l'IDP du VMS dans la configuration SCIM de l'IDP externe pour créer l'association.

Si votre IDP externe se trouve sur un réseau qui ne peut pas communiquer directement avec le réseau sur lequel votre VMS est déployé, vous pouvez utiliser l'URL fournie par un outil de tunneling de communication comme point d'entrée vers l'IDP de votre VMS.

Contenu des noms d'utilisateur

Pour assurer le bon fonctionnement de la procédure de synchronisation de SCIM entre votre IDP externe et le VMS, le nom des identités fournies doit être conforme aux conventions de dénomination de XProtect et ne peut contenir aucun des caractères suivants : ?, \, /, [,].

Supprimer des utilisateurs

Afin de gérer la suppression des utilisateurs conformément à leurs politiques et exigences, il est possible que certains fournisseurs d'identité ne suppriment pas définitivement les utilisateurs du système. Au lieu de cela, les utilisateurs peuvent être désactivés, et donc traités comme s'ils n'existaient plus.

Si une suppression permanente est requise, un administrateur XProtect peut activer un paramètre qui supprime définitivement les utilisateurs du VMS après un nombre de jours spécifié (30 étant la valeur par défaut). Le paramètre est activé et le délai peut être défini via une API. Pour connaître les étapes à suivre, consultez la section Présentation de SCIM.

Mapper des demandes à partir d'un IDP externe vers des rôles dans XProtect

Sur le site de l'IDP externe, l'administrateur doit créer des revendications comprenant un nom et une valeur. Ensuite, la demande est mappée à un rôle dans le VMS, et les privilèges de l'utilisateur seront déterminés par le rôle.

Les revendications que vous souhaitez utiliser dans les rôles doivent être ajoutées à la configuration IDP avant de pouvoir être sélectionnées dans les rôles. Les revendications peuvent être ajoutées dans l'onglet **IDP externe** de la boîte de dialogue **Options** . Onglet IDP externe (options) on page 423. Si une revendication n'est pas ajoutée à la configuration IDP, vous ne pourrez pas la sélectionner dans les rôles.

Lorsque vous utilisez des revendications pour lier des utilisateurs IDP externes à des rôles VMS, les utilisateurs IDP externes ne sont pas ajoutés aux rôles comme des utilisateurs basiques ou AD ordinaires. Au lieu de cela, ils sont liés dynamiquement à chaque nouvelle session sur la base de leurs revendications actuelles.

1. À partir du volet **Navigation du site** dans Management Client, développez le noeud **Sécurité** et sélectionnez **Rôles**.
2. Sélectionnez un rôle, sélectionnez l'onglet **IDP externe**, puis sélectionnez **Ajouter**.
3. Sélectionnez un IDP externe et un nom de revendication et saisissez une valeur de revendication.

   Le nom de la revendication doit être écrit exactement comme le nom de revendication provenant de l'IDP externe.

4. Sélectionnez **OK**.

Si un IDP externe est supprimé, tous les utilisateurs connectés au VMS via l'IDP externe sont aussi supprimés. Toutes les revendications enregistrées qui sont connectées à l'IDP externe sont supprimées et tout mappage des rôles sont également supprimés.

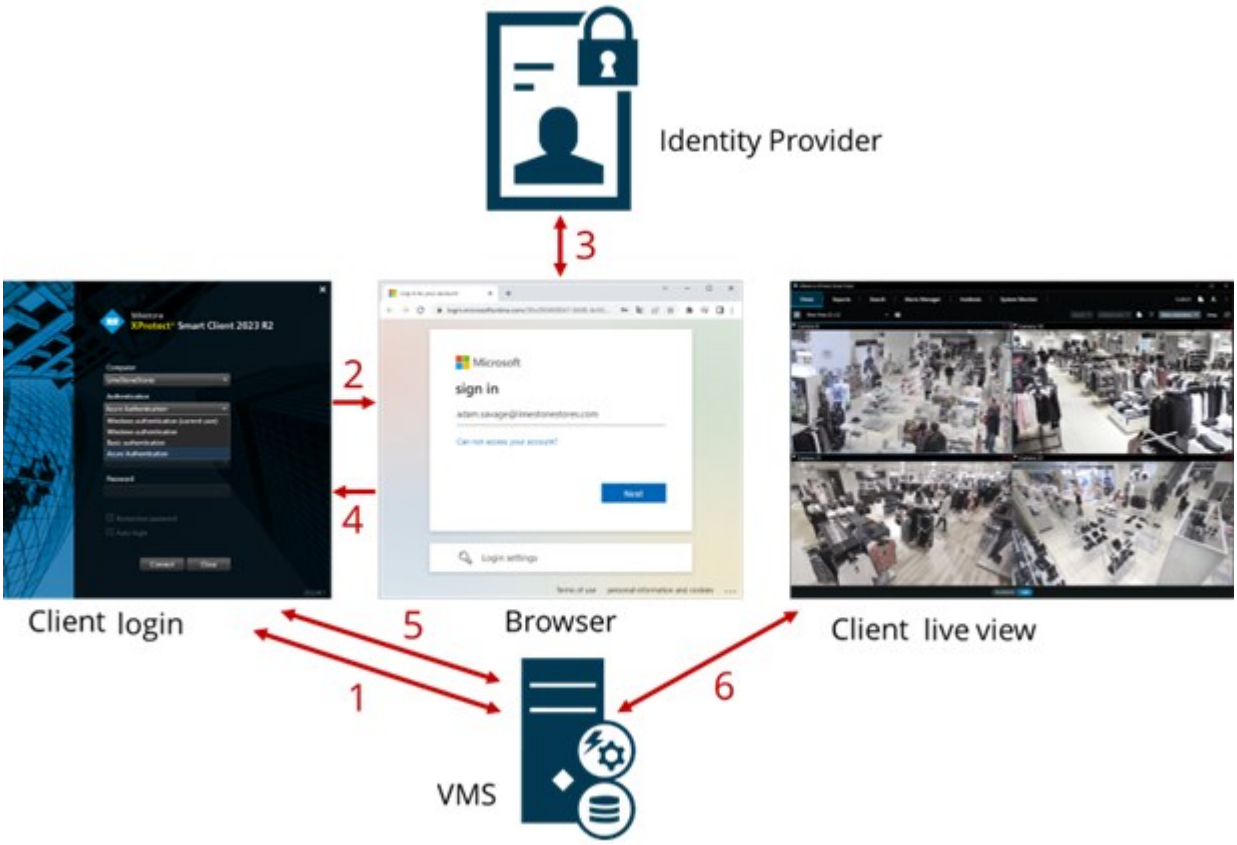
Sous **Rôles effectifs**, vous pouvez obtenir un aperçu du rôle dynamique des utilisateurs IDP externes. Il s'agit de l'appartenance au rôle qui est basée sur la dernière session de connexion de l'utilisateur IDP externe. Pour plus d'informations, voir Afficher les rôles effectifs on page 310.

Connexion via un IDP externe

Vous pouvez vous connecter à XProtect Smart Client, XProtect Management Client, XProtect Web Client et au client XProtect Mobile en utilisant un IDP externe.

Authentification IDP externe

L'illustration suivante donne un aperçu du flux d'authentification IDP externe. Le flux utilise Microsoft Entra ID (Azure) pour illustrer le processus d'authentification.



1. Dans le champ **Ordinateur** de XProtect Smart Client ou XProtect Management Client, saisissez l'adresse de l'ordinateur VMS XProtect et sélectionnez l'IDP externe sous **Authentification**. Les champs **Nom d'utilisateur** et **Mot de passe** sont désactivés.
2. Cliquez sur **Connecter** pour ouvrir la page d'authentification de l'IDP externe à partir d'un navigateur.
3. Sur la page d'authentification, saisissez votre e-mail et cliquez sur **Suivant**.
4. Saisissez votre mot de passe et cliquez sur le bouton de connexion.
5. Lorsque vous recevez la confirmation que l'authentification de l'utilisateur est réussie, vous pouvez fermer le navigateur. Le client VMS poursuit la procédure de connexion normale et, une fois celle-ci terminée, le client s'affiche et vous êtes connecté.

Pour plus d'informations concernant la connexion à XProtect Web Client, voir Se connecter et à propos de la connexion à XProtect Mobile, voir Se connecter à l'application XProtect Mobile.

Sous **Outils** > **Options** > **IDP externe**, vous pouvez configurer le nom de l'IDP externe qui est affiché dans la liste **Authentification**.

Si l'IDP externe est désactivé, par exemple, par une restauration ou un changement de mot de passe, l'option de connexion via IDP externe n'est pas disponible dans la liste **Authentification**. De même, si l'IDP externe est désactivé, le secret du client reçu depuis l'IDP externe disparaît du champ **Secret du client** dans l'onglet **IDP externe** sous **Outils** > **Options**.

Sécurité

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 puis 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.

Pour plus d'informations, voir Assigner et supprimer des utilisateurs et groupes aux/des rôles on page 310 et Rôles (noeud Sécurité) on page 552.

Copier, renommer ou supprimer un rôle

Copier un rôle

Si vous avez un rôle avec des paramètres et/ou autorisations 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**.

> Si vous supprimez un rôle, vous ne supprimez pas automatiquement le groupe de vues basé sur le rôle.

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, saisissez 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 de navigation "**...**". Sélectionnez le type d'objet, entrez le nom et cliquez sur **OK**. Les rôles d'utilisateur s'affichent automatiquement.

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. Sinon, utilisez la fonction **« Avancée... »** pour rechercher des utilisateurs ou 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**.

Créer des utilisateurs de base

Il existe deux types de comptes utilisateur dans Milestone XProtect VMS : les utilisateurs basiques et les utilisateurs Windows.

Les utilisateurs basiques sont des comptes utilisateurs que vous créez dans Milestone XProtect VMS. Il s'agit d'un compte utilisateur système dédié, avec un nom d'utilisateur basique et une authentification par mot de passe pour chaque utilisateur individuel.

Les utilisateurs Windows sont des comptes utilisateurs que vous pouvez ajouter via Active Directory de Microsoft.

Il existe quelques différences entre les utilisateurs basiques et les utilisateurs Windows :

- Les utilisateurs basiques sont authentifiés par une combinaison nom d'utilisateur et mot de passe et sont spécifiques à un système/site. Notez que même si un utilisateur basique créé sur un site fédéré a le même nom et mot de passe qu'un utilisateur de base sur un autre site fédéré, l'utilisateur de base n'a accès qu'au site sur lequel il a été créé.
- Les utilisateurs Windows sont authentifiés à partir de leurs identifiants de connexion Windows et sont spécifiques à une machine.

Configurer les paramètres de connexion pour les utilisateurs basiques

Vous pouvez définir les paramètres de connexion pour les utilisateurs basiques dans un fichier JSON, qui se trouve ici : `\\Program Files\Milestone\Management Server\IIS\IDP\appsettings.json« »`.

Ce fichier vous permet de configurer les paramètres suivants :

LoginSettings	
"ExpireTimeInMinutes": 5	Définir la période de temps (en minutes) après laquelle une session de connexion expirera si l'utilisateur n'effectue aucune action.
LockoutSettings	
"LockoutTimeSpanInMinutes": 5	Définir la période de temps (en minutes) après laquelle un utilisateur

	sera bloqué.
"MaxFailedAccessAttempts": 5	Définir le nombre de tentatives de connexion d'un utilisateur avant d'être bloqué.
PasswordSettings	
"RequireDigit": true	Définir si des chiffres de base (de 0 à 9) sont requis dans un mot de passe.
"RequireLowercase": true	Définir si des minuscules sont requises dans un mot de passe.
"RequireNonAlphanumeric": true	Définir si des caractères spéciaux (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/) sont requis dans un mot de passe.
"RequireUppercase": true	Définir si des majuscules sont requises dans un mot de passe.
"RequiredLength": 8	Définir si le nombre de caractères requis dans un mot de passe. Il existe un minimum de longueur du mot de passe de {0} caractère et un maximum de 255 caractères.
"RequiredUniqueChars": 1	Définir si le minimum de nombre de caractères uniques requis dans un mot de passe. Par exemple, si vous configurez le nombre de caractères uniques à 2 caractères, alors les mots de passe, tels que « aaaaaa, aa, a, b, bb, bbbbbbb » seront rejetés. Au contraire, les mots de passe « abab, abc, aaab, etc. » seront acceptés car ils comportent au moins deux caractères uniques. L'augmentation du nombre de caractères uniques dans un mot de passe augmente la force du mot de passe en évitant des séquences répétitives qui sont facilement devinées.

Pour créer un utilisateur de base sur votre système :

1. Développez **Sécurité** > **Utilisateurs de base**.
2. Dans le volet **Utilisateurs basiques**, faites un clic droit et sélectionnez **Créer un utilisateur basique**.
3. Spécifier un nom d'utilisateur et un mot de passe. Répétez le mot de passe pour être sûr(e) de l'avoir entré correctement.

Le mot de passe doit respecter la complexité définie dans le fichier **appsettings.json** (voir Configurer les paramètres de connexion pour les utilisateurs basiques on page 312).

4. Indiquez si lutilisateur basique doit modifier son mot de passe lors de sa prochaine connexion. Milestone recommande de cocher la case afin que les utilisateurs basiques puissent spécifier leurs propres mots de passe lorsqu'ils se connectent pour la première fois.

   Vous devez décocher la case uniquement lorsque vous créez des utilisateurs basiques qui ne peuvent pas changer leur mot de passe. De tels utilisateurs basiques, par exemple, des utilisateurs système, sont utilisés pour les modules d'extension et l'authentification des services du serveur.

5. Indiquez l'état de l'utilisateur basique sur **Activé** ou **Déconnecté**.

6. Cliquez sur **OK** pour créer l'utilisateur de base.

Voir le status du cryptage vers les clients

Pour vérifier si votre serveur d'enregistrement crypte les connexions :

1. Ouvrez le Management Client.

2. Dans le panneau **Navigation du site**, sélectionnez **Serveurs** > **Serveurs d'enregistrement**. Cette commande ouvre une liste de serveurs d'enregistrement.

3. Dans le volet **Vue d'ensemble**, sélectionnez le serveur d'enregistrement concerné, puis allez sur l'onglet **Info**.
   Si le cryptage est activé vers les clients et serveurs récupérant des flux de données depuis le serveur d'enregistrement, une icône représentant un cadenas apparaîtra devant l'adresse du serveur Web local et l'adresse du serveur Web optionnel.

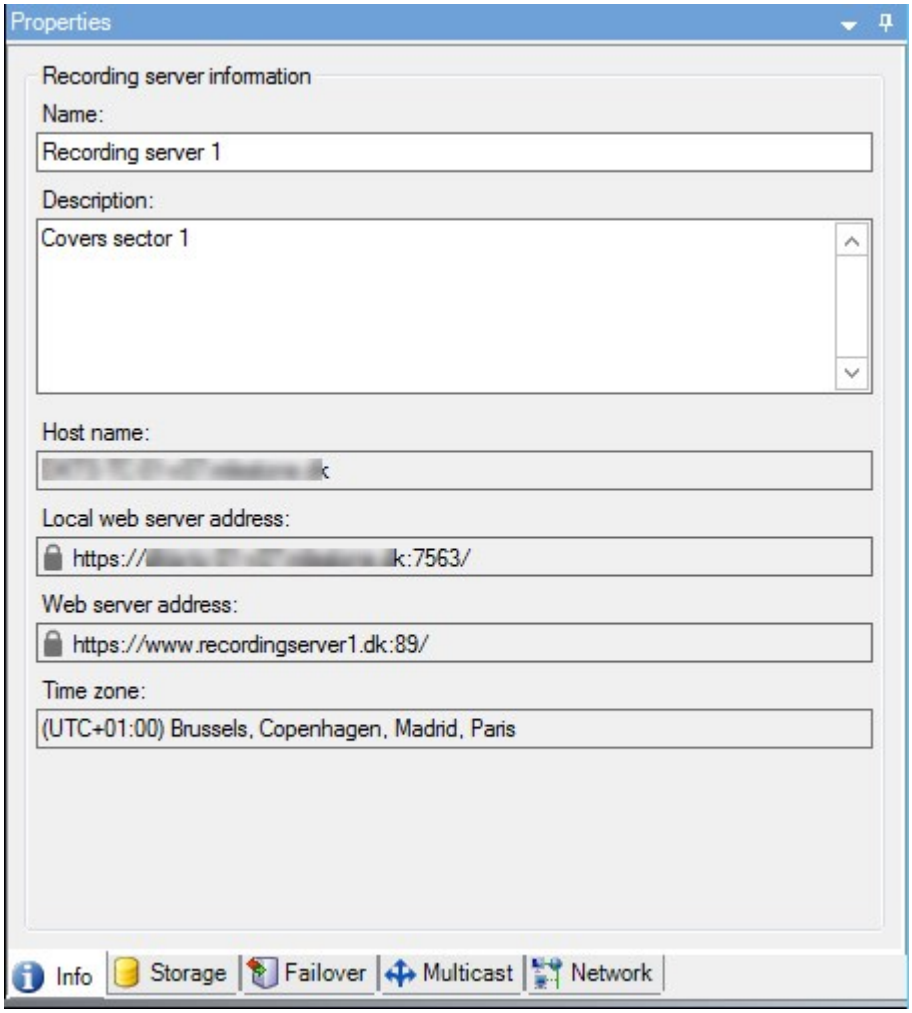


Tableau de bord système

Afficher les tâches en cours sur les serveurs d'enregistrement

La fenêtre **Tâches actuelles** affiche une vue d'ensemble des tâches en cours sous un serveur d'enregistrement spécifique. Si vous avez débuté une tâche qui prend du temps et qui s'exécute en arrière-plan, vous pouvez ouvrir la fenêtre **Tâches actuelles** pour consulter les progrès de la tâche. Parmi les exemples des tâches démarrées par l'utilisateur qui sont longues, figurent les mises à jour du firmware et le mouvement du matériel. Vous pouvez voir les informations sur l'heure de début, l'heure de fin estimée et le progrès de la tâche.

Si la tâche ne suit pas la progression espérée, vous pouvez probablement en trouver la cause dans votre matériel ou réseau. Parmi les exemples figurent un serveur qui ne s'exécute pas, une erreur de serveur, une bande passante trop étroite ou une perte de connexion.

1. Dans le volet **Navigation sur le site**, sélectionnez **Tableau de bord du système** > **Tâches en cours**.
2. Sélectionnez un serveur d'enregistrement pour afficher ses tâches en cours.

Les informations affichées dans la fenêtre **Tâches actuelles** ne sont pas mises à jour de façon dynamique mais il s'agit d'une capture d'écran des tâches actuelles de l'instant où vous avez ouvert la fenêtre. Si la fenêtre est ouverte depuis quelque temps, actualisez les informations en sélectionnant le bouton **Actualiser** situé dans le coin inférieur droit de la fenêtre.

Moniteur système (explications)

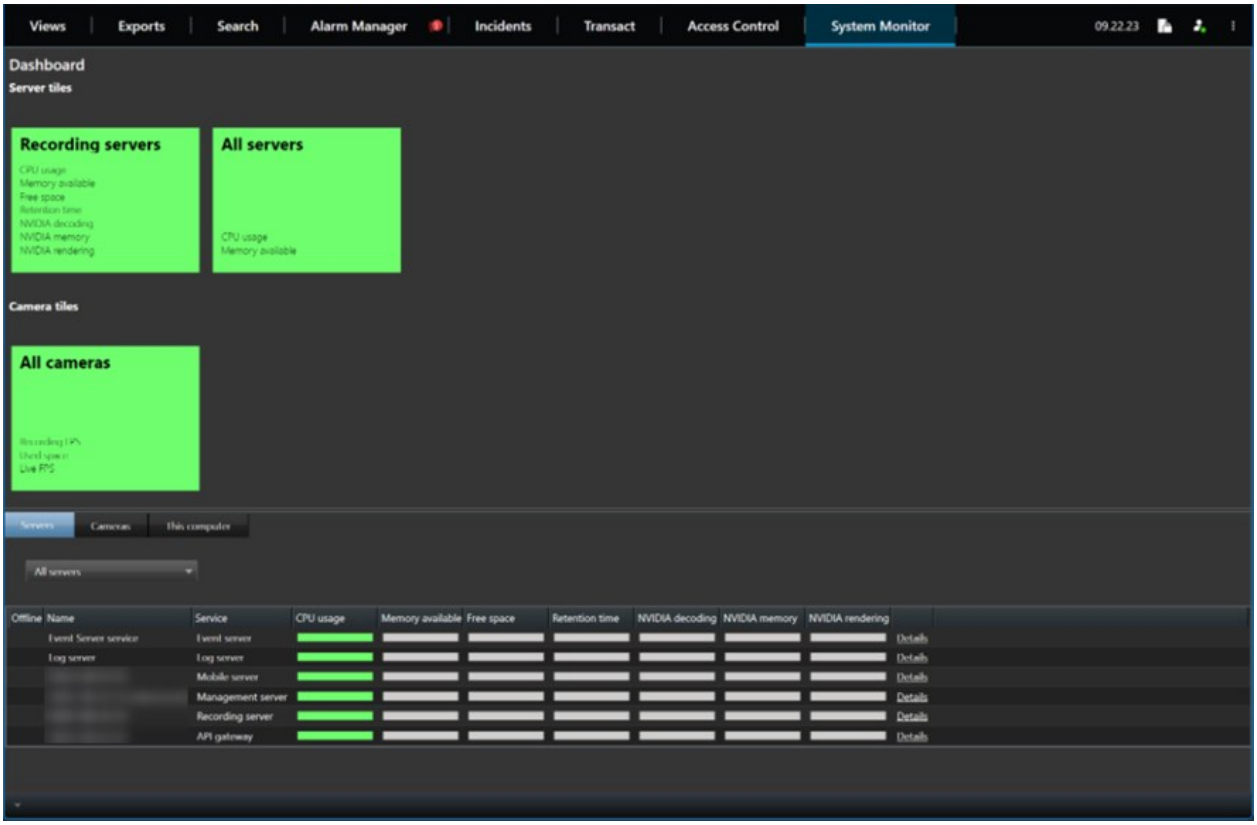
La fonctionnalité du moniteur système requiert que le service Data Collector s'exécute et fonctionne uniquement sur les ordinateurs utilisant un calendrier grégorien (occidental).

Tableau de bord du système (explications)

Dans le **Tableau de bord du moniteur système**, vous pouvez obtenir facilement une vue d'ensemble du bon état votre système de logiciel de gestion des vidéos. L'état de votre matériel est représenté visuellement par des tuiles et leurs couleurs : vert (en cours d'exécution), jaune (avertissement) et rouge (critique). Les tuiles peuvent également afficher des icônes d'erreur ou d'avertissement lorsqu'un ou plusieurs éléments du matériel sont défectueux.

Par défaut, le système affiche des tuiles qui représentent tous les **Serveurs d'enregistrement**, **Toutes les caméras** et **Toutes les caméras**. Vous pouvez personnaliser les paramètres de surveillance de ces tuiles par défaut et créer de nouvelles tuiles. 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.

Les paramètres de surveillance sont, par exemple, l'usage du processeur ou la mémoire disponible pour un serveur. Une tuile surveille uniquement les paramètres de surveillance que vous avez ajoutés à cette tuile. Voir Ajouter une nouvelle tuile de caméra ou de serveur dans le tableau de bord du Moniteur système on page 320, Modifier une tuile de caméra ou de serveur dans le tableau de bord du moniteur système on page 320, et Supprimer une tuile de caméra ou de serveur dans le tableau de bord du Moniteur système on page 320 pour plus d'informations.



Seuils du Moniteur système (explications)

Les seuils du moniteur système vous permettent de définir et ajuster les seuils lorsque les tuiles du **Tableau de bord du moniteur système** doivent indiquer visuellement que le matériel de votre système change d'état. Par exemple, lorsque l'utilisation du CPU d'un serveur passe d'un état normal (vert) à un état d'avertissement (jaune) ou d'un état d'avertissement (jaune) à un état critique (rouge).

Le système a des seuils définis par défaut pour tous les matériels du même type afin que vous puissiez surveiller l'état du matériel de votre système depuis le moment où vous avez installé votre système et celui où vous avez ajouté le matériel. Vous pouvez également configurer des seuils pour des serveurs, caméras, disques et du stockage individuels. Pour modifier les seuils, voir Modifier les seuils lorsque les états du matériel doivent changer on page 321.

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 la fonctionnalité **Intervalle de calcul**. Un bon paramètre de calcul de l'intervalle vous évitera de recevoir des faux positifs sur le dépassement du seuil. Vous recevrez uniquement des alertes sur des problèmes concernant, par exemple, l'utilisation du CPU ou la consommation de la mémoire.

Vous pouvez également configurer des règles (voir Règles (explications)) pour exécuter des actions spécifiques ou activer des alarmes lorsqu'un seuil passe d'un état à un autre.

Afficher l’état en cours de votre matériel et le dépanner si nécessaire

Dans le **Tableau de bord du moniteur système**, vous pouvez obtenir facilement une vue d’ensemble du bon état votre système de logiciel de gestion des vidéos. L’état de votre matériel est représenté visuellement par des tuiles et leurs couleurs : vert (en cours d’exécution), jaune (avertissement) et rouge (critique). Les tuiles peuvent également afficher des icônes d’erreur ou d’avertissement lorsqu’un ou plusieurs éléments du matériel sont défectueux.

Vous pouvez modifier les seuils pour lesquels un matériel se trouve dans un des trois états. Pour plus d’informations, voir Modifier les seuils lorsque les états du matériel doivent changer on page 321.

Le **Tableau de bord du moniteur système** répond aux questions, telles que : tous les services du serveur et des caméras s’exécutent-ils ? L’utilisation du CPU et la mémoire disponible sur les différents serveurs sont-il suffisants pour que tout soit enregistré et disponible au visionnage ?

1. Dans le volet **Navigation sur le site**, sélectionnez **Tableau de bord du système** > **Moniteur système**.
2. Si toutes les tuiles sont vertes et dépourvues d’icônes d’avertissement ou d’erreur, alors tous les paramètres de surveillance et tous les serveurs et toutes les caméras représentés par les tuiles s’exécutent bien.
   Si une ou plusieurs tuiles affichent une icônes d’avertissement ou d’erreur, ou si elles sont complètement jaunes ou vertes, sélectionnez-en une à dépanner.
3. Dans la liste des matériels comportant des paramètres de surveillance (en bas de la fenêtre), trouvez le matériel qui ne s’exécute pas. Placez le curseur de la souris sur la croix rouges située à côté du matériel pour lire quel est le problème.
4. Sinon, sélectionnez **Détails** situé à droite du matériel pour voir quand le problème est survenu. Activez la collecte des données historiques pour consulter l’état de votre matériel au fil du temps. Pour plus d’informations, voir Collecter des données historiques sur l’état du matériel on page 319.
5. Cherchez un moyen de réparer le problème. Par exemple, en redémarrant l’ordinateur, le service du serveur, en remplacement l’élément du matériel défectueux, entre autres.

Afficher l’état historique de votre matériel et imprimer un rapport

Avec le **Moniteur système**, vous pouvez obtenir facilement une vue d’ensemble du bon état votre système de logiciel de gestion des vidéos. Mais aussi à travers une grande période de temps.

Vous vous demandez si l’utilisation du CPU, la bande passante ou tout autre matériel est soumis parfois à des difficultés ? Le moniteur système peut répondre à vos questions et vous pouvez donc décider s’il est judicieux de mettre à niveau votre matériel ou d’en acheter un nouveau pour éviter ces problèmes dans le futur.

N’oubliez pas d’activer la collecte des données historiques. Voir Collecter des données historiques sur l’état du matériel on page 319.

1. Dans le volet **Navigation sur le site**, sélectionnez **Tableau de bord du système** > **Moniteur système**.
2. Dans la fenêtre **Moniteur système**, sélectionnez la tuile comportant le matériel dont vous souhaitez consulter l'état historique ou sélectionnez un serveur ou une caméra depuis la partie inférieure de la fenêtre.
3. Sélectionnez **Détails** situé à droite du serveur ou de la caméra concerné(e).

4. Pour les serveurs, sélectionnez **Historique** situé à droite du matériel sur lequel vous souhaitez enquêter. Pour les caméras, cliquez sur le lien.
5. Si vous souhaitez imprimer un rapport, cliquez sur l'icône du PDF.

Vous ne pouvez créer des rapports historiques qu'avec des données provenant du serveur d'enregistrement sur lequel le périphérique se trouve actuellement.

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 pour ajouter la page **du moniteur système** à la **zone des sites de confiance** avant de poursuivre.

Collecter des données historiques sur l'état du matériel

Vous pouvez activer la collecte des données historiques dans le matériel du système pour consulter les graphiques des états de votre matériel au fil du temps et imprimer le rapport. Pour plus d'informations, voir Afficher l'état historique de votre matériel et imprimer un rapport on page 318.

1. Dans le volet **Navigation sur le site**, sélectionnez **Tableau de bord du système** > **Moniteur système**.
2. Dans la fenêtre **Moniteur système**, sélectionnez **Personnaliser**.
3. Dans la fenêtre **Personnaliser le tableau de bord** qui s'ouvre, sélectionnez **Collecter des données historiques**.
4. Sélectionnez un intervalle d'échantillonnage. Plus l'intervalle est bref, plus il y a de charge sur la base de données SQL Server, la bande passante ou le matériel. L'intervalle d'échantillonnage des données historiques détermine également le niveau de détail des graphiques.

Ajouter une nouvelle tuile de caméra ou de serveur dans le tableau de bord du Moniteur système

Si vous souhaitez surveiller vos caméras ou services dans des petits groupes en fonction de leur localisation physique, ou si vous souhaitez surveiller certains matériels avec différents paramètres de surveillance, vous pouvez ajouter des tuiles supplémentaires dans la fenêtre **Moniteur système**.

1. Dans le volet **Navigation sur le site**, sélectionnez **Tableau de bord du système** > **Moniteur système**.
2. Dans la fenêtre **Moniteur système**, sélectionnez **Personnaliser**.
3. Dans la fenêtre **Personnaliser le tableau de bord** qui s'ouvre, sélectionnez **Nouveau** sous **Tuiles du serveur** ou **Tuiles de la caméra**.
4. Dans la fenêtre **Nouvelle tuile de serveur/Nouvelle tuile de caméra**, sélectionnez les caméras ou les serveurs à surveiller.
5. Sous **Paramètres de surveillance**, cochez ou décochez les cases des paramètres pour ajouter ou supprimer la tuile.
6. Sélectionnez **OK**. La nouvelle tuile de serveur ou de caméra est maintenant ajoutée aux tuiles affichées sur votre tableau de bord.

Modifier une tuile de caméra ou de serveur dans le tableau de bord du moniteur système

Vous pouvez ajuster les paramètres de surveillance si vous souhaitez surveiller vos caméras ou serveurs avec d'autres paramètres de surveillance.

1. Dans le volet **Navigation sur le site**, sélectionnez **Tableau de bord du système** > **Moniteur système**.
2. Dans la fenêtre **Moniteur système**, sélectionnez **Personnaliser**.
3. Dans la fenêtre **Personnaliser le tableau de bord** qui s'ouvre, sélectionnez la tuile que vous souhaitez modifier sous **Tuiles de serveur** ou **Tuiles de caméra** puis cliquez sur **Modifier**.
4. Dans la fenêtre **Modifier la tuile de serveur/caméra du tableau de bord**, sélectionnez toutes les caméras ou tous les serveurs, un groupe de caméras ou de serveurs, ou encore des caméras ou serveurs individuels pour modifier leur paramètres de surveillance.
5. Sous **Paramètres de surveillance**, sélectionnez les paramètres de surveillance que vous souhaitez surveiller.
6. Sélectionnez **OK**.

Supprimer une tuile de caméra ou de serveur dans le tableau de bord du Moniteur système

Si vous n'avez plus besoin de surveiller le matériel représenté par une tuile, vous pouvez supprimer cette dernière.

1. Dans le volet **Navigation sur le site**, sélectionnez **Tableau de bord du système** > **Moniteur système**.
2. Dans la fenêtre **Moniteur système**, sélectionnez **Personnaliser**.
3. Dans la fenêtre **Personnaliser le tableau de bord** qui s'ouvre, sélectionnez la tuile que vous souhaitez modifier sous **Tuiles de serveur** ou **Tuiles de caméra**.
4. Sélectionnez **Supprimer**.

Modifier les seuils lorsque les états du matériel doivent changer

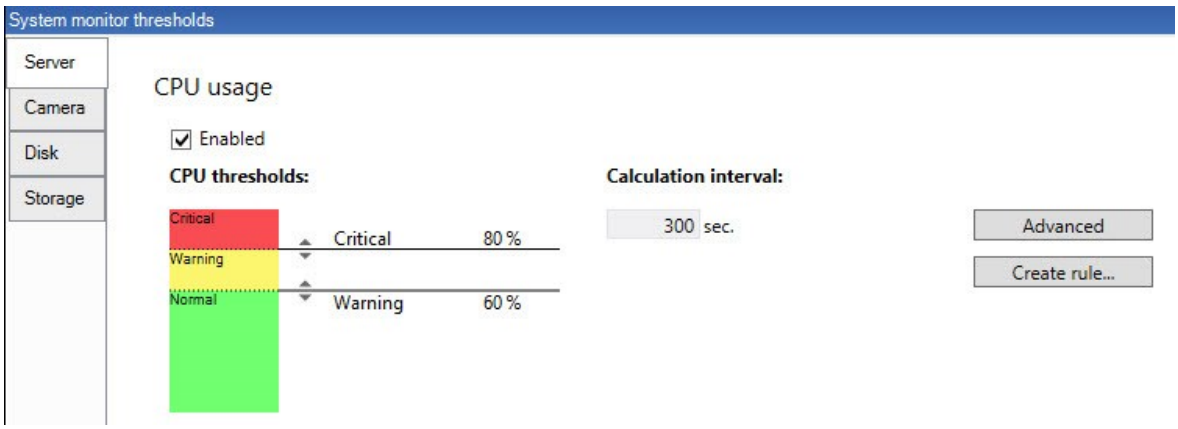
Vous pouvez modifier les seuils pour lesquels votre matériel change entre les trois états sur le **Tableau de bord du moniteur système**. Pour plus d'informations, voir Seuils du Moniteur système (explications) on page 317.

Vous pouvez modifier les seuils de différents types de matériel. Pour plus d'informations, voir Seuils du moniteur système (noeud Tableau de bord du système) on page 622.

Par défaut, le système est configuré pour afficher les seuils de toutes les unités de matériels du même type, par exemple, toutes les caméras ou tous les serveurs. Vous pouvez modifier ces seuils par défaut.

Vous pouvez également configurer des seuils pour des serveurs individuels ou des caméras individuelles, ou une sous-configuration de ces derniers, par exemple, que certaines caméras utilisent un **FPS en direct** ou un **FPS d'enregistrement** plus élevé que d'autres caméras.

1. Dans le volet **Navigation sur le site**, sélectionnez **Tableau de bord du système** > **Seuils du moniteur système**.
2. Cochez la case **Activé** du matériel concerné si vous ne l'avez pas encore activé. La figure ci-dessous illustre un exemple.



3. Faites glisser le curseur de contrôle des seuils vers le haut ou le bas afin d'accroître ou de réduire la valeur du seuil. Chaque élément du matériel affiché dans le contrôle des seuils comporte deux curseurs destinés à séparer les états **Normal**, **Avertissement**, et **Critique**.
4. Indiquez la valeur de l'intervalle de calcul ou conservez la valeur par défaut.
5. Si vous souhaitez configurer les valeurs de chaque élément du matériel, sélectionnez **Avancé**.

6. Si vous souhaitez indiquer des règles pour certains événements ou dans un intervalle de temps spécifique, sélectionnez **Créer une règle**.
7. Une fois que vous avez configuré les niveaux de seuil et les intervalles de calcul, sélectionnez **Fichier** > **Enregistrer** depuis le menu.

Afficher la protection des preuves dans le système

Protection des preuves sous le noeud **Tableau de bord du système** affiche une vue d'ensemble de toutes les données protégées dans le système de surveillance actuel.

Trouver une protection des preuves en filtrant, par exemple, qui l'a créé ou quand.

1. Dans le volet **Navigation sur le site**, sélectionnez **Tableau de bord du système**, > **Protection des preuves**.
2. Vous obtenez une vue d'ensemble dans laquelle vous pouvez trouver la protection des preuves concernées. Vous pouvez appliquer des filtres et trier les différentes métadonnées liées à la protection des preuves.

Les informations affichées dans la fenêtre **Protection des preuves** sont des captures d'écran. Appuyez sur F5 pour actualiser.

Imprimer un rapport avec votre configuration sytème

Vous faites plusieurs choix lorsque vous installez et configurez votre système de logiciel de gestion des vidéos et il peut être utile de les documenter. Au fil du temps, ou même depuis les deux derniers mois, il est également difficile de se rappeler de l'intégralité des paramètres que vous avez modifiés depuis l'installation et la configuration d'origine. C'est pourquoi il est possible d'imprimer un rapport contenant tous les choix de configuration.

Lorsque vous créez un rapport de configuration (au format PDF), vous pouvez ajouter tout élément de votre système au rapport. Vous pouvez par exemple y inclure des licences, la configuration d'un périphérique, la configuration des alarmes et bien plus encore. Vous pouvez sélectionner l'option **Exclure les données sensibles** pour créer un rapport conforme au RGPD (activée par défaut). Vous pouvez également personnaliser la police, la mise en page et la page de garde.

1. Développez **Tableau de bord du système** et sélectionnez **Rapports de configuration**.
2. Sélectionnez les éléments que vous souhaitez inclure ou exclure dans votre rapport.
3. **Facultatif** : Si vous avez sélectionné d'inclure une page de garde, sélectionnez **Page de garde** pour personnaliser les informations sur votre page de garde. Dans la fenêtre qui apparaît, saisissez les informations demandées.
4. Sélectionnez **Mise en format** pour personnaliser votre police, la taille de la page et les marges. Dans la fenêtre qui s'affiche, sélectionnez les paramètres désirés.
5. Quand l'exportation est prête, sélectionnez **Exporter** puis un nom et un emplacement de sauvegarde pour votre rapport.

Seuls les utilisateurs disposant d'autorisations d'administrateur dans le système VMS peuvent créer des rapports de configuration.

Métadonnées

Afficher et masquer des catégories de recherche et filtres de recherche de métadonnées

Les utilisateurs de XProtect Management Client disposant d'autorisations d'administrateur peuvent afficher ou masquer les catégories de recherche de métadonnées et les filtres de recherche de Milestone par défaut dans XProtect Smart Client. Ces catégories et ces filtres de recherche sont masqués par défaut. Il est judicieux de les afficher si votre système de surveillance respectent les exigences (voir Critères de la recherche de métadonnées on page 629).

Ce paramètre affecte tous les utilisateurs de XProtect Smart Client.

Ce paramètre n'affecte pas la visibilité de :

- Tout autre catégorie et filtre de recherche de données qui ne sont pas des métadonnées Milestone, par exemple **Mouvement**, **Signets**, **Alarmes** et **Événements**
- Tout autre catégorie et filtre de recherche tiers

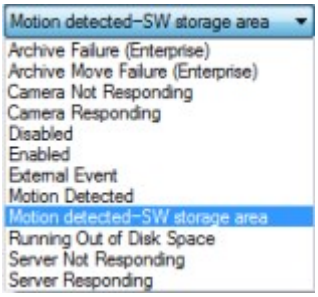
1. Dans XProtect Management Client, dans le volet **Navigation sur site**, sélectionnez **Utilisation des métadonnées** > **Recherche de métadonnées**.
2. Dans le volet **Recherche de métadonnées**, sélectionnez la catégorie de recherche pour laquelle vous souhaitez modifier les paramètres de visibilité.
3. Pour activer la visibilité d'une catégorie de recherche ou d'un filtre recherche, cochez la case correspondante. Pour désactiver la visibilité d'une catégorie de recherche ou d'un filtre recherche, décochez la case correspondante.

Alarmes

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 (noeud Alarmes).

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 lorsque l'alarme est déclenchée.

     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 la définition des alarmes soit activée par un événement, sélectionnez le bouton radio et spécifiez l'événement qui déclenchera la définition des alarmes. Vous devez également spécifier un événement qui désactivera la définition des alarmes.
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.

Modifier les autorisations pour les définitions des alarmes individuelles

Si vous souhaitez que seuls des utilisateurs spécifiques puissent visualiser et gérer une alarme, vous pouvez modifier les autorisations pour la définition des alarmes à partir de XProtect Management Client. Vous pouvez ainsi vous assurer que :

- les utilisateurs ne reçoivent que les alarmes qui les concernent,
- aucun utilisateur non autorisé ne peut réagir aux alarmes.

Utilisez les rôles pour regrouper les utilisateurs qui doivent avoir les mêmes autorisations pour toutes les définitions des alarmes.

Pour modifier les autorisations d'une définition des alarmes :

1. Dans le volet de **Navigation du site**, développez **Sécurité** et sélectionnez le rôle pour lequel vous souhaitez modifier les autorisations.
2. Accédez à l'onglet **Alarmes** et développez **Définitions des alarmes** pour voir la liste des alarmes que vous avez définies.
3. Sélectionnez une définition des alarmes pour modifier les autorisations.

Activer le cryptage

Activer le cryptage depuis et vers le serveur de gestion

Vous pouvez chiffrer la connexion bilatérale entre le serveur de gestion et le Data Collector affilié lorsque vous disposez d'un serveur distant du type suivant :

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

Si votre système contient plusieurs serveurs d'enregistrrement ou serveurs distants, vous devez activer le chiffrement sur tous ces derniers.

Lorsque vous configurez le cryptage sur un groupe de serveurs, il doit être activé avec un certificat appartenant au même certificat de l'AC ou, si ce n'est pas le cas, il doit être désactivé sur tous les ordinateurs du groupe de serveur.

Pré-requis :

- Un certificat d'authentification du serveur est approuvé sur l'ordinateur hébergeant le serveur de gestion

D'abord, vous devez activer le cryptage sur le serveur de gestion.

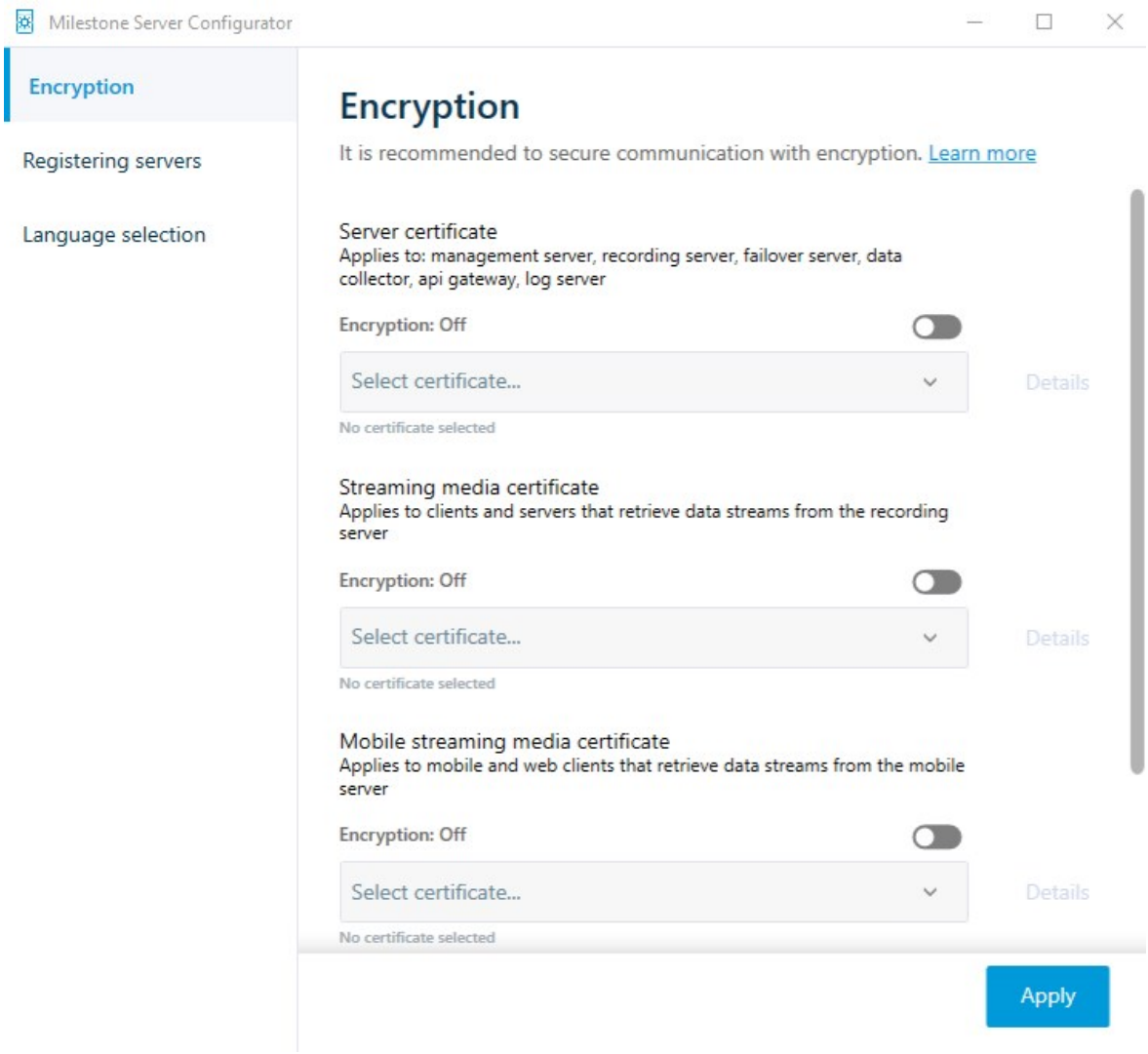
Étapes :

1. Sur un ordinateur où est installé le serveur de gestion, ouvrez le **Server Configurator** à partir de :
   - Le menu Démarrer de Windows

   ou

   - Le Management Server Manager en effectuant un clic droit sur l'icône de Management Server Manager située dans la barre des tâches de l'ordinateur
2. Dans le **Server Configurator**, sous **Certificat du serveur**, activez **Cryptage**.
3. Cliquez sur **Sélectionner un certificat** pour ouvrir une liste des noms de sujet uniques ayant une clé privée et étant installés dans l'ordinateur local dans Windows Certificate Store.
4. Sélectionnez un certificat à utiliser pour crypter la communication entre le serveur d'enregistrement, le serveur de gestion, le serveur de basculement et le Data Collector server.

   Sélectionnez **Détails** pour lire les informations de la Windows Certificate Store sur le certificat sélectionné.



5. Cliquez sur **Appliquer**.

Pour compléter l'activation du cryptage, la prochaine étape consiste à mettre à jour les paramètres de cryptage sur chaque serveur d'enregistrement et chaque serveur disposant d'un Data Collector (Event Server, Log Server, LPR Server, et Mobile Server).

Pour plus d'informations, voir Activer le cryptage du serveur pour les serveurs d'enregistrement ou les serveurs distants on page 327.

Activer le cryptage du serveur pour les serveurs d'enregistrement ou les serveurs distants

Vous pouvez crypter une connexion bidirectionnelle entre le serveur de gestion et le serveur d'enregistrement ou tout autre serveur distant qui utilise le Data Collector.

Si votre système contient plusieurs serveurs d'enregistrrement ou serveurs distants, vous devez activer le chiffrement sur tous ces derniers.

Pour plus d'informations, voir le guide des certificats sur comment sécuriser votre installation de XProtect VMS.

Lorsque vous configurez le cryptage sur un groupe de serveurs, il doit être activé avec un certificat appartenant au même certificat de l'AC ou, si ce n'est pas le cas, il doit être désactivé sur tous les ordinateurs du groupe de serveur.

Pré-requis :

- Vous avez activé le cryptage sur le serveur de gestion, voir Activer le cryptage depuis et vers le serveur de gestion on page 325.

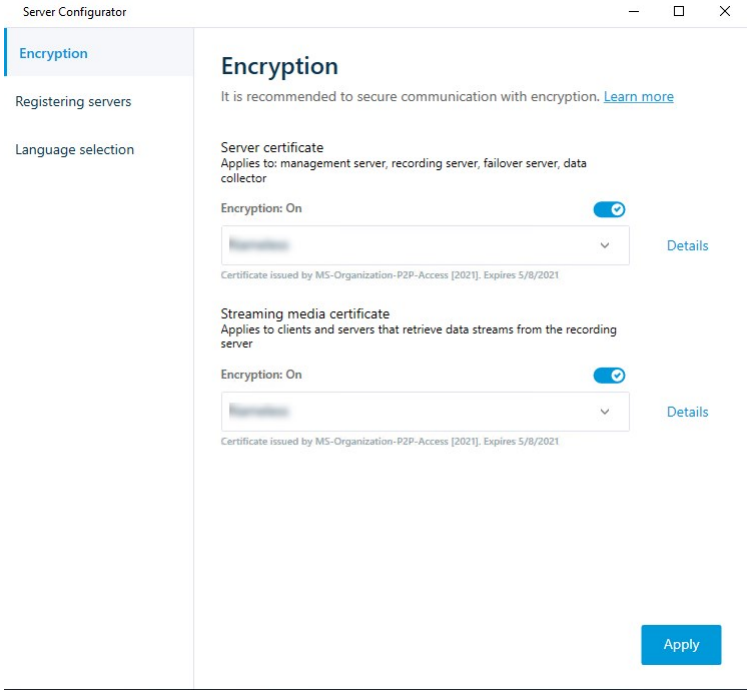
1. Sur un ordinateur où est installé Management Server ou Recording Server, ouvrez le **Server Configurator** à partir de :
   - Le menu Démarrer de Windows

   ou

   - Le gestionnaire de serveurs, en effectuant un clic droit sur l'icône du gestionnaire de serveurs située dans la barre des tâches de l'ordinateur
2. Dans le **Server Configurator**, sous **Certificat du serveur**, activez **Cryptage**.
3. Cliquez sur **Sélectionner un certificat** pour ouvrir une liste des noms de sujet uniques ayant une clé privée et étant installés dans l'ordinateur local dans Windows Certificate Store.
4. Sélectionnez un certificat à utiliser pour crypter la communication entre le serveur d'enregistrement, le serveur de gestion, le serveur de basculement et le serveur de collection de données.

Sélectionnez **Détails** pour lire les informations de la Windows Certificate Store sur le certificat sélectionné.

L'utilisateur du service du Recording Server peut désormais accéder à la clé privée. Ce certificat doit être de confiance sur tous les clients.



5. Cliquez sur **Appliquer**.

Lorsque vous appliquez des certificats, le serveur d'enregistrement s'arrête et redémarre. L'arrêt du service Recording Server vous empêche d'enregistrer et de lire des vidéos en direct pendant que vous vérifiez ou modifiez la configuration de base du serveur d'enregistrement.

Activer le chiffrement du serveur d'événements

Vous pouvez chiffrer la connexion bilatérale entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements , y compris le LPR Server.

Lorsque vous configurez le cryptage sur un groupe de serveurs, il doit être activé avec un certificat appartenant au même certificat de l'AC ou, si ce n'est pas le cas, il doit être désactivé sur tous les ordinateurs du groupe de serveur.

Pré-requis :

- Un certificat d’authentification de serveur est approuvé sur l’ordinateur qui héberge le serveur d’événements

D’abord, activez le chiffrement sur le serveur d’événements.

Étapes :

1. Sur un ordinateur sur lequel est installé un serveur d’événements, ouvrez le **Server Configurator** à partir de :

   - Le menu Démarrer de Windows

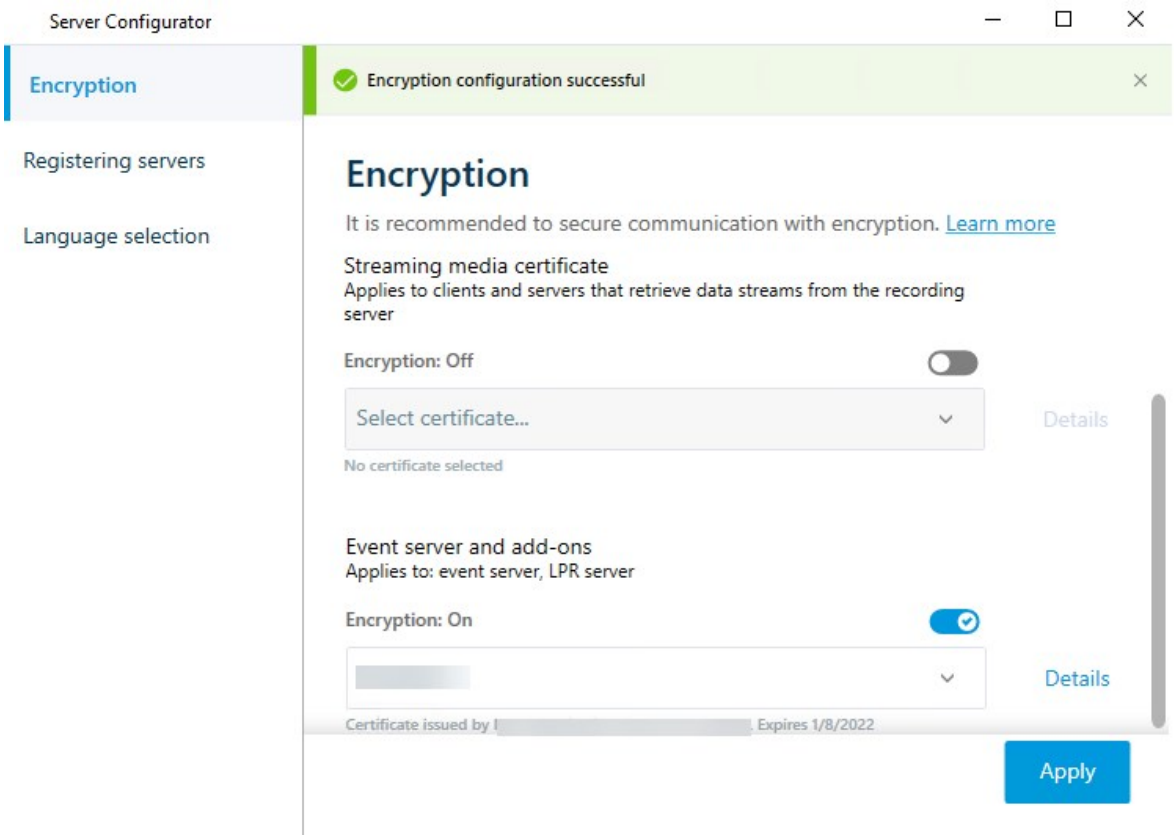
   ou

   - Le Event Server en effectuant un clic droit sur l’icône de Event Server située dans la barre des tâches de l’ordinateur

2. Dans le **Server Configurator**, sous **Serveur d’événements et compléments**, activez **Chiffrement**.
3. Cliquez sur **Sélectionner un certificat** pour ouvrir une liste des noms de sujet uniques ayant une clé privée et étant installés dans l’ordinateur local dans Windows Certificate Store.
4. Sélectionnez un certificat pour chiffrer la communication entre le serveur d’événements et les compléments associés.

   Sélectionnez **Détails** pour lire les informations de la Windows Certificate Store sur le certificat

sélectionné.



5. Cliquez sur **Appliquer**.

Pour terminer l'activation du cryptage, l'étape suivante consiste à mettre à jour les paramètres de cryptage sur chaque extension concernée LPR Server.

Activer le cryptage pour les clients et les serveurs

Vous pouvez chiffrer les connexions depuis le serveur d'enregistrement vers les clients et les serveurs qui diffusent des données en continu à partir du serveur d'enregistrement.

> Lorsque vous configurez le cryptage sur un groupe de serveurs, il doit être activé avec un certificat appartenant au même certificat de l'AC ou, si ce n'est pas le cas, il doit être désactivé sur tous les ordinateurs du groupe de serveur.

Pré-requis :

- Le certificat d'authentification du serveur à utiliser est fiable sur tous les ordinateurs exécutant des services qui collectent des flux de données depuis le serveur d'enregistrement
- XProtect Smart Client et tous les services récupérant des flux de données pour le serveur d'enregistrement doivent être mis à jour à la version 2019 R1 ou une version plus récente
- Certaines solutions tierces utilisant des versions de MIP SDK antérieures à 2019 R1 peuvent avoir besoin d'être mises à jour

Étapes :

1. Sur un ordinateur où est installé le serveur d'enregistrement, ouvrez le **Server Configurator** à partir de :
   - Le menu Démarrer de Windows

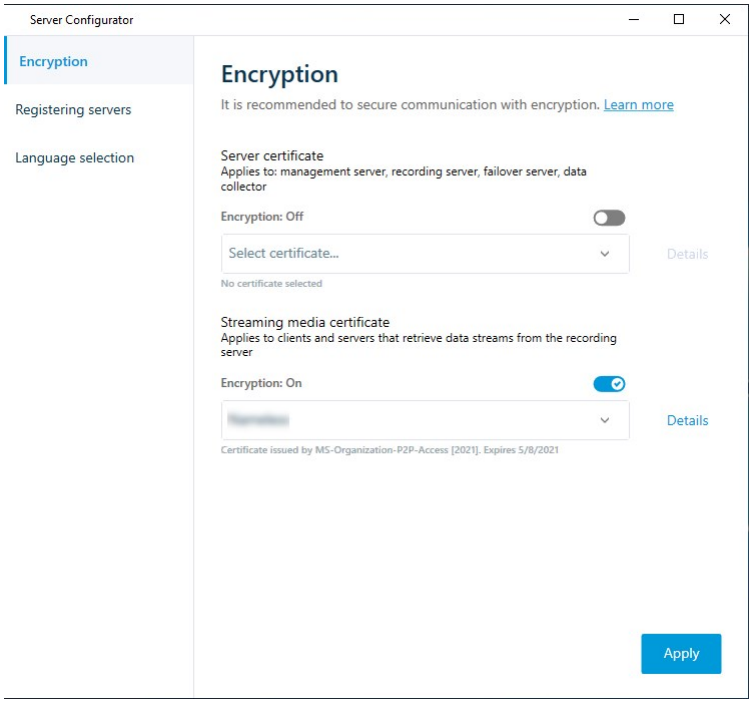
   ou

   - Le Recording Server Manager en effectuant un clic droit sur l'icône de Recording Server Manager située dans la barre des tâches de l'ordinateur
2. Dans le **Server Configurator**, sous **Certificat des flux de média**, activez **Cryptage**.
3. Cliquez sur **Sélectionner un certificat** pour ouvrir une liste des noms de sujet uniques ayant une clé privée et étant installés dans l'ordinateur local dans Windows Certificate Store.
4. Sélectionnez un certificat pour crypter la communication entre les clients et les serveurs récupérant les flux de données depuis le serveur d'enregistrement.

   Sélectionnez **Détails** pour lire les informations de la Windows Certificate Store sur le certificat sélectionné.

   L'utilisateur du service du Recording Server peut désormais accéder à la clé privée. Ce certificat doit être

de confiance sur tous les clients.



5. Cliquez sur **Appliquer**.

> Lorsque vous appliquez des certificats, le serveur d'enregistrement s'arrête et redémarre. L'arrêt du service Recording Server vous empêche d'enregistrer et de lire des vidéos en direct pendant que vous vérifiez ou modifiez la configuration de base du serveur d'enregistrement.

Pour vérifier si le serveur d'enregistrement utilise le cryptage, voir Voir le statut de cryptage des clients.

Activer le cryptage sur le serveur mobile

Pour utiliser un protocole HTTPS sécurisé pour établir une connexion sécurisée entre un serveur mobile et les clients et services, vous devez appliquer un certificat valide au serveur. Le certificat atteste que le titulaire du certificat est autorisé à établir des connexions sécurisées.

Pour plus d'informations, voir le guide des certificats sur comment sécuriser votre installation de XProtect VMS.

> Lorsque vous configurez le cryptage sur un groupe de serveurs, il doit être activé avec un certificat appartenant au même certificat de l'AC ou, si ce n'est pas le cas, il doit être désactivé sur tous les ordinateurs du groupe de serveur.

Les certificats émis par l'AC (Autorité de certification) comportent une chaîne de certificats, et le certificat racine de l'AC se trouve à la racine de cette chaîne. Lorsqu'un périphérique ou un navigateur détecte ce certificat, il compare son certificat racine aux certificats préinstallés sur le système d'exploitation (Android, iOS, Windows, etc.). Si le certificat racine figure dans la liste des certificats préinstallés, le système d'exploitation garantit alors à l'utilisateur que la connexion au serveur est suffisamment sûre. Ces certificats sont émis pour un nom de domaine et ne sont pas gratuits.

Étapes :

1. Sur un ordinateur où est installé un serveur mobile, ouvrez le **Server Configurator** à partir d'une des options suivantes :
   - Le menu Démarrer de Windows

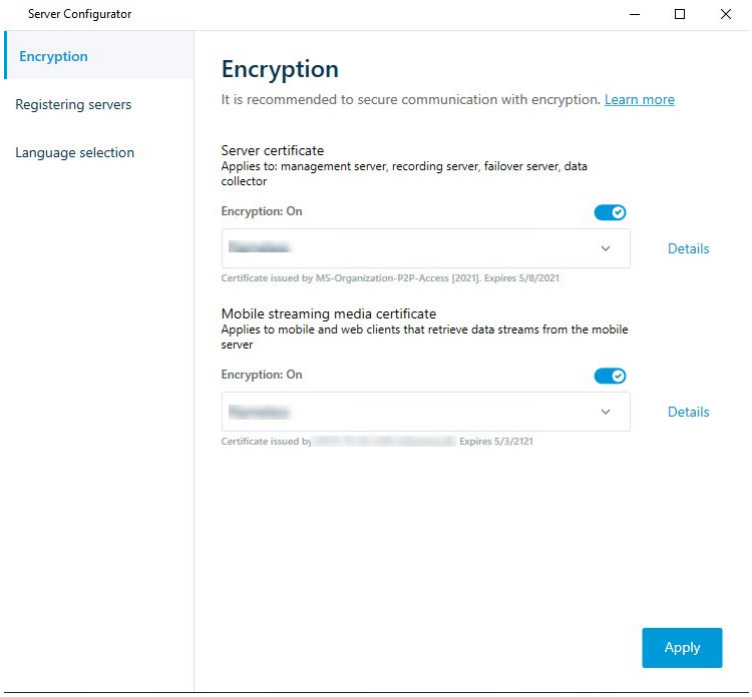
   ou

   - Le Mobile Server Manager en effectuant un clic droit sur l'icône de Mobile Server Manager située dans la barre des tâches de l'ordinateur
2. Dans le **Server Configurator**, sous **Certificat des flux de média mobiles**, activez **Cryptage**.
3. Cliquez sur **Sélectionner un certificat** pour ouvrir une liste des noms de sujet uniques ayant une clé privée et étant installés dans l'ordinateur local dans Windows Certificate Store.
4. Sélectionnez un certificat pour crypter la communication entre le client XProtect Mobile et XProtect Web Client et le serveur mobile.

   Sélectionnez **Détails** pour lire les informations de la Windows Certificate Store sur le certificat sélectionné.

   L'utilisateur du service du Mobile Server peut désormais accéder à la clé privée. Ce certificat doit être de

confiance sur tous les clients.



5. Cliquez sur **Appliquer**.

Lorsque vous appliquez des certificats, le service Mobile Server redémarre.

Milestone Federated Architecture

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.

Option 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 l'utiliser en tant qu'administrateur sur tous les serveurs impliqués dans la hiérarchie des sites fédérés. La manière dont vous connecter les sites dépend du compte utilisateur créé.

Avec un compte utilisateur Windows

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. Ajouter un site à la hiérarchie (voir Ajouter un site à la hiérarchie on page 336).

Avec un compte utilisateur intégré de Windows (service réseau)

1. Commencez l'installation du produit sur le premier serveur devant être utilisé comme serveur de gestion et sélectionnez **Ordinateur unique** ou **Personnalisation**. 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, puis 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. Ajouter un site à la hiérarchie (voir Ajouter un site à la hiérarchie on page 336).

Option 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 (https://docs.microsoft.com/previous-versions/windows/it-pro/windows-2000-server/cc961481(v=technet.10)/).

Milestone recommande Milestone Interconnect pour la création de systèmes à sites multiples avec plusieurs domaines.

Option 3 : connecter des sites dans un ou plusieurs groupes 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. Ajouter un site à la hiérarchie (voir Ajouter un site à la hiérarchie on page 336).

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 le ou les domaines et groupes 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.

Ajouter un site à la hiérarchie

Au fur et à mesure de l'expansion de votre système, vous pouvez ajouter des sites à votre site supérieur et à ses sites enfants aussi longtemps que le système est correctement configuré.

Lors de l'ajout d'un site non sécurisé à Milestone Federated Architecture, assurez-vous que l'option **Autoriser les connexions non sécurisées au serveur** est activée dans **Outils** > **Options** > **Paramètres généraux** dans Management Client.

1. Sélectionnez le panneau **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 quelque temps, un lien entre les deux sites est ajouté dans le panneau **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.

   Si ce n'est **pas** le cas, le site enfant voit s'afficher l'icône d'attente d'acceptation 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 liaison de la part du site parent (voir Accepter les ajouts dans la hiérarchie on page 337).
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 dans la hiérarchie

Lorsqu'un site enfant reçoit une demande de liaison à partir d'un site parent potentiel alors que l'administrateur ne disposait pas d'autorisations administrateur pour le site enfant, l'icône en attente d'acceptation s'affiche.

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 les ajouts dans la hiérarchie**.

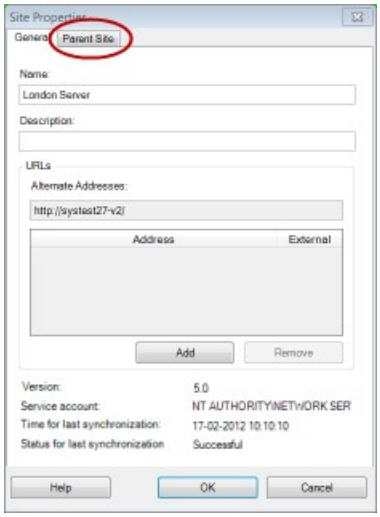
   Si le site exécute la version XProtect Expert, faites un clic droit sur le site dans le panneau **Navigation du site**.
3. Cliquez sur **Oui**.
4. Le nouveau lien parent/enfant est établi et le panneau **Hiérarchie des sites fédérés** est mis à jour avec l'icône de site normale pour le site sélectionné.

> Les modifications apportées aux sites enfants situés à distance du site parent peuvent mettre du temps à se voir reflétées 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 Management Client, dans le panneau **Hiérarchie des sites fédérés**, sélectionnez le site concerné, faites un clic droit et sélectionnez **Propriétés**.



2. Le cas échéant, modifiez ce qui suit :

   Onglet **Généralité** (voir Onglet Généralités on page 647)

   Onglet **Site parent** (voir Onglet Site parent on page 648) **(disponible sur les sites enfants uniquement)**

   > 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**.

Actualiser la hiérarchie des sites

Le système procède régulièrement à une synchronisation automatique de la hiérarchie à tous les niveaux de votre configuration parent/enfant. Vous pouvez l'actualiser manuellement, si vous souhaitez voir les modifications reflétées instantanément dans la hiérarchie, et si vous ne souhaitez pas attendre la prochaine synchronisation automatique.

Vous devez être connecté(e) sur un site pour effectuer une actualisation manuelle. Seules les modifications sauvegardées par ce site depuis la dernière synchronisation sont affichées par le biais d'une actualisation. Par conséquent, les modifications apportées à des niveaux inférieurs dans la hiérarchie pourraient ne pas être affichées par le biais d'une mise à jour manuelle, si les changements n'ont pas encore atteint le site.

1. Connectez-vous au site pertinent.
2. Cliquez avec le bouton droit sur le site supérieur dans le panneau **Hiérarchie des sites fédérés** et cliquez sur **Rafraîchir la hiérarchie des sites**.

   Cela 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.

Mettre à jour les renseignements des sites enfants

> Cette section est utile uniquement si vous utilisez XProtect Corporate ou XProtect Expert 2014 ou une version plus récente.

Dans une grande configuration de Milestone Federated Architecture comportant beaucoup de sites enfants, il peut être facile de perdre la vue d'ensemble et difficile de trouver les informations de contact des administrateurs de chaque site enfant.

Vous pouvez donc ajouter des renseignements supplémentaires dans chaque site enfant. Ces renseignements sont alors disponibles pour les administrateurs dans le site central.

Vous pouvez lire les renseignements du site en passant la souris sur le nom du site dans le volet **Hiérarchie des sites fédérés**. Pour mettre à jour les renseignements sur le site :

1. Connectez-vous au site.
2. Cliquez sur le volet **Navigation du site** puis sélectionnez **Informations du site**.
3. Cliquez sur **Modifier** puis ajoutez les renseignements nécessaires dans chaque catégorie.

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.

Milestone Interconnect

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**.
Prérequis

- Suffisamment de licences de caméras Milestone Interconnect (voir Milestone Interconnect et les licences on page 103).
- Un autre système XProtect configuré et fonctionnel comprenant un compte d'utilisateur (utilisateurs basiques, utilisateur Windows local ou utilisateur Windows Active Directory) disposant d'autorisations pour les périphériques auquel le système XProtect Corporate central doit pouvoir accéder
- Connexion réseau entre le site central XProtect Corporate et les sites distants 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 **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 de la plage 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 panneau **Vue d'ensemble**.

    En fonction des autorisations utilisateur pour 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.

Affecter des autorisations utilisateur

Vous configurez les autorisations utilisateur pour une caméra interconnectée de la même manière que pour d'autres caméras, en créant un rôle et en affectant un accès à des fonctions.

1. Sur le site central, dans le volet **Navigation du site,**, développez **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).
3. Nommez le rôle et configurez les paramètres dans l'onglet **Périphérique** (voir l'onglet Périphérique (rôles)) et l'onglet **Enregistrements à distance** (voir l'onglet Enregistrements à distance (rôle)).

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.

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. Pour plus d'informations, voir Configurations Milestone Interconnect (explications) on page 103.

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 les masques de confidentialité définis dans un site distant. Si vous souhaitez utiliser les mêmes masques de confidentialité, vous devez les 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. Pour plus d'informations, voir Configurations Milestone Interconnect (explications) on page 103.

Pour permettre aux utilisateurs de récupérer des enregistrements, vous devez activer l'autorisation pour le rôle pertinent (voir Rôles (sécurité)).

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 Propriétés, sélectionnez l'onglet **Récupération à distance** et mettez à jour les paramètres (voir Onglet Rappel à distance on page 467).

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 panneau Propriétés, sélectionnez l'onglet **Enregistrer**, puis sélectionnez l'option **Récupérer automatiquement les enregistrements à distance lorsque la connexion est rétablie** (voir Enregistrer et récupérer un enregistrement à distance).
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 les masques de confidentialité définis dans un site distant. Si vous souhaitez utiliser les mêmes masques de confidentialité, vous devez les 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 Milestone (https://www.milestonesys.com/).

Vous ne pouvez pas supprimer les événements prédéfinis.

Exigences :

- 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 on page 341).

Ajouter un événement manuel ou défini par l'utilisateur depuis un 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 terminée.

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 une règle**.
3. Dans l'assistant, sélectionnez **Réaliser une action lors de l'<événement>**.
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 **périphériques/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**.

Smart Maps

Arrière-plans géographiques (explications)

Avant qu'un utilisateur de XProtect Smart Client ne sélectionne un arrière-plan géographique, vous avez d'abord configuré les arrière-plans géographiques dans XProtect Management Client.

- **Plan du monde basique** - utilisez l'arrière-plan géographique standard fourni dans XProtect Smart Client. Aucune configuration n'est requise. Ce plan a été conçu pour servir de référence générale et ne contient pas de fonctions comme les frontières, villes ou autres détails. Cependant, comme les autres arrière-plans géographiques, il contient des données de géoréférence
- **Bing Maps** - connectez-vous à Bing Maps
- **Google Maps** - connectez-vous à Google Maps
- **Milestone Map Service** - connecter à un fournisseur de plan gratuit. Une fois Milestone Map Service d'activé, aucune configuration n'est requise.

  Voir Activer Milestone Map Service

- **OpenStreetMap** - se connecter à :
  - Un serveur de tuile commercial de votre choix
  - Votre propre serveur de tuile en ligne ou local

  Voir Spécifier le serveur de tuile OpenStreetMap

Les options Bing Maps et Google Maps nécessitent un accès Internet et vous devez acheter une clé à Microsoft ou Google.

Milestone Map Service requiert l'accès à Internet.

À moins que vous n'utilisiez votre propre serveur de tuile local, OpenStreetMap nécessite un accès Internet.

N'utilisez pas les services suivants si vous souhaitez que votre système possède une installation conforme aux exigences du RGPD de l'UE :

- Bing Maps
- Google Maps
- Milestone Map Service

Pour plus d'informations sur la protection des données et la collecte des données d'utilisation, voir le Guide de confidentialité du RGPD.

Par défaut, Bing Maps et Google Maps affichent des images satellitaires (Satellite). Vous pouvez modifier les images dans XProtect Smart Client, en choisissant par exemple aérien ou terrain, pour voir différents détails.

Activer Bing Maps ou Google Maps dans Management Client

Vous pouvez rendre la clé disponible à plusieurs utilisateurs en la saisissant pour un profil Smart Client dans Management Client. Tous les utilisateurs étant assignés au profil utiliseront cette clé.

Étapes :

1. Dans Management Client, dans le panneau **Navigation de site**, cliquez sur **Profils Smart Client**.
2. Dans le volet **Smart Client Profils**, sélectionnez le profil Smart Client concerné.
3. Dans le volet **Propriétés**, cliquez sur l'onglet **Smart Map** :
   - Pour Bing Maps, saisissez votre clé basique ou d'entreprise dans le champ **clé Bing Maps**
   - Pour Google Maps, saisissez votre clé API Maps Static dans le champ **clé privée pour Google Maps**

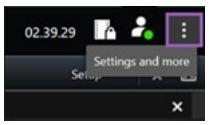
4. Pour empêcher les utilisateurs de XProtect Smart Client d'utiliser une autre clé, cochez la case **Verrouillée**.

Activer Bing Maps ou Google Maps dans XProtect Smart Client

Pour permettre aux opérateurs de XProtect Smart Client d'utiliser une clé différente à celle du profil Smart Client, vous devez saisir la clé dans les paramètres dans XProtect Smart Client.

Étapes :

1. Dans XProtect Smart Client, ouvrez la fenêtre **Paramètres**.



2. Cliquez sur **Smart Map**.
3. En fonction du service de plan que vous voulez utiliser, faites comme suit :
   - Pour Bing Maps, saisissez votre clé dans le champ **clé Bing Maps**. Voir également Intégration de smart map avec Bing Maps (explications) on page 99.
   - Pour Google Maps, saisissez votre clé dans le champ **clé privée pour Google Maps**. Voir également Intégration de smart map avec Google Maps (explications) on page 98.

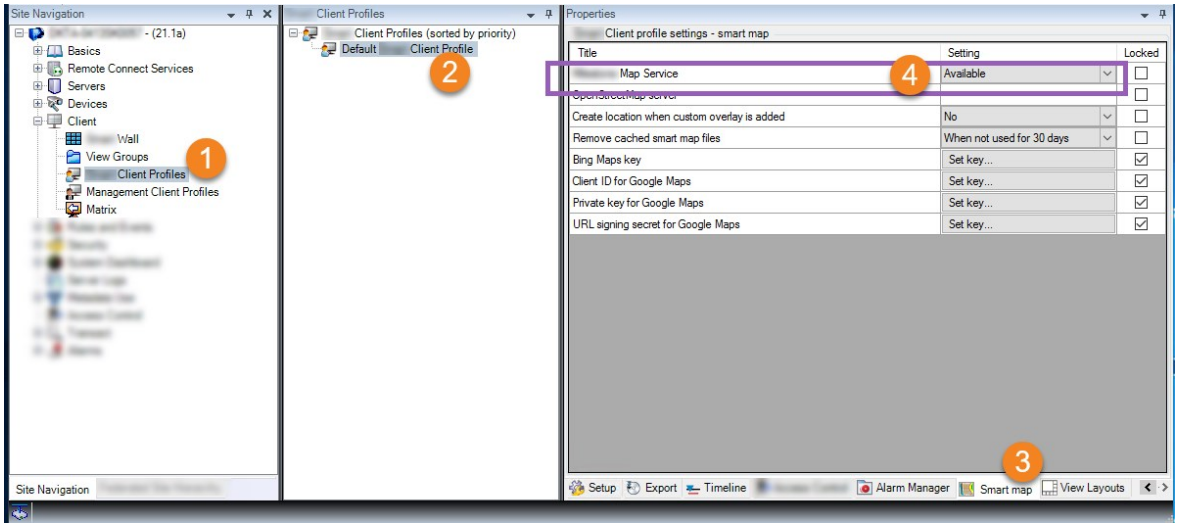
Activer Milestone Map Service

Milestone Map Service est un service en ligne qui vous permet de vous connecter au serveur de tuile du Milestone Systems. Ce dernier utilise un service de plans gratuit et disponible sur le marché.

Après avoir activé Milestone Map Service sur votre Smart Map, cette dernière utilisera Milestone Map Service comme arrière-plan géographique.

Étapes :

1. Dans le panneau **Navigation du site**, développez le nœud **Client** et cliquez sur **Profils Smart Client**.
2. Dans le panneau Vue d'ensemble, sélectionnez le profil Smart Client pertinent.
3. Dans le volet **Propriétés**, cliquez sur l'onglet **Smart Map**.



4. Dans le champ **Milestone Map Service**, sélectionnez **Disponible**.
5. Pour activer ce paramètre dans XProtect Smart Client, cochez la case **Verrouillé**. Les opérateurs XProtect Smart Client ne peuvent alors pas activer ou désactiver Milestone Map Service.
6. Sauvegardez les modifications apportées.

Vous pouvez également activer Milestone Map Service dans le fenêtre **Paramètres** dans XProtect Smart Client.

Milestone Map Service requiert l'accès à Internet.

Si vous êtes protégé par un pare-feu restrictif, il est important d'autoriser l'accès aux domaines utilisés. Vous devrez peut-être autoriser le trafic sortant pour Milestone Map Service en utilisant maps.milestonesys.com sur chaque machine sur laquelle Smart Client est exécuté.

Spécifier le serveur de tuile OpenStreetMap

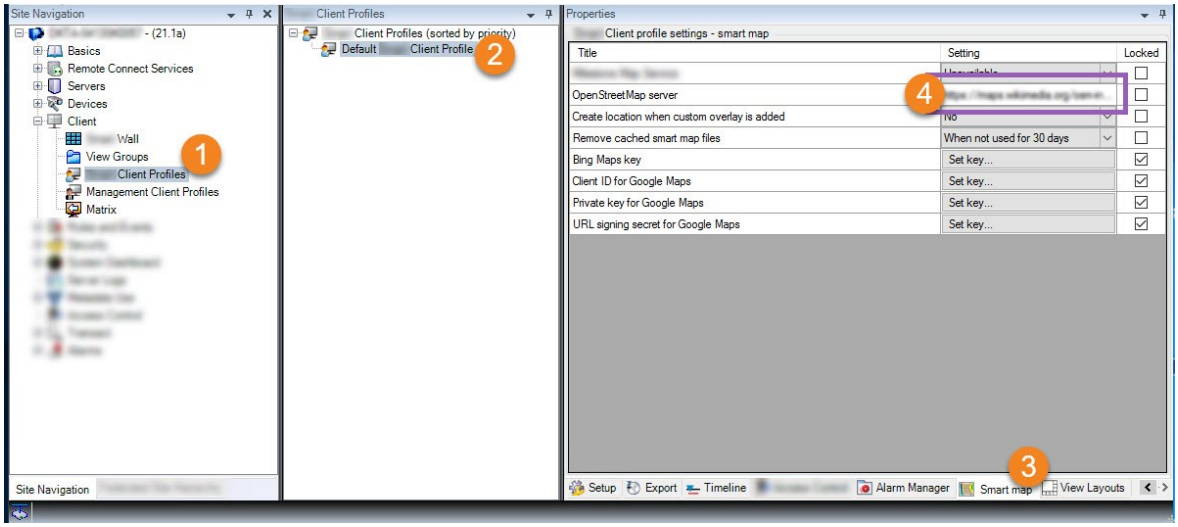
Si vous utilisez l'option **OpenStreetMap** en tant qu'arrière-plan géographique pour votre smart map, vous devez indiquer l'emplacement à partir duquel les images en tuile seront récupérées. Pour ce faire, il vous suffit de préciser l'adresse du serveur de tuile, que ce soit un serveur de tuile commercial ou local, par exemple, si

votre institution dispose de ses propres plans pour des zones telles que des aéroports ou des ports.

> Vous pouvez également spécifier l'adresse du serveur de tuile dans la fenêtre **Paramètres** dans XProtect Smart Client.

Étapes :

1. Dans le panneau **Navigation du site**, développez le nœud **Client** et cliquez sur **Profils Smart Client**.
2. Dans le panneau Vue d'ensemble, sélectionnez le profil Smart Client pertinent.
3. Dans le volet **Propriétés**, cliquez sur l'onglet **Smart map**.



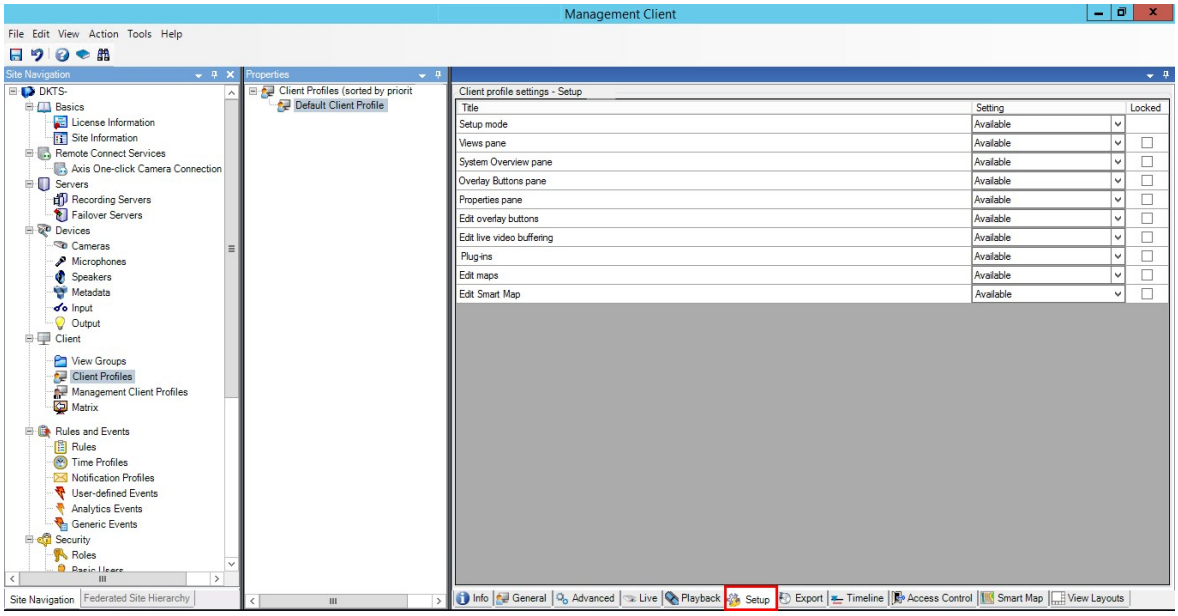
4. Dans le champ **Serveur OpenStreetMap**, saisissez l'adresse du serveur de tuile.
5. Pour activer ce paramètre dans XProtect Smart Client, cochez la case **Verrouillé**. Les opérateurs de XProtect Smart Client ne pourront plus modifier l'adresse.
6. Sauvegardez les modifications apportées.

Activer la modification de la smart map

Les opérateurs peuvent modifier les smart maps dans XProtect Smart Client en mode configuration, uniquement si la modification est activée dans Management Client. Si cette option n'est pas déjà activée, vous devez activer la modification pour chaque profil Smart Client pertinent.

Étapes :

1. Dans le panneau **Navigation du site**, développez le nœud **Client**.
2. Cliquez sur **Smart Client Profils**.



3. Dans le panneau Vue d'ensemble, sélectionnez le profil Smart Client pertinent.
4. Dans le volet **Propriétés**, cliquez sur l'onglet **Configuration**.
5. Dans la liste **Modifier les smart maps**, choisissez **Disponible**.
6. Répétez ces étapes pour chaque profil Smart Client pertinent.
7. Sauvegardez vos modifications. La prochaine fois que les utilisateurs assignés au profil Smart Client que vous avez sélectionné se connecteront au XProtect Smart Client, ils pourront modifier les smart maps.

Pour désactiver la modification, dans la liste **Modifier les smart maps**, choisissez **Indisponible**.

Activer la modification des périphériques dans smart map

Vous devez activer la modification des périphériques par rôle pour, par exemple, permettre aux opérateurs de :

- Placer un périphérique entrant ou un microphone dans un smart map
- Ajuster le champ de vue d'une caméra dans un smart map

Les opérateurs peuvent être autorisés à modifier les types de périphériques suivants dans des smart maps :

- Caméras
- Périphériques d'entrée
- Microphones

Configuration
Avant de commencer, assurez-vous que la modification du smart map a été activée (voir Activer la modification de la smart map on page 348). Vous effectuez ces opérations dans le profil Smart Client auquel le rôle de l'opérateur est assigné.

Étapes :

1. Développez le noeud **Sécurité** > **Roles**.
2. Dans le volet **Rôles**, sélectionnez le rôle auquel votre opérateur est associé.
3. Pour accorder les autorisations d'édition de rôles :
    - Sélectionnez l'onglet **Sécurité globale** dans le volet **Paramètres des rôles**, puis le type de périphérique (par exemple, **Caméras** ou **Entrant**)
    - Dans la colonne **Autoriser**, cochez la case **Contrôle total** ou **Modifier**
4. Sauvegardez les modifications apportées.

Pour activer la modification des différents périphériques, allez à l'onglet **Périphérique**, puis sélectionnez le périphérique pertinent.

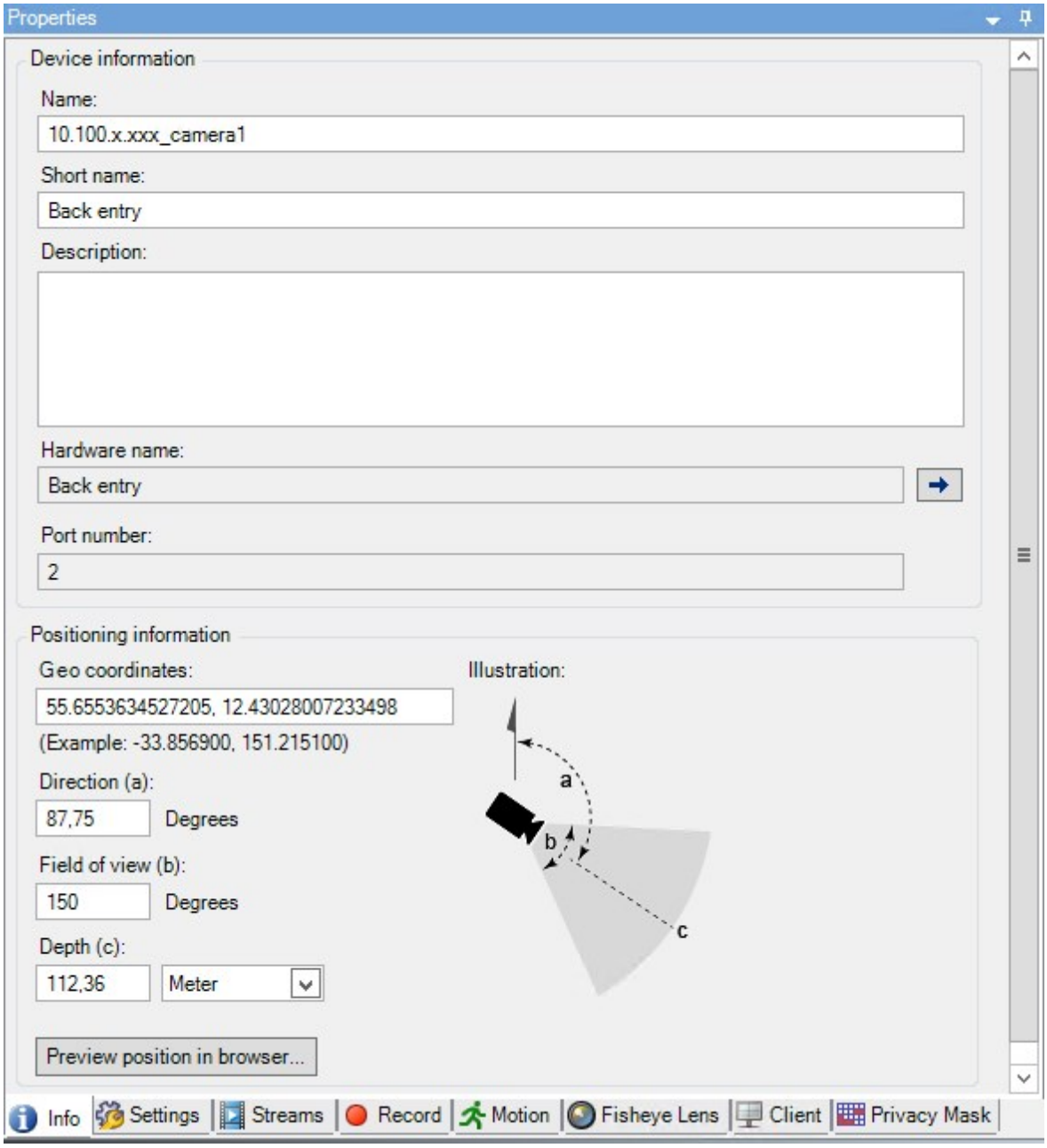
Définir la position d'un périphérique et la direction, le champ de vision et la profondeur d'une caméra (smart map)

Pour vous assurer qu'un périphérique est positionné correctement sur la smart map, vous pouvez définir ses coordonnées géographiques. Pour les caméras, vous pouvez également configurer la direction, le champ de vision et la profondeur de vue. La configuration de ces paramètres ajoutera automatiquement le périphérique à la smart map la prochaine fois qu'un opérateur charge cette dernière dans XProtect Smart Client.

Étapes :

1. Dans Management Client, développez le nœud **Périphériques** et sélectionnez le type de périphérique (par exemple, **Caméras** ou **Entrée**).
2. Dans le volet **Périphériques**, sélectionnez le périphérique d'entrée concerné.

3. Sur l'onglet **Infos**, défilez vers le bas jusqu'à **Informations sur la position**.



4. Spécifiez les coordonnées de latitude et de la longitude dans le champ **Coordonnées géographiques**, dans cet ordre. Utilisez un point comme séparateur et une virgule pour séparer la latitude et la longitude.

   L'ajout des coordonnées géographiques permet aux utilisateurs de XProtect Smart Client d'accéder directement au périphérique sur une smart map et, lorsque le périphérique est ajouté à une smart map, il est automatiquement positionné sur la carte.

   - Pour les caméras :
     1. Dans le champ **Direction**, saisissez une valeur comprise dans la plage allant de 0 à 360 degrés.
     2. Dans le champ **Champ de visualisation**, saisissez une valeur comprise entre 0 et 360 degrés.
     3. Dans le champ **Profondeur**, saisissez la profondeur de vue en mètres ou en pieds.
5. Sauvegardez les modifications apportées.

Vous pouvez également définir les propriétés sur les serveurs d'enregistrement.

Configurer smart map avec Milestone Federated Architecture

Si vous utilisez une smart map dans une Milestone Federated Architecture, tous les périphériques des sites connectés apparaîtront sur cette smart map. Suivez les étapes suivantes pour configurer smart map dans une architecture fédérée.

Pour une présentation générale de Milestone Federated Architecture, voir Configuration de Milestone Federated Architecture on page 105.

1. Avant de connecter le site principal aux sites enfants, assurez-vous que les coordonnées géographiques ont été spécifiées sur tous les périphériques de tous les sites. Les coordonnées géographiques s'ajoutent automatiquement lorsque l'on positionne un périphérique sur la smart map par le biais de XProtect Smart Client, mais vous pouvez aussi les ajouter manuellement dans Management Client, dans les propriétés des périphériques. Pour plus d'informations, voir Définir la position d'un périphérique et la direction, le champ de vision et la profondeur d'une caméra (smart map) on page 350.

2. Vous devez ajouter les opérateurs Smart Client comme utilisateurs Windows sur le site parent et tous les sites fédérés. Au moins sur le site supérieur, les utilisateurs Windows doivent disposer d'autorisations de modification pour la smart map. Les utilisateurs pourront ainsi modifier la smart map du site supérieur et de tous les sites enfants. Ensuite, vous devez déterminer si les utilisateurs Windows des sites enfants ont besoin d'autorisations de modification pour la smart map. Dans Management Client, vous créerez d'abord les utilisateurs Windows sous **Rôles**, puis vous activerez la modification de smart map. Pour plus d'informations, voir Activer la modification de la smart map on page 348.
3. Sur le site supérieur, ajoutez les sites enfants en tant qu'utilisateurs Windows à un rôle avec des autorisations d'administrateur. Lorsque vous spécifiez le type d'objet, cochez la case **Ordinateurs**.
4. Sur chacun des sites enfants, ajoutez le site supérieur en tant qu'utilisateur Windows au même rôle d'administrateur utilisé sur le site supérieur. Lorsque vous spécifiez le type d'objet, cochez la case **Ordinateurs**.
5. Sur le site supérieur, vérifiez que la fenêtre **Hiérarchie des sites fédérés** s'affiche. Dans Management Client, allez dans **Aperçu** et sélectionnez **Hiérarchie des sites fédérés**. Ajoutez tous les sites enfants au site supérieur. Pour plus d'informations, voir Ajouter un site à la hiérarchie on page 336.
6. Vous pouvez maintenant tester si Milestone Federated Architecture fonctionne sur XProtect Smart Client. Connectez-vous au site supérieur en tant qu'administrateur ou opérateur, et ouvrez un aperçu contenant la smart map. Si la configuration a été correctement effectuée, tous les périphériques du site supérieur et des sites enfants apparaîtront sur la smart map. Si vous vous connectez à l'un des sites enfants, vous ne verrez que les périphériques de ce site et ses sites enfants.

Pour modifier les périphériques d'une smart map, par exemple l'élément de vue et l'angle, les utilisateurs ont besoin d'autorisations de modification. Pour plus d'informations, voir Activer la modification des périphériques dans smart map on page 349.

Maintenance

Sauvegarde et restauration de la configuration système

Milestone vous recommande d'effectuer des sauvegardes régulières de votre configuration système en tant que 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. Il est important de protéger vos sauvegardes par le biais de mesures techniques ou organisationnelles.

Sauvegarde et de la restauration de la configuration de votre système (explications)

Le système offre une fonctionnalité intégrée qui sauvegarde toute la configuration du système que vous pouvez définir dans le Management Client. La base de données du serveur de journaux et les fichiers journaux, y compris les fichiers de journal d'activité, 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.

La sauvegarde de votre configuration peut prendre un certain temps. La durée de sauvegarde dépend de :

- Votre configuration système
- Votre matériel
- Si vous avez installé les composants SQL Server, Event Server et Management Server sur un seul ou sur plusieurs serveurs

Chaque fois que vous effectuez une sauvegarde, qu'elle soit manuelle ou programmée, le fichier journal des transactions de la base de données SQL Server est vidé. Pour des informations complémentaires sur comment purger votre fichier de journal des transactions, voir Journal des transactions de la base de données SQL Server (explications) on page 148.

Assurez-vous de connaître les paramètres de votre mot de passe de configuration système lorsque vous créez une sauvegarde.

Pour les systèmes conformes aux normes FIPS 140-2 comportant des exportations et des bases de données multimédias archivées à partir des versions de XProtect VMS antérieures à 2017 R1 qui sont cryptées avec un cryptage non conforme aux normes FIPS, il est nécessaire d'archiver les données dans un emplacement auquel il est possible d'accéder après l'activation du mode FIPS. Pour de plus amples informations sur comment configurer votre XProtect VMS pour qu'il s'exécute conformément au mode FIPS 140-2, voir la section de conformité aux normes FIPS 140-2 dans le guide de durcissement.

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 de service du Management Server de la zone de notification et sélectionnez **Sélectionner le répertoire 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 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**.

Tous les fichiers de configuration concernés du système 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 répertoire temporaire par un clic droit sur l'icône du service du Management Server de la zone de notification, et en sélectionnant Sélectionner le répertoire de sauvegarde partagé.

Restauration d'une configuration système à partir d'une sauvegarde manuelle

Informations importantes

- L'utilisateur qui installe et l'utilisateur qui restaure doivent être des administrateurs locaux de la base de données SQL Server de configuration du système sur le serveur de gestion **et** sur SQL Server.
- 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, lors de la restauration, vous êtes invité à saisir un mot de passe de configuration système, vous devez alors fournir le mot de passe de configuration système qui était valide au moment de la création de la sauvegarde. Sans ce mot de passe, il vous est impossible de restaurer votre configuration à partir de la sauvegarde
- Si vous effectuez une sauvegarde de la base de données SQL Server et que vous la restaurez sur un SQL Server propre, les erreurs de relance de la base de données SQL Server ne fonctionneront pas et vous ne recevrez qu'un message d'erreur générique de la part de SQL Server. Pour éviter cela, réinstallez d'abord votre système XProtect à l'aide du SQL Server propre et restaurez la sauvegarde par-dessus.
- Si la restauration échoue au cours de la phase de validation, vous pouvez redémarrer l'ancienne configuration parce que vous n'avez apporté aucun changement
  En cas d'échec de la restauration à un autre endroit du processus, vous ne pouvez pas revenir à 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 de service du Management Server 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 du système, 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**.

Mot de passe de configuration système (explications)

Vous pouvez choisir de protéger la configuration globale du système en attribuant un mot de passe de configuration du système. Une fois que vous attribuez un mot de passe de configuration système, les sauvegardes de cette dernières sont protégées par ce mot de passe. Les paramètres du mot de passe sont stockés dans un dossier sécurisé de l'ordinateur qui exécute le serveur de gestion. Vous aurez besoin de ce mot de passe pour :

- Restaurer la configuration à partir d'une sauvegarde de configuration qui a été créée avec des paramètres de mot de passe différents à ceux du mot de passe actuel
- Déplacer ou installer le serveur de gestion sur un autre ordinateur en raison d'une panne matérielle (récupération)
- Configurer un serveur de gestion additionnel dans un système en grappe

> Vous pouvez attribuer le mot de passe de configuration système avant ou après l'installation. Il doit respecter les exigences en matière de complexité de Windows, lesquelles sont définies par la politique de Windows concernant les mots de passe.

Il est important que les administrateurs système enregistrent ce mot de passe dans un emplacement sécurisé. Si vous avez attribué un mot de passe de configuration système et que vous effectuez la restauration d'une sauvegarde, vous pourriez être invité à fournir le mot de passe de configuration système. Sans ce mot de passe, il vous est impossible de restaurer votre configuration à partir de la sauvegarde.

Paramètres du mot de passe de configuration système

Vous pouvez modifier les paramètres du mot de passe de configuration système. Dans les paramètres du mot de passe de configuration système, vous pouvez :

- Choisir de protéger par un mot de passe la configuration système en attribuant un mot de passe de configuration système
- Modifier un mot de passe de configuration système
- Choisir de ne pas protéger par un mot de passe la configuration système en supprimant tout mot de passe de configuration système attribué

Modifier les paramètres du mot de passe de configuration système

Lorsque vous changez le mot de passe, il est important que les administrateurs système enregistrent les mots de passe associés aux différentes sauvegardes dans un emplacement sécurisé. Si vous effectuez la restauration d'une sauvegarde, vous pourriez être invité à saisir le mot de passe de configuration système qui était valide au moment de la création de la sauvegarde. Sans ce mot de passe, il vous est impossible de restaurer votre configuration à partir de la sauvegarde.

Après avoir modifié le mot de passe, et si votre serveur de gestion et votre serveur d'événements sont installés sur différents ordinateurs, vous devez également saisir le mot de passe de configuration du système sur le serveur d'événements. Pour plus d'informations, voir Saisir le mot de passe de configuration du système actuel (serveur d'événements).

Vous devez redémarrer les services du serveur de gestion pour appliquer les changements.

1. Accédez à l'icône du serveur de gestion dans la barre d'état et vérifiez que le service s'exécute normalement.
2. Effectuez un clic droit sur l'icône de service du Management Server de la zone de notification et sélectionnez **Modifier les paramètres du mot de passe de configuration système**.
3. La boîte de dialogue pour modifier les paramètres du mot de passe de configuration système s'affiche.

Attribuer un mot de passe

1. Saisissez le nouveau mot de passe dans le champ **Nouveau mot de passe**.
2. Saisissez à nouveau le nouveau mot de passe dans le champ **Confirmer le nouveau mot de passe** puis sélectionnez **Entrer**.
3. Lisez la notification qui s'affiche puis cliquez sur **Oui** pour accepter le changement.
4. Attendez de recevoir la confirmation du changement puis sélectionnez **Fermer**.
5. Vous devez redémarrer les services du serveur de gestion pour appliquer les changements.
6. Après le redémarrage, vérifiez que le serveur de gestion s'exécute normalement.

Supprimer la protection par mot de passe

Vous pouvez annuler la protection par mot de passe si vous n'en avez pas besoin :

1. Cochez la case : **Je choisis de ne pas utiliser de mot de passe de configuration système et je comprends que la configuration système ne sera pas cryptée** puis cliquez sur **entrer**.
2. Lisez la notification qui s'affiche puis cliquez sur **oui** pour accepter le changement.
3. Attendez de recevoir la confirmation du changement puis sélectionnez **Fermer**.
4. Vous devez redémarrer les services du serveur de gestion pour appliquer les changements.
5. Après le redémarrage, vérifiez que le serveur de gestion s'exécute normalement.

Entrer les paramètres du mot de passe de configuration système (récupération)

Si le fichier contenant les paramètres du mot de passe est supprimé en raison d'une panne matérielle ou toute autre raison, il vous faudra saisir les paramètres du mot de passe de configuration système pour accéder à la base de données hébergeant la configuration système. Lors de son installation sur un nouvel ordinateur, vous serez invité à entrer les paramètres du mot de passe de configuration système.

Cependant, si le fichier contenant les paramètres du mot de passe est supprimé ou corrompu, et que l'ordinateur exécutant le serveur de gestion n'a pas d'autres problèmes, vous pouvez entrer les paramètres du mot de passe de configuration système :

1. Accédez à l'icône du serveur de gestion dans la barre d'état.
2. Effectuez un clic droit sur l'icône de service du Management Server de la zone de notification et sélectionnez **Entrer le mot de passe de configuration système**.
3. La boîte de dialogue pour entrer les paramètres du mot de passe de configuration système s'affiche.

La configuration système est protégée par un mot de passe

1. Saisissez le mot de passe dans le champ **mot de passe** puis sélectionnez **Entrer**.
2. Attendez que le mot de passe ait bien été accepté. Sélectionnez **Fermer**.
3. Vérifiez que le serveur de gestion s'exécute normalement.

La configuration système n'est pas protégée par un mot de passe

1. Cochez la case : **Ce système n'utilise pas de mot de passe de configuration système** puis sélectionnez **entrer**.
2. Attendez que le paramètre ait bien été accepté. Sélectionnez **Fermer**.
3. Vérifiez que le serveur de gestion s'exécute normalement.

Sauvegarde manuelle de la configuration de votre système (explications)

Si vous souhaitez effectuer une sauvegarde manuelle de la configuration de la base de données du serveur de gestion contenant la configuration du système, assurez-vous que votre système reste en ligne. Le nom par défaut de la base de données du serveur de gestion est **Surveillance**.

Voici quelques éléments à considérer avant de commencer la sauvegarde :

- Vous ne pouvez pas utiliser une sauvegarde de la base de données SQL Server pour copier des configurations de votre système pour d'autres systèmes
- La sauvegarde de la base de données SQL Server 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'activité, sont stockés dans la base de données du serveur de journaux et **ne font donc pas** partie d'une sauvegarde de la base de données du serveur de gestion. Le nom par défaut de la base de données du serveur de journaux est **SurveillanceLogServerV2**. Vous sauvegardez les deux base de données SQL Server en même temps.

Sauvegarde et restauration de la configuration du serveur d'événements (explications)

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 la base de données SQL Server. 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 arrêter toutes les communications externes pendant que la restauration de la configuration est en cours de chargement.

Sauvegarde et restauration programmées de la configuration du système (explications)

Le serveur de gestion sauvegarde la configuration de votre système dans une base de données SQL Server. Milestone vous recommande de programmer régulièrement des sauvegardes de cette base de données comme mesure de reprise après sinistre. Bien que la perte de la configuration de votre système soit un phénomène rare, cela peut arriver dans des circonstances malheureuses. Heureusement, la sauvegarde ne prend qu'une minute et elle offre également l'avantage de purger le journal de transactions de la base de données 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 manuelle de la configuration de votre système (explications) on page 360.

Lorsque vous sauvegardez/restaurez le serveur de gestion, assurez-vous que la base de données SQL Server comportant la configuration du système est incluse dans la sauvegarde/restauration.

Conditions préalables pour l'utilisation de la sauvegarde et la restauration programmées

Microsoft® SQL Server Management Studio, un outil à télécharger gratuitement depuis leur site Internet (https://www.microsoft.com/en-us/sql-server/sql-server-downloads).

Outre la gestion de SQL Server et de ses bases de données, l'outil comprend des fonctionnalités de sauvegarde et de restauration faciles à utiliser. Téléchargez et installez l'outil sur votre serveur de gestion.

Sauvegarder la configuration du système avec une sauvegarde programmée

1. Lancez Microsoft® SQL Server Management Studio depuis le menu Windows.
2. Lors de la connexion, spécifiez le nom du SQL Server requis. Utilisez le compte sous lequel vous avez créé la base de données SQL Server.
    1. Localisez la base de données SQL Server 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. Le nom par défaut de la base de données SQL est Surveillance.
    2. Faites une sauvegarde de la base de données SQL Server et assurez-vous de :

- Vérifiez que la base de données SQL Server sélectionnée est la correcte
- Vérifiez que le type de sauvegarde est **complète**
- Établissez la programmation pour la sauvegarde récurrente. Vous pouvez en lire d'avantage sur les sauvegardes programmées et automatiques sur le site Internet de Microsoft (https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017
- Vérifier que le chemin proposé est satisfaisant ou de sélectionner 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 du serveur de journaux en procédant de la même manière. Le nom par défaut de la base de données SQL Server du serveur de journaux est **SurveillanceLogServerV2**.

Restauration d'une configuration système à partir d'une sauvegarde programmée

Configuration
Afin d'empêcher les modifications de configuration du système pendant que vous restaurez la base de données de la configuration du système, arrêtez le :

- Service Management Server (voir Services du serveur de gestion on page 376)
- Event Server service (peut être effectué depuis les **Services** de Windows (recherchez **services.msc** sur votre machine. Dans **Services**, localisez **Milestone XProtect Event Server**))
- World Wide Web Publishing Service, également connu sous le nom d'Internet Information Service (IIS). En savois plus sur comment stopper l'IIS (https://technet.microsoft.com/library/cc732317(WS.10).aspx/)

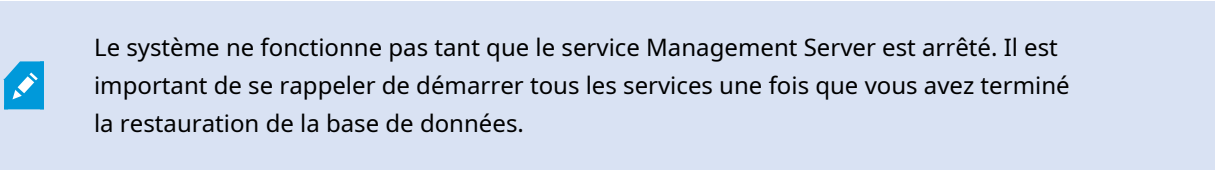
Ouvrez Microsoft® SQL Server Management Studio depuis le menu Windows **Démarrer**.

Dans l'outil, procédez comme suit :

1. Lors de la connexion, spécifiez le nom de votre SQL Server. Utilisez le compte utilisateur sous lequel la base de données SQL Server a été créée.
2. Localisez la base de données SQL Server (son nom par défaut est **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.

3. Faites une restauration de la base de données SQL Server et assurez-vous de :
    - Sélectionner Sauvegarder **à partir** d'un périphérique
    - Sélectionner sauvegarde du support de type **fichier**
    - Localisez et sélectionnez votre fichier de sauvegarde (**.bak**)
    - Sélectionner pour **écraser la base de données existante**
4. Suivez les instructions de l'outil jusqu'à la fin.

Utilisez la même méthode pour restaurer la base de données SQL Server du serveur de journaux avec vos journaux. Le nom par défaut de la base de données SQL Server du serveur de journaux est **SurveillanceLogServerV2**.



Le système ne fonctionne pas tant que le service Management Server est arrêté. Il est important de se rappeler de démarrer tous les services une fois que vous avez terminé la restauration de la base de données.

Sauvegarder la base de données du serveur de journaux

Gérer la base de données du serveur des journaux en utilisant la méthode que vous utilisez lorsque vous gérez la configuration du système comme décrit précédemment. La base de données du serveur des journaux contient tous les journaux système, y compris les erreurs reportées par les serveurs d'enregistrement et les caméras. Le nom par défaut de la base de données du serveur de journaux est **SurveillanceLogServerV2**.

La base de données SQL Server se trouve sur la SQL Server du serveur des journaux. En général, les bases de données SQL Server du serveur des journaux et du serveur de gestion se trouvent sur le même SQL Server. La sauvegarde de la base de données du serveur de journaux n'est pas indispensable puisqu'elle ne contient aucune configuration du système, mais il peut être utile d'avoir accès au journal système avant la sauvegarde/restauration du serveur de gestion.

Scénarios de problèmes et d'échecs de sauvegarde/restauration (explications)

- 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.
- Si vous restaurez une sauvegarde de configuration et que vous saisissez un mot de passe de configuration système incorrect, vous devez alors fournir le mot de passe de configuration système qui était valide au moment de la création de la sauvegarde.

Déplacer le serveur de gestion

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

- **Réseau SQL Server** : Si vous stockez votre configuration système dans une base de données SQL Server sur SQL Server de votre réseau, vous pouvez indiquer l'emplacement de la base de données sur ce SQL Server lors de l'installation du logiciel du serveur de gestion sur votre nouveau serveur de gestion. Dans ce cas, seul applique le paragraphe suivant sur le nom d'hôte et l'adresse IP du serveur de gestion et vous pouvez ignorer le reste de ce sujet :

  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 automatiquement au nom d'hôte et à l'adresse IP de l'ancien serveur de gestion. Si vous donnez au nouveau serveur de gestion un nouveau nom d'hôte et/ou une nouvelle adresse IP, le serveur d'enregistrement ne peut trouver le serveur de gestion et vous devez alors arrêter manuellement chaque service Recording Server dans votre système, changer l'URL de leur serveur de gestion, réenregistrer le serveur d'enregistrement et une fois fait, démarrer le service Recording Server.

- **Local SQL Server** : Si vous enregistrez votre configuration système dans une base de données SQL Server de SQL Server directement sur le serveur de gestion lui-même, il est important que vous sauvegardiez la base de données de configuration du système du serveur de gestion existant avant le transfert. En sauvegardant la base de données SQL Server et ensuite, en la restaurant sur un SQL Server sur le nouveau serveur de gestion, vous évitez d'avoir à reconfigurer vos caméras, règles, profils de temps etc. après le déplacement

> Si vous supprimez le serveur de gestion, vous aurez besoin du mot de passe de configuration du système actuel afin de restaurer la sauvegarde, voir Mot de passe de configuration système (explications) on page 357.

Prérequis

- **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

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.

- **Microsoft® SQL Server Management Studio**
- Que se passe-t-il lorsque le serveur de gestion est indisponible ? Serveurs de gestion indisponibles (explications) on page 365)
- Copier la base de données du serveur de journaux (voir Sauvegarder la base de données du serveur de journaux on page 363)

Serveurs de gestion indisponibles (explications)

- **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 jusqu'à quatre heures** : Lorsque les clients se connectent, ils sont autorisés par le serveur de gestion et peuvent communiquer avec les serveurs d'enregistrement jusqu'à quatre heures. Si le serveur de gestion peut s'exécuter durant ces quatre heures, la plupart de vos utilisateurs ne seront pas affectés
  - **Impossible 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. Il s'agit de la même procédure que pour programmer une sauvegarde programmée. Voir également Sauvegarder la configuration du système avec une sauvegarde programmée on page 361.
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 également Restauration d'une configuration système à partir d'une sauvegarde programmée on page 362.

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 les **Services** de Windows, configurez le **Type de démarrage** des services à **Désactiver**.

> **!** 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 d'accès pour l'endroit 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.

3. Enregistrez le nouveau serveur d'enregistrement sur le serveur de gestion. Pour ce faire, effectuez un clic droit avec votre souris sur l'icône Recording Server Manager de la barre, puis cliquez sur **Enregistrer**. Pour plus d'informations, voir Enregistrer un serveur d'enregistrement on page 210.
4. 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.

Déplacer du 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 protégés par une personne avec la protection des preuves (voir Protection des preuves (explications) on page 83) 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. Pour plus d'informations, voir Remplacer un serveur d'enregistrement on page 366.

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.

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.

Configuration
Avant de démarrer l'assistant :

- Assurez-vous que le nouveau serveur d'enregistrement peut accéder à la caméra physique par le biais du réseau
- Installez un serveur d'enregistrement vers lequel vous souhaitez déplacer un matériel (voir Installation via Download Manager (explications) on page 174 ou Installation silencieuse d'un serveur d'enregistrement on page 188)
- Installez les même version du pack de pilotes de périphériques sur le nouveau serveur d'enregistrement que vous exécutez sur le serveur existant (voir Pilotes de périphériques (explications) on page 157)

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.

> 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.

Diagnostic des problèmes de déplacement du matériel

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

Type d’erreur	Dépannage
Le serveur d’enregistrement n’est pas connecté ou est en mode de basculement.	Assurez-vous que le serveur d’enregistrement est bien en ligne. Vous aurez peut-être à l’enregistrer. Si le serveur est en mode de basculement, patientez et réessayez.
La version du serveur d’enregistrement n’est pas 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.	Assurez-vous de bien avoir autorisé le serveur d’enregistrement ou vérifiez qu’il n’a pas été supprimé.
Échec de la mise à jour de la configuration ou de la communication avec la base de données de configuration.	Assurez-vous que votre SQL Server et la base de données soient connectés et qu’ils fonctionnent.
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 soit 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.
Le stockage d’enregistrement source n’est pas disponible.	Vous tentez de déplacer du matériel avec des périphériques configurés avec un stockage d’enregistrement actuellement hors ligne.

Type d'erreur	Dépannage
	Un stockage d'enregistrement est hors ligne si le disque est hors ligne ou indisponible. Assurez-vous que le stockage d'enregistrement en bien connecté et réessayez.
Tous les stockages des enregistrements disponibles sur le serveur d'enregistrement cible doivent être disponibles.	Vous tentez de déplacer du matériel vers un serveur d'enregistrement où une ou plusieurs stockages des enregistrements sont actuellement hors ligne. Assurez-vous que tous les stockages des enregistrement sur le serveur d'enregistrement cible sont en ligne. Un stockage d'enregistrement est hors ligne si le disque est hors ligne ou indisponible.

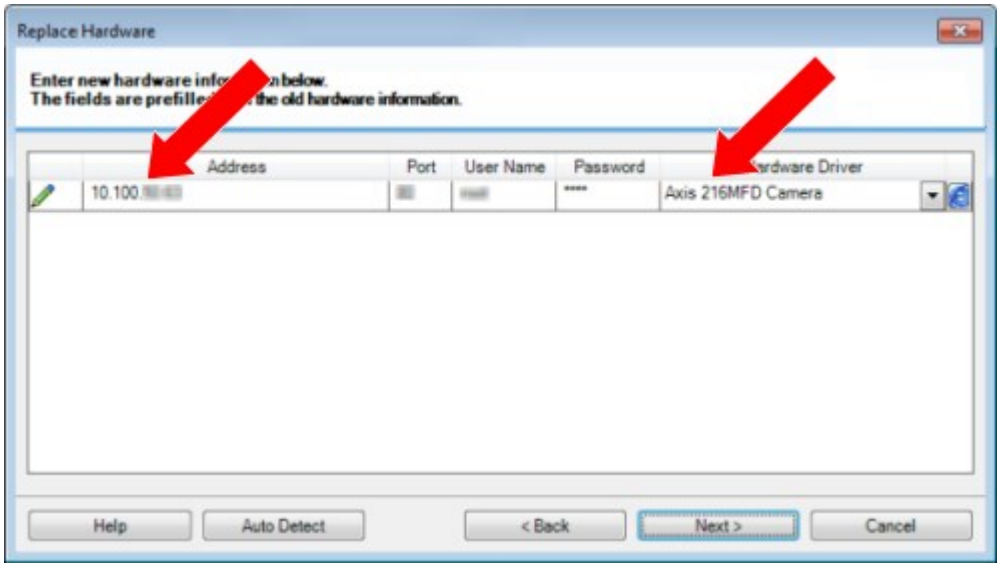
Remplacer le matériel

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 autorisé l'activation automatique des licences (voir Activation automatique des licences (explications) on page 130 et si vous avez utilisé tous les changements apportés aux périphériques sans activation (voir Changements apportés aux périphériques sans activation (explications) on page 131), vous devez activer manuellement vos licences **après** avoir remplacé les périphériques. Si le nouveau nombre de périphériques excède le nombre total de licences de périphériques, vous devez acheter de nouvelles licences de périphériques.

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 connu, sélectionnez le pilote concerné 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**.



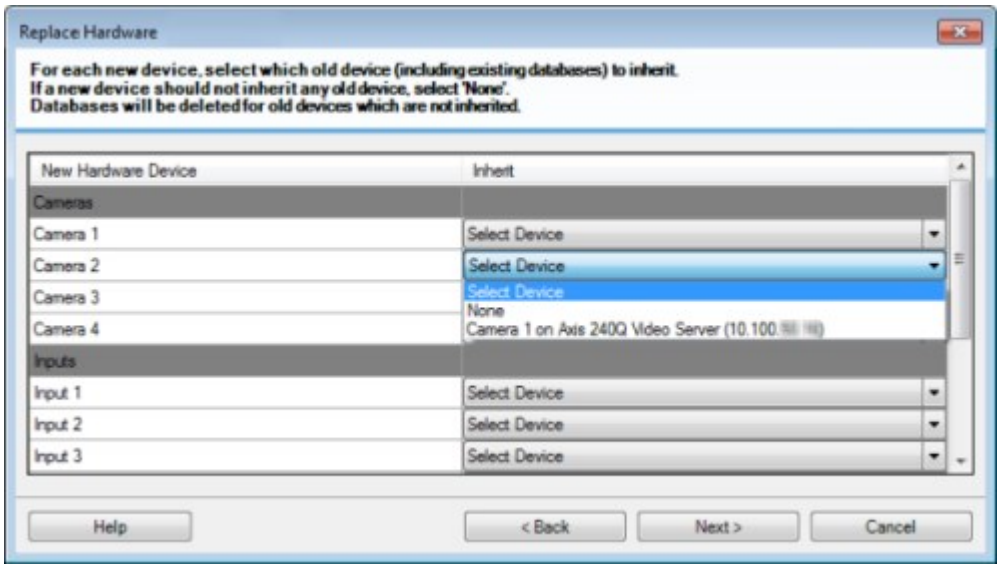
L'assistant est prérempli avec les données du matériel existant. Si vous le remplacez par un périphérique similaire, vous pouvez réutiliser certaines de ces informations, comme, par exemple, les informations concernant le port et le pilote.

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**

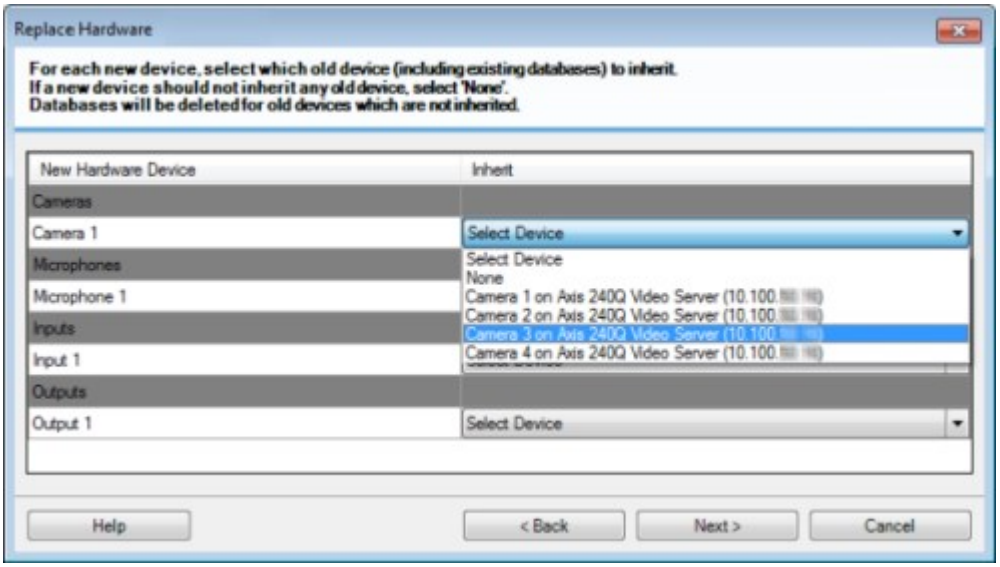
     Cette étape est conçue pour vous aider à cartographier vos périphériques et leurs bases de données, en fonction du nombre de caméras, micros, entrées et sorties individuels, etc., connectés respectivement à l'ancien périphérique et au nouveau.

     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.

     > ⚠ Assurez-vous de cartographier **tous** les microphones, caméras, entrées, sorties, etc. Le contenu cartographié sur **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.

Mettre à jour vos données de matériel

Pour vous assurer que le périphérique matériel et le système utilisent la même version de firmware, vous devez mettre à jour manuellement les données de matériel du périphérique matériel dans le Management Client. Milestone vous recommande de mettre à jour les données matérielles après chaque mise à jour de micrologiciel effectuée sur votre matériel.

Pour obtenir les dernières données de matériel :

1. Dans le volet **Navigation du site**, sélectionnez **Serveurs d'enregistrement**.
2. Développez le serveur d'enregistrement souhaité, puis sélectionnez le matériel dont vous souhaitez obtenir les dernières informations.
3. Dans le volet **Propriétés** de l'onglet **Informations**, cliquez sur le bouton **Mettre à jour** dans le champ **Données de matériel mises à jour pour la dernière fois**.

4. L'assistant vérifie si le système exécute le dernier firmware pour le matériel.

   Sélectionnez **Confirmer** pour mettre à jour les informations dans le Management Client. Une fois la mise à jour terminée, la version de firmware actuelle du périphérique matériel qui est détecté par le système apparaît dans le champ **Version du firmware** de l'onglet **Infos**.

Modifier l'emplacement et le nom d'une base de données SQL Server

Le serveur de gestion, le serveur d'événements, le serveur de journaux, Identity Provider et XProtect Incident Manager se connectent à différentes bases de données SQL Server à l'aide de chaînes de connexion. Ces chaînes de connexion sont stockées dans le registre Windows. Si vous avez modifié l'emplacement ou le nom d'une base de données SQL Server, vous devez modifier toutes les chaînes de connexion qui pointent vers cette base de données SQL Server.

Base de données	Utilisée par
Base de données de surveillance	• Service Management Server • Service Event Server • Pool d'applications VideoOS Management Server • Pool d'applications VideoOS Report Server
Surveillance_IDP	• Pool d'applications VideoOS IDP
Surveillance_IM	• Pool d'applications VideoOS IM
Surveillance_LogServerV2	• Service Log Server

Avant de continuer :

- Sauvegarder les bases de données SQL Server et le registre Windows.
- Assurez-vous que l'utilisateur qui exécute les services connexes et les pools d'applications est le propriétaire de la base de données.
- Achever la migration du contenu de l'ancienne base de données SQL Server vers la nouvelle.

Pour mettre à jour les chaînes de connexion avec le nouvel emplacement et le nouveau nom d'une base de données SQL Server :

1. Arrêtez tous les services du VMS XProtect et pools d'applications qui utilisent la base de données SQL Server.

   > Selon l'architecture de votre système, les services et les pools d'applications peuvent s'exécuter sur des ordinateurs différents. Vous devez arrêter tous les pools d'applications et les services qui se connectent à la même base de données SQL Server.

2. Dans l'Éditeur du registre, accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\VideoOS\Server\ConnectionString`.
3. Mettez à jour les chaînes de connexion avec le nouvel emplacement et le nouveau nom de la base de données SQL Server.

   Les chaînes de connexion par défaut pour toutes les bases de données SQL Server sont les suivantes :

   - **ManagementServer** : `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **EventServer** : `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **ServerService** : `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **ReportServer** : `Data Source=localhost;Initial Catalog=Surveillance;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **IDP** : `Data Source=localhost;Initial Catalog=Surveillance_IDP;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **IncidentManager** : `Data Source=localhost;Initial Catalog=Surveillance_IM;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`
   - **LogServer** : `Data Source=localhost;Initial Catalog=SurveillanceLogServerV2;Integrated Security=True;Max Pool Size=1000;Encrypt=True;Trust Server Certificate=True`

4. Démarrez tous les services XProtect et pools d'applications que vous avez arrêtés à l'étape 1.

Services du serveur de gestion

Sur l'ordinateur qui exécute les services du serveur, vous trouvez les icônes de barre d'état du Gestionnaire de serveur dans la zone de notification. Avec ces icônes, vous pouvez accéder aux informations relatives aux services et effectuer certaines tâches. 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.

Icônes de la barre des tâches du serveur de gestion (explications)

Les icônes de la barre des tâches affichent les différents états des services exécutés sur le serveur de gestion, le serveur d'enregistrement, le serveur d'enregistrement de basculement et le serveur d'événements. Elles sont visibles sur les ordinateurs où sont installés les serveurs, dans la zone de notification :

Management Server Manager icône de la barre des tâches	Recording Server Manager icône de la barre des tâches	Event Server Manager icône de la barre des tâches	Failover Recording Server Manager icône de la barre des tâches	Description
				**En cours** S'affiche lorsqu'un service du serveur est activé et a démarré. Si le service Failover Recording Server est en cours d'exécution, il peut prendre le relais si les serveurs d'enregistrement standards échouent.
				**Arrêté** S'affiche quand le service du serveur s'arrête.

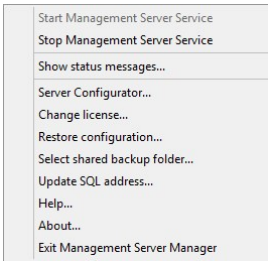
Management Server Manager icône de la barre des tâches	Recording Server Manager icône de la barre des tâches	Event Server Manager icône de la barre des tâches	Failover Recording Server Manager icône de la barre des tâches	Description
				Si le service Failover Recording Server s'arrête, il ne peut prendre le relais si les serveurs d'enregistrement standards échouent.
				**Démarrage** S'affiche quand un service du serveur est en cours de démarrage. Dans des circonstances normales, l'icône de la barre des tâches passe peu après à **En cours**.
				**Arrêt en cours** S'affiche quand un service du serveur est en cours d'arrêt. Dans des circonstances normales, l'icône de la barre des tâches passe peu après à **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

Management Server Manager icône de la barre des tâches	Recording Server Manager icône de la barre des tâches	Event Server Manager icône de la barre des tâches	Failover Recording Server Manager icône de la barre des tâches	Description
				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 Serveur d'enregistrement ou Serveur d'enregistrement de basculement est en cours de fonctionnement, mais pas le service Management Server.

Démarrer ou arrêter le service Management Server

L'icône de la barre d'état Management Server Manager indique l'état du service du Management Server, par exemple **Exécution en cours**. Par le biais de cette icône, vous pouvez démarrer ou arrêter le service Management Server. Si vous arrêtez le service Management Server, vous ne pourrez pas utiliser le Management Client.

1. Dans la zone de notification, cliquez avec le bouton droit sur l'icône de la barre d'état Management Server Manager. 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.

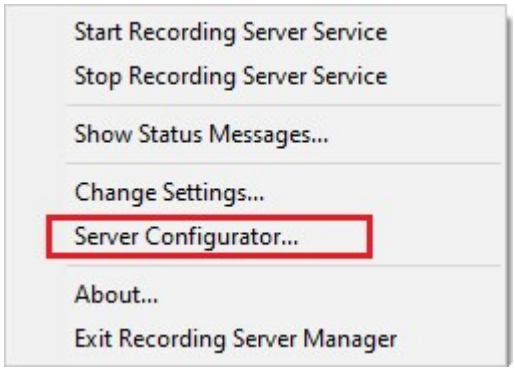
3. Pour arrêter le service, cliquez sur **Arrêter le service Management Server**.

> Pour plus d'informations sur les icônes de la barre des tâches, voir Icônes de la barre des tâches du serveur de gestion (explications) on page 377.

Démarrer ou arrêter le service Recording Server

L'icône de la barre d'état Recording Server Manager indique l'état du service du Recording Server, par exemple **Exécution en cours**. Par le biais de cette icône, vous pouvez démarrer ou arrêter 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 avec le bouton droit sur l'icône de la barre d'état Recording Server Manager. Un menu contextuel s'affiche.

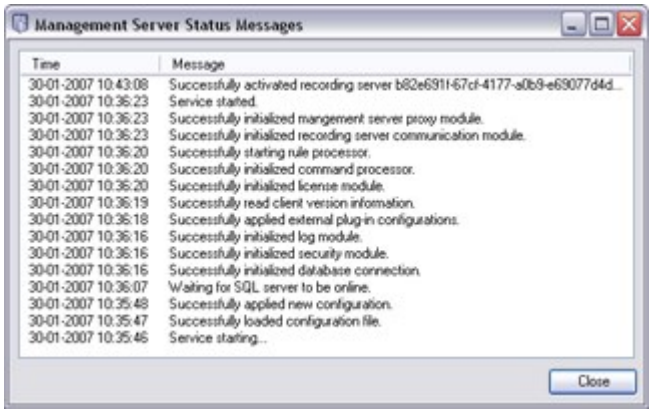


2. Si le service s'est arrêté, cliquez sur **Démarrer le service Recording Server** pour le lancer. L'icône de la barre des tâches reflète son nouvel état.
3. Pour arrêter le service, cliquez sur **Arrêter le service Recording Server**.

> Pour plus d'informations sur les icônes de la barre des tâches, voir Icônes de la barre des tâches du serveur de gestion (explications) on page 377.

Consulter les messages d'état relatifs au serveur de gestion ou au serveur d'enregistrement

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 :



Gérer le cryptage avec le Server Configurator

Utilisez le Server Configurator pour sélectionner des certificats sur les serveurs locaux pour la communication cryptée et enregistrez les services du serveur afin qu'ils puissent communiquer avec les serveurs.

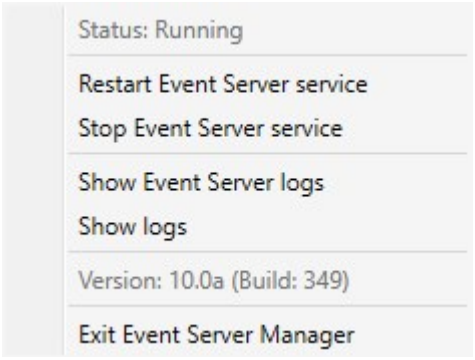
Ouvrez le Server Configurator depuis le menu Démarrer de Windows ou depuis l'icône de la barre des tâches du serveur de gestion ou depuis celle du serveur d'enregistrement. Voir Server Configurator (Utilitaire) on page 437.

Pour plus d'informations, voir le guide des certificats sur comment sécuriser votre installation de XProtect VMS.

Démarrer, arrêter ou redémarrer le service Event Server

L'icône de la barre d'état Event Server Manager indique l'état du service du Event Server, par exemple **Exécution en cours**. 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 plus d'informations, voir Arrêt du service Event Server on page 382.

1. Dans la zone de notification, cliquez avec le bouton droit sur l'icône de la barre d'état Event Server Manager. 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 plus d'informations sur les icônes de la barre des tâches, voir Icônes de la barre des tâches du serveur de gestion (explications) on page 377.

Arrêt du 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. Durant l'arrêt du service beaucoup de zones du système de logiciel de gestion des vidéos cesseront de fonctionner :

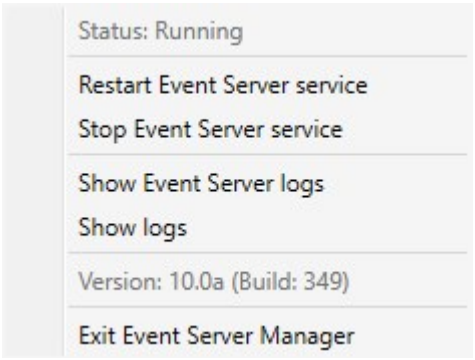
- Aucun événement ou alarme ne sera stocké(e) dans le serveur d'événements. Cependant, les événements système et les événements de périphériques déclencheront encore des actions, telles que le démarrage de l'enregistrement
- Les extensions XProtect ne fonctionnent pas dans XProtect Smart Client et ne peuvent être configurées depuis le Management Client.
- Les événements analytiques ne fonctionnent pas
- Les événements génériques ne fonctionnent pas
- Aucune alarme n'est déclenchée
- Dans XProtect Smart Client, les éléments de vue du plan, 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 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

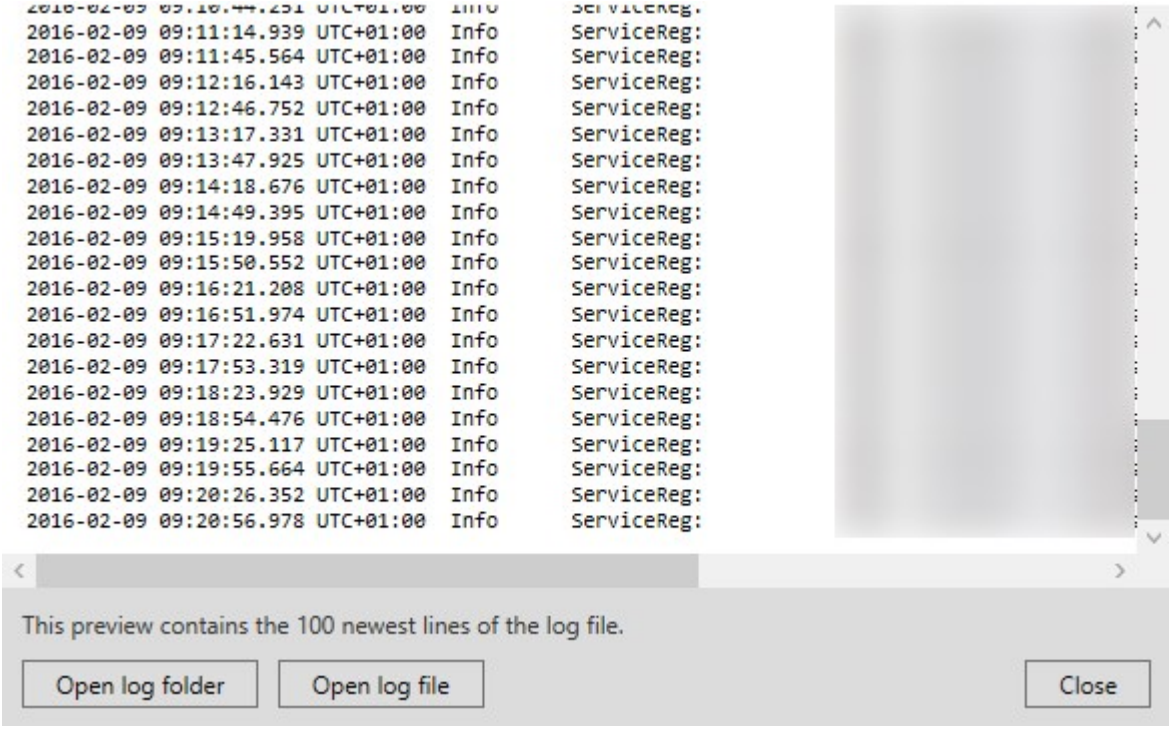
Consulter le Event Server ou les journaux MIP

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 **Serveur d’événements**.

1. Dans la zone de notification, cliquez avec le bouton droit sur l’icône de la barre d’état Event Server Manager. Un menu contextuel s’affiche.



2. Pour consulter les 100 lignes les plus récentes du journal Event Server, 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, revenez au menu contextuel et cliquez sur **Afficher les journaux MIP**. Un programme d'affichage des journaux s'affiche.

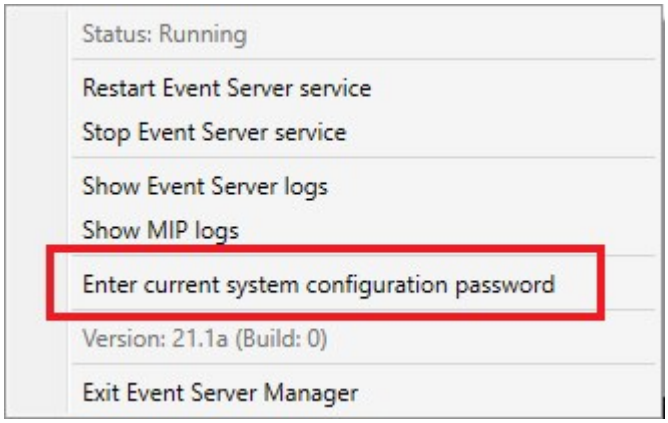
Si une personne supprime le fichier journal du répertoire de journal, les éléments du menu s'affichent en gris. Pour ouvrir le lecteur de journal, vous devez d'abord copier les fichiers journaux dans leur dossier : `C:\ProgramData\Milestone\XProtect Event Server\logs` ou `C:\ProgramData\Milestone\XProtect Event Server\logs\MIP Logs`.

Saisir le mot de passe de configuration du système actuel

Si le mot de passe de configuration du système a été modifié dans le serveur de gestion, vous devez saisir le mot de passe de configuration du système actuel dans le serveur de gestion également.

Si vous ne saisissez pas le mot de passe actuel dans le serveur d'événements, alors les composants du système, tels que le contrôle d'accès, cessera de fonctionner.

1. Dans la zone de notification, cliquez avec le bouton droit sur l'icône de la barre d'état Event Server Manager. Un menu contextuel s'affiche.



2. Pour saisir le mot de passe de configuration du système actuel, cliquez sur **Saisir le mot de passe de configuration du système actuel**. Une fenêtre s'affiche.
3. Saisissez le même mot de passe de configuration du système qui a été saisi dans le serveur de gestion.

Gérer les 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 Event Server
- Service Log Server

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.

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.
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://ipaddress:port/directory* (où le port et le répertoire sont facultatifs). 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). Modifier l'état de confiance modifie également l'état des autres services enregistrés partageant une ou plusieurs URL définies pour le service enregistré pertinent.

Composant	Exigences
Description	Description du service enregistré. La description est utilisée à des fins d'affichage dans le Management Client.
Avancés	Lorsqu'un service est avancé, il dispose de son propre modèle d'URI (par exemple, HTTP, HTTPS, TCP, ou UDP) qui doit être configuré pour chaque adresse d'hôte que vous définissez. Une adresse dhôte a donc de multiples extrémités, ayant chacune leur propre modèle, adresse dhôte et port IP pour ce modèle.

Supprimer des pilotes de périphériques (explications)

Si vous souhaitez supprimer des pilotes de périphériques de votre ordinateur, vous pouvez supprimer les packs de pilotes de périphériques de votre système. Pour ce faire, suivez la procédure Windows standard pour la suppression de programmes.

Si vous possédez plusieurs packs de pilotes de périphériques installés et rencontrez des problèmes pour supprimer les fichiers, vous pouvez utiliser le script du dossier d'installation du pack de pilotes de périphériques pour les supprimer totalement.

Si vous supprimez des pilotes de périphériques, le serveur d'enregistrement et les périphériques de type caméra ne pourront plus communiquer entre eux. Ne supprimez pas les packs de pilotes de périphériques lorsque vous procédez à une mise à niveau parce que vous installez une nouvelle version en la superposant à une ancienne. Vous pouvez supprimer le pack de pilotes de périphériques dans le seul cas où vous désinstallez l'intégralité du système.

Supprimer un serveur d'enregistrement

> ⚠ 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

> ⚠ 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.

Modifier le nom d'hôte sur l'ordinateur du serveur de gestion

Si le serveur de gestion est considéré par son nom de domaine entièrement qualifié ou par son nom d'hôte, la modification du nom d'hôte de l'ordinateur aura des implications dans XProtect qu'il faudra considérer et prendre en compte.

> ⚠ En général, une modification du nom d'hôte d'un serveur de gestion doit être planifiée avec attention en raison des nombreux changements découlant de cette opération.

Les sections suivantes vous offrent un aperçu de certaines implications d'un changement du nom d'hôte.

La validité de certificats

Les certificats sont utilisés pour crypter la communication entre les services, et les certificats sont installés sur tous les ordinateurs qui exécutent un ou plusieurs services XProtect.

Selon la méthode de création des certificats, ces derniers peuvent être liés à l'ordinateur sur lequel ils sont installés, et ils seront uniquement valides aussi longtemps que le nom de l'ordinateur reste inchangé.

Pour en savoir plus sur la manière de créer des certificats, voir Introduction aux certificats.

Si le nom d'un ordinateur est modifié, les certificats utilisés peuvent perdre leur validité et le VMS XProtect ne pourra pas démarrer. Effectuez les étapes suivantes pour configurer et exécuter à nouveau le système :

- Créer de nouveaux certificats et les réinstaller sur tous les ordinateurs de l'environnement.
- Appliquer les nouveaux certificats en utilisant Server Configurator sur chacun des ordinateurs pour activer le cryptage avec les nouveaux certificats.

Cette action déclenchera l'enregistrement des nouveaux certificats et rétablira le système.

Perte des propriétés de données personnalisées pour les services enregistrés

Si vous effectuez une inscription via le Server Configurator après, par exemple, un changement de l'adresse du serveur de gestion, toute modification des informations des services enregistrés sera écrasée. Par conséquent, si vous avez modifié les informations des services enregistrés, les changements doivent être appliqués à nouveau pour tous les services qui sont enregistrés sur le serveur de gestion sur l'ordinateur dont le nom a été modifié.

Les informations qui peuvent être modifiées pour les services enregistrés sont situées sous **Outils** > **Services enregistrés** > **Modifer** :

- De confiance
- Avancés
- Indicateur externe
- Toute URL ajoutée manuellement

Dans Milestone Customer Dashboard, le nom d'hôte apparaîtra inchangé

Milestone Customer Dashboard est un outil en ligne gratuit pour les partenaires et revendeurs Milestone et les utilisateurs VMS XProtect, destiné à gérer et surveiller les installations et licences du logiciel Milestone.

Un changement du nom du serveur de gestion dans un système connecté à Milestone Customer Dashboard ne sera pas automatiquement refléter dans Milestone Customer Dashboard.

L'ancien nom d'hôte apparaîtra dans Milestone Customer Dashboard jusqu'à l'activation d'une nouvelle licence. Par contre, le changement de nom n'aura aucune conséquence dans Milestone Customer Dashboard et une fois qu'une nouvelle activation aura lieu, l'enregistrement sera mis à jour dans la base de données avec le nouveau nom d'hôte. Pour plus d'informations sur Milestone Customer Dashboard, voir Milestone Customer Dashboard (explications).

Le changement du nom d'hôte peut déclencher un changement de l'adresse SQL Server.

Si SQL Server se trouve sur le même ordinateur que le serveur de gestion, et que le nom de cet ordinateur est modifié, l'adresse de SQL Server changera en conséquent. Cela signifie que l'adresse du SQL Server n'aura pas à être mise à jour pour les éléments situés sur différents ordinateurs, de même que pour les composants situés sur l'ordinateur local qui utilisent le nom de l'ordinateur et non localhost pour se connecter à SQL Server.

Cela s'applique en particulier pour le Event Server, qui utilise la même adresse que le Management Server. Cela peut également s'appliquer au Log Server, qui utilise une base de données différente, mais sur le même SQL Server.

Voir Modifier l'emplacement et le nom d'une base de données SQL Server on page 375.

Changement du nom d'hôte dans un Milestone Federated Architecture

La modification du nom de l'ordinateur qui réside dans une configuration de Milestone Federated Architecture aura les implications suivantes, qui s'appliquent lorsque les sites sont connectés au sein des groupes de travail, mais aussi dans les domaines.

L'hôte du site constitue le noeud racine dans l'architecture

Si vous modifiez le nom de l'ordinateur sur lequel s'exécute le site central de l'architecture, tous les noeuds enfants seront automatiquement rattachés à la nouvelle adresse. Dans ce cas, aucune autre action n'est nécessaire apès la modification du nom.

L'hôte du site est un noeud enfant dans l'architecture

Pour éviter des problèmes de connexion lors du changement du nom d'un ordinateur sur lequel s'exécutent un ou plusieurs sites fédérés, vous devez ajouter une adresse alternative au site concerné avant de modifier le nom de l'ordinateur. Le site concerné est le noeud dont l'ordinateur hôte sera renommé. Pour plus d'informations sur les problèmes de connexion en raison de changements de nom d'hôte non préparés ou inattendus et comment les résoudre, voir Problème : Échec de la connexion d'un noeud parent à un noeud enfant dans une configuration Milestone Federated Architecture.

L'adresse alternative doit être ajoutée dans le volet **Propriétés** dans le volet **Navigation du site** ou le volet **Hiérarchie des sites fédérés**. Il est nécessaire de suivre les prérequis suivants :

- Pour être valide, l'adresse alternative doit être ajoutée avant de modifier l'ordinateur hôte
- L'adresse alternative doit refléter le futur nom de l'ordinateur hôte (si renommé)

Voir Configurer les propriétés du site pour plus d'informations sur comment accéder au volet **Propriétés**.

Pour une mise à jour transparente, arrêtez le Management Client sur le noeud qui sert de noeud parent sur celui dont le nom d'hôte sera modifié. Sinon, arrêtez et redémarrez le client après avoir modifié le nom de l'ordinateur. Pour plus d'informations, voir Démarrer ou arrêter le service Management Server.

Assurez-vous également que l'adresse alternative soit reflétée dans le volet **Hiérarchie des sites fédérées** sur votre site central et sinon, arrêtez et redémarrez le Management Client.

Une fois que l'hôte a été renommé et que vous avez redémarré l'ordinateur, le site fédéré basculera automatiquement vers la nouvelle adresse.

Gérer les journaux du serveur

Il existe différents types de journaux de serveur :

- Journal système
- Journal d'activité
- Journaux déclenchés par les règles

Ces derniers consignent l'utilisation du système. Ils sont disponibles dans Management Client sous **Journaux de serveur**.

Pour en savoir plus sur les journaux utilisés pour le dépannage et l'enquête sur les erreurs du logiciel, voir Journaux de débogage (explications) on page 395.

Identifier l'activité des utilisateurs, les événements, les actions et les erreurs

Utiliser les journaux pour obtenir un rapport détaillé de l'activité des utilisateurs, des événements, des actions et des erreurs dans le système.

Pour afficher les journaux dans le Management Client, rendez-vous dans le volet **Navigation sur le site**, puis sélectionnez **Journaux des serveurs**.

Type de journaux	Quels éléments sont-ils enregistrés ?
Journaux système	Informations associées au système
Journaux d'audit	Activité des utilisateurs
Journaux déclenchés par les règles	Les règles dans lesquelles les utilisateurs ont spécifié l'action **Créer une <lentrée au journal>**. Pour en savoir plus sur l'action du <log entry>, voir Actions et actions d'arrêt.

Pour consulter les journaux dans une autre langue, voir Onglet Général (options) on page 416 sous **Options**.

Pour exporter les journaux en tant fichiers présentant des valeurs séparées par des virgules (.csv), consultez la rubrique Exporter les journaux.

Pour modifier les paramètres des journaux, voir Onglet Journaux de serveurs (options) on page 419.

Filtrer les journaux

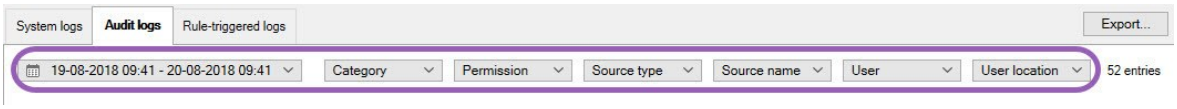
Dans chaque fenêtre des journaux, vous pouvez appliquer des filtres pour afficher les entrées des journaux depuis, par exemple, une plage de temps spécifique, un périphérique ou un utilisateur.

> Les filtres sont générés depuis les entrées de journaux actuellement visibles dans l'interface utilisateur.

1. Dans le volet **Navigation sur le site**, sélectionnez **Journaux des serveurs**. Par défaut, l'onglet **Journaux système** s'affiche.

   Sélectionnez un autre onglet pour naviguer entre les types de journaux.

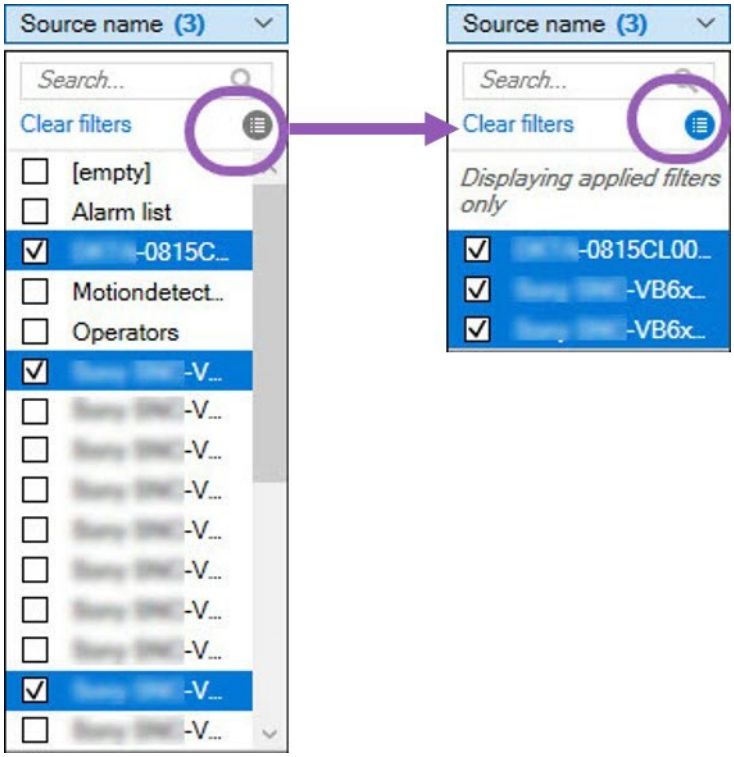
2. Dans les onglets, sélectionnez un groupe de filtres, par exemple, **Catégorie**, **Type de source**, ou **Utilisateur**.

   Une liste de filtre apparaît. Une liste de filtres affiche 1000 filtres.

3. Sélectionnez un filtre pour l'appliquer. Sélectionnez le filtre à nouveau pour le supprimer.

   Facultatif : Dans une liste de filtres, sélectionnez **Afficher les filtres appliqués uniquement** pour n'afficher que les filtres que vous avez appliqués.



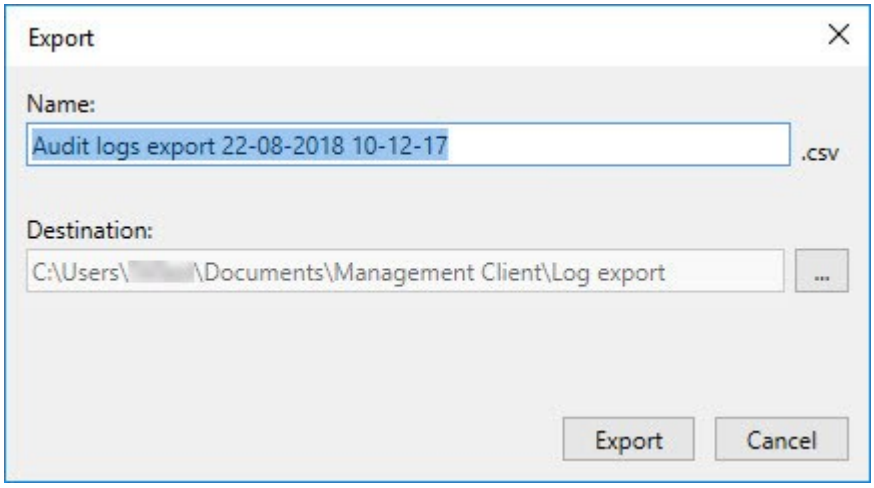
Lorsque vous exportez des journaux, le contenu de votre exportation est modifié en fonction des filtres appliqués. Pour obtenir des informations sur votre exportation, voir Exporter les journaux.

Exporter les journaux

L'exportation de journaux vous permet d'enregistrer les entrées des journaux au-delà de la durée de rétention des journaux par exemple. Vous pouvez exporter les journaux sous forme de fichiers présentant des valeurs séparées par des virgules (.csv).

Pour exporter un journal :

1. Sélectionnez **Exporter** dans le coin supérieur droit. La fenêtre **Exporter** s'ouvre.



2. Dans la fenêtre **Exporter**, dans le champ **Nom**, indiquez un nom pour le fichier journal.
3. Par défaut, les fichiers de journaux exportés sont sauvegardés dans votre dossier **Exportation de journaux**. Pour spécifier un emplacement différent, sélectionnez ... à droite du champ **Destination**.
4. Sélectionnez **Exporter** pour exporter le journal.

Le contenu de votre exportation est modifié en fonction des filtres appliqués. Pour obtenir des informations sur votre exportation, voir Filtrer les journaux.

Rechercher des journaux

Pour chercher un journal, utilisez la fonctionnalité **Critères de recherche** située dans la partie supérieur du panneau des journaux :

1. Précisez vos critères de recherche depuis les listes.
2. Cliquez sur **Actualiser** pour que la page des journaux reflètent vos critères de recherche. Pour effacer vos critères de recherche et retourner à la vue du contenu global des journaux, cliquez sur **Effacer**.

Vous pouvez effectuer un double-clic sur une ligne pour afficher tous les détails dans une fenêtre **Détails des journaux**. De cette façon, vous pouvez également lire les entrées de journaux qui contiennent plus de texte que ne peut afficher une seule ligne.

Changer la langue du journal

1. Dans la partie inférieure du panneau des journaux, dans la liste **Afficher le journal en**, sélectionnez la langue désirée.

2. Le journal s'affiche dans la langue sélectionnée. La prochaine fois que vous ouvrirez le journal, la langue par défaut sera rétablie.

Autoriser les composants de la version 2018 R2 et des versions antérieures à écrire dans les journaux

La version 2018 R3 du serveur de journaux intègre l'authentification pour renforcer la sécurité. Cette option empêche les composants de la version 2018 R2 et des versions antérieures à écrire des journaux dans le serveur de journaux.

Composants affectés :

- XProtect Smart Client
- Module d'extension XProtect LPR
- LPR Server
- Modules d'extension du contrôle d'accès
- Serveur d'événements
- Module d'extension de l'alarme

Si vous utilisez la version 2018 R2 ou une version antérieure des composants énumérés ci-dessus, vous devez déterminer si vous autorisez le composant à écrire sur les journaux dans le nouveau serveur de journaux :

1. Sélectionnez **Outils** > **Options**.
2. Dans la boîte de dialogue **Options**, au bas de l'onglet **Journaux des serveurs**, trouvez la case **Autoriser la version 2018 R2 et les composants antérieurs à écrire dans les journaux**.
    - Cochez la case Autoriser la version 2018 R2 et les composants antérieurs à écrire dans les journaux
    - Décochez la case si vous ne souhaitez pas autoriser la version 2018 R2 et les composants antérieurs à écrire dans les journaux

Journaux de débogage (explications)

Les journaux de débogage permettent d'identifier les défauts et failles du système.

Pour en savoir plus sur les journaux utilisés dans l'utilisation du système, voir Gérer les journaux du serveur on page 391.

Les fichiers journaux de l'installation du XProtect sont situés aux emplacements suivants :

- C:\ProgramData\Milestone\IDP\Logs

  > Cet emplacement est accessible uniquement aux utilisateurs IIS et aux administrateurs. Ces permissions doivent être mises à jour en cas de modification de l'utilisateur IIS.

- C:\ProgramData\Milestone\MIPSDK
- 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 Mobile Server\Logs
- C:\ProgramData\Milestone\XProtect Recording Server\Logs
- C:\ProgramData\Milestone\XProtect Report Web Server\Logs

Dépannage

Problème : Le changement de SQL Server et de l'emplacement de la base de données empêche l'accès à la base de données

Si l'emplacement des bases de données SQL Server et VMS a changé, par exemple en changeant le nom d'hôte de l'ordinateur qui exécute SQL Server, l'accès du serveur d'enregistrement à la base de données est perdu.

Solution : modifiez les chaînes de connexion pour refléter le changement de SQL Server et de la base de données. Voir Modifier l'emplacement et le nom d'une base de données SQL Server on page 375.

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. Depuis le menu **Démarrage** de Windows, sélectionnez **Panneau de configuration**.
2. Dans le **Panneau de configuration**, effectuez un double-clic sur **Ajouter ou supprimer des programmes**.
3. À gauche de la fenêtre **Ajouter ou supprimer des programmes**, cliquez sur **Ajouter/Supprimer des fonctionnalités 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 **Service SMTP** est cochée ou non. Si oui, le Service SMTP est installé.

Si le Service SMTP est installé, choisissez une des solutions suivantes :

Solution 1 : Désactivez SMTP Service, ou réglez-le sur démarrage manuel

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

1. Depuis le menu **Démarrage** de Windows, sélectionnez **Panneau de configuration**.
2. Dans le **Panneau de configuration**, effectuez un double-clic sur **Outils d'administration**.
3. Dans la fenêtre **Outils administratifs**, 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 : Supprimez le Service SMTP

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

1. Depuis le menu **Démarrage** de Windows, sélectionnez **Panneau de configuration**.
2. Dans la fenêtre du **Panneau de configuration**, effectuez un double-clic sur **Ajouter ou supprimer des programmes**.
3. À gauche de la fenêtre **Ajouter ou supprimer des programmes**, cliquez sur **Ajouter/Supprimer des fonctionnalités 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 **Service SMTP**.
6. Cliquez sur **OK**, **Suivant** et **Terminer**.

Problème : Recording Server est mis hors tension lors du basculement du nœud en grappe de Management Server

Si vous configurez une grappe Microsoft pour la redondance de Management Server, le Recording Server ou Recording Server seront mis hors tension lors du basculement de Management Server entre les noeuds en grappe.

Pour y remédier, procédez comme suit :

> Lorsque vous effectuez des changements dans la configuration, sur le gestionnaire du cluster de basculement de Microsoft, mettez en pause le contrôle et la surveillance du service afin que le Server Configurator puisse effectuer les changements et démarrer et/ou arrêter le service Management Server. En cas de modification du type de démarrage du service du cluster de basculement au type manuel, ceci ne devrait pas interférer avecle Server Configurator.

Sur l'ordinateur Management Server :

1. Démarrez le Server Configurator sur tous les ordinateurs où est installé un serveur de gestion.
2. Rendez-vous sur la page **Enregistrement**.
3. Cliquez sur le symbole du stylo ( ) pour modifier l'adresse du serveur de gestion.
4. Modifiez l'adresse du serveur de gestion pour qu'elle corresponde au nom du rôle de cluster hébergeant le Management Server, par exemple `http://MyCluster`.
5. Cliquez sur **Enregistrer**.

Sur les ordinateurs où sont installés les composants qui utilisent le Management Server (par exemple, Recording Server, Mobile Server, Event Server , API Gateway) :

1. Démarrez Server Configurator sur tous les ordinateurs.
2. Rendez-vous sur la page **Enregistrement**.
3. Modifiez l'adresse du serveur de gestion pour qu'elle corresponde au nom du rôle de cluster hébergeant le Management Server, par exemple `http://MyCluster`.
4. Cliquez sur **Enregistrer**.

Problème : Échec de la connexion d'un noeud parent à un noeud enfant dans une configuration Milestone Federated Architecture

Si vous avez renommé l'ordinateur hôte d'un site qui agit en tant que noeud enfant dans un Milestone Federated Architecture, un parent noeud ne pourra pas s'y connecter.

Rétablir la connexion entre un noeud parent et le site

- Détachez le site concerné de son parent. Pour plus di'nformations, voir Détacher un site de sa hiérarchie.
- Rattacher le site en utilisant le nouveau nom de son hôte. Pour en savoir plus, voir Ajouter un site à une hiérarchie.

Pour garantir que les changements prennent effet, vous devriez arrêter et redémarrer le Management Client sur le noeud qui sert de parent noeud à celui dont le nom d'hôte a changé. Pour plus d'informations, voir Démarrer ou arrêter le service Management Server.

Pour plus d'informations sur les conséquences d'un changement du nom d'hôte dans une configuration Milestone Federated Architecture, voir Changements du nom d'hôte dans un Milestone Federated Architecture.

Problème : Le service Azure SQL Database n'est pas disponible

Si vous utilisez Azure SQL Database et que vous rencontrez un problème de connexion lors de l'installation ou pendant le fonctionnement normal, la raison peut être que le service Azure SQL Database est temporairement indisponible.

Azure SQL Database est un service dans lequel la plupart des opérations traditionnelles de maintenance des bases de données sont prises en charge par Microsoft. Le service peut être indisponible pendant de courtes périodes et il est conçu pour se rétablir jusqu'à un certain point sans que l'utilisateur ait à intervenir.

Les erreurs de base de données sont enregistrées dans les fichiers journaux du VMS XProtect avec un numéro d'incident associé, qui peut être communiqué à l'assistance Microsoft en cas d'indisponibilité prolongée d'Azure SQL Database.

Pour en savoir plus, voir Dépannage des problèmes de connexion courants avec Azure SQL Database.

Problème : Problèmes liés à l'utilisation d'un IDP externe

Échec de la connexion

Rediriger URI

La connexion peut échouer si, par exemple, l'URI de redirection est erroné. Pour plus d'informations, voir Ajouter des URI de redirection pour les clients Web on page 426.

Pas de revendications ou revendications non ajoutées aux rôles

Si les utilisateurs d'IDP externe n'ont pas de revendications définies pour eux qui peuvent être utilisées par le VMS XProtect ou si des revendications n'ont pas été ajoutées aux rôles dans le VMS XProtect, une connexion avec l'un des clients échouera même si l'utilisateur d'IDP externe a été authentifié avec succès par l'IDP externe.

Cependant, il est toujours possible pour les utilisateurs d'IDP externe d'accéder au VMS XProtect même si les utilisateurs d'IDP externe n'ont pas de revendication définie pour eux. Dans ce cas, l'administrateur du VMS XProtect doit ajouter manuellement les utilisateurs d'IDP externe à un ou plusieurs rôles après la connexion initiale des utilisateurs d'IDP externe.

L'option d'authentification n'est pas disponible dans la boîte de dialogue de connexion

Si vous saisissez une adresse d'ordinateur incorrecte dans la boîte de dialogue de connexion d'un client, ce dernier n'obtient pas de réponse à l'appel d'API. L'appel d'API est effectué au démarrage du client et à chaque fois que l'adresse est modifiée, et il demande quelles sont les options d'authentification prises en charge par l'installation du VMS XProtect.

Si le client n'obtient pas de réponse à l'appel d'API au démarrage du client, celui-ci reprend par défaut la liste des options d'authentification standard.

Les revendications ne peuvent pas être sélectionnées sur les rôles

Les revendications que vous souhaitez utiliser dans les rôles doivent être ajoutées à la configuration IDP avant de pouvoir être sélectionnées dans les rôles. Les revendications peuvent être ajoutées dans l'onglet **IDP externe** de la boîte de dialogue **Options** : Onglet IDP externe (options) on page 423. Si une revendication n'est pas ajoutée à la configuration IDP, vous ne pourrez pas la sélectionner dans les rôles.

Problème : échec de l'ajout d'utilisateurs Active Directory à des rôles

Il se peut qu'il ne soit pas possible d'ajouter des rôles à un utilisateur Windows Active Directory à partir d'un Management Client qui s'exécute sur un ordinateur différent de celui du serveur de gestion.

Cause

Cela peut se produire si le port 445 du serveur de gestion n'est pas ouvert au trafic entrant.

Solution

Ouvrez le port 445 sur le serveur de gestion XProtect pour les connexions entrantes à partir de tout poste de travail exécutant l'application XProtect Management Client.

Pour plus d'informations, voir Ports utilisés par le système on page 108.

Mise à niveau

Mise à niveau (explications)

Lorsque vous procédez à la mise à niveau, tous les composants actuellement installés dans l'ordinateur sont mis à jour. Il n'est pas possible de supprimer des composants installés lors d'une mise à niveau. Si vous souhaitez supprimer des composants installés, utilisez la fonctionnalité **Ajouter ou supprimer des programmes** de Windows avant ou après une mise à niveau. Lors d'une 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 votre pack de pilotes de périphériques.

La compatibilité rétrospective avec des serveurs d'enregistrement de versions de XProtect antérieures à la présente version 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 recommande que vous mettiez à niveau tous les serveurs d'enregistrement de votre système.

Lorsque vous mettez vos serveurs d'enregistrement à niveau, le système vous demande 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 établir la connexion avec les nouveaux pilotes de périphériques vidéo après avoir redémarré votre système. Cela peut être à cause des nombreuses vérifications internes sur les pilotes qui viennent tout juste d'être installés.

Si vous effectuez une mise à niveau à partir de la version 2017 R3 ou antérieure vers la version 2018 R1 ou ultérieure, et si votre système est équipé de caméras plus anciennes, vous devez télécharger manuellement le pack de pilotes de périphériques avec les anciens pilotes disponibles sur la page de téléchargement de notre site Web (https://www.milestonesys.com/download/). Pour voir si vous avez des caméras qui utilisent des pilotes dans le pack de pilotes de périphériques hérités, rendez-vous sur notre site Web à la page qui suit (https://www.milestonesys.com/support/software/device-packs/).

Si vous passez de la version 2018 R1 ou antérieure à la version 2018 R2 ou ultérieure, il est important auparavant de mettre à niveau tous les serveurs d'enregistrement de votre système à l'aide d'un patch de sécurité. Si vous changez de version sans le correctif de sécurité, les serveurs d'enregistrement ne répondront pas.

Vous trouverez les instructions d'installation du correctif de sécurité sur vos serveurs d'enregistrement, sur notre site Web https://supportcommunity.milestonesys.com/s/article/XProtect-VMS-NET-security-vulnerability-hotfixes-for-2016-R1-2018-R1/.

Si vous souhaitez chiffrer la connexion entre le serveur de gestion et les serveur d'enregistrement, tous les serveurs d'enregistrement doivent être mis à jour vers 2019 R2 ou une version plus récente.

Pour une vue d'ensemble de la séquence de mise à niveau recommandée, voir Mise à jour des meilleures pratiques on page 406

Conditions préalables de mise à niveau

- Préparez votre fichier de licence logicielle (voir Licences (explications) on page 127) (.lic) :
  - **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 licence logicielle. Vous pouvez utiliser le fichier de licence logicielle 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 logicielle. Au cours de l'installation du serveur de gestion, l'assistant vous demandera de préciser l'emplacement du fichier de licence logicielle

  Le système vérifie votre fichier de licence logicielle avant que vous puissiez poursuivre. Les périphériques matériels et autres périphériques déjà ajoutés nécessitant une licence passent en période d'évaluation. Si vous n'avez pas activé l'activation automatique des licences, (voir Activer l'activation automatique des licences on page 135), n'oubliez pas d'activer vos licences manuellement avant que n'expire la période d'évaluation. Si vous n'avez pas de fichier de licence logicielle, veuillez contacter votre revendeur XProtect.
- Assurez-vous d'avoir le logiciel de la **nouvelle version de votre produit** à disposition. Vous pouvez la télécharger depuis la page de téléchargement sur le site Web Milestone.

- Assurez-vous d'avoir sauvegardé la configuration du système (voir Sauvegarde et de la restauration de la configuration de votre système (explications) on page 354)

  Le serveur de gestion sauvegarde la configuration système dans une base de données SQL Server. La base de données SQL Server peut se situer dans une instance SQL Server sur la machine du serveur de gestion elle-même ou dans une instance SQL Server dans le réseau.

  Si vous utilisez une base de données SQL Server dans une instance SQL Server sur votre réseau, le serveur de gestion doit disposer d'autorisations d'administrateur sur l'instance SQL Server chaque fois que vous souhaitez créer, déplacer ou mettre la base de données SQL Server à niveau. Pour une utilisation et en entretien réguliers de la base de données SQL Server, le serveur de gestion nécessite uniquement d'être le propriétaire de la base de données.

- Si vous voulez activer le cryptage lors de l'installation, les certificats nécessaires doivent être installés et fiables sur les ordinateurs concernés. Pour plus d'informations, voir Communication sécurisée (explications) on page 158.

Lorsque vous êtes prêts à démarrer la mise à niveau, suivez les étapes de la procédure dans Mise à jour des meilleures pratiques on page 406.

Mettre à jour le VMS XProtect pour un fonctionnement conforme au mode FIPS 140-2

Depuis la version 2020 R3, le VMS XProtect est configuré pour s'exécuter en utilisant uniquement des instances d'algorithme certifiées conformes aux normes FIPS 140-2.

Pour de plus amples informations sur comment configurer votre XProtect VMS pour qu'il s'exécute conformément au mode FIPS 140-2, voir la section de conformité aux normes FIPS 140-2 dans le guide de durcissement.

> ⚠ Pour les systèmes conformes aux normes FIPS 140-2 comportant des exportations et des bases de données multimédias archivées à partir des versions de XProtect VMS antérieures à 2017 R1 qui sont cryptées avec un cryptage non conforme aux normes FIPS, il est nécessaire d'archiver les données dans un emplacement auquel il est possible d'accéder après l'activation du mode FIPS.

Les étapes ci-dessous décrivent les prérequis nécessaires pour configurer le fonctionnement du VMS XProtect conforme au mode FIPS 140-2 :

1. Désactivez la politique de sécurité Windows FIPS sur tous les ordinateurs qui font partie du VMS, y compris l'ordinateur qui héberge SQL Server.

   Lorsque vous effectuez la mise à jour, vous ne pouvez pas installer le VMS XProtect si le mode FIPS est activé sur le système d'exploitation Windows.

2. Assurez-vous que les intégrations autonomes tierces peuvent s'exécuter dans un système d'exploitation Windows où est activé le mode FIPS.

   Une intégration autonome qui ne s'exécute pas conformément aux normes FIPS 140-2, ne pourra pas s'exécuter une fois le système d'opération Windows configuré pour fonctionner en mode FIPS.

   Pour y pallier :

   - Répertorier tous vos intégrations autonomes du VMS XProtect
   - Contactez le fournisseurs desdites intégrations et demandez-lui si elle sont conformes au mode FIPS 140-2
   - Déployez les intégrations autonomes conformes aux normes FIPS 140-2

3. Assurez-vous que les pilotes et donc leur communication avec les périphériques, sont conformes aux normes FIPS 140-2.

   Le VMS XProtect est garanti et peut assurer le respect du mode FIPS 140-2 de l'opération si les critères suivants sont respectés :

   - Les périphérique utilisent uniquement des pilotes conforme pour se connecter au VMS XProtect

     Voir la section de conformité aux normes FIPS 140-2 dans le guide de durcissement pour plus d'information sur les pilotes qui peuvent assurer et appliquer la conformité.

   - Les périphériques utilisent des packs de pilotes de périphériques version 11.1 ou ultérieures

     Les pilotes des packs de pilotes de périphériques hértités ne peuvent pas garantir une connexion conforme aux normes FIPS 140-2.

   - Les périphériques se connectent via HTTPS et sur le protocole Secure Real-Time Transport Protocol (SRTP) ou le protocole Real Time Streaming Protocol (RTSP) via HTTPS pour le flux vidéo

     > Les modules du pilote ne peuvent pas garantir le respect des normes FIPS 140-2 d'une connexion HTTP. La connexion peut être conforme, mais rien ne garantit sa conformité.

   - L'ordinateur exécutant le serveur d'enregistrement exécute Windows OS avec le mode FIPS activé

4. Assurez-vous que les données des bases de données multimédia sont cryptées avec un cryptage conforme aux normes FIPS 140-2.

   Pour ce faire, exécutez l'outil de mise à niveau de la base de données médias. Pour de plus amples informations sur comment configurer votre XProtect VMS pour qu'il s'exécute conformément au mode FIPS 140-2, voir la section de conformité aux normes FIPS 140-2 dans le guide de durcissement.

5. Avant d'activer le mode FIPS sur le système d'exploitation Windows et après avoir configuré votre système de VMS XProtect et vous être assuré que tous les composants et les périphériques peuvent s'exécuter dans un environnement conforme aux normes FIPS, mettez à jour vos mots de passe logiciels existants sur le XProtect Management Client.

   Pour ce faire, dans le/la Management Client, à partir du serveur d'enregistrement sélectionné dans le nœud des **serveurs d'enregistrement**, faites un clic droit et sélectionnez **Ajouter matériel**. Suivez les indications de l'assistant **Ajouter un matériel**. Cela mettra à jour tous les identifiants actuels et les cryptera conformément aux normes FIPS.

Vous pouvez activer le mode FIPS uniquement après avoir mis à jour l'intégralité du VMS, y compris tous les clients.

Mise à jour des meilleures pratiques

En lire plus sur les critères de mise à jour (voir Conditions préalables de mise à niveau on page 403) dont la restauration de la base de données SQL Server avant de démarrer la mise à niveau actuelle.

Les pilotes de périphériques sont désormais répartis en deux packs de pilotes de périphériques : le pack de pilotes de périphériques régulier équipé des pilotes plus récents et un pack de pilotes de périphériques hérités doté de pilotes plus anciens. Le pack de pilotes de périphériques régulier s'installe toujours automatiquement lors d'une mise à jour ou d'une mise à niveau. Si vous disposez de caméras plus anciennes qui sont équipées de pilotes de périphériques du pack de pilotes de périphériques hérités, et si ce dernier n'est pas encore installé, le système n'installera pas automatiquement le pack de pilotes de périphériques hérités.

Si votre système est équipé de caméras plus anciennes, Milestone vous recommande de vérifier sur cette page si ces dernières utilisent des pilotes de pack de pilotes de périphériques hérités (https://www.milestonesys.com/support/software/device-packs/). Pour vérifier si le pack hérité est déjà installé sur votre système, cherchez dans les dossiers système de XProtect. Si vous devez télécharger le pack de pilotes de périphériques hérités, accédez à la page de téléchargement (https://www.milestonesys.com/download/).

Si votre système est un système **Ordinateur unique**, vous pouvez installer le nouveau programme sur l'installation existante.

Dans un système Milestone Interconnect ou Milestone Federated Architecture, vous devez commencer en mettant à jour le site central, puis les sites à distance.

Dans un système distribué, exécutez la mise à jour dans cette ordre :

1. Mettez à niveau le serveur de gestion avec l'option **Personnaliser** dans le programme d'installation (voir Installer votre système - option personnalisée on page 166).
    1. Sur la page de l'assistant où vous choisissez les composants, tous les composants des serveurs de gestion sont présélectionnés.
    2. Spécifiez SQL Server et la base de données. Choisissez si vous souhaitez conserver la base de données SQL Server que vous utilisez et conserver les données existantes dans la base de données.

    > Lorsque vous démarrez l'installation, vous perdez la fonctionnalité du serveur d'enregistrement de basculement (voir Serveur d'enregistrement de basculement (explications) on page 42).

    > Si vous activez le chiffrement sur le serveur de gestion, les serveurs d'enregistrement sont hors ligne jsuqu'à ce qu'ils soient mis à niveau et que vous ayez activé le chiffrement sur le serveur de gestion (voir Communication sécurisée (explications) on page 158).

2. Mettez à jour serveurs d'enregistrement de basculement. Depuis votre page Web de téléchargement du serveur de gestion (contrôlé par Download Manager), installez Recording Server.

    > Si vous voulez activer le cryptage sur des serveurs d'enregistrement de basculement, et que vous désirez conserver la fonctionnalité de redondance, mettez à jour le serveur d'enregistrement de basculement sans cryptage et activez-le après avoir mis à jour les serveurs d'enregistrement.

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

3. Si vous voulez activer le cryptage depuis les serveurs d'enregistrement ou les serveurs d'enregistrement de basculement vers les clients, et qu'il est important que les clients puissent continuer à récolter des données lors de la mise à jour, mettez à jour tous les clients et services qui recueillent des flux de streaming depuis les serveurs d'enregistrement avant de mettre à jour les serveurs d'enregistrement. Ces clients et services sont :
    - XProtect Smart Client
    - Management Client
    - Management Server
    - Serveur XProtect Mobile
    - XProtect Event Server

- DLNA Server Manager
- Milestone Open Network Bridge
- Les sites collectant des flux de donnée depuis le serveur d'enregistrement par le biais de Milestone Interconnect
- Des intégrations MIP SDK tierces

4. Mettre à niveau les serveurs d'enregistrement. Vous pouvez installer des serveurs d'enregistrement en utilisant l'assistant d'installation (voir Installer le serveur d'enregistrement via Download Manager on page 175) ou via une installation silencieuse (voir Installation silencieuse d'un serveur d'enregistrement on page 188). L'avantage d'une installation silencieuse est qu'elle peut être effectuée à distance.

   > ⚠ Si vous activez le cryptage et que le certificat de l'authentification du serveur sélectionné n'est pas fiable sur tous les ordinateurs l'exécutant, ils seront déconnectés. Pour plus d'informations, voir Communication sécurisée (explications) on page 158.

Continuez ces étapes pour les autres sites de votre système.

Détails de l’interface utilisateur

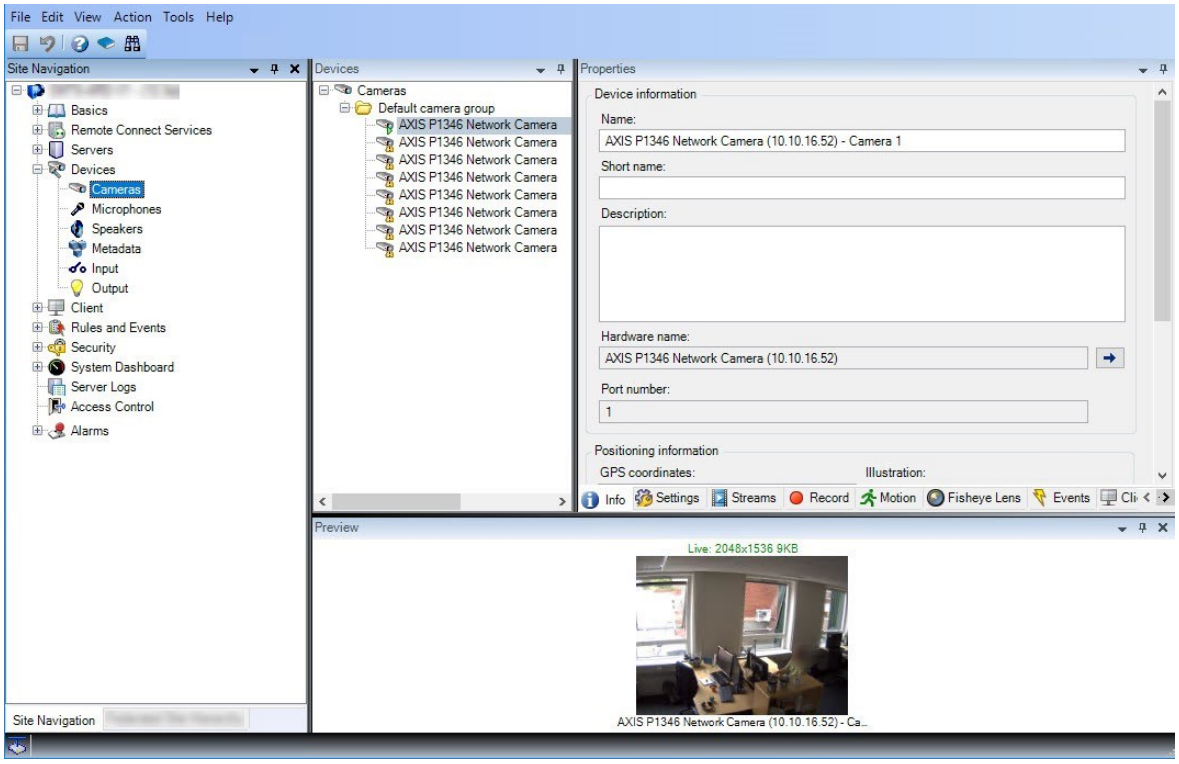
Fenêtres et volets principaux

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

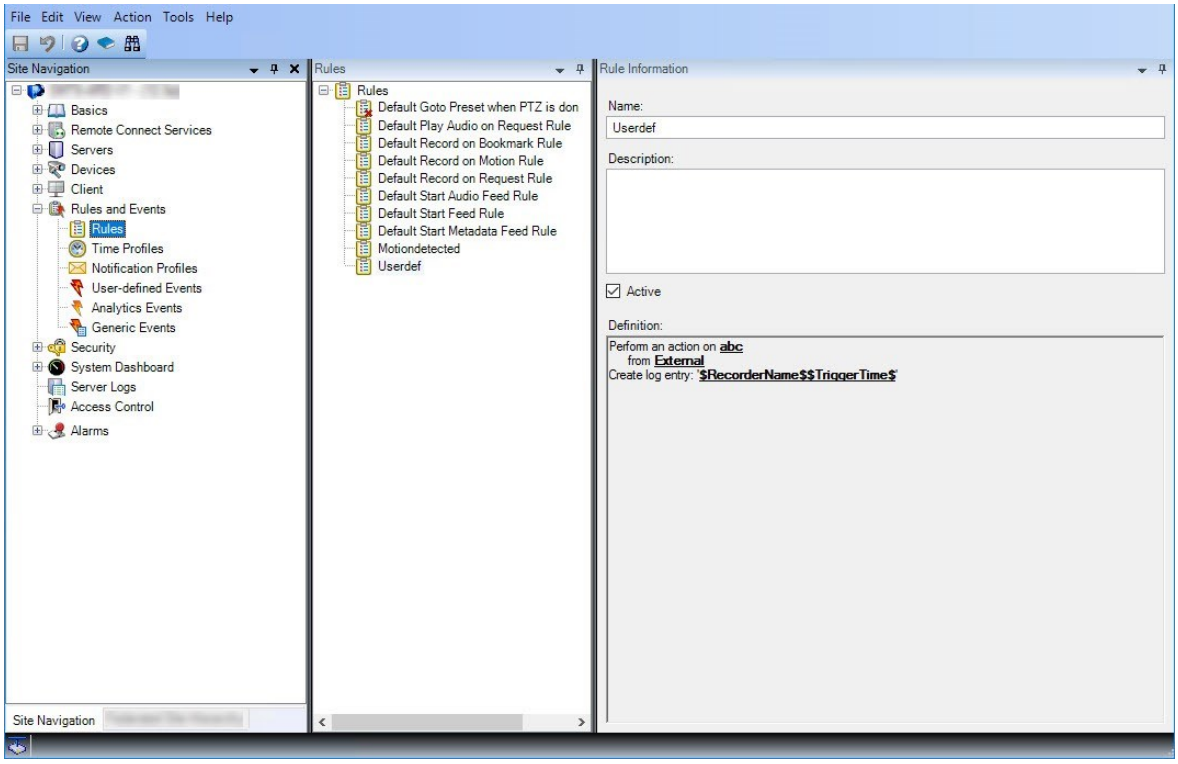
- Configuration système
- Tâche
- Fonctions disponibles

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

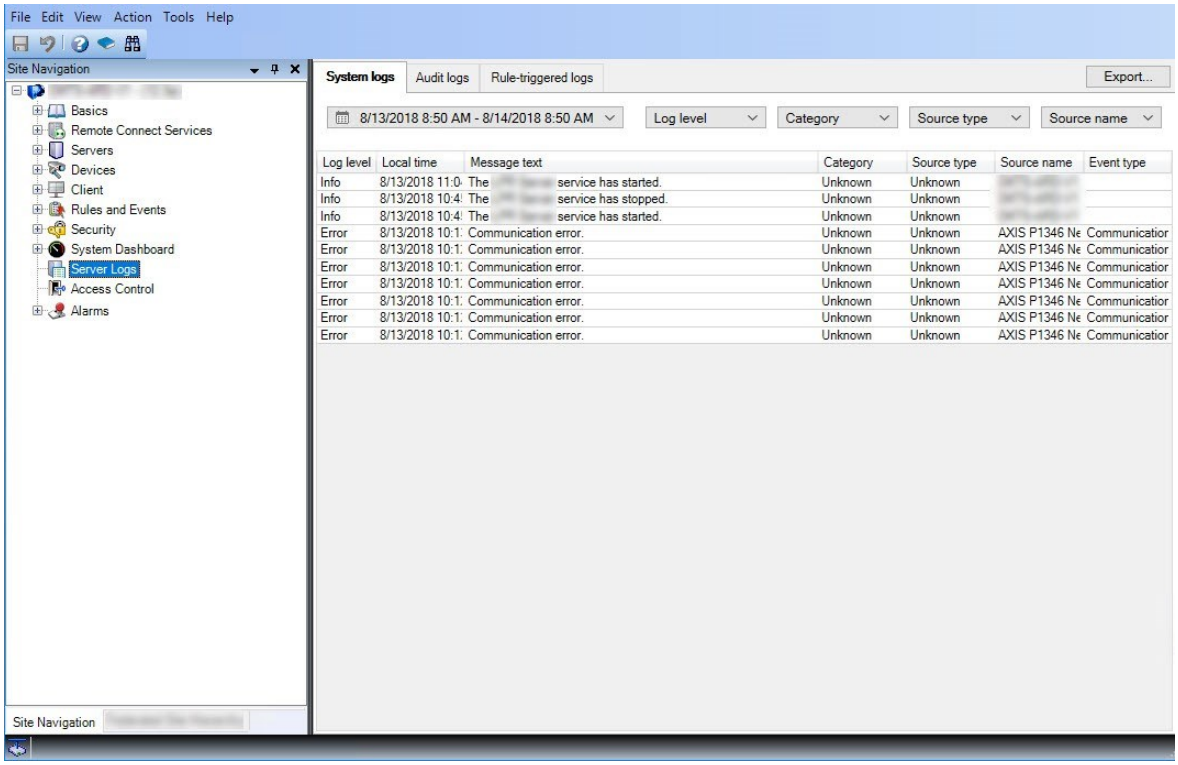
- Lorsque vous travaillez avec des serveurs d’enregistrement et des périphériques :



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

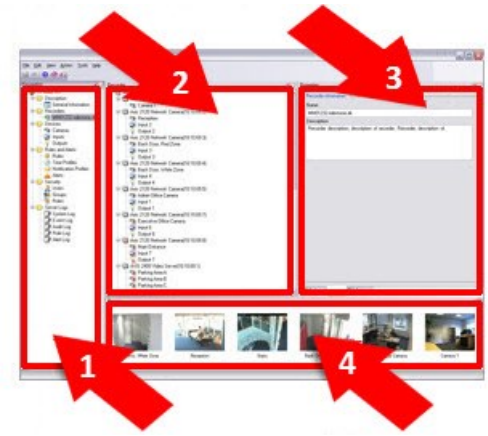


- Lorsque vous affichez des journaux :



Mise en page 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. Panneau Propriétés
4. Volet de prévisualisation

Volet Navigation du 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.

Dans le panneau **Navigation du site**, vous pouvez configurer et gérer votre système pour qu'il corresponde à vos besoins. Si votre système n'est pas un système mono-site, mais qu'il comprend des sites fédérés, vous pourrez gérer ces sites sur le panneau **Hiérarchie des sites fédérés**.

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

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.

Panneau Propriétés

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

Volet de prévisualisation

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.

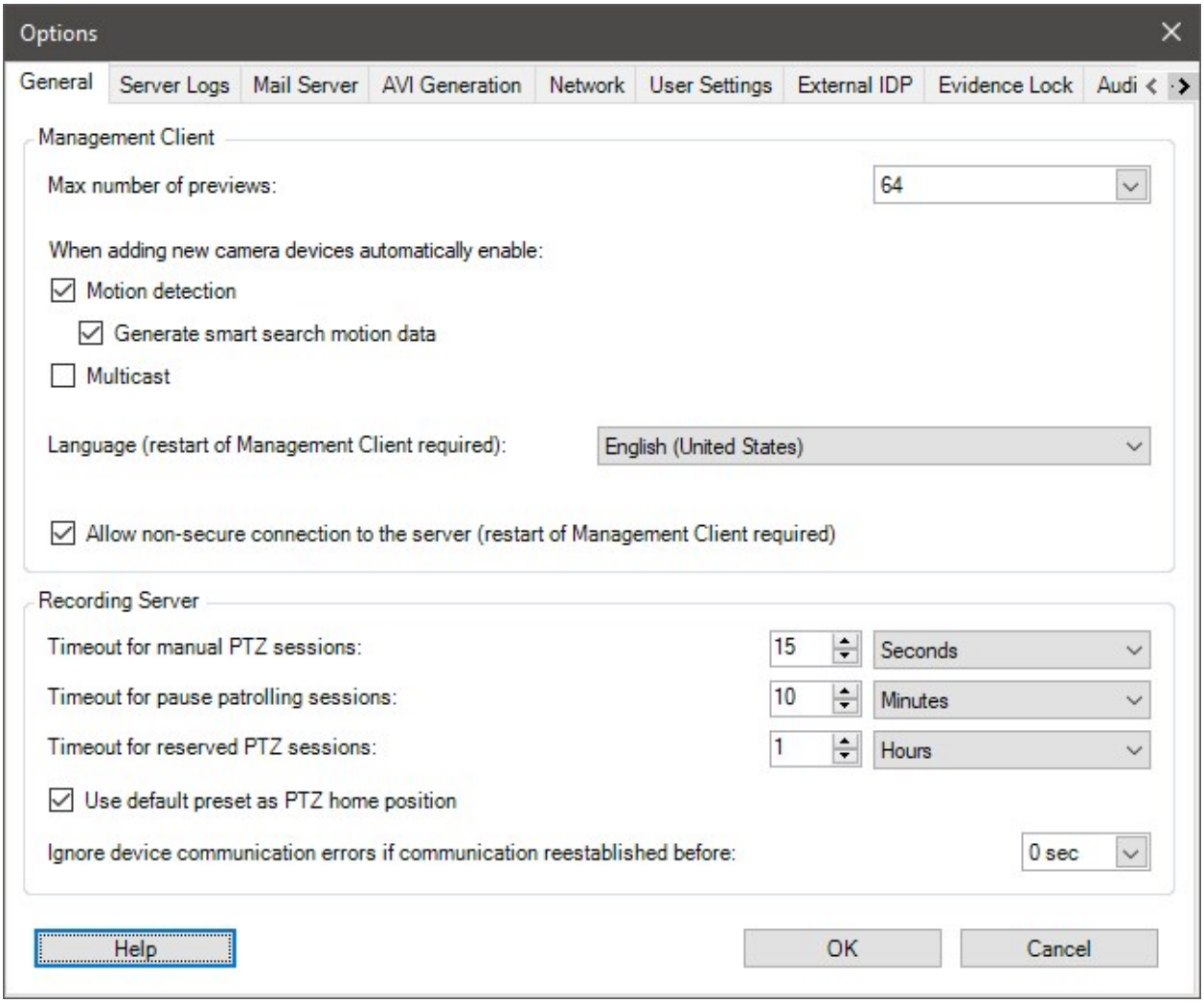
La performance peut être affectée par le volet **Aperçu** lorsque celui-ci affiche des images d'aperçu provenant de plusieurs caméras avec un grand nombre d'images par seconde. Pour contrôler le nombre d'images d'aperçu et leur nombre d'images par seconde, sélectionnez **Options** > **Général** dans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

Paramètres du système (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. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Pour accéder à la boîte de dialogue, sélectionnez **Outils** > **Options**.



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 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. Une grande quantité d’images miniatures combinée à une fluidité d’image élevée peut ralentir le système.
Lors de l’ajout de nouveaux périphériques de type caméra, activer automatiquement : Détection des mouvements	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 : Produire les données de mouvement pour la recherche avancée	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 mouvement pour la recherche avancée sur les nouvelles

Nom	Description
	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.
Autorise une connexion non-sécurisée au serveur	Sélectionnez la case à cocher pour autoriser une connexion non-sécurisée au serveur avec le protocole HTTP. (Aucun utilisateur n'est invité à autoriser une connexion non-sécurisée au serveur). Redémarrer le Management Client pour utiliser ce paramètre.

Serveur d’enregistrement

Nom	Description
Période d’inactivité pour les sessions PTZ manuelles	Les utilisateurs clients disposant des autorisations utilisateur 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.
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.
Utiliser les préréglages par défaut comme position de base de PTZ	Cochez cette case pour utiliser la position prédéfinie par défaut au lieu de la position de base des caméras PTZ lors de l’activation du bouton **Accueil** dans un client. Une position prédéfinie par défaut doit être définie pour la caméra. Si une position prédéfinie par défaut n’est pas définie, rien ne se passera lorsque le bouton **Accueil** est activé dans un client. Par défaut, la case à cocher est décochée. Pour assigner une position prédéfinie par défaut, voir Assigner une position prédéfinie de caméra par défaut on page 267

Nom	Description
Ignorer les erreurs de communication avec le périphérique si la communication est rétablie avant	Le système note toutes les erreurs de communication sur le matériel et les périphériques, mais vous sélectionnez ici combien de temps une erreur de communication doit exister avant que le moteur des règles 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.

Pour plus d'informations, voir Identifier l'activité des utilisateurs, les événements, les actions et les erreurs.

Nom	Description
Journaux	Sélectionnez le type de journal que vous souhaitez configurer : • Journaux système • Journaux d'audit • Journaux déclenchés par les règles
Paramètres	Désactivez ou activez les journaux et spécifiez la durée de rétention. Autorisez la version 2018 R2 et les composants antérieurs à écrire dans les journaux. Pour plus d'informations, voir Autoriser la version 2018 R2 et les composants antérieurs à écrire dans les journaux. 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)

Nom	Description
	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, ainsi que 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 sortant de votre système.
Voir Profils de notification (explications) pour de plus amples informations.

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 : **sender@organization.org**.
Adresse du serveur de messagerie	Saisissez l'adresse du serveur de messagerie SMTP procédant à l'envoi des notifications par e-mail. Exemple : **mailserver.organization.org**.
Port du serveur de messagerie	Le port TCP utilisé pour la connexion au serveur de messagerie. Le port par défaut est 25 pour les connexions non cryptées. Les connexions cryptées utilisent généralement le port 465 ou 587.
Crypter la connexion au serveur	Si vous souhaitez sécuriser la communication entre le serveur de gestion et le serveur de messagerie SMTP, sélectionnez cette case à cocher.

Nom	Description
	La connexion est sécurisée grâce à la commande du protocole de messagerie STARTTLS. Dans ce mode, la session commence sur une connexion non-chiffrée, puis une commande STARTTLS est fournie par le serveur de messagerie SMTP au serveur de gestion pour basculer vers une communication sécurisée qui utilise SSL.
Connexion au serveur requise	Si activée, vous devez indiquer 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.

Voir également Déclencher les notifications par e-mail depuis les règles.

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** 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

Nom	Description
	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. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

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.

Nom	Description
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 de signet par défaut, voir Règles (noeud Règles et événements). • La période de pré-enregistrement pour chaque caméra, voir Gérer le pré-enregistrement.

Pour spécifier les autorisations de signet d'un rôle, consultez Onglet Périphériques (rôles) on page 592.

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 IDP externe (options)

Dans l'onglet **IDP externe** de Management Client, vous pouvez ajouter et configurer un IDP externe et enregistrer des revendications à partir de celui-ci.

Nom	Description
Activé	L'IDP externe est activé par défaut.
Nom	Le nom de l'IDP externe. Le nom apparaît dans le champ **Authentification** de la fenêtre de connexion de votre client.
Autorité d'authentification	Le URL de l'IDP externe.
Ajouter	Ajoutez et configurez un IDP externe. Lorsque vous sélectionnez **Ajouter**, la boîte de dialogue **IDP externe** s'ouvre et vous pouvez saisir les informations de la configuration. Voir **Configurer un IDP externe** sous le tableau.

Nom	Description
Modifier	Modifiez la configuration de l'IDP externe.
Supprimer	Supprimez la configuration de l'IDP externe. Si vous supprimez une configuration d'IDP externe, les utilisateurs qui seront authentifiés par le biais de cet IDP externe ne pourront pas se connecter au VMS XProtect. Si vous ajoutez l'IDP externe à nouveau, les nouveaux utilisateurs seront créés lors de la connexion car l'ID de l'IDP externe aura changé.

Configurer un IDP externe

- Pour ajouter un IDP externe, sélectionnez **Ajouter** dans la section **IDP externe** et saisissez les informations dans le tableau ci-dessous. Vous ne pouvez ajouter qu'un seul IDP externe :

Nom	Description
Nom	Le nom de l'IDP externe que vous saisissez ici apparaît dans le champ **Authentification** dans le journal de la fenêtre de votre client.
ID client et **Clé secrète client**	Doit être obtenu auprès de l'IDP externe. L'ID client et le secret client sont nécessaires pour communiquer en toute sécurité avec l'IDP externe.
Chemin de rappel	Partie d'une URL pour que le flux de redirection d'authentification connecte les utilisateurs. Le flux d'ouverture de session de l'utilisateur est initié dans le VMS XProtect. Un navigateur est lancé avec une page de connexion qui est hébergée par l'IDP externe. Lorsque le processus d'authentification est terminé, le chemin de rappel (adresse de connexion XProtect + /idp/ + chemin de rappel) est invoqué et l'utilisateur est redirigé vers le VMS XProtect. La valeur par défaut est « /signin-oidc ». Le format de redirection

Nom	Description
	Le chemin de rappel est construit par l'adresse de connexion saisie dans le client + /idp/ + le chemin de rappel configuré sur l'IDP externe. L'URI est spécifique au client, de sorte que les URI pour, par exemple, Smart Client et XProtect Web Client seront différents. L'adresse du serveur de gestion est l'adresse que vous entrez dans la boîte de dialogue de connexion dans Smart Client ou XProtect Management Client. Pour XProtect Web Client et XProtect Mobile, l'adresse de redirection est l'adresse saisie + port + /idp/ + chemin de rappel.
Demander la connexion	Indiquez à l'IDP externe si l'utilisateur doit rester connecté ou si une vérification de l'utilisateur est nécessaire. En fonction de l'IDP externe, la vérification peut inclure une vérification du mot de passe ou une connexion complète.
Demande à utiliser pour créer un nom d'utilisateur	Si vous le souhaitez, vous pouvez spécifier quelle revendication de l'IDP externe doit être utilisée pour générer un nom d'utilisateur unique pour l'utilisateur automatiquement configuré dans le VMS. Pour de plus amples informations sur les noms d'utilisateurs uniques créés par les revendications, consultez Noms d'utilisateurs uniques pour les utilisateurs d'IDP externes.
Étendues	Si vous le souhaitez, vous pouvez utiliser des étendues pour limiter le nombre de revendications provenant d'un IDP externe. Si vous savez que les revendications qui sont importantes pour votre VMS se trouvent dans une étendue spécifique, vous pouvez utiliser l'étendue pour limiter le nombre de revendications que vous pouvez obtenir à partir de l'IDP externe.

Enregistrer des demandes

Lorsque vous avez enregistré des revendications à partir de l'IDP externe, vous pouvez mapper les revendications aux rôles dans le VMS pour déterminer les privilèges utilisateur dans le VMS. Pour de plus amples informations, voir Mapper des revendications à partir d'un IDP externe.

- Pour enregistrer des revendications à partir d'un IDP externe, sélectionnez **Ajouter** dans la section **Revendications enregistrées** et saisissez les informations dans le tableau ci-dessous :

Nom	Description
IDP externe	Le nom de l'IDP externe.
Nom de la revendication	Nom de la revendication tel qu'il a été défini dans l'IDP externe. Dans ce champ, le nom de la revendication doit être saisi exactement comme il est défini dans l'IDP externe. Le nom de la revendication n'apparaît nulle part ailleurs dans le Management Client.
Nom d'affichage	Le nom d'affichage d'une demande. C'est le nom que vous verrez dans la configuration des rôles dans Management Client.
Respect casse	Indique si la valeur d'une demande est sensible à la casse. Exemples de valeurs qui sont généralement sensibles à la casse : - Représentations textuelles des ID comme un GUID : F951B1F0-2FED-48F7-88D3-49EB5999C923 or OadFgrDesdFesff= Exemples de valeurs qui ne sont généralement pas sensibles à la casse : - Adresses e-mail - Noms de rôles - Noms de groupes .
Ajouter, **Modifier**, **Supprimer**	Enregistrez et conservez les demandes. Si vous modifiez une revendication sur le site Web de l'IDP externe, une nouvelle connexion au client XProtect est requise par les utilisateurs. Supposons qu'un utilisateur, Bob, doive être opérateur. La revendication est alors ajoutée à Bob sur le site Web de l'IDP externe. Toutefois, si Bob est déjà connecté à XProtect, il doit effectuer une nouvelle connexion pour que la modification prenne effet.

Ajouter des URI de redirection pour les clients Web

L'URI de redirection est l'URI où l'utilisateur est redirigé après une connexion réussie. Les URI de redirection doivent correspondre parfaitement aux adresses des clients Web. Par exemple, vous ne pourrez pas vous connecter via un IDP externe si vous ouvrez XProtect Web Client à partir de **https://localhost:8082/index.html** et l'URI de redirection pour les clients Web que vous avez ajouté est **https://127.0.0.1:8082/index.html**.

Nom	Description
URI	L'URI de XProtect Web Client est au format **https://[mobile server]:[port]/index.html**. Les URI de redirection ne sont pas sensibles à la casse. Saisissez un URI de redirection pour chacune des adresses pouvant être utilisées pour accéder au serveur XProtect Mobile / XProtect Web Client. Par exemple, les URI de redirection peuvent être utilisés à la fois avec et sans les détails du domaine. • https://[nom du périphérique]:8082/index.html • https://[nom complet du périphérique, y compris le domaine]:8082/index.html • https://localhost:8082/index.html • https://127.0.0.1:8082/index.html • https://[IP du serveur]:8082/index.html • https://[IP publique du serveur XProtect Mobile]:[port public]/index.html • https://[DNS public pour le serveur XProtect Mobile]:[port public]/index.html
Ajouter, **Modifier**, **Supprimer**	Enregistrer et entretenir les URI de redirection. Lorsque vous supprimez des URI, vous devez conserver au moins un URI de redirection pour que le système fonctionne.

Onglet Customer dashboard (Tableau de bord client)

Dans l'onglet **Tableau de bord client**, vous pouvez activer ou désactiver 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. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

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
Profils de verrouillage 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 de verrouillage	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 spécifier les autorisations d'accès à la protection de preuves d'un rôle, consultez Onglet Périphériques (rôles) on page 592 pour les paramètres des rôles.

Onglet Messages audio (options)

L'onglet **Messages audio** vous permet de charger des fichiers contenant des messages audio utilisés pour la diffusion des messages, déclenchés par des règles.

Le nombre maximum de fichiers chargés s'élève à 50 et la taille maximale autorisée pour chaque fichier est égale à 1 Mo.

Nom	Description
Nom	Indique le nom du message. Vous saisissez le nom lorsque vous ajoutez un message.

Nom	Description
	Pour charger un message dans le système, cliquez sur **Ajouter**.
Description	Indique une description du message. Vous saisissez la description lorsque vous ajoutez un message. Vous pouvez utiliser le champ de description pour décrire le but ou le message proprement dit.
Ajouter	Permet de charger des messages audio dans le système. Les formats pris en charge sont les formats de fichier audio Windows standard : • .wav • .wma • .flac
Modifier	Permet de modifier le nom et la description ou de remplacer le fichier proprement dit.
Supprimer	Permet de supprimer le message audio de la liste.
Lire	Cliquez sur ce bouton pour écouter le message sur l'ordinateur qui exécute le Management Client.

Pour créer une règle qui déclenche la lecture des messages audio, voir Ajouter une règle.

Pour en savoir plus sur les actions en général que vous pouvez utiliser dans les règles, voir Actions et actions d'arrêt.

Onglet Paramètres de confidentialité

Dans l'onglet **Paramètres de confidentialité**, vous pouvez activer ou désactiver la collecte des données d'utilisation auprès

- des clients mobiles,
- des clients de bureau et des modules d'extension.

En autorisant la collecte des données d'utilisation, vous consentez à ce que Milestone Systems utilise la technologie de Google comme fournisseur tiers avec lequel le traitement des données aux États-Unis ne peut être exclus. Pour plus d'informations sur la protection des données et la collecte des données d'utilisation, voir le Guide de confidentialité du RGPD.

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 fonctionnalité.

Nom	Description
Afficher le volet des propriétés de développement	Si elles sont sélectionnées, les informations de développeur supplémentaires apparaissent pour **Contrôle d'accès** > **Paramètres généraux**. Ce paramètre est uniquement destiné aux développeurs d'intégrations de systèmes de contrôle d'accès.

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.
Port	Indiquez le port utilisé par cette fonction. Le port par défaut est 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.

Nom	Description
Toutes les adresses du réseau ou **Adresses réseau spécifiées**	Indiquez si l'autorisation porte sur les événements de toutes les adresses IP ou/et noms d'hôtes ou seulement sur les événements des adresses IP ou/et noms d'hôte spécifiés dans la **liste des adresses** (voir ci-dessous).
Liste des adresses	Saisissez une liste des adresses IP ou noms d'hôte de confiance. La liste filtre les données entrantes de sorte que seuls les événements de certaines adresses IP ou noms d'hôtes soient autorisés. Vous pouvez utiliser les deux formats d'adresse pour le système de nom de domaine (DNS), IPv4 et IPv6. Vous pouvez ajouter des adresses à votre liste en entrant manuellement chaque adresse IP ou nom d'hôte, ou en important une liste d'adresses externe. • **Saisie manuelle** : Saisissez l'adresse IP ou 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 un fichier .txt et chaque adresse IP ou nom d'hôte doit être sur une ligne séparée

Onglet Alarmes et événements (Options)

Dans l'onglet **Alarmes et événements**, vous pouvez spécifier les paramètres des alarmes, des événements et des journaux. Concernant ces paramètres, voir également Taille limite de la base de données on page 143.

Nom	Description
Désactiver les alarmes pendant	Indiquez le nombre de jours pour le stockage des alarmes avec l'état **Fermé** dans la base de données. Si vous définissez la valeur sur **0**, l'alarme est supprimée après avoir été fermée.

Nom	Description
	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 toutes les autres alarmes pendant	Indiquez le nombre de jour permettant de stocker des alarmes avec l'état **Nouveau**, **En cours** ou **En attente**. Si vous définissez la valeur sur 0, l'alarme s'affiche dans le système, mais elle ne sera pas mémorisée. 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 la journalisation détaillée	Pour conserver un journal plus détaillé pour la communication du serveur d'événements, cochez la case. Il sera stocké pendant le nombre de jours indiqués dans le champ **Conserver les journaux pendant**.
Types d'événement	Indiquez le nombre de jours pour le stockage des événements dans la base de

Nom	Description
	données. Il existe deux possibilités pour le faire : • Vous pouvez spécifier la durée de conservation d'un groupe d'événements entier. Les types d'événements comportant la valeur **Suivre le groupe** peuvent hériter de la valeur du groupe d'événements • Même si vous définissez une valeur pour un groupe d'événements, vous pouvez spécifier la durée de conservation des différents types d'événements.  Si la valeur est **0**, les événements seront pas enregistrés dans la base de données.  Les événements externes (événements définis par l'utilisateur, événements génériques et événements d'entrée) sont définis sur **0** par défaut ; par ailleurs, vous ne pouvez pas modifier cette valeur. Ces types d'événements se produisent de manière si fréquente que le fait de les stocker dans la base de données peut entraîner des problèmes au niveau de la performance.

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 de configurer les événements génériques réels, voir Événements génériques (explications).

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 :

Nom	Description
	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 désactivées. Cochez la case pour activer 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 @, #, +, ~, etc.
Sélecteur type IP	Types d’adresses IP à sélectionner : IPv4, IPv6 ou les deux.

Nom	Description
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>).
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 de tous les octets** : Produit un écho de 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.

Menus des composants

Menus Management Client

Menu Fichier

Vous pouvez enregistrer les modifications apportées à la configuration et quitter l'application. Vous pouvez également restaurer votre configuration, voir Sauvegarde et de la restauration de la configuration de votre système (explications) on page 354.

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.
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.

La période de pré-enregistrement pour chaque caméra, voir Gérer le pré-enregistrement.

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 Gérer les services enregistrés on page 385.
Rôles effectifs	Affichez tous les rôles d'un utilisateur ou groupe sélectionné.
Options	Ouvre la boîte de dialogue qui vous permet de définir et de modifier les paramètres généraux du système. Pour plus d'informations, voir Paramètres du système (boîte de dialogue Options) on page 414.

Menu Aide

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

Server Configurator (Utilitaire)

Propriétés de l'onglet Cryptage

Cet onglet vous permet d'indiquer les propriétés suivantes :

Dans l'environnement du cluster, vous devez configurer votre cluster et assurer qu'il est en cours d'exécution avant de créer des certificats pour tous les ordinateurs dans l'environnement du cluster. Une fois cela fait, vous pouvez installer les certificats et effectuer l'inscription via le Server Configurator pour tous les noeuds dans le cluster. Pour plus d'informations, voir le guide des certificats sur comment sécuriser votre installation de XProtect VMS.

Nom	Description	Tâche
Certificat du serveur	Sélectionnez le certificat à utiliser pour crypter une connexion bidirectionnelle entre le serveur de gestion, les collecteurs de données, le serveur de journaux et les serveurs d'enregistrement.	Activer le cryptage depuis et vers le serveur de gestion Activer le cryptage du serveur pour les serveurs d'enregistrement ou les serveurs distants
Serveur d'événements et extensions	Sélectionnez le certificat à utiliser pour chiffrer la connexion bilatérale entre le serveur d'événements et les composants qui communiquent avec le serveur d'événements , y compris le LPR Server.	Activer le chiffrement du serveur d'événements on page 328
Certificat de flux de multimédia	Sélectionnez le certificat à utiliser pour chiffrer la communication entre les serveurs d'enregistrement et tous les clients, serveurs et intégrations récoltant des flux de données depuis les serveurs d'enregistrement.	Activer le cryptage pour les clients et les serveurs
Certificat de flux de multimédia mobile	Sélectionnez le certificat à utiliser pour crypter la communication entre le serveur mobile et les clients mobiles et Web récupérant les flux de données depuis le serveur mobile.	Activer le cryptage sur le serveur mobile

Enregistrement des serveurs

Nom	Description	Tâche
Adresse du serveur de gestion	L'adresse du serveur de gestion inclut en général le nom d'hôte ou le nom du domaine qualifié complet de l'ordinateur. Par défaut, cette adresse est uniquement active sur un ordinateur dans le VMS XProtect où n'est pas installé le serveur de gestion.	Cliquer pour obtenir plus d'informations sur les conséquences du changement de l'adresse du serveur de gestion depuis un ordinateur où le serveur de gestion est installé :

Nom	Description	Tâche
	En règle générale, l'adresse du serveur de gestion ne doit pas être modifiée sur un ordinateur où est installé le serveur de gestion. Cependant, si, par exemple, vous utilisez le Server Configurator dans une configuration de basculement, vous devez modifier l'adresse depuis l'ordinateur du serveur de gestion. Vous pouvez effectuer cette action dans un environnement de cluster de basculement ou dans un autre scénario de configuration de basculement. • Pour activer le champ de l'**adresse du serveur de gestion** depuis un ordinateur où est installé le serveur de gestion, cliquez sur le symbole du crayon ( ). Si vous mettez à jour l'adresse du serveur de gestion, vous aurez besoin d'accéder à chacun des ordinateurs où sont installés des éléments et mettre à jour les informations de la nouvelle adresse du serveur de gestion.	Modifier le nom d'hôte sur l'ordinateur du serveur de gestion
Enregistrer	Enregistrer les serveurs qui s'exécutent sur l'ordinateur avec le serveur de gestion sélectionné.	Enregistrer un serveur d'enregistrement

Choix de la langue

Utilisez cet onglet pour sélectionnez la langue de Server Configurator. La configuration des langues de Server Configurator correspond à la celle de Management Client.

Nom	Description
Choisir la langue	Choisir la langue de l'interface utilisateur.

Pour éviter les conflits entre le cluster de basculement et VMS Server Configurator, mettez le cluster en pause avant de démarrer les tâches dans le Server Configurator. Le Server Configurator peut avoir besoin d'arrêter les services lorsqu'il applique les changements et que l'environnement du cluster de basculement peut interférer avec cette opération.

État des icônes de la barre des tâches

Les icônes de la barre des tâches dans le tableau affiche les différents états des services qui s'exécutent sur les serveurs dans le VMS XProtect. Les icônes sont disponibles sur les ordinateurs où sont installés des serveurs :

Management Server Manager icône de la barre des tâches	Recording Server Manager icône de la barre des tâches	Event Server Manager icône de la barre des tâches	Failover Recording Server Manager icône de la barre des tâches	Description
				**En cours** S'affiche lorsqu'un service du serveur est activé et a démarré. Si le service Failover Recording Server est en cours d'exécution, il peut prendre le relais si les serveurs d'enregistrement standards échouent.
				**Arrêté**

Management Server Manager icône de la barre des tâches	Recording Server Manager icône de la barre des tâches	Event Server Manager icône de la barre des tâches	Failover Recording Server Manager icône de la barre des tâches	Description
				S'affiche quand le service du serveur s'arrête. Si le service Failover Recording Server s'arrête, il ne peut prendre le relais si les serveurs d'enregistrement standards échouent.
				**Démarrage** S'affiche quand un service du serveur est en cours de démarrage. Dans des circonstances normales, l'icône de la barre des tâches passe peu après à **En cours**.
				**Arrêt en cours** S'affiche quand un service du serveur est en cours d'arrêt. Dans des circonstances normales, l'icône de la barre des tâches passe peu après à **Arrêté**.
				**Dans un état indéterminé**

Management Server Manager icône de la barre des tâches	Recording Server Manager icône de la barre des tâches	Event Server Manager icône de la barre des tâches	Failover Recording Server Manager icône de la barre des tâches	Description
				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 Serveur d'enregistrement ou Serveur d'enregistrement de basculement est en cours de fonctionnement, mais pas le service Management Server.

Démarrer et arrêter des services des icônes de la barre des tâches

Effectuez un clic droit sur les icônes dans la zone de notification pour ouvrir les icônes de la barre des tâches à partir desquelles vous pouvez démarrer et arrêter des services.

- Démarrer ou arrêter le service Management Server
- Démarrer ou arrêter le service Recording Server

Management Server Manager (icône de la barre des tâches)

Utilisez les éléments du menu dans l'icône de la barre des tâches Management Server Manager pour exécuter des tâches depuis le Management Server Manager.

Nom	Description
Démarrage Management Server et **Arrêt Management Server**	Cliquez sur l'élément du menu concerné pour démarrer ou arrêter le service Management Server. Si vous arrêtez le service Management Server, vous ne pourrez pas utiliser le Management Client. L'icône de la barre des tâches indique l'état du service. Pour plus d'informations sur les états des icônes de la barre des tâches, voir Icônes de la barre du gestionnaire du serveur (explications).
Afficher les messages d'état	Afficher une liste des messages d'état horodatés.
Modifier les paramètres du mot de passe de configuration du système	Assigner ou modifier un mot de passe de configuration du système. Vous pouvez également choisir de ne pas protéger par un mot de passe la configuration du système en supprimant tout mot de passe de configuration du système attribué. Modifier les paramètres du mot de passe de configuration système
Saisir le mot de passe de configuration du système	Saisissez un mot de passe. Cette option s'applique si, par exemple, le fichier qui contient les paramètres du mot de passe est supprimé ou corrompu. Pour plus d'informations, voir Saisir le mot de passe de configuration du système.
Configurer un serveur de gestion de basculement	Lancez l'assistant de configuration pour le serveur de gestion de basculement ou ouvrez la page **Gérer votre configuration** pour gérer votre configuration existante. Pour de plus amples informations sur le cluster de basculement, consultez XProtect Management Server Failover on page 56.
Server Configurator	Ouvrir le **Server Configurator** pour enregistrer les serveurs et gérer le cryptage. Pour plus d'informations sur la gestion du cryptage, voir Gérer le cryptage avec le Server Configurator.
Changer la licence	Dans l'ordinateur du serveur de gestion, modifier le code de la licence logicielle. Vous aurez besoin de saisir le nouveau code de la licence pour, par exemple, mettre à niveau votre système XProtect. Pour de plus amples informations, consultez Modifier le code de la licence logicielle.
Restaurer la configuration	Ouvrez la boîte de dialogue à partir de laquelle vous pouvez restaurer la configuration du système. Assurez-vous de lire les informations dans la boîte de

Nom	Description
	dialogue avant de cliquer sur **Restaurer**. Pour plus d'informations, voir Restauration d'une configuration système à partir d'une sauvegarde manuelle.
Sélectionner le fichier de sauvegarde partagé	Configurer un dossier de sauvegarde où stocker votre sauvegarde avant de sauvegarder toute configuration du système. Pour plus d'informations, voir Sélectionner un dossier de sauvegarde partagé.
Mettre à jour l'adresse SQL	Ouvrir l'assistant pour modifier l'adresse SQL Server. Dans le rare cas où un nom d'hôte est modifié, il est nécessaire d'effectuer lesdits changements sur l'adresse du SQL Server. Pour plus d'informations, voir Le changement du nom d'hôte peut déclencher un changement de l'adresse du serveur SQL.

Noeud Basiques

Informations sur les licences (noeud Basique)

Dans la fenêtre **Informations sur les licences**, vous pouvez suivre les licences qui partagent les mêmes fichiers de licence du logiciel sur ce site et tous les autres sites, faire un suivi de vos abonnements Milestone Care et décider comment activer vos licences.

Pour en savoir plus sur les différentes informations et fonctionnalités disponibles dans la fenêtre **Informations sur les licences**, voir Fenêtre Informations sur les licences on page 139.

Informations du site (noeud Basique)

Dans une grande configuration de Milestone Federated Architecture comportant beaucoup de sites enfants, il peut être facile de perdre la vue d'ensemble et difficile de trouver les informations de contact des administrateurs de chaque site enfant.

Vous pouvez donc ajouter des renseignements supplémentaires dans chaque site enfant. Ces renseignements sont alors disponibles pour les administrateurs dans le site central.

Il est possible d'ajouter les informations suivantes :

- Nom du site
- Adresse/emplacement
- Administrateur(s)
- Informations complémentaires

Noeud Services de connexion à distance

Connexion caméra Axis One-click (noeud Services de connexion à distance)

Voici les propriétés de la connexion à la caméra Axis One-Click.

Nom	Description
Mot de passe de la caméra	Saisir/modifier. Fourni avec votre caméra lors de l'achat. Pour de plus amples informations, consultez le manuel de votre caméra ou rendez-vous sur le site Web d'Axis https://www.axis.com/).
Utilisateur de la caméra	Voir les détails concernant le **Mot de passe caméra**.
Description	Saisissez/modifiez une description pour la caméra.
Adresse externe	Saisissez/modifiez l'adresse Web du serveur ST auquel est/sont connectée(s) la/les caméra(s).
Adresse interne	Saisissez/modifiez l'adresse Web du serveur ST auquel est connecté le serveur d'enregistrement.
Nom	Si besoin, modifiez le nom de l'élément.
Clé d'identification du propriétaire	Voir **Mot de passe caméra**.
Mots de passe (pour Dispatch Server)	Saisissez un mot de passe. Doit être identique à celui fourni par le fournisseur de votre système.
Mots de passe (pour serveur ST)	Saisissez un mot de passe. Doit être identique à celui saisi lors de la création du composant Axis One-Click Connection.
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

Nom	Description
	série est souvent, mais pas toujours, identique à l'adresse MAC.
Utiliser les identifiants de connexion	Cochez la case si vous avez décidé d'utiliser des identifiants de connexion 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 serveur ST)	Saisissez un nom d'utilisateur. Doit être identique à celui saisi lors de la création du **composant Axis One-Click Connection**.

Noeud Serveurs

Serveurs (noeud)

Cette section décrit comment installer et configurer les serveurs d'enregistrement et les serveurs d'enregistrement de basculement. Vous apprenez également comment ajouter un nouveau matériel au système et l'interconnecter à d'autres sites.

- Serveurs d'enregistrement (noeud Serveurs) on page 446
- Serveurs de basculement (noeud Serveurs) on page 461

Serveurs d'enregistrement (noeud Serveurs)

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

Les serveurs d'enregistrement sont des ordinateurs où vous avez installé le programme Recording Server, et où vous l'avez configuré pour communiquer avec le 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**.

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.

Fenêtre Paramètres du serveur d'enregistrement

Lorsque vous effectuez un clic droit sur l'icône Recording Server Manager de la barre d'état et que vous sélectionnez **Modifier les paramètres**, vous pouvez spécifier ce qui suit :

Nom	Description
Adresse	Adresse IP (exemple : 123.123.123.123) ou nom d'hôte (exemple : notreserveur) du serveur de gestion auquel le serveur d'enregistrement devrait être connecté. Cette information est nécessaire pour assurer la communication entre le serveur d'enregistrement et le serveur de gestion.
Port	Numéro de port à utiliser lors de la communication avec le serveur de gestion. Le port par défaut est 9000. Vous pouvez le modifier si nécessaire.
Port du serveur Web	Numéro de port à utiliser pour gérer les demandes du serveur Web, par exemple, pour gérer les commandes de contrôles des caméra PTZ et pour gérer les recherches et les demandes en direct depuis XProtect Smart Client. Le port par défaut est 7563. Vous pouvez le modifier si nécessaire.
Crypter les connexions du serveur de gestion au serveur d'enregistrement	Avant d'activer le cryptage et de sélectionner le certificat d'authentification du serveur dans la liste, assurez-vous d'activer en premier le cryptage sur le serveur de gestion et que le certificat du serveur de gestion est de confiance sur le serveur d'enregistrement. Pour plus d'informations, voir Communication sécurisée (explications) on page 158.
Crypter les connexions des clients et services transférant des données	Avant d'activer le cryptage et de sélectionner un certificat d'authentification du serveur de la liste, assurez-vous que le certificat est de confiance sur tous les ordinateurs exécutant les services qui collectent les flux de données depuis le serveur d'enregistrement. XProtect Smart Client et tous les services récupérant des flux de données pour le serveur d'enregistrement doivent être mis à jour à la version 2019 R1 ou une

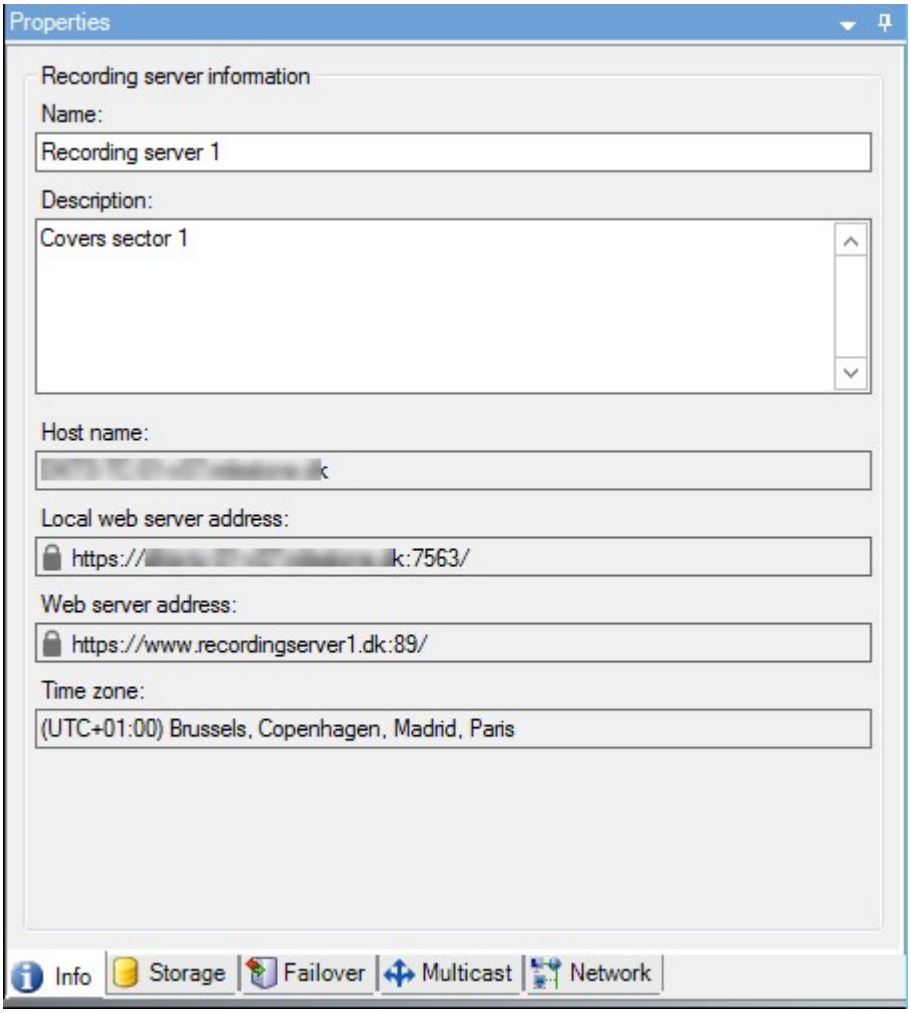
Nom	Description
	version plus récente. Certaines solutions tierces utilisant des versions de MIP SDK antérieures à 2019 R1 peuvent avoir besoin d'être mises à jour. Pour de plus amples informations, voir Communication sécurisée (explications) on page 158. Pour vérifier que votre serveur d'enregistrement utilise le cryptage, voir Voir le status du cryptage vers les clients on page 314.
Détails	Lire les informations de la Windows Certificate Store sur le certificat sélectionné.

Propriétés des serveurs d'enregistrement

Onglet Info (serveur d'enregistrement)

Dans l'onglet **Info**, vous pouvez vérifier ou éditer le nom et la description du serveur d'enregistrement.

Vous pouvez voir le nom d'hôte et les adresses. L'icône en forme de cadenas située devant l'adresse du serveur Web indique que la communication est cryptée entre les clients et les services récupérant les flux de données depuis ce serveur d'enregistrement.



Nom	Description
Nom	Vous pouvez choisir d’entrer un nom pour le serveur d’enregistrement. Le nom est utilisé partout où le périphérique apparaît dans une liste sur 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	Vous pouvez choisir d’entrer une description qui 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.

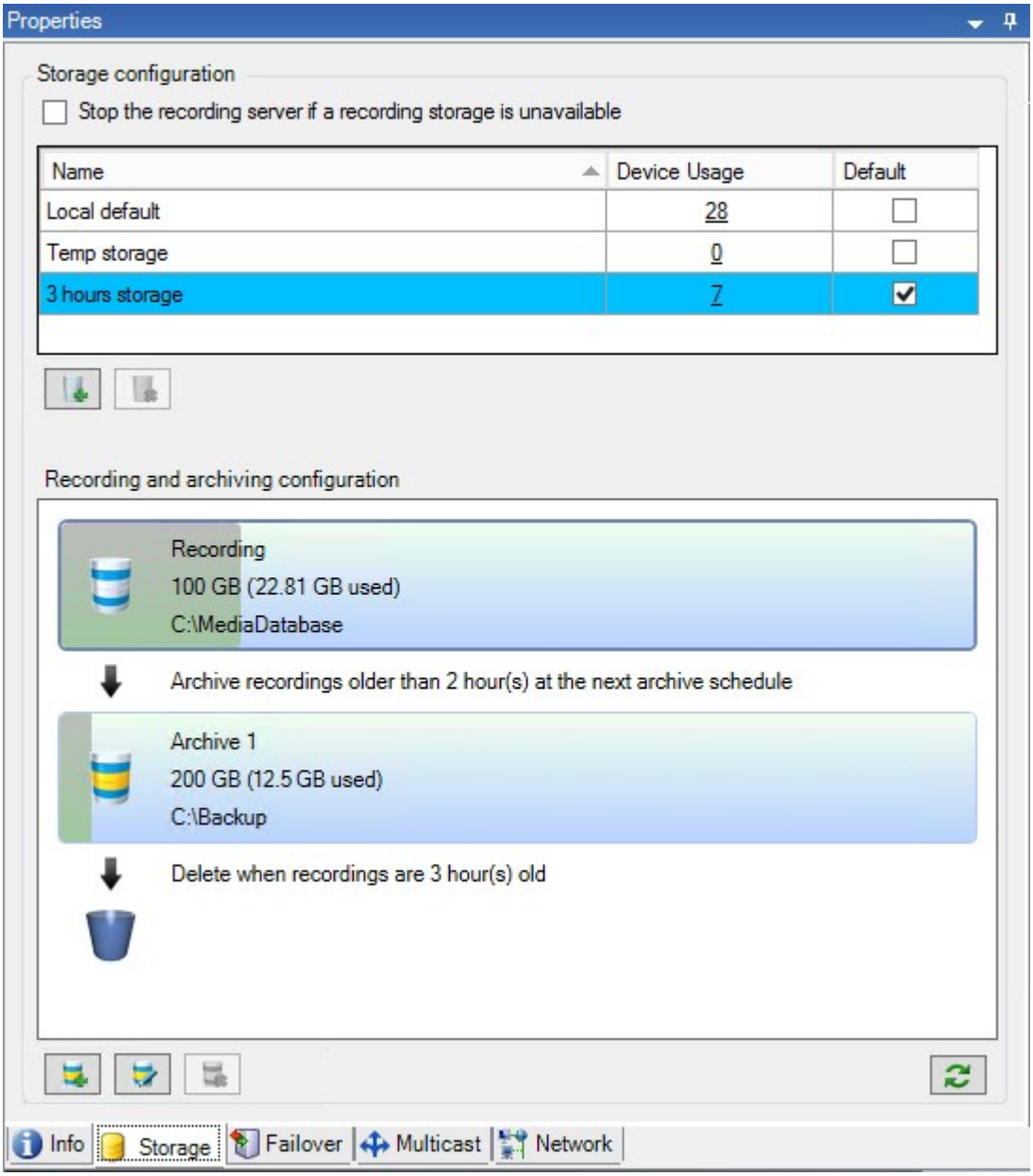
Nom	Description
Adresse locale du serveur Web	Affiche l'adresse locale du serveur Web du serveur d'enregistrement de basculement. Vous utilisez l'adresse locale, par exemple, pour gérer les commandes de contrôle des caméras PTZ, et pour gérer les recherches et les demandes en direct depuis XProtect Smart Client. L'adresse inclue le numéro de port utilisé pour la communication du serveur Web (habituellement, le port 7563). Si vous activez le cryptage des clients et serveurs récupérant les flux de données du serveur d'enregistrement, une icône représentant un cadenas apparaît, ainsi qu'une adresse affichant **https** au lieu de **http**.
Adresse du serveur Web	Affiche l'adresse publique du serveur Web du serveur d'enregistrement sur Internet. Si votre installation utilise un pare-feu ou du routeur NAT, entrez 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 serveur d'enregistrement de basculement. Vous spécifiez l'adresse publique et le numéro de port dans l'onglet **Réseau**. Si vous activez le cryptage des clients et serveurs récupérant les flux de données du serveur d'enregistrement, une icône représentant un cadenas apparaît, ainsi qu'une adresse affichant **https** au lieu de **http**.
Fuseau horaire	Affiche le fuseau horaire sur lequel se trouve le serveur d'enregistrement.

Onglet Stockage (serveur d'enregistrement)

Dans l'onglet **Stockage**, vous pouvez configurer, gérer et visualiser des emplacements de stockage pour un serveur d'enregistrement sélectionné.

Pour le stockage et l'archivage des enregistrements, la barre horizontale affiche la quantité d'espace libre. Vous pouvez spécifier le comportement du serveur d'enregistrement au cas où le stockage des enregistrements est indisponible. Cela est particulièrement utile si votre système comprend des serveurs de basculement.

Si vous utilisez le **Verrouillage des preuves**, une ligne rouge s'affiche pour indiquer l'espace utilisé pour la séquence de verrouillage des preuves.



Propriétés des paramètres de stockage et d'enregistrement

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Dans la boîte de dialogue **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 : `\\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. ⚠ 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

Nom	Description
	lecture. Le système utilise l'algorithme SHA-2 pour la signature numérique.
Cryptage	Sélectionnez le niveau de cryptage des enregistrements : • Aucun • Faible (utilisation du processeur moindre) • Fort (utilisation du processeur supérieure) Le système utilise l'algorithme AES-256 pour le cryptage. Si vous sélectionnez **Faible**, une partie de l'enregistrement sera cryptée. Si vous sélectionnez **Fort**, tout l'enregistrement sera crypté. Si vous choisissez d'activer le cryptage, vous devez également spécifier un mot de passe ci-dessous.
Mot de passe	Saisissez un mot de passe pour les utilisateurs autorisés à consulter les données cryptées. Milestone vous recommande d'utiliser des mots de passe forts. Les mots de passe forts ne contiennent pas de mots qui peuvent se trouver dans un dictionnaire ou qui font partie du nom de l'utilisateur. Ils comportent huit ou plusieurs caractères alphanumériques, des majuscules ou minuscules et des caractères spéciaux.

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

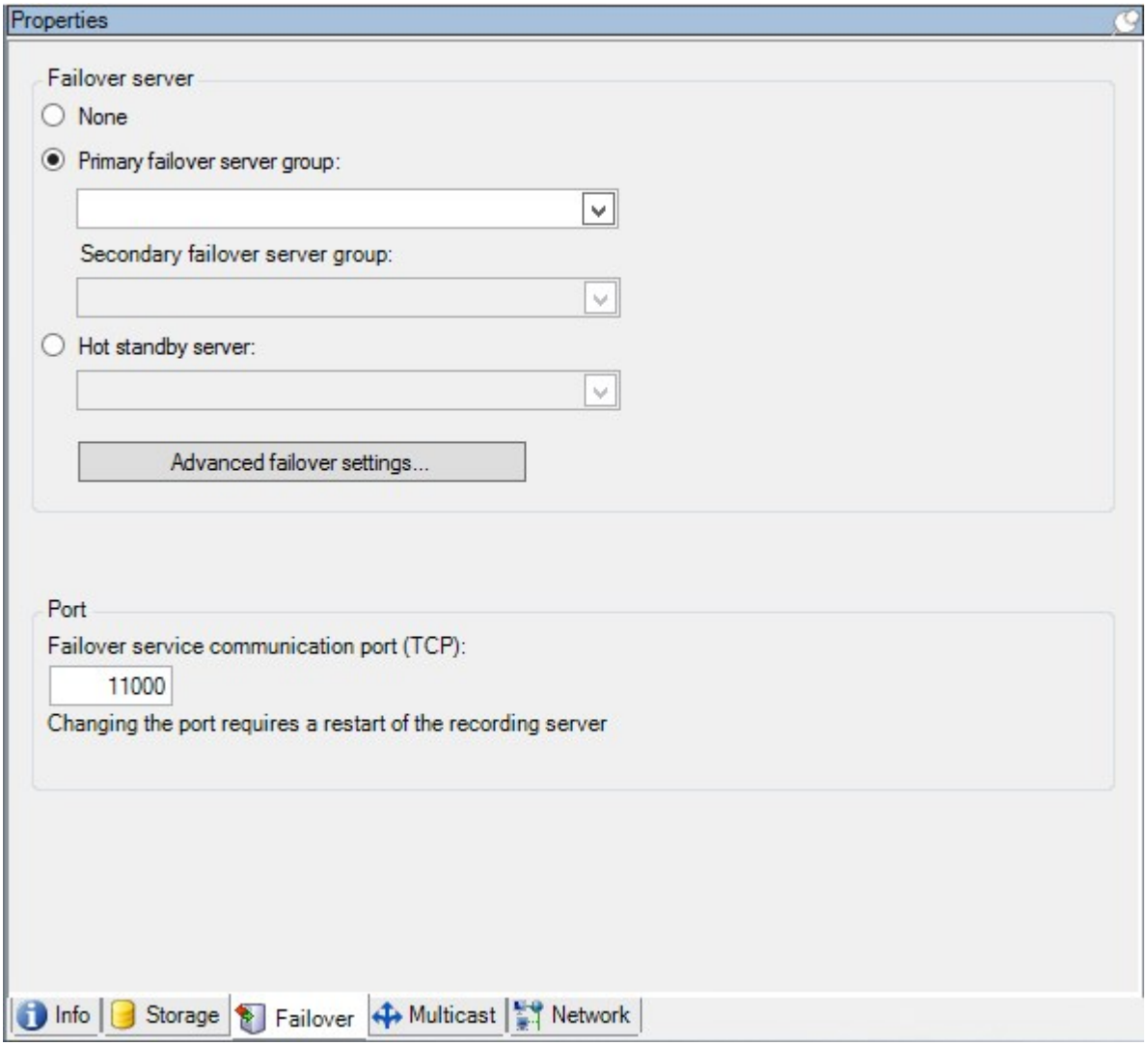
Nom	Description
	pas nécessairement être situé sur l'ordinateur du serveur d'enregistrement. Si le répertoire n'existe pas, vous pouvez le créer. Les disques réseau doivent être indiqués à l'aide du format UNC (Universal Naming Convention), par exemple : `\\server\volume\directory\« »`.
Durée de rétention	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. ⚠ 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).
Réduire la	Pour réduire le FPS lors de l'archivage, sélectionnez la case à cocher **Réduire la fluidité**

Nom	Description
fluidité d'image	**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 Basculement (serveur d'enregistrement)

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Si votre institution utilise des serveurs d'enregistrement de basculement, utilisez l'onglet **Basculement** pour affecter des serveurs de basculement aux serveurs d'enregistrement, voir Propriétés de l'onglet Basculement.



Pour plus de détails sur les serveurs d’enregistrement de basculement, l’installation et les paramètres, les groupes de basculement et leurs paramètres, voir Serveur d’enregistrement de basculement (explications) on page 42.

Propriétés de l’onglet Basculement

Nom	Description
Aucun	Sélectionnez une configuration sans serveur d’enregistrement de basculement.

Nom	Description
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.
Serveur de basculement à affectation unique	Sélectionnez une configuration à affectation unique dotée d'un serveur d'enregistrement dédié en tant que serveur de basculement à affectation unique.
Paramètres de basculement avancés	Ouvre la fenêtre **Paramètres de basculement avancés** : • **Soutien complet** : Active une assistance de basculement complet pour le périphérique • **Uniquement en direct** : Active une assistance de basculement complet pour les flux en direct sur le périphérique • **Désactivé** : Désactive l'assistance de basculement pour le périphérique
Port de communication du 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 basculement. 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)

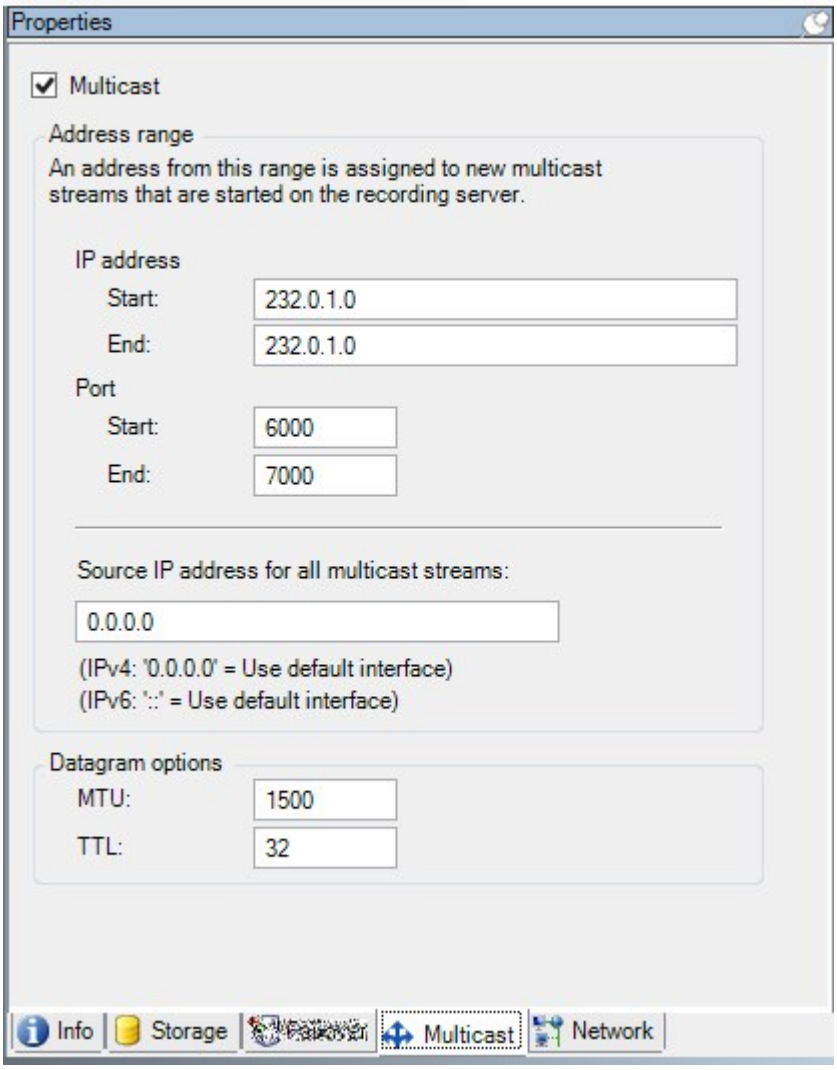
Votre système prend en charge le multicast de diffusions en continu et en direct à partir de serveurs d'enregistrement. Si de multiples utilisateurs de XProtect Smart Client souhaitent visualiser des vidéos en direct à partir de la même caméra, le multicast contribue à économiser une quantité considérable 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.

Si vous utilisez des serveurs de basculement, n'oubliez pas de spécifier également l'adresse IP de la carte d'interface réseau sur les serveurs de basculement (voir Onglet Multicast (serveurs de basculement) on page 464).

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.



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 1000 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**.
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 Web IANA (https://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.

Onglet Réseau (serveur d'enregistrement)

Si vous avez besoin d'accéder au VMS avec XProtect Smart Client sur un réseau public ou non approuvé, Milestone vous recommande d'utiliser une connexion sécurisée via le VPN. Ceci vous permet de vous assurer que la communication entre XProtect Smart Client et le serveur VMS est protégée.

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

Pourquoi utiliser une adresse publique ?

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 à Internet, le système de surveillance doit répondre avec l'adresse publique du serveur d'enregistrement. C'est l'adresse du pare-feu ou du routeur NAT (Network Address Translation), et souvent aussi un autre numéro de port. L'adresse et le port peuvent ensuite être redirigés à l'adresse locale et au port du serveur.

Serveurs de basculement (noeud Serveurs)

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Un serveur d'enregistrement de basculement est un serveur d'enregistrement supplémentaire qui peut prendre le relais du serveur d'enregistrement standard si celui-ci devient indisponible. Vous pouvez configurer un serveur d'enregistrement de basculement avec deux modes, en tant que **serveur d'enregistrement de basculement à froid** ou en tant que **serveur de basculement à affectation unique (à chaud)**.

Les serveurs d'enregistrement de basculement sont installés comme les serveurs d'enregistrement standard (voir Installer un serveur d'enregistrement de basculement via Download Manager on page 183). Une fois que vous avez installé les serveurs d'enregistrement de basculement, ils sont visibles dans le Management Client. Milestone vous recommande d'installer chaque serveur d'enregistrement de basculement sur un ordinateur distinct. Assurez-vous de configurer les serveurs d'enregistrement de basculement avec la bonne adresse IP ou le bon nom d'hôte du serveur de gestion. Les autorisations utilisateur pour le compte d'utilisateur sous lequel s'exécute le service du serveur de basculement sont fournies lors du processus d'installation. Il s'agit des :

- Autorisations Marche/Arrêt pour démarrer et arrêter le serveur d'enregistrement de basculement
- Autorisations d'accès en Lecture/Écriture pour lire ou modifier le fichier RecorderConfig.xml

Si un certificat est sélectionné pour le cryptage, alors l'administrateur doit accorder l'autorisation Lire à l'utilisateur du serveur de basculement sur la clé privée sélectionnée.

Si le serveur d'enregistrement de basculement prend le contrôle depuis le serveur d'enregistrement utilisant le cryptage, Milestone recommande de préparer également le serveur d'enregistrement de basculement pour qu'il utilise le cryptage. Pour plus d'informations, voir Communication sécurisée (explications) on page 158 et Installer un serveur d'enregistrement de basculement via Download Manager on page 183.

Vous pouvez spécifier quel type d'assistance de basculement vous souhaitez pour chaque périphérique. Pour chaque périphérique d'un serveur d'enregistrement, vous pouvez sélectionner un basculement complet, uniquement en direct ou aucune assistance de basculement. Ceci vous aide à accorder une priorité à vos ressources de basculement 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.

Lorsque votre système se trouve en mode de basculement, vous ne pouvez pas remplacer ou déplacer un matériel, mettre à jour le serveur d'enregistrement, ou changer les configurations du périphérique telles que les paramètres de stockage ou les paramètres du flux vidéo.

Serveurs d'enregistrement de basculement à froid

Dans une configuration de serveur de basculement à froid, vous regroupez plusieurs serveurs d'enregistrement de basculement dans un groupe de basculement. L'ensemble du groupe de basculement se consacre à prendre le relais de plusieurs serveurs d'enregistrement présélectionnés au cas où l'un d'entre eux ne serait plus disponible. Vous pouvez créer autant de groupes que vous le souhaitez (voir Serveurs d'enregistrement de basculement groupes pour une veille à froid on page 228).

Le regroupement a un avantage évident : par la suite, lorsque vous spécifiez les serveurs d'enregistrement de basculement devant prendre le relais d'un serveur d'enregistrement, vous sélectionnez un groupe de serveurs d'enregistrement de basculement. Si le groupe choisi contient plus d'un serveur d'enregistrement de basculement, vous savez que vous avez plus d'un serveur d'enregistrement de basculement à disposition si jamais un serveur d'enregistrement était indisponible. Vous pouvez spécifier un groupe de serveurs de basculement secondaire, qui prendra le relais du groupe primaire si tous les serveurs d'enregistrement du groupe primaire sont occupés. Un serveur d'enregistrement de basculement peut uniquement faire partie d'un seul groupe à la fois.

Les serveurs d'enregistrement de basculement d'un groupe de basculement sont classés de façon séquentielle. Cette séquence détermine l'ordre dans lequel les serveurs d'enregistrement de basculement doivent prendre le relais d'un serveur d'enregistrement. Par défaut, la séquence reflète l'ordre dans lequel vous avez incorporé les serveurs d'enregistrement de basculement dans le groupe de basculement ; le premier arrivé étant classé en premier dans la séquence. Vous pouvez le modifier si nécessaire.

Serveurs d'enregistrement de basculement à affectation unique

Dans une configuration de serveur d'enregistrement de basculement à affectation unique, vous pouvez dédier un serveur d'enregistrement de basculement pour qu'il prenne le relais d'**un** seul serveur d'enregistrement. Pour cette raison, le système peut conserver ce serveur d'enregistrement de basculement en mode « veille », ce qui signifie qu'il est synchronisé avec la configuration correcte/actuelle du serveur d'enregistrement auquel il est dédié et qu'il peut prendre le relais bien plus rapidement qu'un serveur d'enregistrement de basculement à froid. 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 assigner des serveurs de basculement qui font déjà partie d'un groupe de basculement en tant que serveurs d'enregistrement à affectation unique.

Validation du serveur d'enregistrement de basculement

Pour valider une fusion des données vidéo d'un serveur de basculement au serveur d'enregistrement, vous devez rendre le serveur d'enregistrement indisponible en arrêtant le service du serveur d'enregistrement ou en éteignant l'ordinateur du serveur d'enregistrement.

Toute interruption manuelle du réseau que vous pouvez provoquer en débranchant le câble réseau ou en bloquant le réseau avec un outil de test ne constitue pas une méthode valide.

Info Propriétés de l'onglet Serveur de basculement

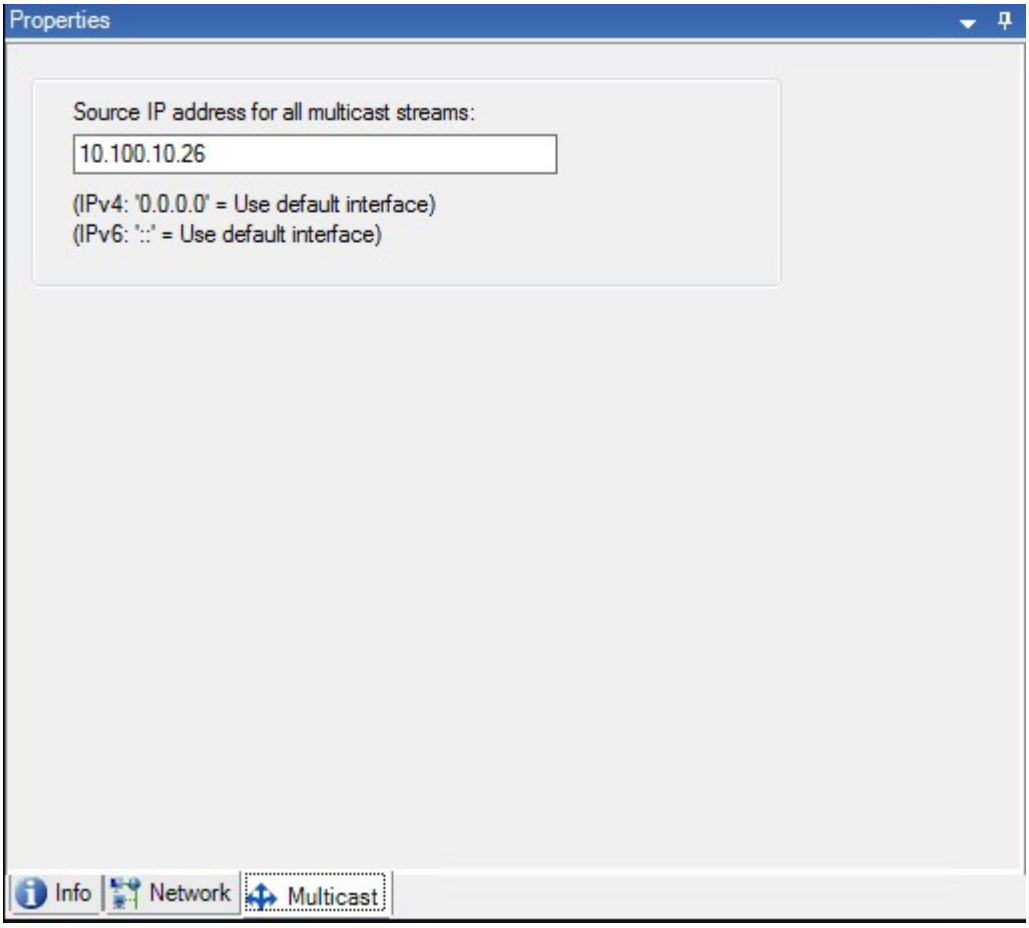
Spécifiez les propriétés du serveur d'enregistrement de basculement suivantes :

Nom	Description
Nom	Le nom du serveur d'enregistrement de basculement 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 basculement, par exemple de quel serveur d'enregistrement il prend le relais.
Nom de l'hôte	Affiche le nom de l'hôte du serveur d'enregistrement de basculement. Vous ne pouvez pas le modifier.
Adresse locale du serveur Web	Affiche l'adresse locale du serveur Web du serveur d'enregistrement de basculement. Vous utilisez l'adresse locale, par exemple, pour gérer les commandes de contrôle des caméras PTZ, et pour gérer les recherches et les demandes en direct depuis XProtect Smart Client. L'adresse inclue le numéro de port utilisé pour la communication du serveur Web (habituellement, le port 7563). Si le serveur d'enregistrement de basculement prend le contrôle depuis le serveur d'enregistrement utilisant le cryptage, vous aurez également besoin de préparer le serveur d'enregistrement de basculement pour qu'il utilise le cryptage. Si vous activez le cryptage des clients et serveurs récupérant les flux de données du serveur d'enregistrement, une icône représentant un cadenas apparaît, ainsi qu'une

Nom	Description
	adresse affichant **https** au lieu de **http**.
Adresse du serveur Web	Affiche l'adresse publique du Serveur Web du serveur d'enregistrement de basculement sur Internet. Si votre installation utilise un pare-feu ou du routeur NAT, entrez 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 serveur d'enregistrement de basculement. Vous spécifiez l'adresse publique et le numéro de port dans l'onglet **Réseau**. Si vous activez le cryptage des clients et serveurs récupérant les flux de données du serveur d'enregistrement, une icône représentant un cadenas apparaît, ainsi qu'une adresse affichant **https** au lieu de **http**.
Port UDP	Le numéro de port utilisé pour la communication entre les serveurs d'enregistrement de basculement. Le port par défaut est 8844.
Emplacement de la base de données	Spécifiez le chemin conduisant à la base de données utilisée par le serveur d'enregistrement de basculement pour le stockage des enregistrements. Vous ne pouvez pas modifier le chemin de la base de données lorsque le serveur d'enregistrement de basculement prend le relais d'un serveur d'enregistrement. Le système applique les modifications lorsque le serveur d'enregistrement de basculement ne prend plus le relais du serveur d'enregistrement.

Onglet Multicast (serveurs de basculement)

Si vous utilisez des serveurs de basculement et que vous avez activé le multicast de la diffusion en direct, vous devez préciser l'adresse IP de la carte d'interface réseau que vous utilisez - à la fois sur les serveurs d'enregistrement et les serveurs de basculement.



Pour plus d'informations sur le multicast, voir Activez le multicast pour le serveur d'enregistrement on page 224.

Info Propriétés de l'onglet Groupe de basculement

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

Propriétés de l’onglet Séquence de groupe de basculement

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

Serveur à distance pour Milestone Interconnect

Milestone Interconnect™ vous permet d’intégrer un nombre d’installations plus petites, physiquement fragmentées et des installations XProtect distantes avec un 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.

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.

Nom	Description
Pilote	Identifie le pilote prenant en charge la connexion au serveur distant.
Adresse	L'adresse IP ou le nom d'hôte du matériel.
IE	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.

Onglet Paramètres (serveur à distance)

Dans l'onglet **Paramètres**, vous pouvez voir 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 **Récupération à distance**, vous pouvez gérer les paramètres de récupération 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.
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 une récupération automatique ou une demande de récupération à partir du XProtect Smart Client en dehors de l'intervalle de temps, elle est acceptée, mais n'est pas commencée 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 de ces options ne s'applique à la lecture directe des enregistrements à distance. Toutes les caméras configurées pour être lues directement sont disponibles pour une lecture en direct et utilisent la bande passante selon les besoins.

Noeud Périphériques

Périphériques (noeud Périphériques)

Les périphériques apparaissent dans le Management Client lorsque vous ajoutez du matériel à l'aide de l'assistant **Ajouter matériel**. Voir Ajouter un matériel on page 231.

Vous pouvez gérer les périphériques via les groupes de périphériques à condition qu'ils partagent les mêmes propriétés, voir Groupes de périphériques (explications) on page 63.

Vous pouvez également gérer les périphériques de manière individuelle.

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.

Pour toutes les autres configurations et gestions des caméras, développez **Périphériques** dans le volet Navigation du site, puis sélectionnez un périphérique :

- **Caméras**
- **Microphones**
- **Haut-parleurs**
- **Métadonnées**
- **Entrées**
- **Sorties**

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**.

> Pour plus d'informations sur le matériel pris en charge, voir la page du matériel supporté sur le site Web de Milestone (https://www.milestonesys.com/support/tools-and-references/supported-devices/).

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 le statut des périphériques :

Caméra	Micro	Haut-parleur	Métadonnées	Entrée	Sortie	Description
						**Périphérique activé et récupération de données** : Le périphérique est

Caméra	Micro	Haut-parleur	Métadonnées	Entrée	Sortie	Description
						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.

Caméra	Micro	Haut-parleur	Métadonnées	Entrée	Sortie	Description
						**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**.
						**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

Caméra	Micro	Haut-parleur	Métadonnées	Entrée	Sortie	Description
						exemple si le serveur d'enregistrement est hors ligne.
						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**.

Caméras (noeud Périphériques)

Les périphériques de la caméra sont ajoutés automatiquement lorsque vous ajoutez un matériel sur le système et qu'ils sont activés par défaut.

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. La règle par défaut peut être désactivée et/ou modifiée selon les besoins.

Suivez cet ordre de configuration pour effectuer les tâches les plus courantes liées à la configuration d'un périphérique de caméra :

1. Configurez les paramètres de la caméra, voir l'onglet Paramètres (périphériques).
2. Configurez les flux, voir l'onglet Flux (périphériques).
3. Configurez le mouvement, voir l'onglet Mouvement (périphériques).
4. Configurez l'enregistrement, voir l'onglet Enregistrer (périphériques) et Surveiller les bases de données pour les périphériques.
5. Configurez les autres paramètres selon vos besoins.

Microphones (noeud Périphériques)

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 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.

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. La règle par défaut peut être désactivée et/ou modifiée selon les besoins.

Vous pouvez configurer les périphériques de microphones sur ces onglets :

- Onglet Info, voir Onglet Info (périphériques)
- Onglet Paramètres, voir Onglet Paramètres (périphériques)
- Onglet Enregistrement, voir onglet Enregistrement (périphériques)
- Onglet Événements, voir Onglet Événements (périphériques)

Hauts-parleurs (noeud Périphériques)

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 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.

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. La règle par défaut peut être désactivée et/ou modifiée selon les besoins.

Vous pouvez configurer les périphériques de haut-parleurs sur les onglets suivants :

- Onglet Info, voir Onglet Info (périphériques)
- Onglet Paramètres, voir Onglet Paramètres (périphériques)
- Onglet Enregistrement, voir onglet Enregistrement (périphériques)

Métadonnées (noeud Périphériques)

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. La règle par défaut peut être désactivée et/ou modifiée selon les besoins.

Vous pouvez configurer les périphériques de métadonnées sur les onglets suivants :

- Onglet Info, voir Onglet Info (périphériques)
- Onglet Paramètres, voir Onglet Paramètres (périphériques)
- Onglet Enregistrement, voir onglet Enregistrement (périphériques)

Entrée (noeud Périphériques)

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 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.

Vous pouvez configurer les périphériques d'entrée sur les onglets suivants :

- Onglet Info, voir Onglet Info (périphériques)
- Onglet Paramètres, voir Onglet Paramètres (périphériques)
- Onglet Événements, voir Onglet Événements (périphériques)

Sortie (noeud Périphériques)

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 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.

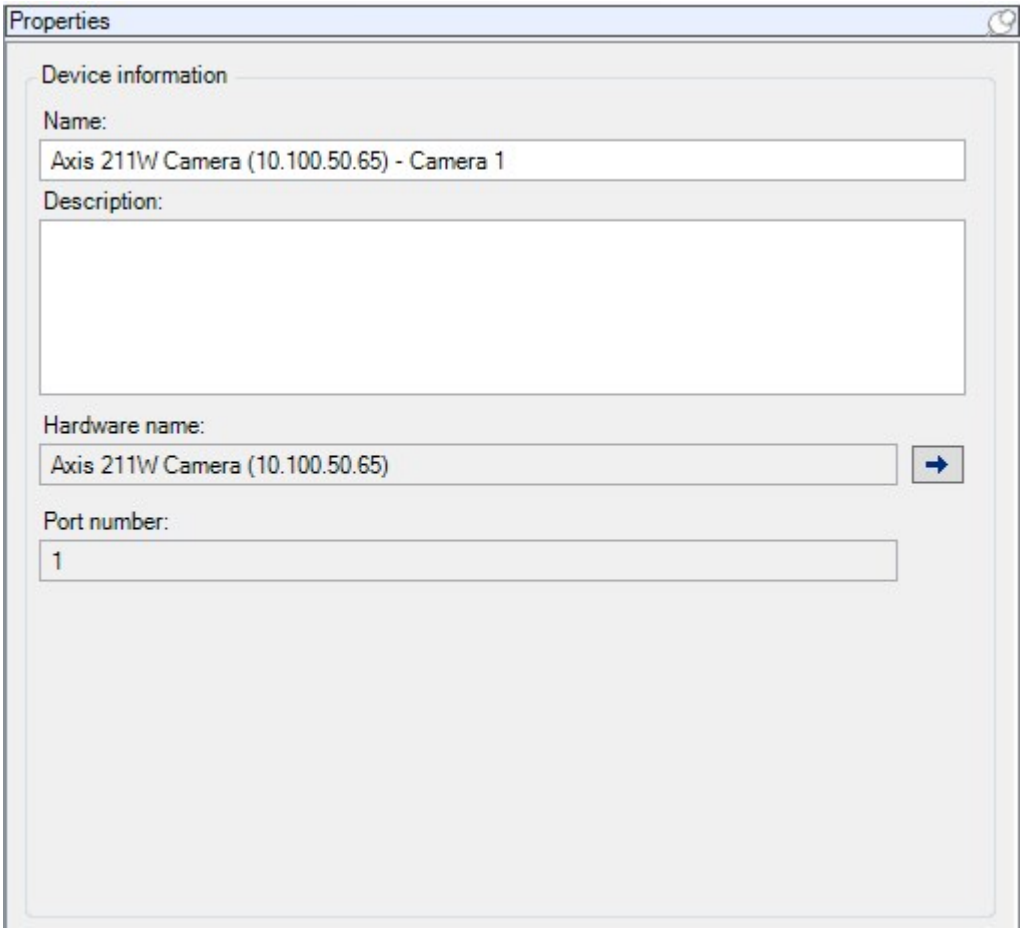
Vous pouvez configurer les périphériques de sortie sur les onglets suivants :

Onglet Info, voir

- Onglet Info, voir Onglet Info (périphériques)
- Onglet Paramètres, voir Onglet Paramètres (périphériques)

Onglet Périphériques

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**.



Propriétés de l'onglet Infos

Nom	Description
Nom	Le nom est utilisé partout où le périphérique apparaît dans une liste sur le système et les clients.

Nom	Description
	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**.
Abréviation	Pour appliquer une abréviation pour la caméra, saisissez-la ici. La longueur maximale de caractères est de 128. Si vous utilisez une smart map, l'abréviation s'affiche automatiquement avec la caméra sur la smart map. Sinon, le nom complet s'affiche.
Coordonnées géographiques	Saisissez l'emplacement géographique de la caméra au format **latitude, longitude**. La valeur que vous saisissez détermine la position de l'icône de caméra sur la smart map dans XProtect Smart Client et client XProtect Mobile. Le champ est principalement destiné à smart map et aux intégrations tierces.
Direction	Saisissez le sens de visualisation de la caméra mesuré par rapport à un point en direction du nord sur un axe vertical. La valeur que vous saisissez détermine la direction de l'icône de caméra sur la smart map dans XProtect Smart Client et client XProtect Mobile.

Nom	Description
	La valeur par défaut est 0,0.  Le champ est principalement destiné à smart map et aux intégrations tierces.
Champ de vision	Saisissez la largeur du champ de vision en degrés. La valeur que vous saisissez définit l'angle du champ de vision pour l'icône caméra sur la smart map dans XProtect Smart Client et client XProtect Mobile. La valeur par défaut est 0,0.  Le champ est principalement destiné à smart map et aux intégrations tierces.
Profondeur	Saisissez la profondeur du champ de vision en mètres ou en pieds. La valeur que vous saisissez définit la longueur du champ de vision pour l'icône caméra sur la smart map dans XProtect Smart Client et client XProtect Mobile. La valeur par défaut est 0,0.  Le champ est principalement destiné à smart map et aux intégrations tierces.
Aperçu de l'emplacement sur le navigateur	Pour vérifier que vous avez saisi les coordonnées géographiques appropriées, cliquez sur le bouton. Google Maps s'ouvre dans votre navigateur Internet standard à la position que vous avez spécifiée.  Le champ est principalement destiné à smart map et aux intégrations tierces.

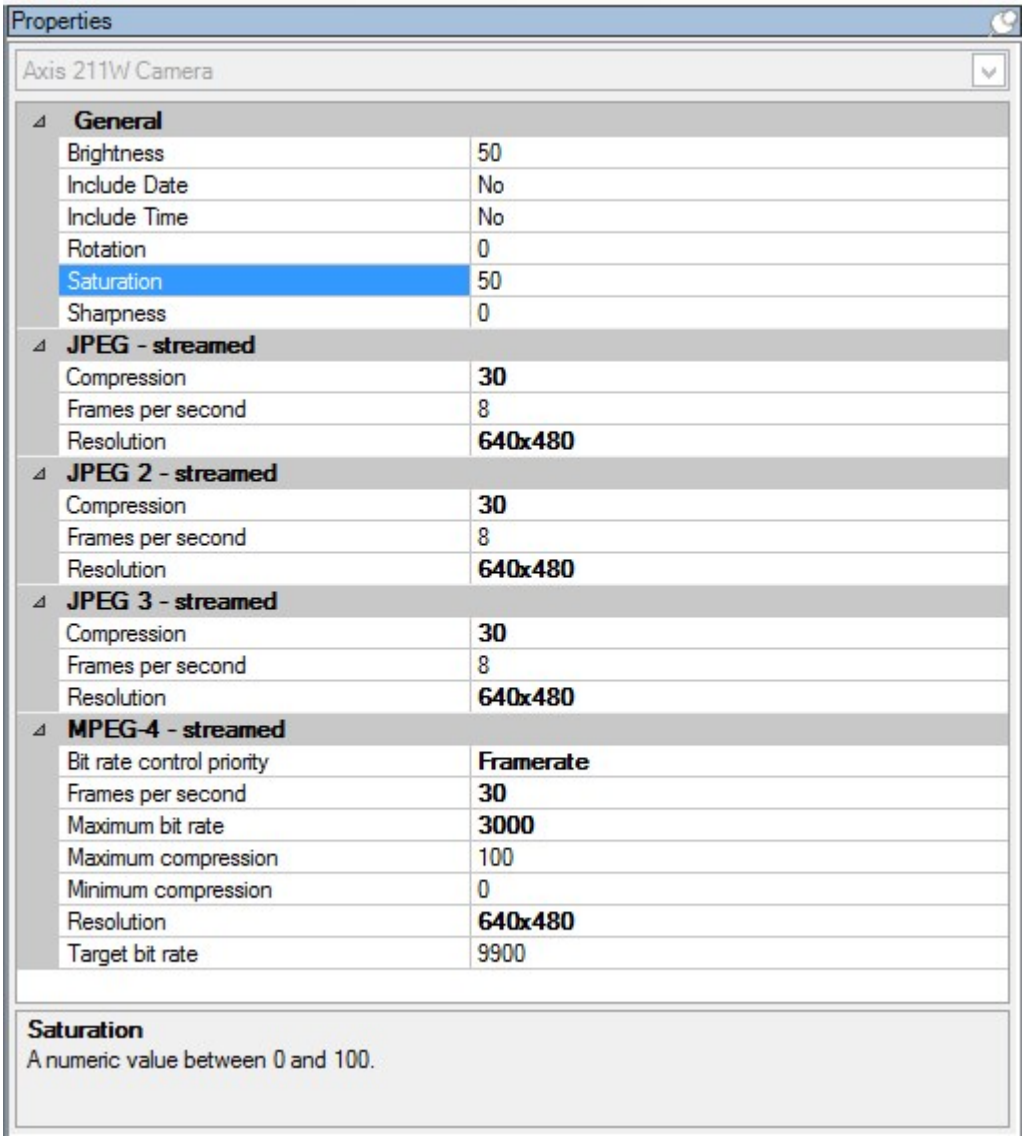
Onglet Paramètres (périphériques)

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 :



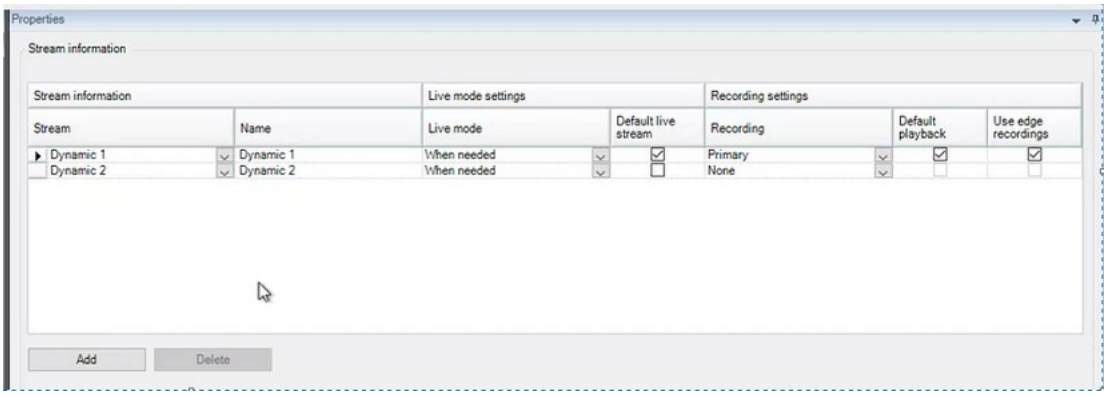
Pour plus d'informations sur les paramètres des caméras, voir Afficher ou modifier les paramètres des caméras.

Onglet Flux (périphériques)

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. Si vous utilisez la lecture adaptative, deux flux doivent être créés.



Tâches dans l'onglet Flux

Nom	Description
Ajouter	Cliquer pour ajouter un flux à la liste. Ajouter un flux

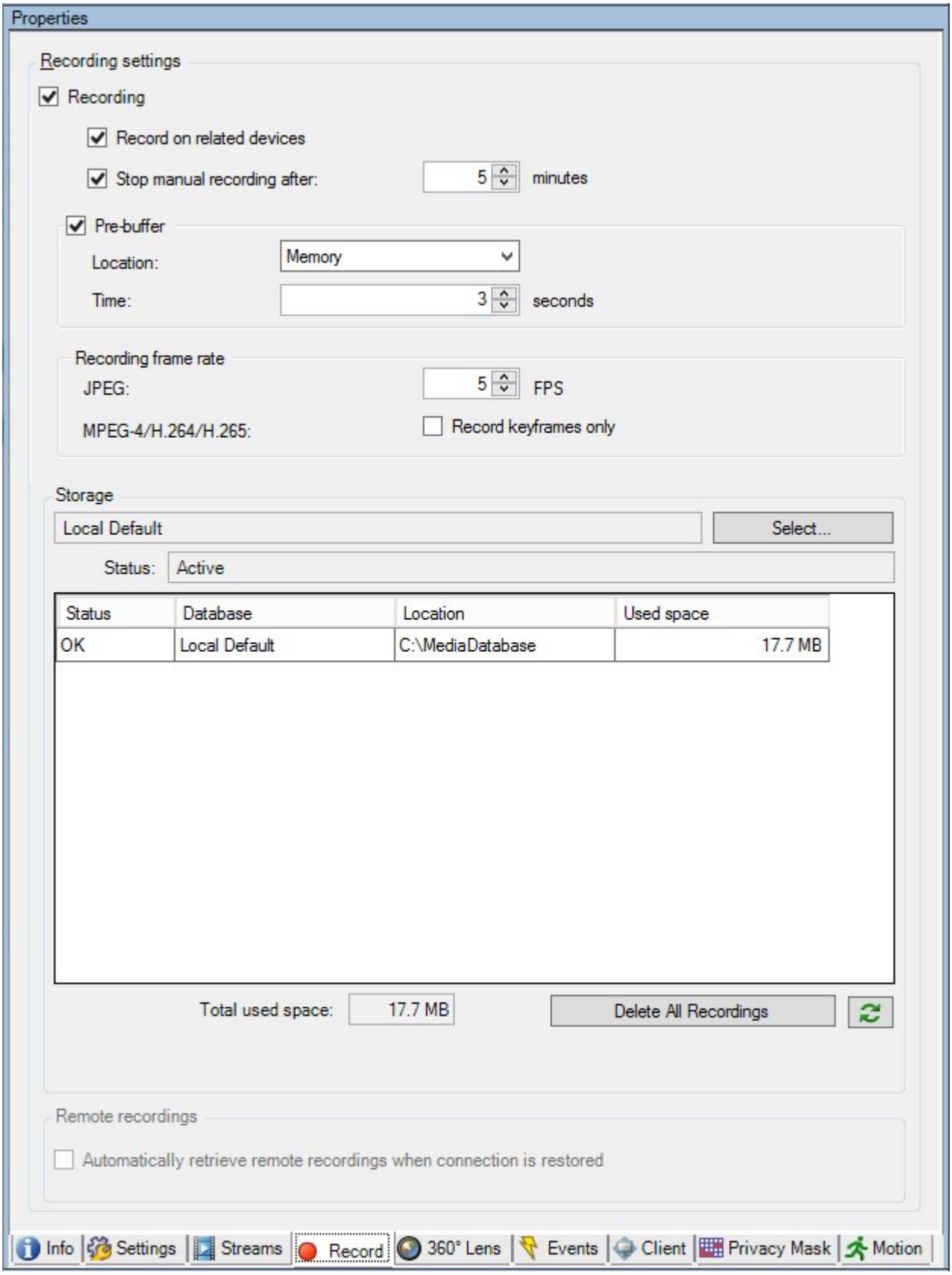
Onglet Enregistrement (périphériques)

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.


Properties
Recording settings
Recording
Record on related devices
Stop manual recording after:
5
minutes
Pre-buffer
Location:
Memory
Time:
3
seconds
Recording frame rate
JPEG:
5
FPS
MPEG-4/H.264/H.265:
Record keyframes only
Storage
Local Default
Select...
Status:
Active
Status
Database
Location
Used space
OK
Local Default
C:\MediaDatabase
17.7 MB
Total used space:
17.7 MB
Delete All Recordings
Remote recordings
Automatically retrieve remote recordings when connection is restored
Info
Settings
Streams
Record
360° Lens
Events
Client
Privacy Mask
Motion

Tâches dans l'onglet Enregistrer

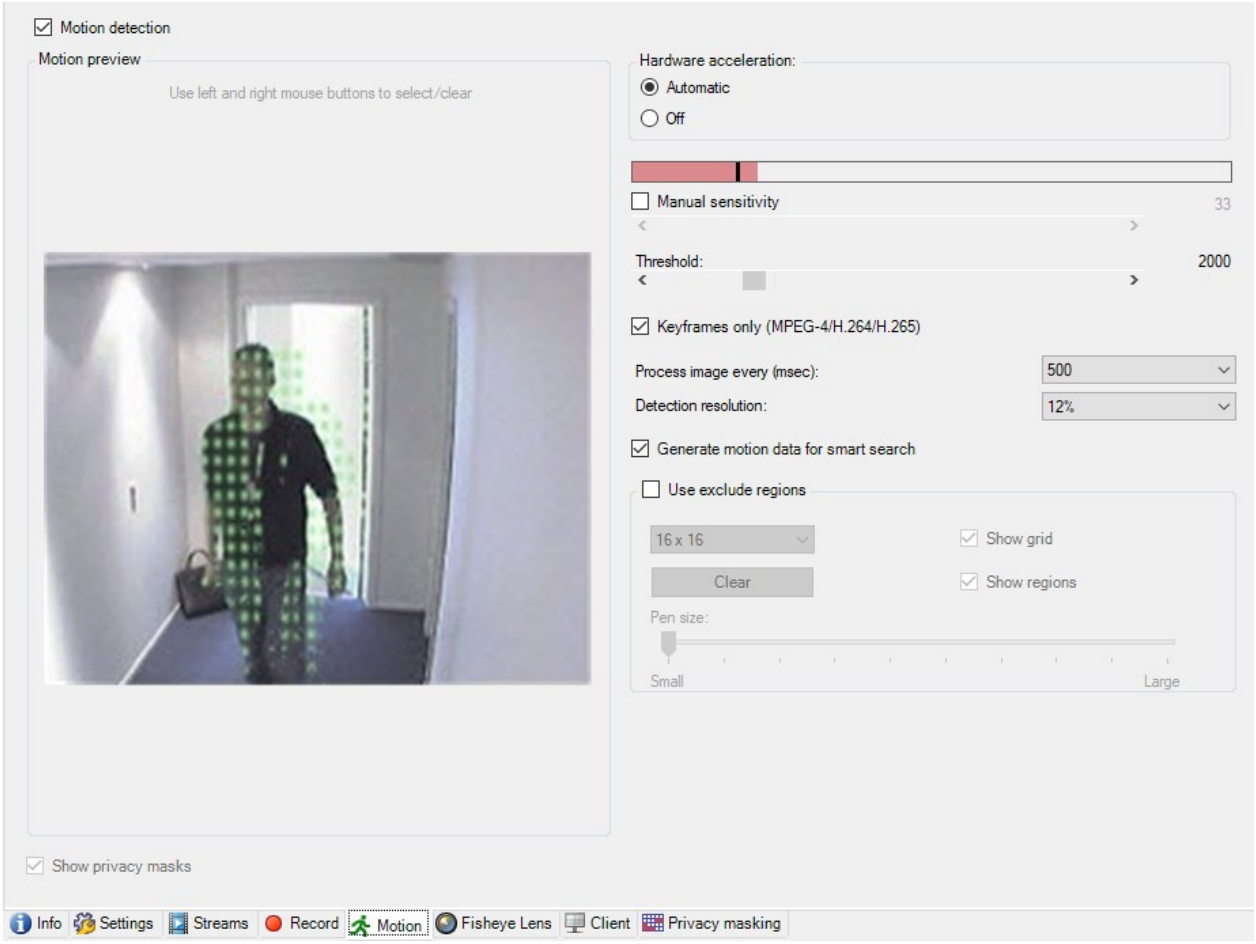
Nom	Description
Enregistrement	Activer/désactiver l'enregistrement Activer l'enregistrement sur les périphériques connexes
Pré-enregistrement	Pré-enregistrement et stockage des pré-enregistrements (explications) Gérer la mise en mémoire-tampon préalable Gérer l'enregistrement manuel
Fluidité d'image de l'enregistrement	Spécifier la fluidité d'image de l'enregistrement Activer l'enregistrement des images-clés
Stockage	Surveiller l'état des bases de données pour les périphériques
Sélectionner	Plus de périphériques d'un stockage à un autre
Supprimer tous les enregistrements	Utilisez ce bouton si vous avez ajouté tous les périphériques dans le groupe sur le même serveur : Supprimer des enregistrements
Rappeler les enregistrements à distance automatiquement lorsque la connexion est rétablie	Enregistrer et rappeler l'enregistrement à distance

Onglet Mouvement (périphériques)

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.



Tâches dans l'onglet Mouvement

Nom	Description
Détection des mouvements	Activer et désactiver la détection du mouvement
Accélération du matériel	Sélectionner **Automatique** pour activer l'accélération du matériel ou **Off** pour désactiver le paramètre. Pour plus d'informations, voir Activer ou désactiver l'accélération du matériel.
Masques de confidentialité	Si vous avez défini des zones comportant des masques de confidentialité permanents, vous pouvez cocher la case **Masques de confidentialité** pour afficher les masques de confidentialité dans l'onglet **Mouvement**. Vous définissez les zones

Nom	Description
	comportant des masques de confidentialité dans Onglet Masquage de confidentialité (périphériques) on page 496. Aucune détection du mouvement dans les zones couvertes par les masque de confidentialité permanents.
Sensibilité manuelle	Déterminer **dans quelle mesure chaque pixel** de l'image doit changer avant que l'on considère qu'il y a mouvement : Activer la sensibilité manuelle pour définir le mouvement
Seuil	Déterminer **dans quelle mesure les pixels** de l'image doit changer avant que l'on considère qu'il y a mouvement : Spécifier le seuil pour définir le mouvement
Images-clés uniquement (MPEG-4/H.264/H.265)	Cocher cette case pour application la détection du mouvement sur les images-clés uniquement et non sur l'intégralité 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.
Traiter les images tous les (msec.)	Sélectionner un intervalle de traitement d'image parmi la liste pour déterminer la fréquence à laquelle le système exécute l'analyse de la détection du mouvement. Par exemple, toutes les 1000 millisecondes correspond 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.
Résolution de la détection	Sélectionner une résolution de la détection dans la liste pour optimiser la performance de la détection du mouvement. Seul le pourcentage de l'image sélectionné est analysé, 25 % par exemple. 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

Nom	Description
	utilisée pour effectuer l'analyse, mais se traduit également par une détection de mouvement moins précise.
Générer des données de mouvement pour la recherche intelligente	L'activation de cette case à cocher permet au système de générer des données de mouvements concernant 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. Le système ne génère pas les données de mouvement dans les zones couvertes par des masques de confidentialité permanents, mais uniquement pour les zones comportant des masques de confidentialité amovibles (voir Détection du mouvement (explications)). Le seuil de détection du mouvement et les zones à exclure n'influencent pas les données de mouvement générées. • Spécifiez le paramètre par défaut pour la génération des données de recherche avancée sous **Outils** > **Options** > **Général**.
Utiliser l'exclusion de zones	Exclure la détection du mouvement des zones spécifiques d'une vue de la caméra : Spécifier l'exclusion de régions pour la détection de mouvement

Onglet Préréglages (périphériques)

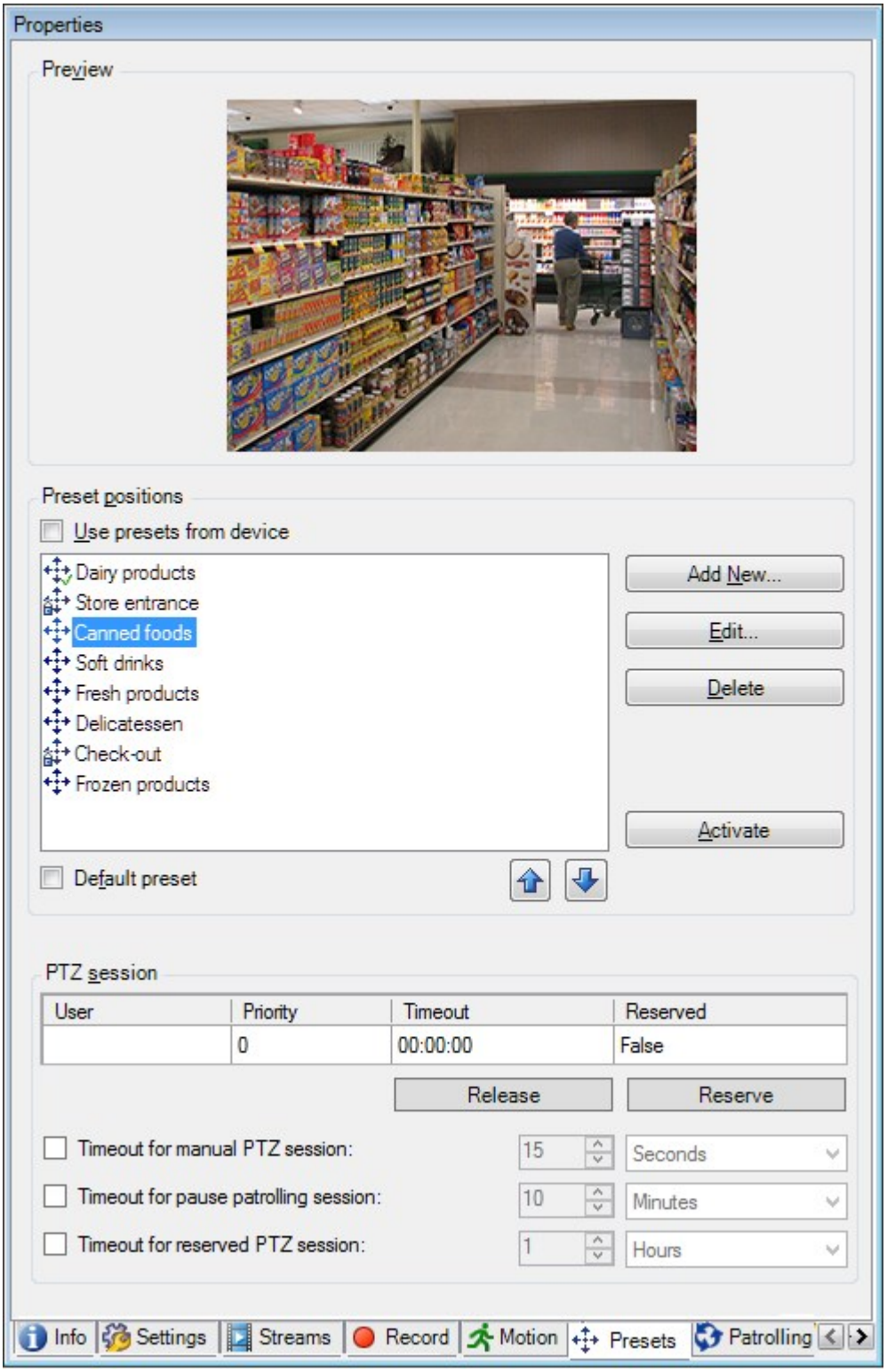
Les périphériques suivants possèdent un onglet **Préréglages** :

- 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 assignez une permission PTZ aux rôles dans l'onglet Sécurité générale (voir Onglet Sécurité globale (rôles) on page 555) ou l'onglet PTZ (voir Onglet PTZ (rôles) on page 607).


Properties
Preview
Preset positions
Use presets from device
Dairy products
Store entrance
Canned foods
Soft drinks
Fresh products
Delicatessen
Check-out
Frozen products
Add New...
Edit...
Delete
Activate
Default preset
PTZ session
User
Priority
Timeout
Reserved
0
00:00:00
False
Release
Reserve
Timeout for manual PTZ session:
15
Seconds
Timeout for pause patrolling session:
10
Minutes
Timeout for reserved PTZ session:
1
Hours
Info
Settings
Streams
Record
Motion
Presets
Patrolling

Tâches dans l'onglet Préréglages

Nom	Description
Nouveau	Ajouter une position prédéfinie pour une caméra dans le système : Ajouter une position prédéfinie (type 1)
Utiliser des préréglages à partir du périphérique	Ajouter une position prédéfinie pour des caméras PTZ sur la caméra elle-même : Utiliser les positions prédéfinies de la caméra (type 2)
Préréglage par défaut	Assigner l'une des positions prédéfinies d'une caméra PTZ à la position prédéfinie par défaut de la caméra : Assigner une position PTZ prédéfinie par défaut de la caméra par défaut
Modifier	Modifier une position prédéfinie existante, définie dans le système : Modifier une position PTZ prédéfinie pour une caméra (type 1 uniquement) Modifier le nom d'une position prédéfinie dans la caméra : Renommer une position PTZ prédéfinie pour une caméra (type 2 uniquement)
Verrouillé	Cocher cette case pour verrouiller une position PTZ prédéfinie. Vous pouvez verrouiller une position prédéfinie si vous souhaitez empêcher les utilisateurs de XProtect Smart Client ou les utilisateurs disposant d'autorisations de sécurité limitées de mettre à jour ou de supprimer un préréglage. Les préréglages verrouillés sont indiqués par l'icône  . Vous verrouillez les réglages prédéfinis dans le cadre de l'ajout (voir Ajouter une position prédéfinie (type 1)) et de la modification (voir Modifier une position prédéfinie (type 1 seulement)).
Activer	Cliquer sur ce bouton pour tester une position PTZ prédéfinie de la caméra : Tester une position PTZ prédéfinie (type 1 uniquement).
Réserver et **Lancer**	Éviter que d'autres utilisateurs ne prennent le contrôle sur une caméra et qu'ils ne lancent la réservation. Les administrateurs dotés d'autorisations de sécurité suffisantes pour exécuter une

Nom	Description
	session PTZ réservée peuvent exécuter la caméra PTZ dans ce mode. Ceci évite que d'autres utilisateurs prennent le contrôle de la caméra. Avec des autorisations suffisantes, vous pouvez lancer des sessions PTZ réservées à d'autres utilisateurs : Réserver et lancer des sessions PTZ.
Sesson PTZ	Surveiller si la système est en cours de patrouille ou si un utilisateur a pris le contrôle : Propriétés des sessions PTZ on page 487« ». Voir l'état des caméras PTZ et gérer les temps d'expiration des caméras : Spécifier les temps d'expiration des sessions PTZ.

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 d'expiration	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

Les cases à cocher dans la section **Session PTZ** vous permettent de modifier les temps d'expiration suivant 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**.

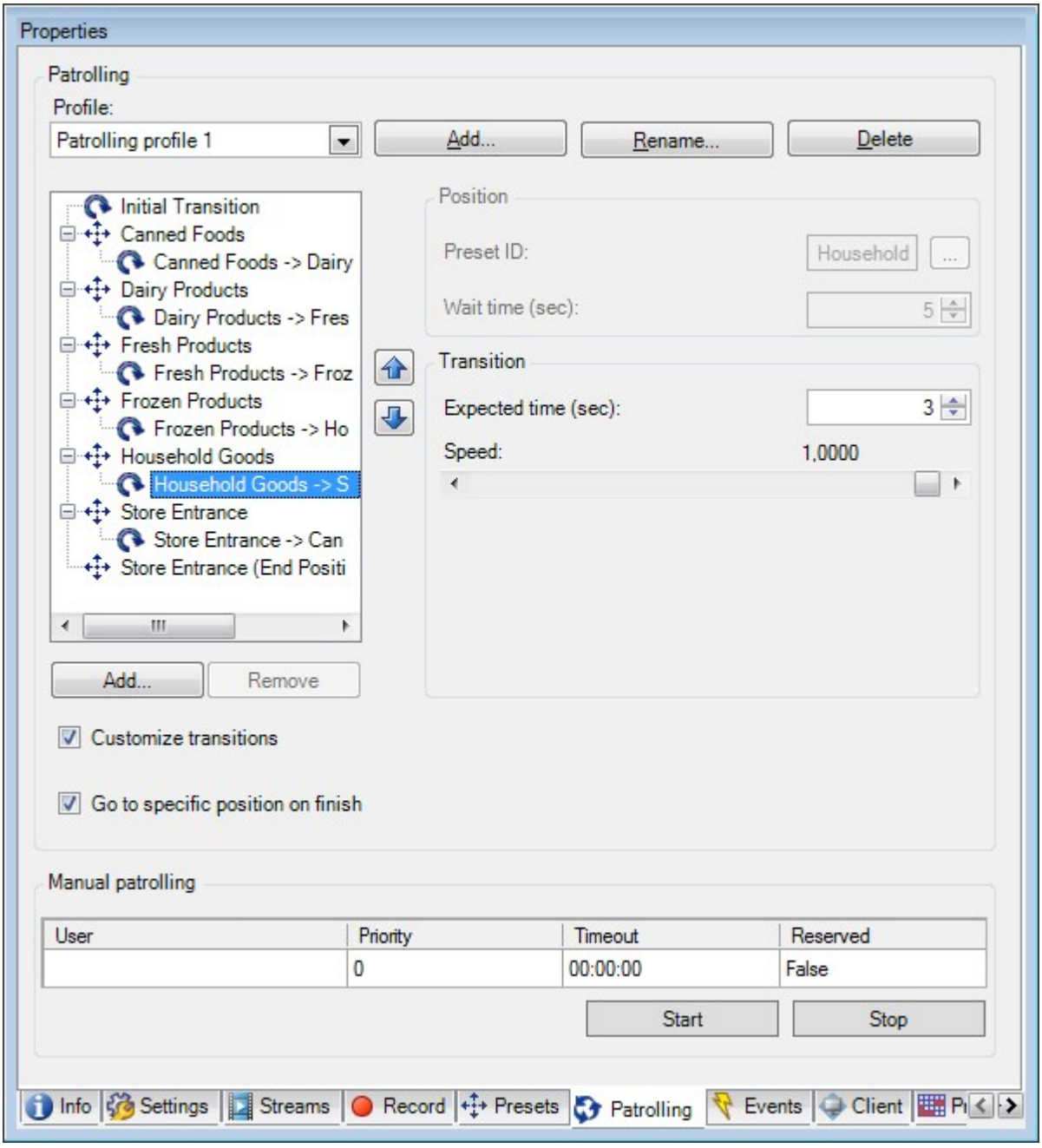
Onglet Patrouilles (périphériques)

Les périphériques suivants possèdent un onglet **Patrouille** :

- Caméras PTZ

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 travailler avec la patrouille, vous devez spécifier au moins deux positions PTZ prédéfinies dans l'onglet **Préréglages**, voir Ajouter une position PTZ prédéfinie (type 1).

L'onglet **Patrouille** qui affiche un profil de patrouille avec des transitions personnalisées :


Properties
Patrolling
Profile:
Patrolling profile 1
Add...
Rename...
Delete
Initial Transition
Canned Foods
Canned Foods -> Dairy
Dairy Products
Dairy Products -> Fres
Fresh Products
Fresh Products -> Froz
Frozen Products
Frozen Products -> Ho
Household Goods
Household Goods -> S
Store Entrance
Store Entrance -> Can
Store Entrance (End Positi
Position
Preset ID:
Household
Wait time (sec):
5
Transition
Expected time (sec):
3
Speed:
1,0000
Add...
Remove
Customize transitions
Go to specific position on finish
Manual patrolling
User
Priority
Timeout
Reserved
0
00:00:00
False
Start
Stop
Info
Settings
Streams
Record
Presets
Patrolling
Events
Client

Tâches dans l'onglet Patrouille

Nom	Description
Ajouter	Ajouter un profil de patrouille
ID de préréglage	Spécifier des positions prédéfinies dans un profil de patrouille
Temps d'attente (sec.)	Spécifier la durée à chaque position prédéfinie
Personnaliser les transitions	Personnaliser les transitions (PTZ)
Atteindre une position spécifique à la fin	Spécifier une position de fin durant a patrouille
Patrouille manuelle	Surveiller si la système est en cours de patrouille ou si un utilisateur a pris le contrôle.
Démarrage et **Arrêt**	Utiliser les boutons **Démarrage** et **Arrêt** pour démarrer et arrêter une patrouille manuelle. Voir Spécifier les temps d'expiration des sessions PTZ pour plus d'informations sur comment spécifier la durée avant que ne reprenne la patrouille régulière pour toutes les caméras PTZ ou pour les caméras PTZ individuelles.

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.

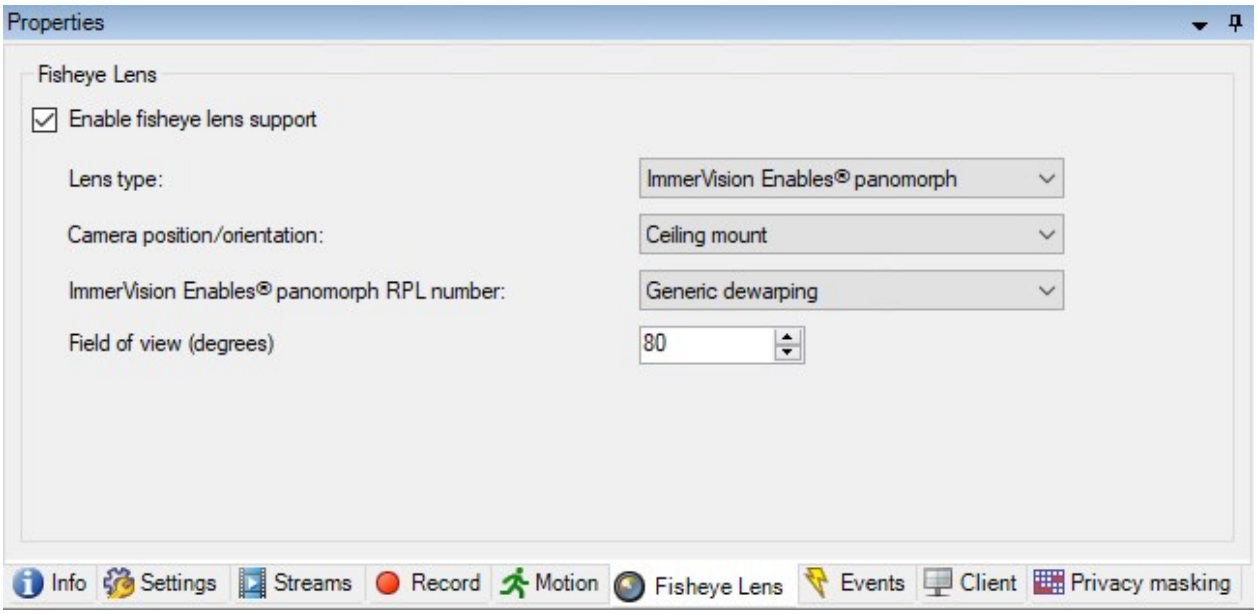
Nom	Description
Priorité	Affiche la priorité PTZ de l'utilisateur. Vous ne pouvez prendre le contrôle que de sessions PTZ d'utilisateurs ou de profils de patrouille ayant une priorité inférieure à la vôtre.
Délai d'expiration	Affiche le temps restant des sessions PTZ manuelles ou réservées actuelles.
Réservé	Indique si la session actuelle est une session PTZ réservée ou non. • **Vrai** : Réservé • **Faux** : Non réservé

Onglet Lentille fisheye (périphériques)

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.



Tâche dans l'onglet Objectif fisheye

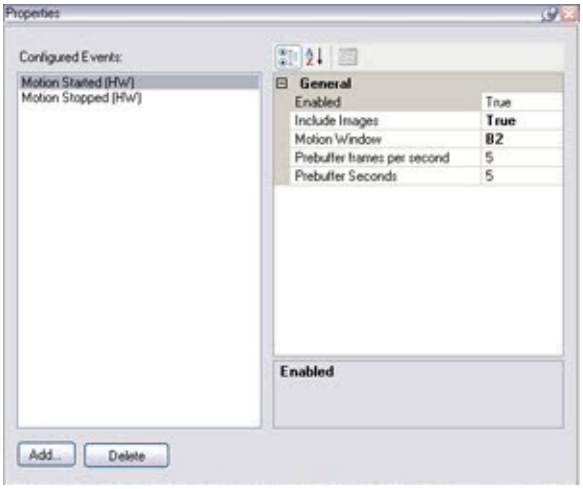
Nom	Description
Activer l'assistance pour l'objectif fisheye	Activer et désactiver la prise en charge fisheye

Onglet Événements (périphériques)

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.



Tâches dans l'onglet Événements

Nom	Description
Ajouter et **Supprimer**	Ajouter un événement pour un périphérique on page 277 et Supprimer un événement pour un périphérique on page 277

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)

Les périphériques suivants possèdent un onglet **Client** :

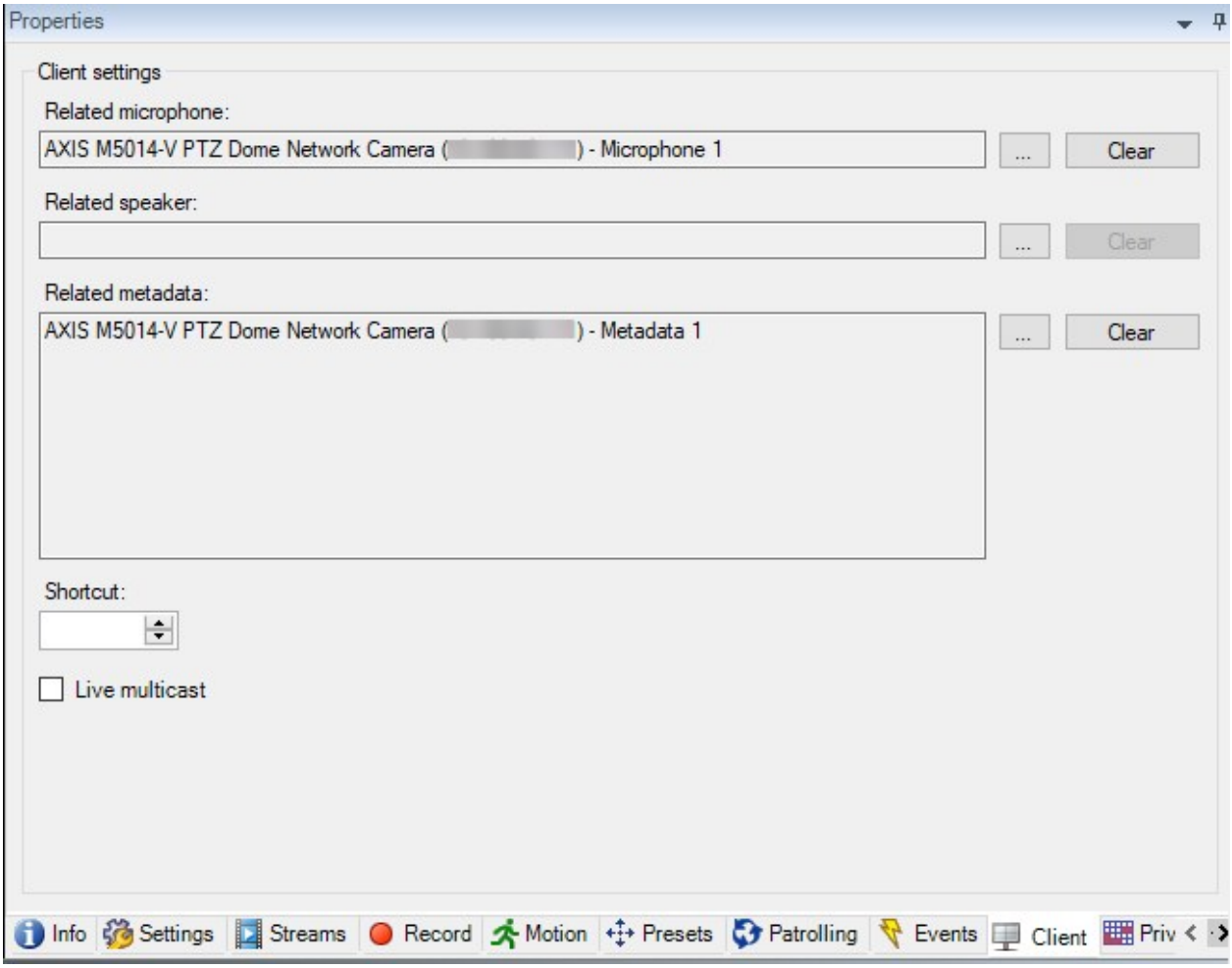
- Caméras

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 associés enregistrent également lorsque les caméras enregistrent, voir Activer l'enregistrement sur les périphériques connexes on page 249.

Vous pouvez également activer la **Multiduffusion en direct** sur la caméra. Cela signifie que la caméra effectue une multidiffusion en direct aux clients par le biais du serveur d'enregistrement.

> Les flux de multidiffusion ne sont pas cryptés, même si le serveur d'enregistrement utilise le cryptage.



Propriétés de l'onglet Client

Nom	Description
Microphone connexe	Spécifiez depuis quel microphone de la caméra les utilisateurs XProtect Smart Client écoutent la radio par défaut. L'utilisateur XProtect Smart Client peut choisir l'écoute par un autre microphone manuellement le cas échéant. Spécifiez le microphone lié à la caméra de la vidéo push pour diffuser une vidéo avec l'audio. Les microphones connexes enregistrent lorsque la caméra enregistre.
Haut-parleur	Spécifiez depuis quels haut-parleurs de la caméra les utilisateurs XProtect Smart

Nom	Description
connexe	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.
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 la caméra. • Créez chaque raccourci de sorte qu'il identifie de manière unique la caméra • Le numéro de raccourci d'une caméra ne peut pas avoir plus de quatre chiffres
Multicast en direct	Le système prend en charge le multicast de flux en direct depuis le serveur d'enregistrement vers XProtect Smart Client. Pour permettre la multidiffusion des flux en direct depuis la caméra, sélectionnez la boîte à cocher. La multidiffusion en direct ne fonctionne que sur le flux que vous avez spécifié comme étant le flux de la caméra par défaut dans l'onglet **Flux**. Vous devez également configurer le mode multicast pour le serveur d'enregistrement. Voir Activez le multicast pour le serveur d'enregistrement on page 224. Les flux de multidiffusion ne sont pas cryptés, même si le serveur d'enregistrement utilise le cryptage.

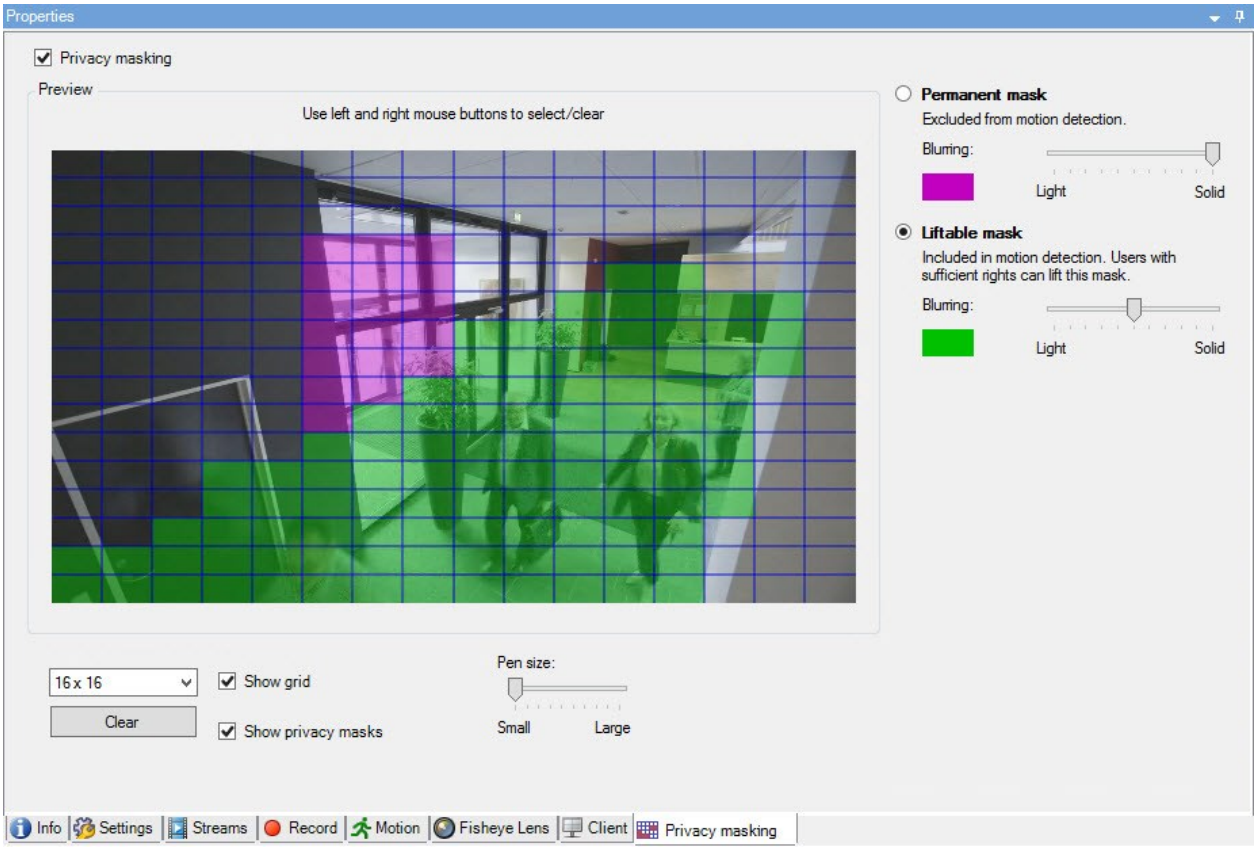
Onglet Masquage de confidentialité (périphériques)

> Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Les périphériques suivants possèdent un onglet **Masque de confidentialité** :

- Caméras

L'onglet **Masquage de confidentialité** vous permet d'activer et de configurer le masque de confidentialité de la caméra sélectionnée.



Tâches dans l'onglet Masquage de confidentialité

Nom	Description
Masquage de confidentialité	Activer/désactiver le masquage de confidentialité Masquage de confidentialité (explications)
Masque permanent et **Masque amovible**	Définir si vous souhaitez un masque de confidentialité permanent ou amovible : Définir les masques de confidentialité

Tâches liées aux masquage de confidentialité

Tâche	Description
Changer le délai d'expiration pour les masques de confidentialité levés pour le profil Smart Client associé avec le rôle qui a la permission de lever des masques de confidentialité.	Changez le délai d'expiration des masques de confidentialité
Activer ou désactiver la permission de lever des masques de confidentialité pour un rôle.	Donner aux utilisateurs l'autorisation d'enlever les masques de confidentialité
Créer un rapport sur les périphériques avec des informations relatives aux paramètres actuels de masquage de confidentialité de vos caméras.	Créez un rapport de configuration de votre configuration du masquage de confidentialité

Onglet Masquage de confidentialité (propriétés)

Nom	Description
Taille de la grille	La taille de grille sélectionnée détermine la densité de la grille, peut importe si cette dernière est visible ou non dans l'aperçu.

Nom	Description
	Les valeurs disponibles sont 8×8, 16×16, 32×32 ou 64×64.
Effacer	Supprime **tous** les masques de confidentialité que vous avez spécifiés.
Afficher la grille	Cochez la case **Afficher la grille** pour afficher le quadrillage.
Afficher les masques de confidentialité	Lorsque vous cochez la case **Afficher les masques de confidentialité** (option par défaut), les masques de confidentialité permanents apparaissent en violet et les masques relevables en vert. Milestone vous recommande de laisser la case **Afficher les masques de confidentialité** sélectionnée afin que vos collègues et vous-même puissiez voir la configuration actuelle de la protection de confidentialité.
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.
Masque permanent	Apparaît en violet dans l'aperçu sur cet onglet et sur l'onglet **Mouvement**. Les masques de confidentialité permanents sont toujours visibles dans XProtect Smart Client et ne peuvent pas être levés. Peuvent servir à couvrir les zones de la vidéo qui ne requièrent jamais de surveillance, comme les zones publiques où la surveillance n'est pas autorisée. La détection du mouvement est exclue des masques de confidentialité permanents. Vous indiquez la couverture des masques de confidentialité comme étant pleins ou comme ayant un certain niveau de flou. Les paramètres de couverture s'appliquent aussi bien à la vidéo en direct qu'à la vidéo enregistrée.
Masque amovible	Apparaît en ver dans l'aperçu sur cet onglet. Les masques de confidentialité peuvent être relevés dans XProtect Smart Client par des utilisateurs disposant d'autorisations utilisateur suffisantes. Par défaut, les masques de confidentialité sont levés pendant 30 minutes ou jusqu'à ce que l'utilisateur les applique à nouveau. N'oubliez pas que les masques de confidentialité sont relevés de toutes les caméras auxquelles l'utilisateur a accès. Si l'utilisateur de XProtect Smart Client ne dispose pas de l'autorisation pour lever

Nom	Description
	des masques de confidentialité, le système demandera un utilisateur ayant l'autorisation d'autoriser le levage. Vous indiquez la couverture des masques de confidentialité comme étant pleins ou comme ayant un niveau de flou. Les paramètres de couverture s'appliquent aussi bien à la vidéo en direct qu'à la vidéo enregistrée.
Flou	Sélectionnez le niveau de flou des masques de confidentialité dans les clients ou la couverture sur plein à l'aide du curseur. Par défaut, la couverture des zones ayant des masques de confidentialité permanents sont pleins (opaque). Par défaut, les masque de confidentialité relevables sont moyennement flous. Vous pouvez informer les utilisateurs du client au sujet de l'apparence des masques de confidentialité relevables et permanents afin qu'ils soient à mesure de les distinguer.

Fenêtre Propriétés du matériel

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

> ⚠ 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.

Onglet Info (matériel)

Pour plus d'informations sur l'onglet **Info** des serveurs distants, voir Onglet Info (serveur distant) on page 466.

Nom	Description
Nom	Saisissez 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** : 
Modèle	Identifie le modèle du périphérique.
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	L'adresse IP ou le nom d'hôte du matériel.
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.
Version du firmware :	La version de firmware du périphérique matériel. Pour vous assurer que le système affiche la version actuelle, exécutez l'assistant **Mettre à jour les données de matériel** après chaque mise à jour du firmware.
Dernière modification du mot de passe	Le champ **Dernière modification du mot de passe** indique l'horodatage du dernier changement de mot de passe en fonction des paramètres de l'heure locale de l'ordinateur où a été modifié le mot de passe.

Nom	Description
Dernière mise à jour des données du logiciel :	Heure et date de la dernière mise à jour des données de matériel.

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.

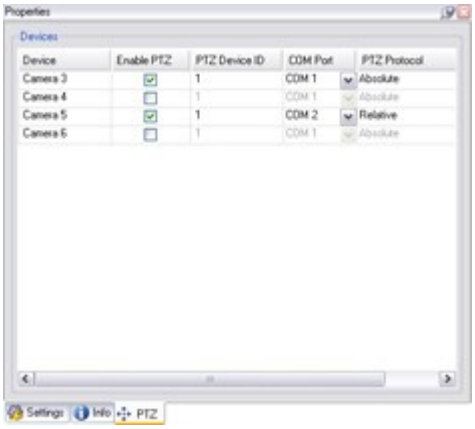
Pour plus d'informations sur l'onglet **Paramètres** des serveurs distants, voir Onglet Paramètres (serveur à distance) on page 467.

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.

Noeud Client

Clients (noeud)

Cet article décrit comment personnaliser l'interface utilisateur pour les opérateurs dans XProtect Smart Client et pour les administrateurs du système dans le Management Client.

Smart Wall (Noeud client)

Smart WallPropriétés de

Onglet Infos

Dans l'onglet **Info** pour une définition de Smart Wall, vous pouvez ajouter et modifier les propriétés de Smart Wall.

Nom	Description
Nom	Le nom de la définition Smart Wall. S'affiche dans XProtect Smart Client sous forme de nom du groupe de vues de Smart Wall.
Description	Une description de la définition Smart Wall. Cette description est utilisée uniquement dans le cadre de XProtect Management Client.
Texte d'état	Affichez la caméra et les informations de statut du système dans les éléments de vue de

Nom	Description
	la caméra.
Pas de barre de titre	Masquez la barre de titre sur tous les écrans caméras du mur vidéo.
Barre de titre	Affichez la barre de titre sur tous les écrans caméras du mur vidéo.

Onglet Préréglages

Dans l'onglet **Préréglages** pour une définition de Smart Wall, vous pouvez ajouter et modifier les préréglages[1] Smart Wall.

Nom	Description
Ajouter nouveau	Ajouter un préréglage à votre définition Smart Wall. Saisir un nom et une description pour le préréglage.
Modifier	Modifier le nom ou la description d'un préréglage.
Supprimer	Supprimer un préréglage.
Activer	Appliquez le préréglage des moniteurs Smart Wall configurés pour utiliser le préréglage. Pour appliquer un préréglage automatiquement, vous devez créer une règle qui utilise le préréglage.

Onglet Disposition

Dans l'onglet **Disposition** pour une définition de Smart Wall, vous placez les moniteurs de sorte que leurs positions ressemblent au montage des moniteurs physiques sur le mur vidéo. La disposition est également utilisée dans XProtect Smart Client.

---

[1]Une couche prédéfinie pour un ou plusieurs moniteurs Smart Wall dans XProtect Smart Client. Les préréglages déterminent les caméras affichées et la manière dont le contenu est structuré sur chaque moniteur du mur vidéo.

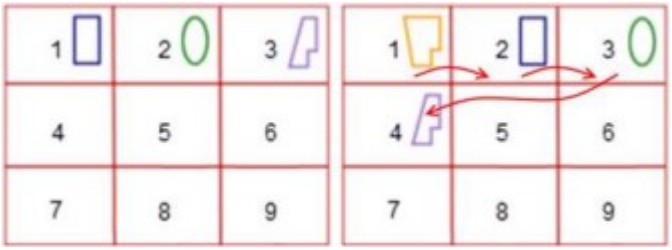
Nom	Description
Modifier	Ajuster le positionnement des moniteurs.
Déplacement	Pour déplacer un moniteur vers une nouvelle position, sélectionnez le moniteur puis déplacez-le vers la position souhaitée, ou cliquez sur l'une des flèches pour déplacer le moniteur dans la direction souhaitée.
Boutons de zoom	Faire un zoom avant ou un zoom arrière de la prévisualisation de la disposition Smart Wall pour garantir le bon positionnement des moniteurs.
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 Infos

Dans l'onglet **Info** pour un moniteur dans un préréglage Smart Wall, vous pouvez ajouter plusieurs 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 XProtect 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 est affiché sur un moniteur avec une disposition ne comportant pas de préréglage lorsqu'un nouveau préréglage Smart Wall est déclenché ou sélectionné

Nom	Description
	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.
Élément de préréglage vide	Définit ce qui est affiché dans un élément avec un élément de préréglage ne comportant pas de préréglage lorsqu'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 l'insertion des caméras dans la disposition du moniteur lorsqu'elle est vue dans XProtect Smart Client : • **Indépendant** : seul le contenu de l'élément de disposition sélectionné change. Le reste du contenu dans la disposition reste tel quel. • **Lié** : le contenu des éléments de la disposition est poussé vers la droit. Si, par exemple, une caméra est insérée dans la position 1, l'ancienne caméra de la position 1 est poussée vers la position 2, l'ancienne caméra de la position 2 est poussée vers la position 3, etc. Voici un exemple illustré : 

Onglet Préréglages

Dans l'onglet **Préréglages** pour un moniteur dans un préréglage Smart Wall, vous pouvez modifier la disposition de la vue et le contenu du moniteur dans le préréglage Smart Wall sélectionné.

Nom	Description
Préposition	Une liste de Smart Wall préréglages pour la définition Smart Wall sélectionnée.
Modifier	Cliquez sur **Modifier** pour modifier la disposition et le contenu de l'écran sélectionné. Double-cliquez sur une caméra pour la supprimer. 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, puis cliquez sur **OK**.

Profils Smart Client (nœud client)

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Sur les onglets suivants, vous pouvez 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.

Pour créer ou modifier des profils Smart Client, développez **Client** et sélectionnez **Profils Smart Client**.

Onglet Info (Profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
Info	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.

Onglet Général (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
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 activer ou désactiver certains onglets dans XProtect Smart Client. Les paramètres des **Messages d'erreur de la caméra**, des **Messages d'erreur du serveur** et du **Message d'erreur de la vidéo en direct** vous permettent de contrôler si ces messages d'erreur sont affichés sous forme de recouvrement, d'image noire avec recouvrement, ou s'ils sont masqués. Le **Message d'arrêt de la vidéo en direct** est affiché dans XProtect Smart Client lorsque le flux de la caméra en direct est arrêté. Par exemple, lorsque la caméra n'envoie plus d'images même lorsqu'elle est connectée. ⚠ Si vous **masquez** les messages d'erreur de la caméra, l'opérateur risque de ne pas voir que la connexion à une caméra a été perdue. Le paramètre **Caméras autorisées lors de la recherche** vous permet de contrôler combien de caméras les opérateurs peuvent ajouter à leurs recherches dans XProtect Smart Client. La configuration d'une limite du nombre de caméras peut vous aider à éviter une surcharge du système. Le paramètres de l'**Aide en ligne** vous permet de désactiver le système d'aide dans XProtect Smart Client. Le paramètre des **Tutoriels vidéo** vous permettent de désactiver le bouton **Tutoriels vidéo** dans XProtect Smart Client. Le bouton redirige les opérateurs vers la page des tutoriels vidéo : https://www.milestonesys.com/support/help-yourself/video-tutorials/

Onglet Avancé (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
Avancés	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 multicœurs 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. Le mode **désentrelacement** vous permet de convertir votre vidéo dans un 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. Le **flux adaptatif** permet à XProtect Smart Client de sélectionner automatiquement les flux vidéo en direct avec la meilleure correspondance de résolution pour les flux requis par l'élément de vue. Cela diminue le chargement sur le CPU et le GPU, et améliore donc la capacité et la performance de décodage de l'ordinateur. Cela requiert la multidiffusion des flux vidéo en direct avec différentes résolutions à configurer, voir Gérer la multidiffusion. Le flux adaptatif peut être appliqué à la fois en direct et en mode lecture. Concernant le flux adaptatif, le mode lecture est appelé lecture adaptative. La lecture adaptative nécessite que deux flux soient définis pour l'enregistrement. Pour plus d'informations sur l'ajout de flux aux flux adaptatifs en mode en direct et pour la lecture adaptative, consultez Ajouter un flux on page 252.

Onglet En direct (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
En direct	Disponibilité du mode En direct et d'autres fonctionnalités associées au direct, de la lecture de la caméra, des boutons de recouvrement, et des cadres de sélection, et également des modules d'extension MIP associés au direct.

Onglet Relecture (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
Lecture	Disponibilité du mode Lecture et d'autres fonctionnalités associés à la lecture, de l'agencement des rapports d'impression, de la relecture indépendante, des signets, des cadres de sélection et également des modules d'extension MIP associés à la lecture.

Onglet Configuration (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
Configuration	Disponibilité de la configuration générale/des volets/boutons, du plug-in MIP associé à la configuration et des autorisations permettant de modifier un plan et de modifier la zone tampon de vidéo en direct.

Onglet Exportation (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
Exporter	Les chemins d'accès, les masques de confidentialité, les formats d'images fixes 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.

Onglet Chronologie (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
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. Vous pouvez également indiquer s'il faut afficher des données ou marqueurs supplémentaires à partir d'autres sources.

Onglet Contrôle d'accès (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
Contrôle d'accès	Sélectionnez si les notifications de demande d'accès doivent apparaître sur l'écran XProtect Smart Client quand elles sont déclenchées par des événements.

Onglet Gestionnaire d'alarme (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
Gestionnaire d'alarme	Spécifiez si :

Onglet	Description
	• Les notifications sur le bureau liées aux alarmes doivent s'afficher sur les ordinateurs où XProtect Smart Client est installé. Les notifications apparaîtront uniquement si XProtect Smart Client est en cours d'exécution, même s'il est minimisé  Les notifications sur le bureau liées aux alarmes n'apparaissent que lorsque les alarmes ont une certaine priorité, **Moyenne** ou **Haute**, par exemple. Pour configurer quelles priorités d'alarme déclenchent les notifications, rendez-vous dans **Alarmes** > **Paramètres des données de l'alarme** > **Niveaux des données de l'alarme**. Pour chaque priorité d'alarme requise, cochez la case **Activer les notifications sur le bureau**. Voir Paramètres des données de l'alarme (noeud Alarmes). • Les alarmes doivent jouer des notifications sonores sur les ordinateurs où XProtect Smart Client est installé. Les notifications sonores sont uniquement jouées si XProtect Smart Client est en cours d'exécution, même s'il est minimisé  Les notifications sonores des alarmes sont jouées uniquement lorsqu'un son est associé à l'alarme. Pour associer des sons aux alarmes, rendez-vous dans **Alarmes** > **Paramètres des données des alarmes** > **Niveaux des données des alarmes**. Pour chaque priorité d'alarme requis, sélectionnez le son à associer à l'alarme. Voir Paramètres des données de l'alarme (noeud Alarmes).

Onglet Smart Map (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
Smart Map	Spécifier des paramètres pour la fonctionnalité smart map. Vous pouvez spécifiez si : • Milestone Map Service est disponible pour être utilisé en tant qu'arrière-plan géographique • OpenStreetMaps est disponible pour être utilisé en tant qu'arrière-plan géographique • XProtect Smart Client créera automatiquement des emplacements lorsqu'un utilisateur ajoute une disposition personnalisée à la Smart Map. Vous pouvez également préciser à quelle fréquence vous voulez que le système supprime les données relatives aux smart maps sur votre ordinateur. Pour aider XProtect Smart Client à afficher smart map plus rapidement, le client enregistre les données du plan dans le cache de votre ordinateur. Avec le temps ceci pourrait ralentir votre ordinateur. Le cache ne s'applique pas pour Google Maps. Si vous souhaitez utiliser Bing Maps ou Google Maps en tant qu'arrière-plan géographique, saisissez une clé Bing Maps API key ou une clé Maps Static API de Google.

Profils Management Client (nœud client)

Cette fonction n'est disponible que dans XProtect Corporate.

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.

Composant	Exigences
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. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

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 panneau **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**.

Élément de navigation	Description
Serveurs	Permet à l'utilisateur administrateur associé au profil Management Client de voir les **Serveurs d'enregistrement** et les **Serveurs de basculement**.
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 événements	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**, la **Protection 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, ainsi que le Journal déclenché par les règles.
Contrôle d'accès	Permet à l'utilisateur administrateur associé au profil Management Client de voir les fonctionnalités 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 des périphériques 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 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 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 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 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 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 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**.

Sites fédérés

Dans cette rubrique, décidez si un utilisateur administrateur associé au profil Management Client est autorisé à voir le panneau de **Hiérarchie des sites fédérés**.

Noeud Règles et événements

Règles (noeud Règles et événements)

Votre système contient un certain nombre de règles par défaut que vous pouvez utiliser sans autre forme de configuration pour les fonctions élémentaires. 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**.
Lire le message audio sur demande	Veille à ce que la vidéo soit enregistrée automatiquement lorsqu'une requête externe se produit. 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.
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. La mise en mémoire-tampon préalable configurable dans l'onglet Enregistrement doit être identique ou supérieure à la durée de pré-enregistrement.

Règle par défaut	Description
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.
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

Règle par défaut	Description
	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 dans 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
Lire le message audio sur demande	Exécuter une action sur un message audio sur demande Lire le message audio à partir des métadonnées disponibles sur les périphériques ayant la priorité 1
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
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

Règle par défaut	Texte à saisir
	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

Profils des notifications (noeud Règles et Événements)

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.

Composant	Exigences
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.
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 afficheront les enregistrements présentés espacées d'une demi-seconde.

Composant	Exigences
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.

Vue d'ensemble des événements

Lorsque vous créez 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.

Matériel - Événements configurables :

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	Survient lorsqu'un signet est marqué en mode En direct 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	A lieu lorsqu'une communication avec un périphérique est bien arrêtée.

Événement	Description
arrêtée (Périphérique)	
Verrouillage des preuves modifié	Se produit quand une preuve protégée est modifiée pour les périphériques par un utilisateur client ou via le MIP SDK.
Preuves verrouillées	Se produit quand une protection des preuves est créée pour les périphériques par un utilisateur client ou via le MIP SDK.
Preuves déverrouillées	Se produit quand la protection des preuves est supprimée pour les périphériques par un utilisateur client ou via le MIP SDK.
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	Survient lorsque le dépassement de capacité (voir Dépassement de la capacité d'alimentation démarré on page 523) termine.
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

Événement	Description
	autorisations 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 également Matériel - Événements configurables : on page 521.
Mouvement arrêté	A lieu lorsque le mouvement n'est plus détecté dans la vidéo reçue. Voir également Mouvement démarré on page 524. 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

Événement	Description
	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 également Matériel - Événements configurables : on page 521.
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 désactivée. 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.

Événement	Description
Erreur : paramètres modifiés	A lieu lorsqu'une tentative de modification des paramètres d'un périphérique échoue.

Événements externes - Événements prédéfinis :

Événement	Description
Demander la diffusion d'un message audio	Activé lorsque la lecture de messages audio est requise via le MIP SDK. Au travers du 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 semblables) à votre système.
Demander le départ de l'enregistrement	Activé lorsque le démarrage des enregistrements est demandé via MIP SDK. Au travers du 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 semblables) à votre système.
Demande Arrêter l'enregistrement	Activé lorsque l'arrêt des enregistrements est demandé via MIP SDK. Au travers du 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 semblables) à 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 l'utilisateur :

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 également Événements définis par l'utilisateur (explications) on page 92.

Serveurs d'enregistrement :

Événement	Description
Archive disponible	A lieu lorsqu'une archive d'un serveur d'enregistrement est disponible après avoir été indisponible. Voir également Archive non disponible on page 527.
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 institution.
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.
La base de données supprime les fichiers avant la taille de rétention fixée	Se produit lorsque l'horaire de rétention est atteint avant la taille limite de la base de données.
La base de données supprime les fichiers avant l'horaire de rétention fixé	Se produit lorsque la taille limite de la base de données est atteinte avant l'horaire de rétention fixé.
Disque de base de données pleine - Archivage	A lieu lorsqu'un disque de base de données n'a plus d'espace libre. Un disque de base de données est saturé lorsqu'il contient moins de 5 Go d'espace libre : Les plus anciennes données d'une base de données seront toujours auto-

Événement	Description
automatique	archivées (ou supprimées si aucune archive suivante n'est définie) dès qu'il y a moins de 5 Go d'espace libre.
Disque de base de données plein - Suppression en cours	Se produit lorsqu'un disque de base de données est plein et qu'il reste moins d'1 Go d'espace libre. Les données sont supprimées même si une nouvelle archive 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.
Zone de stockage de base de données disponible	A lieu lorsqu'un stockage d'un serveur d'enregistrement est disponible après avoir été indisponible. Voir également Zone de stockage de base de données non disponible on page 528. 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**.
Zone de 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 institution.
Erreur de communication de basculement cryptée	Survient lorsqu'il y a une erreur de communication SSL entre le serveur de basculement et les serveurs d'enregistrement surveillés.
Basculement commencée	A lieu lorsqu'un serveur d'enregistrement de basculement se substitue à un serveur d'enregistrement. Voir également Serveurs de basculement (noeud).

Événement	Description
Basculement arrêtée	A lieu lorsqu'un serveur d'enregistrement devient à nouveau disponible, et peut se substituer au serveur d'enregistrement de basculement.

Événements moniteur système

Les événements du moniteur système sont déclenchés par le dépassement des valeurs limites configurées dans le nœud des **Seuils du moniteur système**. Voir également Afficher l'état en cours de votre matériel et le dépanner si nécessaire on page 318.

Cette fonctionnalité nécessite que le service Data Collector soit en cours d'exécution.

Moniteur système - Serveur :

Événement	Description
Utilisation du processeur critique	Se produit lorsque l'utilisation du CPU dépasse le seuil critique du CPU.
Usage du processeur normal	Se produit lorsque l'utilisation du CPU retombe sous le seuil d'alerte du CPU.
Avertissement d'usage du processeur	Se produit lorsque l'utilisation du CPU dépasse le seuil d'alerte du CPU ou redevient inférieur au seuil critique du CPU.
Utilisation de la mémoire critique	Se produit lorsque l'utilisation de la mémoire dépasse le seuil critique de la mémoire.
Utilisation de la mémoire normale	Se produit lorsque l'utilisation de la mémoire redevient inférieure au seuil d'alerte de la mémoire.
Avertissement d'utilisation de la mémoire	Se produit lorsque l'utilisation de la mémoire dépasse le seuil d'alerte de la mémoire ou redevient inférieur au seuil d'utilisation critique de la mémoire.

Événement	Description
Décodage critique NVIDIA	Se produit lorsque l'utilisation du décodage NVIDIA dépasse le seuil critique de NVIDIA.
Décodage normal NVIDIA	Se produit lorsque l'utilisation du décodage NVIDIA redevient inférieur au seuil d'alerte de NVIDIA.
Avertissement du décodage NVIDIA	Se produit lorsque l'utilisation du décodage NVIDIA dépasse le seuil d'alerte du décodage NVIDIA ou redevient inférieur au seuil critique de NVIDIA.
Mémoire critique NVIDIA	Se produit lorsque l'utilisation de la mémoire NVIDIA dépasse le seuil critique de la mémoire NVIDIA.
Mémoire normale NVIDIA	Se produit lorsque l'utilisation de la mémoire NVIDIA redevient inférieure au seuil d'alerte de NVIDIA.
Avertissement de la mémoire NVIDIA	Se produit lorsque l'utilisation de la mémoire NVIDIA dépasse le seuil d'alerte de la mémoire NVIDIA ou redevient inférieure au seuil critique de NVIDIA.
Rendu critique NVIDIA	Se produit lorsque l'utilisation de NVIDIA dépasse le seuil critique du NVIDIA.
Rendu normal de NVIDIA	Se produit lorsque l'utilisation de NVIDIA redevient inférieure au seuil d'alerte du NVIDIA.
Avertissement du rendu NVIDIA	Se produit lorsque l'utilisation de la mémoire NVIDIA dépasse le seuil d'alerte du rendu NVIDIA ou redevient inférieure au seuil critique de NVIDIA.
Disponibilité du service critique	Se produit lorsqu'un service de serveur s'arrête de fonctionner. Il n'existe aucune valeur de seuil pour cet événement.
Disponibilité du service normale	Se produit lorsque l'état d'un service de serveur se remet à fonctionner. Il n'existe aucune valeur de seuil pour cet événement.

Moniteur système - Caméra :

Événement	Description
FPS en direct critique	Se produit lorsque le FPS en direct devient inférieur au seuil critique de FPS en direct.
FPS en direct normal	Se produit lorsque le FPS en direct dépasse le seuil d'alerte de FPS en direct.
Avertissement FPS en direct	Se produit lorsque le FPS)en direct devient inférieur au seuil critique de FPS en direct ou dépasse le seuil critique de celui-ci.
FPS d'enregistrement critique	Se produit lorsque le FPS d'enregistrement devient inférieur au seuil critique du FPS d'enregistrement.
FPS d'enregistrement normal	Se produit lorsque le FPS d'enregistrement dépasse le seuil d'alerte du FPS d'enregistrement.
Avertissement FPS d'enregistrement	Se produit lorsque le FPS en direct devient inférieure au seuil d'alerte FPS d'enregistrement ou dépasse le seuil critique de FPS d'enregistrement.
Espace utilisé critique	Se produit lorsque l'espace utilisé pour les enregistrements par une caméra spécifique dépasse le seuil critique d'espace utilisé.
Espace utilisé normal	Se produit lorsque l'espace utilisé pour les enregistrements par une caméra spécifique redevient inférieur au seuil d'alerte d'espace utilisé.
Avertissement d'espace utilisé	Se produit lorsque l'espace utilisé pour les enregistrements par une caméra spécifique dépasse le seuil d'alerte d'espace utilisé ou devient inférieur au seuil critique d'espace utilisé.

Moniteur système - Disque :

Événement	Description
Espace libre critique	Se produit lorsque l'espace de stockage utilisé dépasse le seuil critique d'espace

Événement	Description
	libre.
Espace libre normal	Se produit lorsque l'espace de stockage utilisé devient inférieur au seuil critique d'espace libre.
Avertissement d'espace libre	Se produit lorsque l'espace de stockage utilisé dépasse le seuil d'alerte d'espace utilisé ou redevient inférieur au seuil critique d'espace libre.

Moniteur système - Stockage :

Événement	Description
Durée de rétention critique	Se produit lorsque le système prédit que l'espace libre de stockage sera plus vite consommé que la valeur de seuil critique du temps de rétention. Par exemple, lorsque les données des flux vidéo consomment l'espace de stockage plus rapidement que prévu.
Durée de rétention normale	Se produit lorsque le système prédit que l'espace libre de stockage sera plus vite consommé que la valeur de seuil d'alerte du temps de rétention. Par exemple lorsque les données des flux vidéo consomment l'espace de stockage à la vitesse prévue.
Avertissement de durée de rétention	Se produit lorsque le système prédit que l'espace de stockage sera plus vite consommé que la valeur de seuil d'alerte du temps de rétention ou moins rapidement que la valeur de seuil critique du temps de rétention. Par exemple, lorsque les données des flux vidéo consomment l'espace de stockage plus rapidement que prévu en raison d'un nombre de mouvements accrus détectés par les caméras configurées pour passer en mode enregistrement en cas de détection de mouvement.

Autre :

Événement	Description
Échec d'activation automatique des licences	Se produit lorsque l'activation automatique des licences a échoué. Il n'existe aucune valeur de seuil pour cet événement.
Modification du mot de passe programmée commencée	A lieu lorsque démarre la programmation du changement du mot de passe.
Modification du mot de passe programmée effectuée avec succès	Se produit lorsqu'une programmation du changement du mot de passe s'achève sans erreur.
Modification du mot de passe programmée effectuée avec des erreurs	Se produit lorsqu'une programmation du changement du mot de passe s'achève avec des erreurs.

Les événements provenant des extensions et des intégrations XProtect :

Les événements provenant des extensions et des intégrations XProtect peuvent être utilisés dans le système de règles, par exemple :

- Les événements analytiques peuvent également être utilisés dans le système de règles

Actions et actions d'arrêt

Un ensemble d'actions et d'actions d'arrêt sont disponibles pour créer des règles dans l'assistant **Gérer les règles**. Vous pouvez disposer d'un plus grand nombre d'actions si l'installation de votre système utilise des extensions XProtect ou des modules d'extension spécifiques au fournisseur. Pour chaque type d'action, des informations quant à l'action d'arrêt sont répertoriées si nécessaire.

Assistant Gérer les règles

Action	Description
Démarrer l'enregistrement sur <périphériques>	Commencez l'enregistrement et la sauvegarde des données dans la base de données des périphériques choisis.

Action	Description
	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 les appareils sur lesquels 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-enregistrement pour les périphériques 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 <périphériques>	Lancez 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 sont 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 automatiquement à spécifier l'action d'arrêt : **Arrêter un flux**. Vous pouvez également indiquer d'autres actions d'arrêt. Utiliser l'action d'arrêt obligatoire **Arrêter un flux** pour arrêter un flux

Action	Description
	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. ⚠ 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 <préréglages>	Définit le XProtect Smart Wall sur un préréglage sélectionné. Spécifiez le préréglage sur l'onglet **Préréglages 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 <moniteur> 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 <moniteur> 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

Action	Description
	temps.
Supprimer <caméras> du moniteur <moniteur> <Smart Wall>	Arrêtez 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.
Définir la fluidité d'image en direct sur <périphériques>	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 de la sélection de 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 <périphériques>	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 quelles 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

Action	Description
	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 <périphériques>	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**. Lors de la sélection de 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 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 <périphérique> à l'aide de <profil> avec priorité PTZ <priorité>	Démarre 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.

Action	Description
	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 = 1 000 • Bas = 2 000 • Moyen = 3 000 • Élevé = 4 000 • Très élevé = 5 000 Lors de la sélection de 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	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

Action	Description
<périphériques>	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 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 <préréglages> pour <périphérique> avec la priorité PTZ <priorité>	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.

Action	Description
	 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 <périphériques> avec la priorité PTZ <priorité>	Déplace une caméra ou plusieurs caméras spécifiques sur leurs positions prédéfinies par défaut respectives, toutefois, toujours conformément à la priorité. Lors de la sélection de 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 <état>	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.

Action	Description
	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 <périphérique>	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. Les paramètres du signet sont contrôlés à partir de la boîte de dialogue **Options**. Lors de la sélection de 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.
Lire le <message> audio sur les <périphériques> en <priorité>	Lit un message audio sur des périphériques sélectionnés qui sont déclenchés par un événement. Les périphériques sont surtout des haut-parleurs ou des caméras. Ce type d’action vous impose de charger le message dans le système sur l’onglet **Outils** > **Options** > **Messages audio**. Vous pouvez créer davantage de règles pour le même événement et envoyer des messages différents à chaque périphérique, mais toujours selon une priorité. Les priorités qui contrôlent la séquence sont celles qui s’appliquent à la règle et au périphérique pour un rôle sur l’onglet **Audio** : • Si un message est lu et qu’un autre message ayant la même priorité est envoyé au même haut-parleur, le premier message se termine, puis le second commence • Si un message est lu et qu’un autre message ayant une priorité plus élevée est envoyé au même haut-parleur, le premier message sera interrompu et le second commence immédiatement

Action	Description
Envoyer la notification à <profil>	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. 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 <entrée au journal>	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 <périphériques>	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 souhaités, et les périphériques sur lesquels les démarrer. Ce type d'action exige que vous ayez au moins un ou plusieurs modules d'extension installés sur votre système.

Action	Description
	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 <périphériques>	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.
Appliquer les nouveaux paramètres sur <périphériques>	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.

Action	Description
Définir Matrix pour afficher <périphériques>	Fait apparaître la vidéo de caméras sélectionnées sur un ordinateur pouvant afficher de la vidéo déclenchée par Matrix, tel qu'un ordinateur sur lequel vous avez installé XProtect Smart Client. Lors de la sélection de 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. Dans le cadre 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 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 généré automatiquement 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.

Action	Description
	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.
Rappeler et sauvegarder les enregistrements à distance depuis les <périphériques>	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. 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 <heure de début / de fin> et <périphériques>	Récupère et stocke les enregistrements à distance de périphériques choisis (qui prennent en charge l'enregistrement local) au cours d'une période spécifiée. 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.
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.

Action	Description
Déclencher <événement défini par l'utilisateur> 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 l'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.
Afficher <notification de demande d'accès>	Vous permet d'accéder aux notifications de demande d'accès 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 des caméras de contrôle d'accès connexes. Ce type d'action exige que vous ayez au moins un module d'extension 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.
Modifier le mot de passe sur les périphériques matériel	Change le mot de passe sur les périphériques sélectionnés pour un mot de passe généré aléatoirement en fonction des exigences du mot de passe pour le périphérique concerné. Pour un liste des périphériques pris en charge, voir Trouver un matériel. Cette action est seulement disponible lorsque vous configurez une règle qui utilise le type de règle **Effectuer une action sur un <recurring time>**. Les événements suivants sont disponibles pour l'action :

Action	Description
	• Modification du mot de passe programmée commencée on page 533 • Modification du mot de passe programmée effectuée avec succès on page 533 • Modification du mot de passe programmée effectuée avec des erreurs on page 533 Ce type d'action n'a pas d'action d'arrêt. Vous pouvez consulter la progression de cette action dans le nœud **Tâches actuelles**. Pour plus d'informations, voir Afficher les tâches en cours sur les serveurs d'enregistrement on page 315. Pour consulter les résultats de l'action - allez sur le nœud **Journaux du serveur**, dans l'onglet **Journaux du système**. Pour plus d'informations, voir Onglet Journaux de serveurs (options) on page 419. Pour plus d'informations, voir Journaux système (onglet).

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 test de l'événement analytique**. Solution/explication : Enregistrez 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

Condition	Description	Messages d’erreur et solutions
		cochez la case **Activé**.
Adresse permise	L’adresse IP ou 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** :

Message d’erreur	Solution
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 Event Server.
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	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

Message d’erreur	Solution
du serveur d’événements	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 Event Server 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	Le plus probable est que votre machine ne figure pas dans la liste des d’adresses IP ou noms d’hôtes autorisés.
Erreur interne dans le serveur d’événements	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.

Événements génériques et sources de données (propriétés)

> Cette fonctionnalité fonctionne uniquement si le serveur d'événements XProtect est installé.

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 `(User001 OR Door053) AND Sunday` 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 `User001` ou `Door053`, puis il analyse les résultats pour voir quels paquets contiennent également le mot `Sunday`. • `AND` : Avec un opérateur `AND`, vous indiquez que les termes des deux côtés de l'opérateur `AND` doivent être présents **Exemple** : Les critères de recherche `User001 AND Door053 AND Sunday` ne renvoient un résultat que si les termes `User001`, `Door053` et `Sunday` sont inclus dans votre expression. Il ne suffit pas qu'un ou deux des termes soient présents. Plus vous combinez de termes avec AND, moins vous obtenez de résultats. • `OR` : Avec un opérateur `OR`, vous indiquez que l'un ou l'autre terme doit être présent **Exemple** : Les critères de recherche `"User001" OR "Door053" OR "Sunday"` renvoient tous les résultats contenant `User001`, `Door053` ou `Sunday`. Plus vous combinez de termes avec `OR`, plus vous obtenez de résultats.

Composant	Exigences
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 `User001` et `Door053`, l'événement est déclenché si le paquet reçu contient les termes `User001` et `Door053` et `Sunday` car vos deux termes requis sont contenus dans le paquet reçu • **Correspondance** : 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 **Correspondance** à **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 élevée) et 999999 (priorité la plus faible). 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**.

Webhooks (nœud Règles et Événements)

Dans le nœud **Webhooks**, vous pouvez créer, modifier et supprimer des points de terminaison de webhook.

Les champs suivants sont disponibles lors de la création et de la modification de webhooks :

Champ	Description
Nom	Saisissez un nom unique pour le point de terminaison webhook. Le nom de webhook ne peut être vide.
Adresse	Le URL du serveur Web ou de l'application auquel vous souhaitez envoyer des données d'événement. Si le URL du serveur Web est mis à jour, vous devez mettre à jour l'URL du webhook dans le nœud webhook. L'utilisation de HTTP via des réseaux non sécurisés (comme l'Internet ouvert) expose tous les événements en texte brut.
Jeton	Saisissez un jeton utilisé pour sécuriser la communication avec d'autres applications en validant la source du POST HTTP. L'utilisation d'un jeton pour sécuriser la communication est facultative mais recommandée.
Version de l'API	La version du plug-in webhook et de l'API utilisés pour la fonctionnalité webhook.

Noeud Sécurité

Rôles (noeud Sécurité)

Onglet Info (rôles)

> Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Dans l'onglet **Infos** d'un rôle, vous pouvez modifier les paramètres suivants :

Nom	Description
Nom	Saisissez un nom pour le rôle.
Description	Saisissez une description pour le rôle.
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.
Profil de verrouillage des preuves	Sélectionnez un profil de protection 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(e) automatiquement. Vous ne pouvez pas appliquer ceci au rôle d'**Administrateurs** par défaut.
Autoriser la connexion au Smart Client	Cochez la case pour permettre aux utilisateurs associés à ce rôle de se connecter au XProtect Smart Client. L'accès à Smart Client n'est pas autorisé par défaut. Décochez la case pour refuser l'accès au XProtect Smart Client.
Autoriser la	Cochez la case pour permettre aux utilisateurs associés à ce rôle de se

Nom	Description
connexion au client XProtect Mobile	connecter au client XProtect Mobile. L'accès au client XProtect Mobile n'est pas autorisé par défaut. Décochez la case pour refuser l'accès au client XProtect Mobile.
Autoriser la connexion au XProtect Web Client	Cochez la case pour permettre aux utilisateurs associés à ce rôle de se connecter au XProtect Web Client. L'accès à XProtect Web Client n'est pas autorisé par défaut. Décochez la case pour refuser l'accès au XProtect Web Client.
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 un responsable. Pour permettre aux administrateurs d'autoriser des utilisateurs, configurez l'autorisation **Autoriser les 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 aux rôles (voir Assigner et supprimer des utilisateurs et groupes aux/des rôles on page 310). Vous pouvez assigner des utilisateurs et de groupes Windows ou des utilisateurs basiques (voir Utilisateurs (explications) on page 72).

IDP externe (rôles)

Dans l'onglet **IDP externe**, vous pouvez afficher les revendications existantes et ajouter de nouvelles revendications pour les rôles.

Nom	Description
IDP externe	Le nom de l'IDP externe.
Nom de la revendication	Une variable qui est définie dans l'IDP externe.
Valeur de la revendication	La valeur de la demande, comme un nom de groupe, qui peut être utilisée pour affecter le rôle approprié à l'utilisateur.

Onglet Sécurité globale (rôles)

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Dans l'onglet **Sécurité globale**, vous pouvez configurer les autorisations globales des rôles. Pour chaque composant disponible dans votre système, définissez des autorisations d'accès pour les rôles en configurant **Autoriser** ou **Refuser**. Lorsqu'un rôle n'a pas accès à un composant, celui-ci n'est pas visible dans l'onglet **Sécurité globale** pour l'utilisateur dans ce rôle.

Vous pouvez définir plus d'autorisations d'accès pour XProtect Corporate que les autres produits VMS XProtect. Cela tient au fait que vous pouvez seulement configurer des autorisations d'administrateur différentes dans XProtect Corporate, tandis que vous pouvez configurer les autorisations globales pour un rôle qui utilise un client XProtect Smart Client, XProtect Web Client ou XProtect Mobile dans tous les produits.

Les paramètres de sécurité globaux s'appliquent uniquement au site actuel.

Si vous associez un utilisateur à plusieurs rôles et que vous sélectionnez **Refuser** pour un paramètre de sécurité pour un rôle et **Autoriser** pour un autre, l'autorisation **Refuser** prime sur l'autorisation **Autoriser**.

Dans ce qui suit, les descriptions présentent ce qui se produit au niveau de chaque autorisation individuelle pour les différents composants du système si vous sélectionnez **Autoriser** pour le rôle pertinent. Si vous utilisez XProtect Corporate, vous pouvez voir quels sont les paramètres disponibles **uniquement** pour votre système 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**, 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 autorisations que vous pouvez configurer par l'intermédiaire des MIP SDK.

> Si vous souhaitez échanger votre licence de base XProtect Corporate contre une licence de l'un des autres produits, assurez-vous de retirer toutes les autorisations de sécurité disponibles pour XProtect Corporate uniquement. Si vous ne supprimez pas ces autorisations, vous ne pourrez pas terminer l'échange.

Serveur de gestion

> Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Connecter	Permet aux utilisateurs de se connecter au Management Server. Cette permission est activée par défaut. Vous pouvez temporairement refuser une permission de connexion de rôles à des fins de maintenance puis réautoriser l'accès au système. **Cette permission doit être sélectionnée afin d'autoriser l'accès au système.**

Autorisation de sécurité	Description
Lire	 Cette autorisation est une autorisation administrative hautement réservée, qui autorise des droits d'accès significatifs au VMS XProtect, dont l'accès à des données sensibles, telles que les identifiants de connexion configurés dans le système. Active l'autorisation permettant d'accéder à un large éventail de fonctionnalités, y compris : • Se connecter avec le Management Client • Liste des tâches actuelles • Journaux de serveurs Il permet également d'accéder à : • Services de connexion à distance • Profils Smart Client • Profils Management Client • Matrix • Profils de temps • Serveurs enregistrés et API d'enregistrement de service Cette autorisation révèle également des informations sensibles au client : • Les identifiants de connexion pour les IDP externes configurés • Les identifiants de connexion, adresses IP et toute autre information de l'ensemble des caméras dans le VMS XProtect • Les identifiants de connexion du serveur de messagerie configuré • Les identifiants de connexion des Matrix configurés • Les identifiants de connexion configurés des fonctionnalités Milestone Interconnect • Les identifiants de connexion configurés de l'activation des licences Cette autorisation ne révèle pas les identifiants de connexion des utilisateurs du VMS

Autorisation de sécurité	Description
	XProtect. Cela comprend les utilisateurs basiques, les utilisateurs Windows ainsi que les utilisateurs d'IDP externes.
Modifier	Active l'autorisation permettant 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 éléments suivants : • Services de connexion à distance • Groupes de périphériques • Matrix • Profils de temps • Profils de notification • Serveurs enregistrés  Active l'autorisation permettant de configurer les plages IP locales lors de la configuration du réseau sur le serveur d'enregistrement.
État API	Active l'autorisation permettant d'exécuter des demandes concernant l'état API situé sur le serveur d'enregistrement. Cela signifie que le rôle pour lequel cette autorisation est activée dispose d'un accès suffisant pour lire l'état des éléments situés sur le serveur d'enregistrement.
Hiérarchie des sites fédérés	Active l'autorisation permettant d'ajouter ou de détacher le site actuel à d'autres sites dans une hiérarchie de sites fédérée.  Si vous autorisez uniquement l'accès à un site enfant, l'utilisateur peut toujours le connecter au site parent.
Sauvegarde de	Active l'autorisation permettant de créer des sauvegardes de la configuration du

Autorisation de sécurité	Description
configuration	système à l'aide de la fonction de sauvegarde et de restauration du système.
Autoriser des utilisateurs	Active l'autorisation permettant d'autoriser les 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 l'autorisation permettant de gérer des autorisations pour le serveur de gestion. Permet également aux utilisateurs de créer, de supprimer et de modifier les fonctionnalités suivantes : • Rôles • Utilisateurs basiques • Profils Smart Client • Profils Management Client

Serveurs d'enregistrement

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Modifier	Active l'autorisation permettant de modifier des propriétés sur les serveurs d'enregistrement, sauf pour les paramètres de configuration du réseau qui nécessitent

Autorisation de sécurité	Description
	une autorisation de modification sur le serveur de gestion.
Supprimer	Active l'autorisation permettant de supprimer 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 périphériques 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 l'autorisation permettant d'ajouter du matériel sur les serveurs d'enregistrement.
Gérer le stockage	Active l'autorisation permettant d'administrer 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.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité pour des serveurs d'enregistrement.

Serveurs de basculement

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant d'accéder aux serveurs de basculement dans le Management Client et de les consulter.
Modifier	Active l'autorisation permettant de créer, de mettre à jour, de supprimer, de déplacer et d'activer ou de désactiver les serveurs de basculement dans le Management Client.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité pour les serveurs de basculement.

Serveurs Mobile

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant d'accéder aux serveurs de basculement dans le Management Client et de les consulter.
Modifier	Active l'autorisation permettant de modifier et de supprimer des serveurs mobiles dans le Management Client.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité pour les serveurs mobiles.

Matériel

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Modifier	Active l'autorisation permettant de modifier des propriétés du matériel.
Supprimer	Active l'autorisation permettant de supprimer le matériel. Si un des dispositifs matériels contient des preuves verrouillées, vous pouvez uniquement supprimer le matériel lorsque le serveur d'enregistrement est hors ligne.
Commandes du gestionnaire	Active l'autorisation permettant d'envoyer des commandes spécifiques aux pilotes et par conséquent, de contrôler les fonctionnalités et la configuration sur le périphérique proprement dit. L'autorisation **Commandes du pilote** est destinée à des plug-ins MIP spécialement développés dans les clients uniquement. Il ne contrôle pas les tâches de configuration standard.
Voir les mots de passe	Active l'autorisation permettant d'afficher les mots de passe sur les périphériques matériels dans la boîte de dialogue **Modifier le matériel**.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité pour le matériel.

Caméras

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant de visualiser les caméras dans les clients et dans le Management Client.
Modifier	Active l'autorisation permettant de modifier les propriétés pour les caméras dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver une caméra.
Visualisation en direct	Active l'autorisation permettant de consulter des vidéos en direct à partir des caméras dans les clients et dans le Management Client.
Voir des vues en direct restreintes	Active l'autorisation permettant de consulter des vidéos restreintes en direct à partir des caméras dans les clients et dans le Management Client.
Lecture	Active l'autorisation permettant de lire des vidéos enregistrées à partir des caméras dans tous les clients.
Lire des enregistrements restreints	Active l'autorisation permettant de lire des vidéos restreintes enregistrées à partir des caméras dans tous les clients.
Rappeler les enregistrements à distance	Active l'autorisation permettant de récupérer les enregistrements dans les clients à partir des caméras se trouvant sur des sites distants ou sur le stockage externe des caméras.
Lire les séquences	Active l'autorisation permettant de lire les informations séquentielles liées à la lecture de vidéo enregistrée dans les clients, par exemple.

Autorisation de sécurité	Description
Recherche avancée	Active l’autorisation permettant de lire la fonction de recherche avancée dans les clients.
Exporter	Active l’autorisation permettant d’exporter des enregistrements à partir des clients.
Créer des signets	Active l’autorisation permettant de créer des signets dans des vidéos enregistrées et en direct dans les clients.
Lire les signets	Active l’autorisation permettant de rechercher et de lire les détails de signet dans les clients.
Modifier les signets	Active l’autorisation permettant de modifier des signets dans les clients.
Supprimer des signets	Active l’autorisation permettant de supprimer des signets dans les clients.
Créer et étendre la protection des preuves	Active l’autorisation permettant de créer et d’étendre la protection des preuves dans les clients.
Lire le verrouillage des preuves	Active l’autorisation permettant de rechercher et de lire la protection de preuves dans les clients.
Supprimer et réduire le verrouillage des preuves	Active l’autorisation permettant de supprimer ou de réduire la protection de preuves dans les clients.
Créer et élargir des restrictions en direct et de lecture	Active l’autorisation permettant de créer et détendre la restriction dans les clients.
Lire des restrictions en direct et de lecture	Active l’autorisation d’affichage de la liste des restrictions existantes dans les clients.
Supprimer et réduire des restrictions en direct et de lecture	Active l’autorisation permettant de supprimer et réduire les restrictions dans les clients.

Autorisation de sécurité	Description
Démarrer l'enregistrement manuel	Active l'autorisation permettant de lancer l'enregistrement vidéo manuel dans les clients.
Arrêter l'enregistrement manuel	Active l'autorisation permettant d'arrêter l'enregistrement vidéo manuel dans les clients.
Commandes AUX	Active l'autorisation permettant 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.
Manuel PTZ	Active l'autorisation permettant d'utiliser 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 l'autorisation permettant de déplacer des caméras PTZ vers des positions prédéfinies, de démarrer et d'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 l'autorisation **PTZ manuel**.
Gérer les positions prédéfinies PTZ ou les profils de patrouille	Active l'autorisation permettant d'ajouter, de modifier et de supprimer les préréglages PTZ 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 l'autorisation **PTZ manuel**.
Verrouiller/Déverrouiller des positions prédéfinies PTZ	Active l'autorisation permettant de bloquer et de débloquer les préréglages PTZ dans le Management Client. Ceci empêche ou autorise d'autres utilisateurs à changer les positions prédéfinies dans les clients et dans le Management Client.
Réserver des sessions PTZ	Active l'autorisation permettant de paramétrer les caméras PTZ en mode de session réservée dans les clients et dans le

Autorisation de sécurité	Description
	Management Client. Dans une session PTZ réservée, d'autres utilisateurs dotés d'une priorité PTZ plus élevée ne peuvent pas prendre le contrôle. Pour autoriser ce rôle à utiliser d'autres fonctions PTZ sur la caméra, activez l'autorisation **PTZ manuel**.
Libérer les sessions PTZ	Active l'autorisation permettant de libérer les sessions PTZ d'autres utilisateurs du Management Client. Vous pouvez toujours libérer vos propres sessions PTZ, même sans cette permission.
Supprimer des enregistrements	Active l'autorisation permettant de supprimer des enregistrements vidéo stockés à partir du système via le Management Client.
Enlever les masques de confidentialité	Active l'autorisation permettant de lever provisoirement les masques de confidentialité dans XProtect Smart Client. Il active également la permission visant à autoriser d'autres utilisateurs de XProtect Smart Client à lever les masques de confidentialité. Le levage des masques de confidentialité s'applique uniquement aux masques de confidentialité configurés en tant que masques de confidentialité relevables dans Management Client.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité pour la caméra dans le Management Client.

Microphones

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l’autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l’autorisation permettant de visualiser les microphones dans les clients et dans le Management Client.
Modifier	Active l’autorisation permettant de modifier les propriétés des microphones dans le Management Client. Il permet également aux utilisateurs d’activer ou de désactiver des microphones.
Écoute en direct	Active l’autorisation permettant d’écouter l’audio en direct à partir des haut-parleurs dans les clients et dans le Management Client.
Écouter de l’audio restreint en direct	Active l’autorisation permettant d’écouter l’audio restreint en direct à partir des haut-parleurs dans les clients et dans le Management Client.
Lecture	Active l’autorisation permettant de lire l’audio enregistrée à partir des microphones dans les clients.
Lire des enregistrements restreints	Active l’autorisation permettant de lire l’audio restreint enregistré à partir de microphones dans les clients.
Rappeler les enregistrements à distance	Active l’autorisation permettant 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	Permet à l’autorisation de lire les informations de séquence liées, par exemple, à l’onglet **Lecture** dans les clients.
Exporter	Active l’autorisation permettant d’exporter des enregistrements à partir des clients.

Autorisation de sécurité	Description
Créer des signets	Active l’autorisation permettant de créer des signets dans les clients.
Lire les signets	Active l’autorisation permettant de rechercher et de lire les détails de signet dans les clients.
Modifier les signets	Active l’autorisation permettant de modifier des signets dans les clients.
Supprimer des signets	Active l’autorisation permettant de supprimer des signets dans les clients.
Créer et étendre la protection des preuves	Active l’autorisation permettant de créer et d’étendre la protection de preuves dans les clients.
Lire le verrouillage des preuves	Active l’autorisation permettant de rechercher et de lire les détails de la protection de preuves dans les clients.
Supprimer et réduire le verrouillage des preuves	Active l’autorisation permettant de supprimer ou de réduire la protection de preuves dans les clients.
Créer et élargir des restrictions en direct et de lecture	Active l’autorisation permettant de créer et détendre la restriction sur les microphones dans les clients.
Lire des restrictions en direct et de lecture	Active l’autorisation d’affichage de la liste des restrictions existantes sur les microphones dans les clients.
Supprimer et réduire des restrictions en direct et de lecture	Active l’autorisation permettant de supprimer et réduire les restrictions sur les microphones dans les clients.

Autorisation de sécurité	Description
Démarrer l'enregistrement manuel	Active l'autorisation permettant de lancer l'enregistrement audio manuel dans les clients.
Arrêter l'enregistrement manuel	Active l'autorisation permettant d'arrêter l'enregistrement audio manuel dans les clients.
Supprimer des enregistrements	Active l'autorisation permettant de supprimer les enregistrements stockés du système.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité dans le Management Client pour les microphones.

Haut-parleurs

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant de visualiser les haut-parleurs dans les clients et dans le Management Client.
Modifier	Active l'autorisation permettant de modifier les propriétés des haut-parleurs dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver des

Autorisation de sécurité	Description
	haut-parleurs.
Écoute en direct	Active l’autorisation permettant d’écouter l’audio en direct à partir des haut-parleurs dans les clients et dans le Management Client.
Écouter de l’audio restreint en direct	Active l’autorisation permettant d’écouter l’audio restreint en direct à partir des haut-parleurs dans les clients et dans le Management Client.
Parole	Active l’autorisation permettant de parler dans les haut-parleurs au sein des clients.
Lecture	Active l’autorisation permettant de lire l’audio enregistré à partir des haut-parleurs dans les clients.
Lire des enregistrements restreints	Active l’autorisation permettant de lire l’audio enregistré à partir des haut-parleurs dans les clients.
Rappeler les enregistrements à distance	Active l’autorisation permettant de récupérer les enregistrements dans les clients à partir des haut-parleurs se trouvant sur des sites distants ou sur le stockage externe des caméras.
Lire les séquences	Active l’autorisation permettant d’utiliser la fonctionnalité Séquences tout en parcourant l’audio enregistré à partir des haut-parleurs dans les clients.
Exporter	Active l’autorisation permettant d’exporter l’audio enregistré à partir des haut-parleurs dans les clients.
Créer des signets	Active l’autorisation permettant de créer des signets dans les clients.
Lire les signets	Active l’autorisation permettant de rechercher et de lire les détails de signet dans les clients.

Autorisation de sécurité	Description
Modifier les signets	Active l’autorisation permettant de modifier des signets dans les clients.
Supprimer des signets	Active l’autorisation permettant de supprimer des signets dans les clients.
Créer et étendre la protection des preuves	Active l’autorisation permettant de créer ou d’étendre la protection de preuves pour protéger l’audio enregistré dans les clients.
Lire le verrouillage des preuves	Active l’autorisation permettant de visualiser l’audio enregistré protégé par la protection de preuves dans les clients.
Supprimer et réduire le verrouillage des preuves	Active l’autorisation permettant de supprimer ou de réduire la protection de preuves sur l’audio protégé dans les clients.
Créer et élargir des restrictions en direct et de lecture	Active l’autorisation permettant de créer et détendre la restriction sur les haut-parleurs dans les clients.
Lire des restrictions en direct et de lecture	Active l’autorisation d’affichage de la liste des restrictions existantes sur les haut-parleurs dans les clients.
Supprimer et réduire des restrictions en direct et de lecture	Active l’autorisation permettant de supprimer et réduire les restrictions sur les haut-parleurs dans les clients.
Démarrer l’enregistrement manuel	Active l’autorisation permettant de lancer l’enregistrement audio manuel dans les clients.
Arrêter	Active l’autorisation permettant d’arrêter l’enregistrement

Autorisation de sécurité	Description
l'enregistrement manuel	audio manuel dans les clients.
Supprimer des enregistrements	Active l'autorisation permettant de supprimer les enregistrements stockés du système.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité dans le Management Client pour les haut-parleurs.

Métadonnées

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant de recevoir des métadonnées dans les clients.
Modifier	Active l'autorisation permettant de modifier les propriétés des métadonnées dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver des périphériques de métadonnées.
En direct	Active l'autorisation permettant de recevoir des métadonnées en direct à partir des caméras dans les clients.

Autorisation de sécurité	Description
Voir des vues en direct restreintes	Active l'autorisation permettant de recevoir des métadonnées restreintes en direct à partir des caméras dans les clients.
Lecture	Active l'autorisation permettant de relire les données enregistrées à partir des périphériques à métadonnées dans les clients.
Lire des enregistrements restreints	Active l'autorisation permettant de relire les données restreintes enregistrées à partir des périphériques à métadonnées dans les clients.
Rappeler les enregistrements à distance	Active l'autorisation permettant de rappeler les enregistrements dans les clients à partir des périphériques de métadonnées se trouvant sur des sites distants ou sur le stockage externe des caméras.
Lire les séquences	Permet à l'autorisation de lire les informations de séquence liées, par exemple, à l'onglet **Lecture** dans les clients.
Exporter	Active l'autorisation permettant d'exporter des enregistrements dans les clients.
Créer et étendre la protection des preuves	Active l'autorisation permettant de créer la protection de preuves dans les clients.
Lire le verrouillage des preuves	Active l'autorisation permettant de visualiser la protection de preuves dans les clients.
Supprimer et réduire le verrouillage des preuves	Active l'autorisation permettant de supprimer ou de réduire la protection de preuves dans les clients.
Créer et élargir des restrictions en direct et de lecture	Active l'autorisation permettant de créer et détendre la restriction sur les métadonnées dans les clients.

Autorisation de sécurité	Description
Lire des restrictions en direct et de lecture	Active l'autorisation d'affichage de la liste des restrictions existantes sur les métadonnées dans les clients.
Supprimer et réduire des restrictions en direct et de lecture	Active l'autorisation permettant de supprimer et réduire les restrictions sur les métadonnées dans les clients.
Démarrer l'enregistrement manuel	Active l'autorisation permettant de lancer l'enregistrement manuel des métadonnées dans les clients.
Arrêter l'enregistrement manuel	Active l'autorisation permettant d'arrêter l'enregistrement audio manuel dans les clients.
Supprimer des enregistrements	Active l'autorisation permettant de supprimer les enregistrements stockés du système.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité dans le Management Client pour les métadonnées.

Entrée

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant de visualiser les périphériques d'entrée dans les clients et dans le Management Client.
Modifier	Active l'autorisation permettant de modifier les propriétés des périphériques d'entrée dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver un périphérique d'entrée.
Gérer la sécurité	Active l'autorisation de gérer les autorisations de sécurité dans le Management Client pour les périphériques d'entrée.

Sortie

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant de visualiser les périphériques de sortie dans les clients.
Modifier	Active l'autorisation permettant de modifier les propriétés des périphériques de sortie dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver un périphérique de sortie.

Autorisation de sécurité	Description
Activer	Active l'autorisation permettant d'activer les sorties dans les clients.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité des périphériques de sortie dans le Management Client.

Smart Wall

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation de gérer toutes les autorisations de sécurité sur XProtect Management Client.
Lire	Active l'autorisation de visualisation d'un mur vidéo dans XProtect Smart Client.
Modifier	Active l'autorisation de modifier des propriétés pour la définition de Smart Wall dans XProtect Management Client.
Supprimer	Active l'autorisation permettant de supprimer les définitions Smart Wall dans XProtect Management Client.
Opérer	Autorise l'autorisation d'activer et de modifier des définitions Smart Wall, par exemple pour modifier et activer des préréglages ou pour appliquer des caméras sur les vues dans XProtect Smart Client et dans XProtect Management Client. Vous pouvez associer **Opérer** avec des profils de temps qui définissent le moment où l'autorisation utilisateur s'applique.

Autorisation de sécurité	Description
Créer Smart Wall	Active l'autorisation de créer de nouvelles définitions de Smart Wall dans le XProtect Management Client.
Gérer la sécurité	Active l'autorisation de gérer les permissions de sécurité dans XProtect Management Client pour la définition de Smart Wall.
Lecture	Active l'autorisation de lecture de données enregistrées à partir d'un mur vidéo dans XProtect Smart Client. Vous pouvez associer **Lecture** avec des profils de temps qui définissent le moment où l'autorisation utilisateur s'applique.

Groupes de vues

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant de visualiser les groupes de vues dans les clients et dans le Management Client. Les groupes de vues sont créées dans le Management Client.
Modifier	Active l'autorisation permettant de modifier les propriétés sur le groupes de vues dans le Management Client.

Autorisation de sécurité	Description
Supprimer	Active l'autorisation permettant de supprimer des groupes de vues dans le Management Client.
Opérer	Active l'autorisation permettant d'utiliser des groupes de vue dans XProtect Smart Client, c'est-à-dire, de créer et de supprimer des sous-groupes et des vues.
Créer un groupe de vues	Active l'autorisation permettant de créer des groupes de vues dans le Management Client.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité des groupes de vue dans le Management Client.

Événements définis par l'utilisateur

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant de visualiser des événements définis par les utilisateurs dans les clients.
Modifier	Active l'autorisation permettant de modifier les propriétés sur des événements définis par l'utilisateur dans le Management Client.
Supprimer	Active l'autorisation permettant de supprimer des événements définis par l'utilisateur dans le Management Client.

Autorisation de sécurité	Description
Déclencher	Active l'autorisation permettant de déclencher des événements définis par l'utilisateur dans les clients.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité des événements définis par l'utilisateur dans le Management Client.
Créer un événement défini par l'utilisateur	Active l'autorisation permettant de créer des événements définis par l'utilisateur dans le Management Client.

Evénement analytique

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant de visualiser des événements analytiques dans le Management Client.
Modifier	Active l'autorisation permettant de modifier des propriétés pour les événements analytiques dans le Management Client.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité des événements analytiques dans le Management Client.

Événements génériques

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant de visualiser des événements génériques dans les clients et dans le Management Client.
Modifier	Active l'autorisation permettant de modifier des propriétés pour les événements génériques dans le Management Client.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité dans le Management Client pour les événements génériques.

Matrix

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant de sélectionner et d'envoyer une vidéo au destinataire Matrix à partir des clients.
Modifier	Active l'autorisation permettant de modifier les propriétés d'un Matrix dans le Management Client.
Supprimer	Active l'autorisation permettant de supprimer un Matrix dans le Management Client.

Autorisation de sécurité	Description
Créer Matrix	Active l'autorisation permettant de créer un nouveau Matrix dans le Management Client.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité dans le Management Client pour tous les Matrix.

Règles

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant de visualiser des règles existantes dans le Management Client.
Modifier	Active l'autorisation permettant de modifier les propriétés des règles et de définir le 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 l'autorisation permettant de supprimer des règles du Management Client. Il requiert également que l'utilisateur dispose de permissions de lecture sur tous les périphériques affectés par la règle.
Créer une règle	Active l'autorisation permettant de créer des nouvelles règles dans le Management

Autorisation de sécurité	Description
	Client. Il requiert également que l'utilisateur dispose de permissions de lecture sur tous les périphériques affectés par la règle.
Gérer la sécurité	Active l'autorisation de gérer les permissions de sécurité dans le Management Client pour toutes les règles.

Sites

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant 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 l'autorisation permettant de gérer les autorisations de sécurité sur tous les sites.

Moniteur système

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant de visualiser les moniteurs système dans XProtect Smart Client.
Modifier	Active l'autorisation permettant de modifier les propriétés des moniteurs système dans le Management Client.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité de tous les moniteurs système dans le Management Client.

Alarmes

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Gestion	Active l'autorisation permettant de gérer des alarmes dans le Smart Client. Par

Autorisation de sécurité	Description
	exemple, modifier les priorités des alarmes, réaffecter des alarmes à d'autres utilisateurs, accuser réception des alarmes, modifier l'état d'alarme de plusieurs alarmes (par exemple de **Nouveau** à **Affecté**). Pour modifier les paramètres des alarmes, vous devez également disposer de l'autorisation **Modifier les paramètres des alarmes**. L'onglet **Alarmes et événements** de la boîte de dialogue **Options** n'apparaît que lorsque vous choisissez d'autoriser cette fonction.
Vue	Permet d'afficher l'onglet **Gestionnaire d'alarmes** dans XProtect Smart Client et de récupérer les alarmes et les paramètres d'alarme par le biais de l'API. Pour afficher les alarmes dans XProtect Smart Client, vous devez activer l'autorisation **Afficher** pour au moins une définition des alarmes. Par défaut, les alarmes provenant de solutions tierces sont affichées.
Désactiver alarmes	Active l'autorisation permettant de désactiver les alarmes.
Recevoir des notifications	Active l'autorisation permettant de recevoir des notifications sur les alarmes dans les clients XProtect Mobile et dans XProtect Web Client.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité des alarmes.
Modifier les paramètres de l'alarme	Active l'autorisation de modifier les définitions des alarmes, les états des alarmes, les catégories d'alarmes, les sons d'alarmes, la rétention des alarmes et la rétention des événements. Pour modifier les paramètres des alarmes, vous devez également disposer de l'autorisation **Gérer**.

Définitions des alarmes

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Vue	Active l'autorisation d'afficher les définitions des alarmes, les états des alarmes, les catégories d'alarmes, les sons d'alarmes, la rétention des alarmes et la rétention des événements.
Écrire	Active l'autorisation **Afficher**
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité pour les définitions d'alarmes.

Recherche de métadonnées

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l'autorisation permettant de visualiser la fonctionnalité **Utilisation des métadonnées** dans Management Client et ses paramètres connexes, mais sans activer l'autorisation de modifier les paramètres.
Modifier la configuration de la recherche de métadonnées	Active l'autorisation permettant d'activer ou de désactiver les catégories de recherche de métadonnées, par exemple, les métadonnées de personnes ou de véhicules dans le Management Client.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité pour les recherches de métadonnées.

Rechercher

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Lire des recherches publiques	Active l'autorisation permettant de visualiser et d'ouvrir les recherches publiques sauvegardées dans XProtect Smart Client.
Créer des recherches publiques	Active l'autorisation permettant de sauvegarder les recherches nouvellement configurées comme recherches publiques dans XProtect Smart Client.
Modifier des recherches publiques	Active l'autorisation permettant de modifier les détails ou la configuration des recherches publiques sauvegardées dans XProtect Smart Client, par exemple le nom, la description, les caméras et les catégories de recherche.
Supprimer des recherches publiques	Active l'autorisation permettant de supprimer les recherches publiques sauvegardées.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité de la recherche dans le Management Client.

Journaux des serveurs

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l’autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire les entrées du journal système	Active l’autorisation permettant d’afficher les entrées du journal système.
Lire les entrées du journal d’activité	Active l’autorisation permettant d’afficher les entrées du journal d’audit.
Lire les entrées du journal déclenchées par une règle	Active l’autorisation permettant d’afficher les entrées du journal déclenchées par une règle.
Lire la configuration du journal	Active l’autorisation permettant de lire les paramètres du journal dans **Outils** > **Options** > **Journaux du serveur**.
Mettre à jour la configuration du journal	Active l’autorisation permettant de modifier les paramètres du journal dans **Outils** > **Options** > **Journaux du serveur**.
Gérer la sécurité	Active l’autorisation permettant de gérer les autorisations de sécurité des alarmes.

Sources de transactions

Autorisation de sécurité	Description
Contrôle total	Active l’autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active l’autorisation permettant d’afficher les propriétés des sources de transaction dans le Management Client.
Modifier	Active l’autorisation permettant de modifier les propriétés des sources de transaction dans le Management Client.
Gérer la sécurité	Active l’autorisation permettant de gérer les autorisations de sécurité pour toutes les sources de transaction dans le Management Client.

Définitions des transactions

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Lire	Active la transaction permettant d'afficher les propriétés des définitions de transactions dans le Management Client.
Modifier	Active la transaction permettant de modifier les propriétés des définitions de transactions dans le Management Client.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité pour toutes les définitions de transaction dans le Management Client.

Contrôle d'accès

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Modifier	Active l'autorisation permettant de modifier les propriétés des systèmes de contrôle d'accès dans le Management Client.
Utiliser le contrôle d'accès	Permet à l'utilisateur d'utiliser les fonctions relatives au contrôle d'accès dans les clients.

Autorisation de sécurité	Description
Voir la liste des détenteurs de cartes	Permet à l'utilisateur d'afficher la liste des détenteurs de cartes sur l'onglet **Contrôle d'accès** dans les clients.
Recevoir des notifications	Permet à l'utilisateur de recevoir des notifications concernant les demandes d'accès dans les clients.
Gérer la sécurité	Active l'autorisation permettant de gérer les autorisations de sécurité de tous les systèmes de contrôle d'accès.

Floutage de confidentialité

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Gestion	Actuellement non utilisée.
Vue	Permet à l'utilisateur d'utiliser la fonctionnalité de floutage de confidentialité dans XProtect Smart Client.
Gérer la sécurité	Actuellement non utilisée.

Pense-bêtes

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Gestion	Permet à l'utilisateur de créer, de modifier et de supprimer des pense-bêtes dans XProtect Smart Client.
Vue	Permet à l'utilisateur de voir les pense-bêtes dans XProtect Smart Client.
Gérer la sécurité	Actuellement non utilisée.

Multipièce audio

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Gestion	Actuellement non utilisée.
Vue	Permet à l'utilisateur d'utiliser Multipièces Audio dans XProtect Smart Client.
Gérer la sécurité	Actuellement non utilisée.

Reconnaissance de plaque (LPR)

Si votre système s’exécute avec XProtect LPR, spécifiez les autorisations suivantes pour l’utilisateur :

Autorisation de sécurité	Description
Contrôle total	Active l’autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Afficher l’onglet de reconnaissance de plaque dans les applications clientes	Autorise l’utilisation des fonctionnalités XProtect LPR de XProtect Smart Client.
Gérer la reconnaissance de plaque	Autorise les opérations suivantes : • ajout, d’importation, modification, exportation et suppression des listes de correspondances dans le Management Client. • ajout et suppression de plaques d’immatriculation des listes de correspondances dans XProtect Smart Client. • suppression, désactivation et configuration des caméra de reconnaissance des plaques d’immatriculation existantes.
Afficher le nœud de reconnaissance de plaque dans Management Client	Autorise les opérations suivantes : • ajout, suppression et configuration de listes de correspondances ; • ajout, suppression et configuration des caméras de reconnaissance de plaque ; • ajout, suppression et configuration des serveurs de reconnaissance de plaque ; • ajout, suppression et configuration des alias du style de plaque d’immatriculation.
Gérer la sécurité	Active l’autorisation permettant de gérer les autorisations de sécurité de la reconnaissance de plaque dans le Management Client.

Webhooks

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

Autorisation de sécurité	Description
Contrôle total	Active l'autorisation permettant de gérer toutes les entrées de sécurité sur cette partie du système.
Modifier	Active l'autorisation permettant de modifier les propriétés des webhooks dans Management Client.
Lire	Active l'autorisation permettant d'afficher les propriétés des webhooks dans Management Client.
Gérer la sécurité	Active l'autorisation permettant de gérer les permissions de sécurité dans Management Client pour tous les webhooks.

Modules d'extension MIP

Au travers du MIP SDK, un vendeur tiers peut développer des modules d'extension personnalisés pour votre système, par exemple, l'intégration à des systèmes de contrôle d'accès externes ou similaires.

Onglet Périphériques (rôles)

Les fonctions disponibles dépendent du système que vous utilisez. Consultez la liste complète de fonctionnalités, qui est disponible sur la page de présentation du produit sur le site Web Milestone (https://www.milestonesys.com/products/software/xprotect-comparison/).

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 autorisations de 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. Vous pouvez également sélectionner les périphériques individuels dans le groupe de périphériques afin de vérifier exactement à quel périphérique l'autorisation appropriée s'applique.

Autorisations liées à la caméra

Spécifier les autorisations suivantes pour les caméras :

Nom	Description
Lire	La ou les caméra(s) sélectionnée(s) seront visibles dans les clients.
Visualisation en direct	Permet de visionner les vidéos de la ou des caméra(s) sélectionnée (s) en direct dans les clients. Pour XProtect Smart Client, il nécessite que l'autorisation d'afficher l'onglet **En direct** des clients ait été accordée au rôle. Cette autorisation est accordée dans le cadre des autorisations de l'application. Spécifiez le profil de temps ou conservez la valeur par défaut.
Voir des vues en direct restreintes	Permet de visionner les vidéos restreintes de la ou des caméra(s) sélectionnée(s) en direct dans les clients. Pour XProtect Smart Client, il nécessite que l'autorisation d'afficher l'onglet **En direct** ait été accordée au rôle. Cette autorisation est accordée dans le cadre des autorisations de l'application. 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 limitation.
Lire des enregistrements restreints	Permet la lecture des vidéos restreintes 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.

Nom	Description
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.
Exporter	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 les signets	Permet de recherches et de lire des détails des signets dans les clients.
Modifier les 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.
Créer et étendre la protection 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

Nom	Description
	Nécessite que les autorisations utilisateur associées à tous les périphériques soient incluses dans la protection de preuves.
Supprimer et réduire le 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 Nécessite que les autorisations utilisateur associées à tous les périphériques soient incluses dans la protection de preuves.
Lire le verrouillage des preuves	Permet à l'utilisateur du client de rechercher et de lire les détails des preuves verrouillées.
Créer et élargir des restrictions en direct et de lecture	Permet à l'utilisateur du client de : • Créer une restriction en direct sur la caméra • Créer une restriction de lecture sur les enregistrements de la caméra • Ajouter une nouvelle caméra à une restriction en direct ou en lecture • Prolonger la période de restriction des enregistrements de la caméra

Nom	Description
	Nécessite que les autorisations utilisateur associées à tous les périphériques soient incluses dans la restriction.
Lire des restrictions en direct et de lecture	Permet à l'utilisateur du client de : • Consulter une liste des restrictions en direct et de lecture existantes sur la caméra • Filtrer et rechercher la liste des restrictions en direct et en lecture sur la caméra
Supprimer et réduire des restrictions en direct et de lecture	Permet à l'utilisateur du client de : • Supprimer une restriction en direct sur la caméra • Supprimer une restriction de lecture sur les enregistrements de la caméra • Réduire la période de restriction des enregistrements de la caméra • Modifier les paramètres de la restriction en direct ou en lecture Nécessite que les autorisations utilisateur associées à tous les périphériques soient incluses dans la restriction.

Autorisations liées au microphone

Spécifier les autorisations suivantes pour les microphones :

Nom	Description
Lire	Le ou les microphone(s) sélectionné(s) seront visibles dans les clients.

Nom	Description
Écoute en direct	Permet d'écouter l'audio en direct des microphones sélectionnés dans les clients. Pour XProtect Smart Client, il nécessite que l'autorisation d'afficher l'onglet **En direct** ait été accordée au rôle. Cette autorisation est accordée dans le cadre des autorisations de l'application. Spécifiez le profil de temps ou conservez la valeur par défaut.
Écouter de l'audio restreint en direct	Permet d'écouter la vidéo restreinte en direct du ou des microphone(s) sélectionné(s) dans les clients. Pour XProtect Smart Client, il nécessite que l'autorisation d'afficher l'onglet **En direct** ait été accordée au rôle. Cette autorisation est accordée dans le cadre des autorisations de l'application. Spécifiez le profil de temps ou conservez la valeur par défaut.
Lecture > Dans le profil de temps	Permet la lecture de l'audio enregistrée 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 enregistrée du ou des microphone(s) sélectionné(s) en direct dans les clients. Spécifiez une limite de lecture ou n'appliquez aucune restriction.
Lire des enregistrements restreints	Permet la lecture de l'audio restreint enregistré du ou des microphone(s) sélectionné(s) en direct dans les clients. Spécifiez le profil de temps ou conservez la valeur par défaut.
Lire les séquences	Permet de lire des informations séquentielles liées à l'explorateur de séquence dans les clients, par exemple.
Exporter	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	Permet d'arrêter l'enregistrement manuel de l'audio du ou des

Nom	Description
l'enregistrement manuel	microphone(s) sélectionné(s) en direct dans les clients.
Lire les signets	Permet de recherches et de lire des détails des signets dans les clients.
Modifier les 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.
Créer et étendre la protection 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 Nécessite que les autorisations utilisateur associées à tous les périphériques soient incluses dans la protection de preuves.
Supprimer et réduire le 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

Nom	Description
	Nécessite que les autorisations utilisateur associées à tous les périphériques soient incluses dans la protection de preuves.
Lire le verrouillage des preuves	Permet à l'utilisateur du client de rechercher et de lire les détails des preuves verrouillées.
Créer et élargir des restrictions en direct et de lecture	Permet à l'utilisateur du client de : • Créer une restriction en direct sur le microphone • Créer une restriction de lecture sur les enregistrements audio • Ajouter un nouveau microphone à une restriction en direct ou en lecture • Prolonger la période de restriction des enregistrements audio Nécessite que les autorisations utilisateur associées à tous les périphériques soient incluses dans la restriction.
Lire des restrictions en direct et de lecture	Permet à l'utilisateur du client de : • Consulter une liste des restrictions en direct et de lecture existantes sur le microphone • Filtrer et rechercher la liste des restrictions en direct et en lecture sur le microphone
Supprimer et réduire des restrictions en direct et de lecture	Permet à l'utilisateur du client de : • Supprimer une restriction en direct sur le microphone • Supprimer une restriction de lecture sur les enregistrements audio

Nom	Description
	• Réduire la période de restriction des enregistrements audio • Modifier les paramètres de la restriction en direct ou en lecture Nécessite que les autorisations utilisateur associées à tous les périphériques soient incluses dans la restriction.

Autorisations liées au haut-parleur

Spécifier les autorisations suivantes pour les haut-parleurs :

Nom	Description
Lire	Le ou les haut-parleur(s) sélectionné(s) seront visibles dans les clients.
Écoute en direct	Permet d'écouter l'audio en direct du ou des haut-parleur(s) sélectionné(s) dans les clients. Pour XProtect Smart Client, il nécessite que l'autorisation d'afficher l'onglet **En direct** ait été accordée au rôle. Cette autorisation est accordée dans le cadre des autorisations de l'application. Spécifiez le profil de temps ou conservez la valeur par défaut.
Écouter de l'audio restreint en direct	Permet d'écouter la vidéo restreinte en direct du ou des haut-parleur(s) sélectionné(s) dans les clients. Pour XProtect Smart Client, il nécessite que l'autorisation d'afficher l'onglet **En direct** ait été accordée au rôle. Cette autorisation est accordée dans le cadre des autorisations de l'application. Spécifiez le profil de temps ou conservez la valeur par défaut.
Lecture > Dans le profil de temps	Permet la lecture de l'audio enregistrée du ou des haut-parleur(s) sélectionné(s) en direct dans les clients. Spécifiez le profil de

Nom	Description
	temps ou conservez la valeur par défaut.
Lecture > Limiter la lecture à	Permet la lecture de l’audio enregistrée du ou des haut-parleur(s) sélectionné(s) en direct dans les clients. Spécifiez une limite de lecture ou n’appliquez aucune restriction.
Lire des enregistrements restreints	Permet la lecture de l’audio restreint enregistré du ou des haut-parleur(s) sélectionné(s) en direct dans les clients. Spécifiez le profil de temps ou conservez la valeur par défaut.
Lire les séquences	Permet de lire des informations séquentielles liées à l’explorateur de séquence dans les clients, par exemple.
Exporter	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 les signets	Permet de recherches et de lire des détails des signets dans les clients.
Modifier les 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.
Créer et étendre la protection des preuves	Permet à l’utilisateur du client de :

Nom	Description
	• 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 Nécessite que les autorisations utilisateur associées à tous les périphériques soient incluses dans la protection de preuves.
Supprimer et réduire le 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 Nécessite que les autorisations utilisateur associées à tous les périphériques soient incluses dans la protection de preuves.
Lire le verrouillage des preuves	Permet à l'utilisateur du client de rechercher et de lire les détails des preuves verrouillées.
Créer et élargir des restrictions en direct et de lecture	Permet à l'utilisateur du client de : • Créer une restriction en direct sur les haut-parleurs • Créer une restriction de lecture sur les enregistrements audio

Nom	Description
	• Ajouter un nouveau microphone à une restriction en direct ou en lecture • Prolonger la période de restriction des enregistrements audio Nécessite que les autorisations utilisateur associées à tous les périphériques soient incluses dans la restriction.
Lire des restrictions en direct et de lecture	Permet à l'utilisateur du client de : • Consulter une liste des restrictions en direct et de lecture existantes sur les haut-parleurs • Filtrer et rechercher la liste des restrictions en direct et en lecture sur les haut-parleurs
Supprimer et réduire des restrictions en direct et de lecture	Permet à l'utilisateur du client de : • Supprimer une restriction en direct sur les haut-parleurs • Supprimer une restriction de lecture sur les enregistrements audio • Réduire la période de restriction des enregistrements audio • Modifier les paramètres de la restriction en direct ou en lecture Nécessite que les autorisations utilisateur associées à tous les périphériques soient incluses dans la restriction.

Autorisations liées aux métadonnées

Spécifier les autorisations suivantes pour les périphériques à métadonnées :

Nom	Description
Lire	Active l’autorisation permettant d’afficher les périphériques à métadonnées et de récupération de données à partir de ces derniers dans les clients.
Modifier	Active l’autorisation permettant de modifier les propriétés des métadonnées. Il permet également aux utilisateurs d’activer ou de désactiver les périphériques de métadonnées dans le Management Client et par le biais du MIP SDK.
Visualisation en direct	Active l’autorisation permettant de visualiser les métadonnées en direct à partir des caméras dans les clients. Pour XProtect Smart Client, il nécessite que l’autorisation d’afficher l’onglet **En direct** ait été accordée au rôle. Cette autorisation est accordée dans le cadre des autorisations de l’application.
Voir la restriction en direct	Active l’autorisation permettant de visualiser les métadonnées restreintes en direct à partir des caméras dans les clients. Pour XProtect Smart Client, il nécessite que l’autorisation d’afficher l’onglet **En direct** ait été accordée au rôle. Cette autorisation est accordée dans le cadre des autorisations de l’application.
Lecture	Active l’autorisation permettant de relire les données enregistrées à partir des périphériques à métadonnées dans les clients.
Lire des enregistrements restreints	Active l’autorisation permettant de relire les données enregistrées à partir des périphériques à métadonnées restreints dans les clients.
Lire les séquences	Active l’autorisation permettant d’utiliser la fonctionnalité Séquences tout en parcourant les données enregistrées à partir des périphériques à métadonnées dans les clients.
Exporter	Active l’autorisation permettant d’exporter l’audio enregistré à

Nom	Description
	partir des périphériques à métadonnées dans les clients.
Créer et étendre la protection des preuves	Active l'autorisation permettant de créer et d'étendre la protection de preuves sur les métadonnées dans les clients.
Lire le verrouillage des preuves	Active l'autorisation permettant de visualiser la protection de preuves sur les métadonnées dans les clients.
Supprimer et réduire le verrouillage des preuves	Active l'autorisation permettant de supprimer ou de réduire la protection de preuves sur les métadonnées dans les clients.
Démarrer l'enregistrement manuel	Active l'autorisation permettant de lancer l'enregistrement manuel des métadonnées dans les clients.
Arrêter l'enregistrement manuel	Active l'autorisation permettant d'arrêter l'enregistrement manuel des métadonnées dans les clients.
Créer et élargir des restrictions en direct et de lecture	Permet à l'utilisateur du client de : • Créer une restriction en direct sur les métadonnées du périphérique • Créer une restriction de lecture sur les métadonnées du périphérique • Ajouter de nouvelles métadonnées à une restriction en direct ou en lecture • Prolonger la période de restriction des métadonnées du périphérique

Nom	Description
	Nécessite que les autorisations utilisateur associées à tous les périphériques soient incluses dans la restriction.
Lire des restrictions en direct et de lecture	Permet à l'utilisateur du client de : • Consulter une liste des restrictions en direct et de lecture existantes sur les métadonnées du périphérique • Filtrer et rechercher la liste des restrictions en direct et en lecture sur les métadonnées du périphérique
Supprimer et réduire des restrictions en direct et de lecture	Permet à l'utilisateur du client de : • Supprimer une restriction en direct sur les métadonnées du périphérique • Supprimer une restriction de lecture sur les métadonnées du périphérique • Réduire la période de restriction des métadonnées du périphérique • Modifier les paramètres de la restriction en direct ou en lecture Nécessite que les autorisations utilisateur associées à tous les périphériques soient incluses dans la restriction.

Autorisations liées à l'entrée

Spécifier les autorisations suivantes pour les périphériques d'entrée :

Nom	Description
Lire	La ou les entrées sélectionnées seront visibles dans les clients.

Autorisations liées à la sortie

Spécifier les autorisations suivantes 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 autorisations relatives aux caméras Pan/Tilt/Zoom (PTZ) peuvent être configurées 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.

Spécifier les autorisations suivantes pour PTZ :

Nom	Description
Manuel PTZ	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 défini dans l'onglet **Infos** 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 défini dans l'onglet **Infos** pour ce rôle. Pour autoriser ce rôle à utiliser d'autres fonctions PTZ sur la caméra, activez l'autorisation **PTZ manuel**.

Nom	Description
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.
Gérer les positions prédéfinies PTZ ou les profils de patrouille	Détermine l'autorisation permettant d'ajouter, de modifier et de supprimer les préréglages PTZ et les profils de patrouille sur la caméra sélectionnée, dans le Management Client et XProtect Smart Client. Pour autoriser ce rôle à utiliser d'autres fonctions PTZ sur la caméra, activez l'autorisation **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 l'autorisation permettant 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 l'autorisation **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. Spécifier les autorisations suivantes 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)

Spécifier les autorisations suivantes pour les enregistrements à distance :

Nom	Description
Rappeler les enregistrements à distance	Active l'autorisation permettant de rappeler les enregistrements des clients à partir des caméras, des microphones, des haut-parleurs et des périphériques à métadonnées se trouvant dans des sites distants ou sur le stockage externe des caméras.

Onglet Smart Wall (rôles)

Grâce aux rôles, vous pouvez attribuer à vos clients utilisateurs des autorisations d'utilisateur en rapport avec Smart Wall :

Nom	Description
Lire	Autorise les utilisateurs à afficher le Smart Wall sélectionné dans XProtect Smart Client.

Nom	Description
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 XProtect Smart Client et à activer les préréglages.
Lecture	Autorise les utilisateurs à lire les données enregistrées à partir du Smart Wall sélectionné dans XProtect Smart Client.

Onglet Événement externe (rôles)

Spécifier les autorisations relatives aux événements externes suivantes :

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.

Spécifier les autorisations suivantes pour les groupes de vues :

Nom	Description
Lire	Active l'autorisation permettant de visualiser les groupes de vues dans les clients et dans le Management Client. Les groupes de vues sont créées dans le Management Client.
Modifier	Active l'autorisation permettant de modifier les propriétés des groupes de vues dans le Management Client.
Supprimer	Active l'autorisation permettant de supprimer des groupes de vues dans le Management Client.
Opérer	Active l'autorisation d'utilisation de groupes de vues dans XProtect Smart Client. Autrement dit, la création et la suppression de sous-groupes et de vues.

Onglet Serveurs (rôles)

La spécification des autorisations d'un rôle dans l'onglet **Serveurs** n'est appropriée que si votre système fonctionne dans une configuration Milestone Federated Architecture.

Nom	Description
Sites	Active l'autorisation permettant 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 Configuration de Milestone Federated Architecture on page 105 pour plus d'informations.

Onglet Matrix (rôles)

Si vous avez configuré des destinataires Matrix sur votre système, vous pouvez configurer des autorisations 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.

Les autorisations suivantes sont disponibles :

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 centrale et un meilleur contrôle de votre installation (incluant tout autre serveur XProtect), vous pouvez utiliser l'onglet **Alarmes** pour spécifier les autorisations d'alarme dont devraient disposer les utilisateurs et les groupes dotés du rôle sélectionné pour définir la façon de traiter les alarmes dans les clients.

Dans **Alarmes**, vous spécifiez les autorisations pour les alarmes :

Autorisation de sécurité	Description
Gestion	Active l'autorisation permettant de gérer des alarmes dans le Smart Client. Par exemple, modifier les priorités des alarmes, réaffecter des alarmes à d'autres utilisateurs, accuser réception des alarmes, modifier l'état d'alarme de plusieurs alarmes (par exemple de **Nouveau** à **Affecté**). Pour modifier les paramètres des alarmes, vous devez également disposer de l'autorisation **Modifier les paramètres des alarmes**. L'onglet **Alarmes et événements** de la boîte de dialogue **Options** n'apparaît que lorsque vous choisissez d'autoriser cette fonction.
Vue	Permet d'afficher l'onglet **Gestionnaire d'alarmes** dans XProtect Smart Client et de récupérer les alarmes et les paramètres d'alarme par le biais de l'API. Pour afficher les alarmes dans XProtect Smart Client, vous devez activer l'autorisation **Afficher** pour au moins une définition des alarmes. Par défaut, les alarmes provenant de solutions tierces sont affichées.
Désactiver alarmes	Active l'autorisation permettant de désactiver les alarmes.

Autorisation de sécurité	Description
Recevoir des notifications	Active l'autorisation permettant de recevoir des notifications sur les alarmes dans les clients XProtect Mobile et dans XProtect Web Client.
Modifier les paramètres de l'alarme	Active l'autorisation de modifier les définitions des alarmes, les états des alarmes, les catégories d'alarmes, les sons d'alarmes, la rétention des alarmes et la rétention des événements. Pour modifier les paramètres des alarmes, vous devez également disposer de l'autorisation **Gérer**.

Dans **Définitions des alarmes**, vous spécifiez les autorisations pour une définition d'alarme spécifique :

Nom	Description
Vue	Active l'autorisation d'afficher les définitions des alarmes, les états des alarmes, les catégories d'alarmes, les sons d'alarmes, la rétention des alarmes et la rétention des événements.
Écrire	Active l'autorisation **Afficher**

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 d'afficher la liste des détenteurs de cartes sur l'onglet **Contrôle d'accès** dans les clients.
Recevoir des notifications	Permet à l'utilisateur de recevoir des notifications concernant les demandes d'accès dans les clients.

Onglet Reconnaissance de plaque (rôles)

Si votre système s'exécute avec XProtect LPR, spécifiez les autorisations suivantes pour les utilisateurs :

Nom	Description
Afficher l'onglet de reconnaissance de plaque dans les applications clientes	Autorise l'utilisation des fonctionnalités XProtect LPR de XProtect Smart Client.
Gérer la reconnaissance de plaque	Autorise les opérations suivantes : • ajout, d'importation, modification, exportation et suppression des listes de correspondances dans le Management Client. • ajout et suppression de plaques d'immatriculation des listes de correspondances dans XProtect Smart Client. • suppression, désactivation et configuration des caméra de reconnaissance des plaques d'immatriculation existantes.
Afficher le nœud de reconnaissance de plaque dans Management Client	Autorise les opérations suivantes : • ajout, suppression et configuration de listes de correspondances ; • ajout, suppression et configuration des caméras de reconnaissance de plaque ; • ajout, suppression et configuration des serveurs de reconnaissance de plaque ; • ajout, suppression et configuration des alias du style de plaque d'immatriculation.

Onglet Incidents (rôles)

Si vous avez XProtect Incident Manager, vous pouvez spécifier les autorisations suivantes pour vos rôles.

Pour attribuer à un rôle d'administrateur de Management Client les autorisations de gérer ou de consulter les propriétés de l'incident, sélectionnez le nœud **Propriétés de l'incident**.

Pour donner à un opérateur de XProtect Smart Client l'autorisation de consulter vos propriétés d'incident définies, sélectionnez **Propriétés de l'incident** et autorisez leur **Accès**. Pour les autorisations générales

concernant la gestion ou la consultation des projets d'incident, sélectionnez le nœud **Projet d'incident**. Développez le nœud **Projet d'incident**, puis sélectionnez un ou plusieurs sous-nœuds pour attribuer des autorisations quant à ces fonctionnalités ou capacités spécifiques supplémentaires.

Nom	Description
Gestion	Autorisation de gérer (consulter, créer, modifier et supprimer) les paramètres et propriétés liés à une fonctionnalité, ou de consulter un élément de l'interface utilisateur représenté par le nœud sélectionné dans Management Client ou XProtect Smart Client.
Vue	Autorisation de voir (mais pas créer, modifier ou supprimer) les paramètres et propriétés liés à une fonctionnalité, de consulter des propriétés d'incidents définies ou de consulter un élément de l'interface utilisateur représenté par le nœud sélectionné dans Management Client ou XProtect Smart Client.

Onglet Santé (rôles)

Si votre système s'exécute avec XProtect Hospital Assist, spécifiez les autorisations suivantes pour les utilisateurs :

Autorisations liées au floutage de confidentialité

Nom	Description
Gestion	Actuellement non utilisée.
Vue	Active la fonctionnalité de floutage de confidentialité dans XProtect Smart Client.

Autorisations liées aux Sticky Notes

Nom	Description
Gestion	Autorise la création, la modification et la suppression de pense-bêtes dans XProtect Smart Client.
Vue	Active la fonctionnalité Sticky Notes dans XProtect Smart Client.

Autorisations liées à Multipièces Audio

Nom	Description
Gestion	Actuellement non utilisée.
Vue	Permet au rôle d'utiliser la fonctionnalité d'écoute et de conversation pour la fonctionnalité Multipièces Audio dans XProtect Smart Client.

Onglet Webhooks (rôles)

Si votre système s'exécute avec des webhooks, spécifiez les autorisations suivantes pour les utilisateurs :

Nom	Description
Modifier	Active l'autorisation permettant de modifier les propriétés des webhooks dans Management Client.
Lire	Active l'autorisation permettant d'afficher les propriétés des webhooks dans Management Client.

Onglet Transact (rôles)

Si votre système s'exécute avec XProtect Transact, spécifiez les autorisations suivantes pour les utilisateurs :

Sources de transactions

Nom	Description
Modifier	Active l'autorisation permettant de modifier les propriétés des sources de transaction dans Management Client.
Lire	Active l'autorisation permettant d'afficher les propriétés des sources de transaction dans Management Client.

Définitions des transactions

Nom	Description
Modifier	Active l'autorisation permettant de modifier les propriétés des définitions de transaction dans Management Client.
Lire	Active l'autorisation permettant d'afficher les propriétés des définitions de transaction dans Management Client.

Onglet MIP (rôles)

Au travers du MIP SDK, un vendeur tiers peut développer des modules d'extension personnalisés pour votre système, par exemple, l'intégration à des systèmes de contrôle d'accès externes ou similaires. Les modules d'extension tiers auront leurs propres paramètres dans des onglets individuels.

Les paramètres que vous modifiez dépendent du module d'extension. L'onglet **MIP** vous permet de trouver les paramètres personnalisés des modules d'extension.

Utilisateur de base (noeud sécurité)

Il existe deux types de comptes utilisateur dans Milestone XProtect VMS : les utilisateurs basiques et les utilisateurs Windows.

Les utilisateurs basiques sont des comptes utilisateurs que vous créez dans Milestone XProtect VMS. Il s'agit d'un compte utilisateur système dédié, avec un nom d'utilisateur basique et une authentification par mot de passe pour chaque utilisateur individuel.

Les utilisateurs Windows sont des comptes utilisateurs que vous pouvez ajouter via Active Directory de Microsoft.

Il existe quelques différences entre les utilisateurs basiques et les utilisateurs Windows :

- Les utilisateurs basiques sont authentifiés par une combinaison nom d'utilisateur et mot de passe et sont spécifiques à un système/site. Notez que même si un utilisateur basique créé sur un site fédéré a le même nom et mot de passe qu'un utilisateur de base sur un autre site fédéré, l'utilisateur de base n'a accès qu'au site sur lequel il a été créé.
- Les utilisateurs Windows sont authentifiés à partir de leurs identifiants de connexion Windows et sont spécifiques à une machine.

Noeud Tableau de bord du système

Noeud du tableau de bord système

Sous le noeud **Tableau de bord système**, vous trouverez différentes fonctions de surveillance de votre système et de ses composants système.

Nom	Description
Tâche actuelle	Pour obtenir un aperçu des tâches en cours sur un serveur d'enregistrement sélectionné.
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.
Verrouillage des preuves	Obtenez une vue d'ensemble de toutes les données protégées dans le système.
Rapports de configuration	Imprimez un rapport avec votre configuration système. Vous pouvez choisir ce qui est inclus dans le rapport.

Tâches en cours (noeud Tableau de bord du système)

La fenêtre **Tâches actuelles** affiche une vue d'ensemble des tâches en cours sous un serveur d'enregistrement spécifique. Si vous avez débuté une tâche qui prend du temps et qui s'exécute en arrière-plan, vous pouvez ouvrir la fenêtre **Tâches actuelles** pour consulter les progrès de la tâche. Parmi les exemples des tâches démarrées par l'utilisateur qui sont longues, figurent les mises à jour du firmware et le mouvement du matériel. Vous pouvez voir les informations sur l'heure de début, l'heure de fin estimée et le progrès de la tâche.

Les informations affichées dans la fenêtre **Tâches actuelles** ne sont pas mises à jour de façon dynamique mais il s'agit d'une capture d'écran des tâches actuelles de l'instant où vous avez ouvert la fenêtre. Si la fenêtre est ouverte depuis quelque temps, actualisez les informations en sélectionnant le bouton **Actualiser** situé dans le coin inférieur droit de la fenêtre.

Moniteur système (noeud Tableau de bord du système)

La fonctionnalité du **Moniteur système** vous fournit un aperçu visuel rapide de l'état actuel des serveurs et caméras de votre système.

Fenêtre du tableau de bord du moniteur système

Tuiles

La partie supérieure de la fenêtre du **Tableau de bord du moniteur système** affiche des tuiles de couleur qui représentent l'état du serveur et de la caméra de votre système.

Les tuiles changent d'état et donc de couleur en fonction des seuils configurés sous le noeud **Seuils du moniteur système**. Pour plus d'informations, voir Seuils du moniteur système (noeud Tableau de bord du système) on page 622. La définition des seuils et donc des couleurs des tuiles correspond à ce qui suit :

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 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**.

Liste des matériels avec des paramètres de surveillance

Si vous cliquez sur une tuile, vous pouvez voir l'état de chaque paramètre de surveillance sélectionné pour chaque matériel représenté par la tuile dans la partie inférieure de la fenêtre du **Tableau de bord du moniteur système**.

Exemple : Les paramètres de surveillance FPS LIVE d'une caméra ont atteint l'état Avertissement.

Fenêtre Personnaliser le tableau de bord

Sélectionnez **Personnaliser** dans le coin supérieur droit de la fenêtre pour ouvrir la fenêtre **Personnaliser le tableau de bord**.

Dans la fenêtre **Personnaliser le tableau de bord**, vous pouvez sélectionner la tuile à créer, modifier ou à supprimer. Lors de la création ou la modification des tuiles, vous pouvez sélectionner le matériel ou les paramètres de surveillance que vous souhaitez surveiller dans la tuile.

Fenêtre Détails

Si vous sélectionnez une tuile et qu'ensuite vous sélectionnez le bouton **Details** situé à droite d'une caméra ou d'un serveur depuis la liste des matériels avec des paramètres de surveillance, vous pouvez, selon le matériel sélectionné, afficher les informations du système et créer des rapports sur :

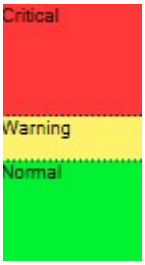
Matériel	Information
Serveur de gestion	Affiche les données de : • Utilisation du CPU • Mémoire disponible Sélectionner **Historique** pour afficher les statistiques de l'historique de votre matériel et créer un rapport basé sur les données susmentionnées.
Serveur(s) d'enregistrement	Affiche les données de : • Utilisation unité centrale • Mémoire disponible • Disques • Stockage • Réseau • Caméras Sélectionner **Historique** pour afficher les statistiques de l'historique de votre matériel et créer un rapport basé sur les données susmentionnées.
Serveurs d'enregistrement de basculement	Affiche les données de : • Utilisation unité centrale • Mémoire disponible • Serveurs d'enregistrement surveillés

Matériel	Information
	Sélectionner **Historique** pour afficher les statistiques de l'historique de votre matériel et créer un rapport basé sur les données susmentionnées.
Serveurs de journaux, serveurs d'événements et plus	Affiche les données de • Utilisation unité centrale • Mémoire disponible Sélectionner **Historique** pour afficher les statistiques de l'historique de votre matériel et créer un rapport basé sur les données susmentionnées.
Caméras	Affiche les données de : • Stockage • Espace utilisé • FPS direct (par défaut) • Enregistrement FPS • Format vidéo en direct • Enregistrement du format vidéo • Données média reçues (Kbit/s) • Mémoire disponible Sélectionner le nom de la caméra pour consulter ses données historiques et créer un rapport sur : • Données reçues depuis la caméra • Utilisation du disque caméra

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 pour ajouter la page **du moniteur système** à la **zone des sites de confiance** avant de poursuivre.

Seuils du moniteur système (noeud Tableau de bord du système)

Les seuils du moniteur système vous permettent de définir et ajuster les seuils lorsque les tuiles du **Tableau de bord du moniteur système** doivent indiquer visuellement que le matériel de votre système change d'état. Par exemple, lorsque l'utilisation du CPU d'un serveur passe d'un état normal (vert) à un état d'avertissement (jaune) ou d'un état d'avertissement (jaune) à un état critique (rouge).



Exemple de seuils entre les trois états

Vous pouvez modifier les seuils pour des serveurs, caméras, disques et du stockage, et tous les seuils ont des boutons et des paramètres communs.

Éléments de l'interface utilisateur communs

Boutons et paramètres	Description	Unité
Intervalle de calcul	Il existe souvent des petites pannes dans la connexion vers les différents matériels. Si vous spécifiez un intervalle de calcul de 0 seconde, ces pannes déclencheront des alarmes sur les changements dans l'état du matériel. Définissez donc un intervalle de calcul avec une certaine longueur. Si vous définissez un intervalle de calcul d'une (1) minute, cela signifie que vous recevrez uniquement des alertes si la valeur moyenne pour la minute complète dépasse le seuil. Un bon paramètre de calcul de l'intervalle vous évitera de recevoir des faux positifs. Vous recevrez uniquement des alertes sur des problèmes concernant, par exemple, l'utilisation du CPU ou la consommation de la mémoire. Pour modifier les valeurs des intervalles de calcul, voir Modifier les seuils lorsque les états du matériel doivent changer on page 321.	secondes
Avancés	Si vous sélectionnez le bouton **Avanc**, vous pouvez définir les seuils et les intervalles de calcul pour des serveurs, caméras et disques	-

Boutons et paramètres	Description	Unité
	individuels et pour du stockage. Pour plus d'informations, voir ci-dessous.	
Créer une règle	Vous pouvez associer des événements du **Moniteur système** et des règles pour déclencher des actions, par exemple, lorsque l'utilisation du CPU d'un serveur est critique ou lorsqu'un disque commence à manquer d'espace. Pour plus d'informations, voir Règles et événements (explications) on page 88 et Ajouter des règles on page 294.	-

Seuils de serveur

Seuil	Description	Unité
Utilisation du CPU	Les seuils correspondant à l'usage du processeur sur les serveurs que vous surveillez.	%
Mémoire disponible	Les seuils correspondant à la RAM en cours d'utilisation sur les serveurs que vous surveillez.	Mo
Décodage NVIDIA	Les seuils correspondant à l'usage du décodeur NVIDIA sur les serveurs que vous surveillez.	%
Mémoire NVIDIA	Les seuils correspondant à la RAM NVIDIA en cours d'utilisation sur les serveurs que vous surveillez.	%
Rendu de NVIDIA	Les seuils correspondant au rendu NVIDIA sur les serveurs que vous surveillez.	%

Seuils de caméras

Seuil	Description	Unité
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.	%
FPS d'enregistrement	Les seuils pour le FPS des caméras en cours d'utilisation lorsque le système enregistre de la vidéo sur les caméras que vous surveillez.	%
Espace utilisé	Les seuils correspondant à l'espace utilisé par les caméras que vous surveillez.	Go

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 où 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

Protection des preuves (noeud Tableau de bord du système)

Protection des preuves sous le noeud **Tableau de bord du système** affiche une vue d'ensemble de toutes les données protégées dans le système de surveillance actuel.

Les métadonnées suivantes sont disponibles pour toutes les protections des preuves :

- 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

Les informations affichées dans la fenêtre **Protection des preuves** sont des captures d'écran. Appuyez sur F5 pour actualiser.

Rapports de configuration (noeud Tableau de bord du système)

Vous faites plusieurs choix lorsque vous installez et configurez votre système de logiciel de gestion des vidéos et il peut être utile de les documenter. Au fil du temps, ou même depuis les deux derniers mois, il est également difficile de se rappeler de l'intégralité des paramètres que vous avez modifiés depuis l'installation et la configuration d'origine. C'est pourquoi il est possible d'imprimer un rapport contenant tous les choix de configuration.

Les paramètres suivants sont disponibles lors de la création et l'impression des rapports de configuration :

Nom	Description
Rapports	Une liste des éléments qu'il est possible d'inclure dans le rapport de configuration.
Sélectionner tout	Ajoute tous les éléments de la liste **Rapports** dans le rapport de configuration.
Effacer tout	Supprime tous les éléments de la liste **Rapports** du rapport de configuration.
Page de couverture	Pour personnaliser la page de couverture du rapport.
Formatage	Pour formater le rapport.
Exclure les données sensibles	Efface les données personnelles, telles que les noms d'utilisateurs, les adresses e-mail et tout autre type de données sensibles du rapport de configuration pour qu'il respecte les normes du RGPD. Les informations concernant le détenteur de la licence ne sont jamais incluses dans le rapport.
Exporter	Sélectionner un emplacement pour y enregistrer le rapport et le créer au format PDF.

Noeud Journaux des serveurs

Noeud Journaux des serveurs

Journaux système (onglet)

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 de journal	Info, avertissement, ou erreur.
Heure locale	Horodaté en heure locale du serveur de votre système.
Texte du message	Numéro d'identification de l'incident journalisé.
Catégorie	Type d'incident journalisé.
Type de source	Type d'équipement sur lequel l'incident journalisé est intervenu, par exemple, serveur ou périphérique.
Nom de la source	Nom de l'équipement sur lequel l'incident journalisé est intervenu.
Type d'événement	Type d'événement correspondant à l'incident journalisé.

Journaux d'activités (onglet)

Chaque ligne dans un journal représente une entrée de journal. Une entrée de journal contient un certain nombre de champs d'informations :

Nom	Description
Heure locale	Horodaté en heure locale du serveur de votre système.
Texte du message	Affiche une description de l'incident journalisé.
Autorisation	Informations indiquant si l'action de l'utilisateur distant était autorisée ou non.
Catégorie	Type d'incident journalisé.
Type de source	Type d'équipement sur lequel l'incident journalisé est intervenu, par exemple, serveur ou périphérique.
Nom de la source	Nom de l'équipement sur lequel l'incident journalisé est intervenu.
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.

Journaux déclenchés par les règles (onglet)

Chaque ligne dans un journal représente une entrée de journal. Une entrée de journal contient un certain nombre de champs d'informations :

Nom	Description
Heure locale	Horodaté en heure locale du serveur de votre système.
Texte du message	Affiche une description de l'incident journalisé.
Catégorie	Type d'incident journalisé.
Type de source	Type d'équipement sur lequel l'incident journalisé est intervenu, par exemple, serveur ou périphérique.

Nom	Description
Nom de la source	Nom de l'équipement sur lequel l'incident journalisé est intervenu.
Type d'événement	Type d'événement correspondant à l'incident journalisé.
Nom de la règle	Nom de la règle qui déclenche la journalisation de l'entrée.
Nom du service	Nom du service sur lequel l'incident journalisé est intervenu.

Noeud Utilisation des métadonnées

Métadonnées et recherche de métadonnées

Pour gérer et configurer les dispositifs de métadonnées, voir Afficher et masquer des catégories de recherche et filtres de recherche de métadonnées on page 323.

Définition des métadonnées

Les métadonnées sont 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 générées par :

- Le périphérique lui-même en fournissant les données.
- Un système tiers ou une intégration via un pilote de métadonnées générique

Recherche de métadonnées

La recherche de métadonnées est toute recherche d'enregistrements vidéo dans XProtect Smart Client qui utilisent des catégories de recherche et des filtres de recherche liés aux métadonnées.

Les catégories de recherche de métadonnées de Milestone par défaut sont :

- Emplacement : Les utilisateurs peuvent définir des coordonnées géographiques et un rayon de recherche à partir de ces coordonnées.
- Personnes : Les utilisateurs peuvent rechercher le genre, la taille et l'âge approximatifs, et choisir d'afficher les résultats avec des visages.
- Véhicules : Les utilisateurs peuvent rechercher la couleur, la vitesse et le type de véhicule, et rechercher une plaque d'immatriculation spécifique.

Critères de la recherche de métadonnées

Pour obtenir des résultats de recherche, vous devez respecter l'un des critères suivants :

- Avoir au moins un périphérique dans votre système de vidéosurveillance pouvant effectuer des analyse vidéo et étant correctement configuré
- Avoir un service de traitement vidéo dans votre système de vidéosurveillance qui génère des métadonnées

Dans tous les cas, les métadonnées doivent être au format de métadonnées requis.

Pour plus d'informations, voir la documentation pour l'intégration de la recherche de métadonnées.

Noeud Contrôle d'accès

Onglet Paramètres généraux (contrôle d'accès)

Nom	Description
Activer	Active ou désactive le système de contrôle d'accès intégré. Si vous désactivez ce paramètre, votre système XProtect ne recevra plus d'événements de contrôle d'accès. Les systèmes de contrôle d'accès intégrés sont activés et visibles dans XProtect Smart Client par défaut pour les utilisateurs disposant d'autorisations suffisantes. Parfois, vous devrez peut-être désactiver les événements de contrôle d'accès, au cours d'une maintenance par exemple, pour ne pas générer d'alarmes inutiles.
Nom	Ajoutez ou modifiez le nom de l'intégration du système de contrôle d'accès qui s'affiche dans Management Client et d'autres clients.
Description	Ajoutez une description de l'intégration du contrôle d'accès (facultatif).
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 l'heure de la dernière importation de la configuration à partir du système de contrôle d'accès.
Rafraîchir la	Si vous avez apporté des modifications à la configuration du système de contrôle

Nom	Description
configuration	d’accès intégré (par ex. l’ajout ou la suppression d’une porte) et que vous souhaitez les appliquer à XProtect, cliquez sur ce bouton. Après avoir cliqué sur le bouton, un résumé des modifications de configuration du système de contrôle d’accès s’affiche. 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	Si le système de contrôle d’accès prend en charge des autorisations utilisateur différenciées, activez une connexion supplémentaire pour les utilisateurs clients. Si vous activez ce paramètre, le système de contrôle d’accès ne sera plus disponible sur le client XProtect Mobile. Ce paramètre n’est visible que si le module d’extension d’intégration prend en charge les autorisations différenciées des utilisateurs.

Paramètres potentiels

Les exemples de paramètres suivants peuvent apparaître, en fonction du module d’extension du système de contrôle d’accès avec lequel vous effectuez l’intégration. Les noms des paramètres et leur contenu sont importés à partir du module d’extension.

Nom	Description
Adresse	Saisissez l’adresse du serveur qui héberge 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 du système de contrôle d’accès, qui doit être l’administrateur du système de contrôle d’accès intégré dans XProtect.
Mot de passe	Le champ du mot de passe est masqué par défaut. Cliquez sur le bouton pour saisir le mot de passe administrateur du système de contrôle d’accès à enregistrer. Une fois enregistré, le mot de passe est vérifié.

Onglet Portes et caméras associées (contrôle d’accès)

Utilisez cet onglet pour lier les points d’accès de porte aux caméras, aux microphones et aux haut-parleurs.

- Vous devez attribuer des caméras aux points d’accès de porte au moment de configurer l’intégration, mais vous pouvez les modifier ultérieurement.
- Les microphones et les haut-parleurs sont automatiquement liés via leurs caméras associées.

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 Coordonnées GPS (contrôle d’accès)

Lorsque vous ajoutez les coordonnées GPS d’une unité de contrôle d’accès, celle-ci apparaît automatiquement sur les smart maps dans XProtect Smart Client.

Nom	Description
Unités de contrôle d’accès	Sélectionnez l’unité de contrôle d’accès dont vous souhaitez ajouter les coordonnées GPS.

Nom	Description
Coordonnées GPS	Saisissez les coordonnées GPS de l'unité de contrôle d'accès au format latitude, longitude. La valeur que vous saisissez détermine la position de l'icône d'unité de contrôle d'accès sur la smart map dans XProtect Smart Client.

Onglet Événements de contrôle d'accès (contrôle d'accès)

Les catégories d'événements organisent les événements et influencent le comportement du contrôle d'accès. Par exemple, vous pouvez définir une alarme qui se déclenche pour plusieurs types d'événements.

Nom	Description
Événement de contrôle d'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 des événements et les utilisateurs peuvent le filtrer dans XProtect Smart Client.
Type de source	Indique l'unité de contrôle d'accès qui peut déclencher l'événement de contrôle d'accès.
Catégorie d'événements	Attribuez des catégories d'événements aux événements de contrôle d'accès. Vous pouvez ajouter plusieurs catégories. Le système XProtect mappe automatiquement les catégories d'événements pertinentes aux événements lors de l'intégration et crée une configuration par défaut. Vous pouvez modifier le mappage à tout moment. Les catégories d'événements intégrées sont : • Accès refusé • Accès accordé • Demande d'accès • Alarme • Erreur

Nom	Description
	• Avertissement : Les événements et catégories d'événements propres au module d'extension d'intégration peuvent être affichés, et vous pouvez également définir vos catégories d'événements. ⚠ Si vous modifiez les catégories d'événements dans XProtect Corporate, veillez à ce que les règles de contrôle d'accès existantes fonctionnent toujours.
Catégories définies par les utilisateurs	Vous permet de créer, de modifier ou de supprimer des catégories d'événements définies par l'utilisateur. La création de catégories d'événements est utile lorsque les catégories intégrées ne répondent pas à vos exigences. Cela peut être le cas, par exemple, si vous définissez des événements déclencheurs pour des actions de contrôle d'accès. Les catégories s'appliquent à tous les systèmes d'intégration ajoutés au système XProtect. Elles permettent de configurer un traitement sur l'ensemble des systèmes, par exemple sur la définition des alarmes. Si vous supprimez une catégorie d'événement définie par l'utilisateur, un avertissement s'affiche si la catégorie en question est utilisée par l'une de vos intégrations. Si vous la supprimez quand même, toutes les configurations qui l'utilisent, comme les actions de contrôle d'accès, ne fonctionneront plus.

Onglet Notification de demande d'accès (contrôle d'accès)

Vous pouvez personnaliser l'affichage de vos notifications de demande d'accès dans XProtect Smart Client au déclenchement d'un événement donné.

Nom	Description
Nom	Entrez un nom pour la notification de demande d'accès.
Ajouter une notification de	Cliquez pour ajouter et définir des notifications de demande d'accès.

Nom	Description
demande d'accès	Pour supprimer une notification, cliquez sur **X** situé à droite. Si vous vous connectez au site parent en utilisant XProtect Smart Client dans Milestone Federated Architecture, les notifications de demande d'accès des sites enfants s'affichent également.
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. Vous pouvez également spécifier le son que vous souhaitez utiliser pour alerter l'utilisateur à l'apparition de la notification.
Ajouter une commande	Sélectionnez les commandes à afficher sous forme de boutons dans les fenêtres de notification de demande d'accès dans XProtect Smart Client. • Commandes de demande d'accès associées : active toutes les commandes associées aux opérations de demande d'accès disponibles sur l'unité source. Par exemple **Ouvrir la porte**. • Toutes les commandes associées : active toutes les commandes sur l'unité source. • Commande de contrôle d'accès : active une commande de contrôle d'accès sélectionnée. • Commande de système : active une commande prédéfinie dans le système XProtect. Pour supprimer une commande, cliquez sur **X** situé à droite.

Onglet Détenteur de carte (contrôle d'accès)

Utilisez l'onglet **Détenteurs de carte** pour consulter les informations disponibles sur les détenteurs de carte dans le système de contrôle d'accès.

Nom	Description
Rechercher un détenteur	Saisissez le nom d'un détenteur de carte. Si le nom existe dans le système, il

Nom	Description
de carte	apparaîtra dans la liste.
Nom	Affiche les noms des détenteurs de carte récupérés à partir du système de contrôle d'accès.
Type	Affiche le type de détenteur de carte, par exemple : • Employé • Garde • Invité

Si l'intégration de votre système de contrôle d'accès permet d'ajouter et de supprimer des fichiers images dans XProtect, vous pouvez charger des images vers les profils des détenteurs de carte. Cette fonctionnalité est utile si l'intégration du système de contrôle d'accès ne stocke pas déjà d'images de détenteurs de carte.

Tous les systèmes de contrôle d'accès ne prennent pas en charge l'ajout de photos de détenteurs de carte via XProtect.

Nom	Description
Sélectionner une image	Spécifiez un chemin d'accès à un fichier contenant une image du détenteur de carte. Ce bouton est masqué si le système de contrôle d'accès intégré gère les images et n'autorise pas les modifications d'images dans XProtect. • Vous pouvez utiliser des fichiers aux formats .bmp, .png et .jpg. • Les images sont redimensionnées afin de maximiser la vue. • Milestone vous recommande d'utiliser une image carrée.
Supprimer l'image	Cliquez pour supprimer l'image. Si une photo du détenteur de carte est également disponible dans le système de contrôle d'accès intégré, cette dernière sera affichée à la place.

Nœud Incidents

Propriétés de l’incident (nœud Incidents)

Les informations suivantes décrivent les paramètres liés à XProtect Incident Manager.

Vous pouvez configurer toutes les propriétés de l’incident pour vos opérateurs de XProtect Smart Client sur ces onglets :

- Types
- États
- Catégories
- Catégorie 1-5

Toutes les propriétés de l’incident ont les paramètres suivants :

Nom	Description
Nom	Les noms des propriétés de l’incident ne sont pas nécessairement uniques, mais utiliser des noms et des descriptions univoques des propriétés de l’incident peut s’avérer avantageux dans de nombreuses situations.
Description	Une explication supplémentaire de la propriété définie de l’incident. Par exemple, si vous avez créé une catégorie intitulée *Emplacement*, sa description pourrait être *Où l’incident a-t-il eu lieu ?*

Noeud Transactions

Sources de transactions (noeud Transaction)

Le tableau suivant décrit les propriétés des sources de transactions.

Pour plus d’informations sur l’ajout d’une source, voir Ajouter une source de transaction (assistant).

Sources de transaction (propriétés)

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 d'une source de transaction désactivée 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.
Définitions des transactions	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

Nom	Description
	• **Port** : saisissez le nom du port du serveur TCP correspondant à la source de transaction
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'octets pour indiquer lorsqu'un octet est transmis. La plupart des périphériques nécessite 1 • **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

Définitions des transactions (noeud Transaction)

Le tableau suivant décrit les propriétés des définitions à utiliser dans les sources de transaction.

Pour plus d'informations sur la création et l'ajout de définitions de transaction, voir Créer et ajouter des définitions de transactions.

Définitions de transaction (propriétés)

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

Nom	Description
	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.
Début de 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.
Arrêt de 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.
Type de correspondance	Sélectionnez le type de correspondance à utiliser pour rechercher le modèle 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 **Modèle de début** et **Modèle de fin** • Utiliser des jokers : La recherche identifie les séries qui contiennent ce que vous avez saisi dans les champs **Modèle de début** et **Modèle 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 1 chiffre. Si vous avez saisi "# pastèque", la recherche identifie les séries qui contiennent par exemple "1 pastèque". ? correspond à 1 caractère. Par exemple, vous pouvez saisir « Commencer la trans?ction » pour identifier les séries qui contiennent « Commencer la transaction »

Nom	Description
	• 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://docs.microsoft.com/dotnet/standard/base-types/regular-expression-language-quick-reference/)
Données brutes	Les séries de données de transaction provenant de la source de transaction connectée s'affichent dans cette section.
Modèle de début	Précisez un modèle 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.
Modèle de fin	Précisez un modèle de fin pour indiquer la fin de la transaction. Un modèle de fin n'est pas obligatoire, mais peut s'avérer utile si les données reçues 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 modèle 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 **Modèle de début**.
Ajouter un filtre	Utilisez le bouton **Ajouter des filtres** 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 des sauts de ligne pour reproduire l'apparence des tickets d'origine dans XProtect Smart Client.
Texte de filtre	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

Nom	Description
	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**.
Supprimez les caractères de contrôle qui ne sont pas définis comme étant des filtres de texte	Supprimez les caractères non imprimables qui n’ont pas été supprimés après l’ajout des filtres. Dans le volet **Données brutes** et la section **Prévisualisation**, vous pouvez voir comment les chaînes des données de transactions changent lorsque vous activez ou désactivez ce paramètre.
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.

Noeud Alarmes

Définitions des alarmes (noeud Alarmes)

Lorsque votre système enregistre un événement, vous pouvez le configurer afin qu’il génère 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.

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 à propos de l’alarme et la manière de résoudre le problème qui a déclenché cette alarme. Le texte s’affiche dans XProtect Smart Client lorsque l’utilisateur gère l’alarme.
Evénement 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 temporel	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 également Vue d'ensemble des événements. Vous pouvez aussi utiliser les définitions de l'événement global/manuel. Voir également Événements définis par l'utilisateur (explications).

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.

Plans :

Nom	Description
Vue Gestionnaire d'alarme	Assignez une Smart Map ou un plan à l'alarme lorsque celle-ci apparaît dans XProtect Smart Client > **Gestionnaire d'alarme**. Une smart map affiche les alarmes si celles-ci sont déclenchées par un périphérique et si ce dernier est ajouté à une smart map.

Autre :

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.
Propriétaire de l'alarme initiale	Sélection d'un utilisateur par défaut responsable de l'alarme.
Priorité initiale de l'alarme	Sélectionnez une priorité pour l'alarme. Utilisez ces priorités dans XProtect Smart Client pour définir l'importance d'une alarme.
Catégorie d'alarme	Sélectionnez une catégorie pour l'alarme, par exemple **Fausse alarme** ou **Investigation requise**.
Evénements 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.
Alarme assignée au Administrateurs	Cochez la case à cocher pour inclure des utilisateurs dans un rôle d'administrateur dans la liste **Assigné à**. La liste **Assigné à** se trouve dans les détails de l'alarme dans l'onglet **Gestion des alarmes** dans XProtect Smart Client. Décochez la case à cocher pour filtrer les utilisateurs ayant un rôle d'administrateur depuis la liste **Assigné à** pour réduire la liste.

Paramètres des données de l’alarme (noeud Alarmes)

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 ou 3). Ces niveaux de priorité servent à configurer le paramètre de **Priorité initiale 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 des sons par défaut ou ajoutez-en plus dans **Paramètres de son**.
Répéter le son	Décidez si le son ne doit être joué qu’une fois, ou plusieurs fois jusqu’à ce que l’opérateur dans XProtect Smart Client clique sur l’alarme dans la liste d’alarmes.
Activez les notifications sur le bureau	Vous pouvez activer ou désactiver les notifications sur le bureau pour chaque priorité d’alarme. Si vous utilisez un XProtect VMS qui prend en charge les profils Smart Client, vous devez également activer les notifications sur les profils Smart Client requis. Voir Onglet Gestionnaire d’alarme (profils Smart Client) on page 510.

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 de nouveaux états avec les 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 **Catégorie initiale de l'alarme**. Le niveau 99 est réservé à l'alarme Alerte d'urgence dans le client XProtect Mobile.
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	Utilisez > pour sélectionner les colonnes à mettre la disposition dans la *Liste des alarmes* 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 du son (noeud Alarmes)

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 sons intègre un certain nombre de sons Windows par défaut. Vous pouvez également ajouter de nouveaux son (.wav ou .mp3).
Ajouter	Ajouter des sons. Naviguez dans les fichiers son pour télécharger un ou plusieurs fichiers .wav ou .mp3.
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.

Hiérarchie des sites fédérés

Propriétés des sites fédérés

Cette section décrit l'onglet **Général** et l'onglet **Site parent**.

Onglet Généralités

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.
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 atteintes depuis l'extérieur 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.

Nom	Description
Temps de la dernière synchronisation	Date et heure de la dernière synchronisation de la hiérarchie.
État pour 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 concernant le site parent du site auquel vous êtes actuellement connecté. L'onglet n'est pas visible si votre site n'a pas de 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 atteintes depuis l'extérieur 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 pour la dernière synchronisation	L'état de la dernière synchronisation de la hiérarchie. Cela peut être soit **Réussi**, soit **Échoué**.

Milestone Husky IVO System Health

Husky IVO System Health (Noeud)

Le nœud affiche les données d'intégrité du système de toutes les unités Husky IVO qui se sont connectées avec succès à XProtect Management Client, avec la liste des noms d'appareils et l'état général de chaque unité.

Sélectionnez le nom d'une unité dans le nœud pour afficher les principales statistiques sur l'intégrité du système de cette unité dans une nouvelle page.

Seules les données relatives à l'intégrité du système des unités Husky IVO peuvent être affichées dans le nœud.

Le nœud Husky IVO System Health n'est accessible qu'après l'installation du module d'extension Husky IVO System Health sur l'ordinateur XProtect Management Client.

Le nœud Husky IVO System Health est actuellement publié en tant que version bêta. L'apparence et les fonctions de la version finale peuvent différer de celles de la version bêta.

Indicateurs d'état de l'intégrité du système

Les indicateurs d'état général affichés sur le nœud sont les suivants :

- **Tout va bien** : Aucun problème n'est à signaler.
- **À besoin d'attention** : Un ou plusieurs problèmes ont été détectés et requièrent votre attention.
- **Données manquantes** : L'état ne peut pas être signalé en raison de l'insuffisance des données.

Actualisation des données relatives à l'intégrité du système

Les données relatives à l'intégrité du système sont automatiquement mises à jour à intervalles fixes de 5 minutes et ne peuvent pas être actualisées manuellement.

Pour plus d'informations, voir Husky IVO System Health on page 57

helpfeedback@milestone.dk

À propos de Milestone

Milestone Systems est un fournisseur leader de l'édition de logiciels de gestion de vidéo sur plate-forme ouverte : une technologie qui permet au monde de découvrir comment garantir la sécurité, protéger les actifs et augmenter l'efficacité commerciale. Milestone Systems permet une communauté de plate-forme ouverte qui alimente la collaboration et l'innovation par le développement et l'utilisation de la technologie de la vidéo en réseau, avec des solutions fiables et évolutives qui ont fait leurs preuves sur plus de 150 000 sites à travers le monde. Fondée en 1998, Milestone Systems opère en tant que société autonome du Canon Group. Pour plus d'informations, rendez-vous à l'adresse https://www.milestonesys.com/.