MAKE THE
WORLD SEE

Milestone Systems

XProtect® Mobile Server 2020 R3

Manuel de l'administrateur

milestone

Table des matières

Copyright, marques et exclusions

Marques

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

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

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

Exonération de responsabilité

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

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

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

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

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

Vue d'ensemble

XProtect Mobile (explications)

XProtect Mobile est constitué de trois composants :

- Client XProtect Mobile

  Le client XProtect Mobile est une application de surveillance portable que vous pouvez installer et utiliser sur votre périphérique Android ou Apple. Vous pouvez utiliser autant d'installations du XProtect Mobile client que nécessaire.

  Pour en savoir plus, téléchargez le manuel de l'utilisateur du client XProtect Mobile sur le site Internet de Milestone Systems (https://www.milestonesys.com/support/help-yourself/manuals-and-guides/).

- XProtect Web Client

  XProtect Web Client vous permet de visionner des vidéos en direct dans votre navigateur Web et de télécharger des enregistrements. XProtect Web Client est installé automatiquement lors de l'installation du serveur XProtect Mobile.

  Pour en savoir plus, téléchargez le manuel de l'utilisateur du client XProtect Web Client sur le site Internet de Milestone Systems (https://www.milestonesys.com/support/help-yourself/manuals-and-guides/).

- Serveur XProtect Mobile
- Module d'extension XProtect Mobile
- Mobile Server Manager

Le serveur XProtect Mobile, le module d'extension XProtect Mobile et Mobile Server Manager sont abordés dans ce manuel.

Serveur XProtect Mobile (explications)

Le serveur XProtect Mobile gère les ouvertures de session sur le système à partir du client XProtect Mobile ou XProtect Web Client.

Un serveur XProtect Mobile distribue les flux vidéo des serveurs d'enregistrement vers le client XProtect Mobile ou XProtect Web Client. Ainsi, la configuration est sécurisée, dans la mesure où les serveurs d'enregistrements ne sont jamais connectés à Internet. Lorsqu'un serveur XProtect Mobile reçoit des flux vidéo des serveurs d'enregistrement, il gère également la conversion complexe des codecs et des formats permettant la diffusion de vidéos sur le périphérique mobile.

Vous devez installer le serveur XProtect Mobile sur n'importe quel ordinateur à partir duquel vous souhaitez accéder aux serveurs d'enregistrement. Lorsque vous installez le serveur XProtect Mobile, connectez-vous à l'aide d'un compte doté de droits d'administrateur. Autrement, il est possible que votre installation échoue (voir Installer le serveur XProtect Mobile sur la page 14).

Le serveur XProtect Mobile prend en charge la diffusion directe et le flux adaptatif en mode en direct (pour XProtect Expert et XProtect Corporate seulement).

Graphique de comparaison des produits

VMS XProtect comprend les produits suivants :

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

La liste complète des fonctionnalités est disponible sur la page de présentation du produit sur le site Web Milestone(https://www.milestonesys.com/solutions/platform/product-index/).

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

Nom	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
Sites par SLC	1	1	Multisite	Multisite	Multisite
Serveurs d'enregistrement par SLC	1	1	Illimité	Illimité	Illimité
Périphériques par serveur d'enregistrement	8	48	Illimité	Illimité	Illimité
Milestone Interconnect™	-	Site distant	Site distant	Site distant	Site central/distant
Milestone Federated Architecture™	-	-	-	Site distant	Site central/distant
Basculement sur serveur d'enregistrement	-	-	-	Affectation multiple et affectation	Affectation multiple et affectation

Nom	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
				unique	unique
Services de connexion à distance	-	-	-	-	✓
Prise en charge stockage bord	-	-	✓	✓	✓
Stockage de vidéo multiniveau	Base de données En direct + 1 archive	Base de données En direct + 1 archive	Base de données En direct + 1 archive	Bases de données actives + archives illimitées	Bases de données actives + archives illimitées
Notification SNMP	-	-	-	✓	✓
Droits d'accès utilisateur contrôlés dans le temps	-	-	-	-	✓
Réduire la fluidité d'image (affinage)	-	-	-	✓	✓
Cryptage des données vidéo (serveur d'enregistrement)	-	-	-	✓	✓
Signature de base de données (serveur d'enregistrement)	-	-	-	✓	✓
Niveaux de priorité PTZ	1	1	3	32000	32000
PTZ élargie (réserver une patrouille et une session PTZ à partir de XProtect Smart Client)	-	-	-	✓	✓

Nom	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
Verrouillage des preuves	-	-	-	-	✓
Fonction du signet	-	-	Manuelle uniquement	Manuelle et à partir de règles	Manuelle et à partir de règles
Multidiffusion directe ou multiflux direct / Flux adaptatif	-	-	-	✓	✓
Diffusion directe	-	-	-	✓	✓
Sécurité globale	Droits de l'utilisateur client	Droits de l'utilisateur client	Droits de l'utilisateur client	Droits de l'utilisateur client	Droits de l'utilisateur client/ Droits d'utilisation administrateur
Profils XProtect Management Client	-	-	-	-	✓
Profils XProtect Smart Client	-	-	3	3	Illimité
XProtect Smart Wall	-	-	-	facultatif	✓
Moniteur système	-	-	-	✓	✓
Smart Map	-	-	-	✓	✓
Vérification en deux étapes	-	-	-	-	✓
Assistance DLNA	-	✓	✓	✓	✓

Nom	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
Masquage de confidentialité	-	✓	✓	✓	✓
Gestion des mots de passe périphériques			✓	✓	✓

Exigences et considérations

Pré-requis pour l'utilisation de XProtect Mobile

Avant de pouvoir commencer à utiliser XProtect Mobile, vous devez vous assurer d'avoir les éléments suivants :

- Un VMS en fonctionnement, installé et configuré avec au moins un utilisateur
- Des caméras et des vues configurées dans XProtect Smart Client
- Un périphérique portable fonctionnant sous Android, ou iOS, avec accès à Google Play, ou l'App Store℠, sur lequel vous pouvez télécharger l'application du client XProtect Mobile
- Un navigateur Web pour l'exécution de XProtect Web Client

Pour en savoir plus sur les exigences, consultez la Configuration système de XProtect Mobile sur la page 11.

Configuration système de XProtect Mobile

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

- Pour trouver les exigences pour le client XProtect Mobile, sélectionnez le produit **XProtect Mobile**
- Pour trouver les exigences pour XProtect Web Client, sélectionnez **XProtect Web Client** l'icône du produit
- Pour connaître les exigences relatives au serveur XProtect Mobile, sélectionnez l'icône du produit XProtect que vous avez installé
- Les exigences relatives au module d'extension XProtect Mobile sont les suivantes :
    - Un Management Client en cours de fonctionnement
    - Le module d'extension Milestone est installé pour s'intégrer à votre VMS

Exigences relatives à la configuration des notifications

- Vous devez associer une ou plusieurs alarmes à un ou plusieurs événements et règles. Ceci est exigé pour les notifications système
- Assurez-vous que votre accord Milestone Care™ avec Milestone Systems est à jour
- Votre système doit avoir accès à Internet

Pour plus d'informations, voir :

Configurer les notifications Push sur le serveur XProtect Mobile sur la page 52

Onglet Notifications sur la page 27

Exigences pour la configuration Smart Connect

- Votre serveur XProtect Mobile doit utiliser une adresse IP publique. L'adresse peut être statique ou dynamique, mais il est généralement conseillé d'utiliser des adresses IP statiques
- Vous devez disposer d'une licence valide pour Smart Connect

Exigences pour la configuration de la vérification en deux étapes de l'utilisateur

- Vous avez installé un serveur SMTP
- Vous avez ajouté des utilisateurs et des groupes à votre système XProtect dans le Management Client sur le nœud **Rôles** du volet **Navigation sur le site**. Dans le rôle pertinent, sélectionnez l'onglet **Utilisateurs et Groupes**
- Si vous avez mis votre système à niveau à partir d'une version précédente de XProtect, vous devez redémarrer le serveur mobile pour permettre l'activation de la fonction de vérification en deux étapes

Pour plus d'informations, voir :

Configurer des utilisateurs pour une vérification en deux étapes par e-mail sur la page 59

Onglet Vérification en deux étapes sur la page 28

Exigences pour la configuration de vidéo push

- Chaque canal nécessite une licence de périphérique matériel
- Pour établir l'audio avec une vidéo push :
    1. Téléchargez et installez la version 10.3 ou une version plus récente de Milestone XProtect Device Pack.
    2. Téléchargez et installez la version 13.2 ou une version plus récente de XProtect Mobile Server Installer.exe.
    3. Redémarrez le service Recording Server.

Configuration de la diffusion directe

XProtect Mobile prend en charge la diffusion directe en mode en direct (pour XProtect Expert et XProtect Corporate uniquement).

Conditions de la configuration des caméras pour la diffusion directe

Pour utiliser la diffusion directe dans XProtect Web Client et dans le client XProtect Mobile, vous devez avoir la configuration de caméra suivante :

- Les caméras doivent prendre en charge le code H.264 (pour tous les clients) ou le code H.265 (pour le client XProtect Mobile seulement)
- Il est recommandé de configurer la valeur de la **taille GOP** à **1 seconde** et le paramètre **FPS** doit comporter une valeur supérieure à **10** FPS

Installation

Installer le serveur XProtect Mobile

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

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

> XProtect Mobile Le serveur s'installe automatiquement lorsque vous installez l'option Ordinateur unique.

Pour installer le serveur XProtect Mobile :

1. Saisissez l'URL suivant dans votre navigateur : *http://[adresse du serveur de gestion]/installation/admin* où [adresse du serveur de gestion] est l'adresse IP, ou le nom d'hôte du serveur de gestion.
2. Cliquez sur **Toutes les langues** pour le programme d'installation du serveur XProtect Mobile.
3. Lancez le fichier téléchargé. Ensuite, cliquez sur **Oui** pour tous les avertissements. La procédure de décompression commence alors.
4. Choisissez la langue du programme d'installation. Ensuite, cliquez sur **Continuer**.
5. Lisez et acceptez le contrat de licence. Ensuite, cliquez sur **Continuer**.
6. Sélectionnez le type d'installation :
   - Cliquez sur **Typique** pour installer le serveur XProtect Mobile et le module d'extension
   - Cliquez sur **Personnalisé** pour installer uniquement le serveur ou uniquement le module d'extension. Par exemple, l'installation du module d'extension seul est utile si vous voulez utiliser Management Client pour gérer des serveurs XProtect Mobile, mais que vous n'avez pas besoin du serveur XProtect Mobile sur cet ordinateur

     > Le module d'extension XProtect Mobile est nécessaire sur l'ordinateur qui exploite Management Client pour gérer les serveurs XProtect Mobile dans Management Client.

7. Pour une installation personnalisée seulement : Sélectionnez les composants que vous souhaitez installer. Ensuite, cliquez sur **Continuer**.

8. Sélectionnez un compte du service pour le serveur mobile. Ensuite, cliquez sur **Continuer**.

   Pour changer ou modifier les identifiants de connexion du compte de service à un stade ultérieur, vous devrez réinstaller le serveur mobile.

9. Dans le champ **URL du serveur**, saisissez l'adresse du serveur de gestion principal.
10. Pour une installation personnalisée seulement : Spécifiez les ports de connexion pour la communication avec le serveur mobile. Ensuite, cliquez sur **Continuer**.

    Dans une installation typique, les ports de connexion ont les numéros de port par défaut (8081 pour le port HTTP et 8082 pour le port HTTPS).

11. Spécifiez le cryptage du serveur mobile. Ensuite, cliquez sur **Continuer**.

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

    - Entre les serveurs mobiles et 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
    - Entre les serveurs mobiles et les clients. Choisissez un certificat dans la rubrique **Certificat de flux de multimédia** pour activer le cryptage entre le serveur mobile et les clients récoltant des flux de données depuis le serveur mobile

    Si vous n'activez pas le cryptage, des fonctionnalités sur certains clients ne seront pas disponibles. Pour plus d'informations, voir Exigences du cryptage du serveur mobile pour les clients sur la page 41.

    Pour plus d'informations sur l'établissement d'une communication sécurisée sur votre système, voir Cryptage des données du serveur mobile (explications) sur la page 40 ou le Milestone guide sur les certificats.

    Vous pouvez également activer le cryptage après l'installation complétée depuis l'icône Mobile Server Manager de la barre des tâches du système d'exploitation (voir Activer le cryptage sur le serveur mobile sur la page 46).

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

Vous êtes prêt pour la configuration de XProtect Mobile (voir Paramètres du serveur mobile sur la page 16).

Configuration

Paramètres du serveur mobile

Dans Management Client, vous pouvez configurer et modifier une liste de paramètres du serveur XProtect Mobile accessible par le biais d'onglets dans la barre d'outils inférieure de la section **Propriétés** du serveur mobile. À partir de là, vous pouvez :

- Activer ou désactiver la configuration générale des fonctionnalités du serveur (voir Onglet Généralités sur la page 16)
- Configurer les paramètres de connectivité du serveur et configurer la fonctionnalité Smart Connect (voir Onglet Connectivité sur la page 18)
- Voir l'état actuel du serveur et les utilisateurs actifs répertoriés (voir Onglet État du serveur sur la page 21)
- Configurer les paramètres de la performance pour activer la diffusion directe ou le flux adaptatif, ou bien configurer les limites du flux vidéo transcodé (voir Onglet Performances sur la page 22)
- Configurer les paramètres de l'enquête (voir Onglet Enquêtes sur la page 25)
- Configurer les paramètres de vidéo push (voir Onglet Vidéo push sur la page 26)
- Configurer, activer et désactiver le système et les notifications push (voir Onglet Notifications sur la page 27)
- Activez et configurez une étape de connexion supplémentaire pour les utilisateurs (voir Onglet Vérification en deux étapes sur la page 28)

Onglet Généralités

Le tableau suivant décrit les paramètres de cet onglet.

Généralités

Nom	Description
Nom du serveur	Saisissez un nom de serveur XProtect Mobile.
Description	Saisissez une description facultative du serveur XProtect Mobile.
Serveur Mobile	Afficher le nom du serveur XProtect Mobile sélectionné.
Méthode de	Sélectionnez la méthode d'authentification à utiliser lorsque des utilisateurs se

Nom	Description
connexion	connectent au serveur. Vous pouvez choisir entre : • **Automatique** • **Authentification Windows** • **Authentification basique**

Fonctions

Le tableau ci-dessous décrit comment vous contrôlez la disponibilité des fonctionnalités de XProtect Mobile.

Nom	Description
Activer XProtect Web Client	Activez l'accès pour XProtect Web Client. Cette fonction est activée par défaut.
Activer la vue Toutes les caméras	Inclure la vue **Toutes les caméras**. Cette vue affiche toutes les caméras qu'un utilisateur est autorisé à consulter sur un serveur d'enregistrement. Cette fonction est activée par défaut.
Activer les actions (sorties et événements)	Activez l'accès aux actions dans le client XProtect Mobile et XProtect Web Client. Cette fonction est activée par défaut. Si vous désactivez cette fonction, les utilisateurs du client ne peuvent pas voir les sorties et les événements, même s'ils sont correctement configurés.
Activer un audio entrant	Activer la fonction audio entrant dans XProtect Web Client et client XProtect Mobile. Cette fonction est activée par défaut.
Activer l'option Push-to-talk	Activer la fonctionnalité Push-to-talk (PTT) dans XProtect Web Client et client XProtect Mobile. Cette fonction est activée par défaut.
Refuser l'accès au serveur XProtect Mobile au rôle d'administrateur intégré	Activez cette fonction pour empêcher les utilisateurs assignés au rôle d'administrateur intégré d'accéder à la vidéo sur le client XProtect Mobile ou sur XProtect Web Client.

Paramètres des journaux

Vous pouvez afficher les informations des paramètres des journaux.

Nom	Description
Emplacement du fichier journal	Spécifiez à quel emplacement le système enregistre les fichiers journaux.
Activer les journaux pendant	Affichez le nombre de jours pendant lesquels les journaux sont conservés. Cette durée est fixée par défaut à trois jours.

Sauvegarde de la configuration

Si votre système possède plusieurs serveurs XProtect Mobile, vous pouvez utiliser la fonction de sauvegarde pour exporter les paramètres actuels et les importer sur d'autres serveurs XProtect Mobile.

Nom	Description
Importer	Importez un fichier XML avec une nouvelle configuration de serveur XProtect Mobile.
Exporter	Exportez votre configuration de serveur XProtect Mobile. Votre système enregistre la configuration dans un fichier XML.

Onglet Connectivité

Les paramètres de l'onglet **Connectivité** sont utilisés pour les tâches suivantes :

- Configurer les paramètres de connexion sur la page 50
- Envoyer un message par e-mail aux utilisateurs sur la page 50
- Activer les connexions sur un réseau complexe sur la page 50
- Activez le dispositif de découverte Plug and Play universel sur votre routeur sur la page 49

Pour plus d'informations, voir Smart Connect (explications) sur la page 49.

Vous pouvez configurer la connexion du client XProtect Mobile et des utilisateurs XProtect Web Client au serveur XProtect Mobile lorsque vous ouvrez le **Server Configurator** lors de l'installation ou en effectuant un clic droit sur l'icône de la barre d'état Mobile Server Manager une fois l'installation achevée. Le type de connexion peut être HTTPS ou HTTP. Pour plus d'informations, voir Activer le cryptage sur le serveur mobile sur la page 64.

Généralités

Nom	Description
Délai client expiré (HTTP)	Définissez un délai de fréquence à laquelle le client XProtect Mobile et XProtect Web Client doivent indiquer au serveur XProtect Mobile qu'ils sont opérationnels. La valeur par défaut est de 30 secondes. Milestone vous recommande de ne pas augmenter le délai.
Activer la découverte UPnP	Le serveur XProtect Mobile peut ainsi être découvert sur le réseau par le biais des protocoles UPnP. Le client XProtect Mobile présente une fonctionnalité d'analyse permettant de trouver les serveurs XProtect Mobile basés sur UPnP.
Activer le mappage automatique des ports	Lorsque le serveur XProtect Mobile est installé derrière le pare-feu, un mappage des ports est requis sur le routeur. Les clients peuvent ainsi continuer à accéder au serveur depuis Internet. L'option **Activer le mappage automatique des ports** permet au serveur XProtect Mobile de réaliser ce mappage des ports par lui-même dans la mesure où le routeur est configuré pour cela.
Activer Smart Connect	Smart Connect vous permet de vérifier que le serveur XProtect Mobile est configuré correctement sans avoir à vous connecter à l'aide d'un périphérique mobile ou d'une tablette à des fins de validation. Cette fonction simplifie également le processus de connexion pour les utilisateurs du client.

Accès Internet

Nom	Description
Configurer l'accès Internet personnalisé	Si vous utilisez le mappage de ports UPnP pour diriger les connexions vers une connexion spécifique, cochez la case **Configurer un accès personnalisé à Internet**. Ensuite, saisissez l'**adresse IP ou le nom d'hôte**, ainsi que le port à utiliser pour la connexion. Par exemple, vous devrez peut-être procéder ainsi si votre routeur ne prend pas en charge UPnP ou si vous avez une chaîne de routeurs.
Désactiver l'adresse par défaut	Désactivez les adresses IP par défaut pour vous connecter au serveur mobile uniquement à l'aide d'une adresse IP ou d'un nom d'hôte personnalisés.
Sélectionner pour récupérer l'adresse IP de manière dynamique	Si vos adresses IP changent souvent, cochez la case **Sélectionner pour récupérer l'adresse IP de manière dynamique**.
Port HTTP	Entrer le numéro du port pour la connexion HTTP. Le numéro par défaut est 8081.
Port HTTPS	Entrer le numéro du port pour la connexion HTTPS. Le numéro par défaut est 8082.
Adresses du serveur	Répertorie toutes les adresses IP qui sont connectées au serveur mobile.

Notification Smart Connect

Nom	Description
Envoyer l'invitation par e-mail à	Saisissez l'adresse e-mail du destinataire d'une notification Smart Connect.
Langue de l'e-mail	Spécifiez la langue à utiliser dans l'e-mail.
Jeton Smart Connect	Un identifiant unique que les utilisateurs de périphériques mobiles peuvent utiliser pour se connecter au serveur XProtect Mobile.
Lien vers Smart Connect	Un lien que les utilisateurs de périphériques mobiles peuvent utiliser pour se connecter au serveur XProtect Mobile.

Onglet État du serveur

Voir les détails de l'état de votre serveur XProtect Mobile. Les détails sont en lecture seule :

Nom	Description
Serveur en cours d'exécution depuis	Affiche la date et l'heure du dernier démarrage du serveur XProtect Mobile.
Utilisation unité centrale	Indique l'utilisation réelle du processeur sur le serveur mobile.
Bande passante externe	Affiche la bande passante actuellement utilisée entre le client XProtect Mobile ou XProtect Web Client et le serveur mobile.

Utilisateurs actifs

Affichez les détails de l'état du client XProtect Mobile ou de XProtect Web Client actuellement connectés au serveur XProtect Mobile.

Nom	Description
Nom d'utilisateur	Affiche le nom d'utilisateur pour chaque utilisateur du client XProtect Mobile ou de XProtect Web Client connecté au serveur mobile.
État	Indique la relation actuelle entre le serveur XProtect Mobile et le client XProtect Mobile ou l'utilisateur XProtect Web Client en question. Les états possibles sont les suivants : • **Connecté** : Un état initial lorsque les clients et le serveur échangent des clés et des certificats cryptés • **Identifié** : Le client XProtect Mobile ou l'utilisateur XProtect Web Client est connecté au système XProtect.
Utilisation de la bande passante vidéo (kB/s)	Affiche la bande passante totale des flux vidéo qui sont actuellement ouverts pour chaque client XProtect Mobile ou utilisateur XProtect Web Client.

Nom	Description
Utilisation de la bande passante audio (kB/s)	Affiche la bande passante totale des flux audio qui sont actuellement ouverts pour chaque utilisateur XProtect Web Client.
Flux vidéo transcodés	Affiche le nombre de flux vidéo transcodés qui sont actuellement ouverts pour chaque client XProtect Mobile ou utilisateur XProtect Web Client.
Diffusions vidéo directes	Affiche le nombre de diffusions vidéo directes qui sont actuellement ouverts pour chaque client XProtect Mobile ou utilisateur XProtect Web Client (pour XProtect Expert et XProtect Corporate seulement).
Flux audio transcodés	Indique le nombre total de flux audio transcodés qui sont actuellement ouverts pour chaque utilisateur XProtect Web Client.

Onglet Performances

Dans l'onglet **Performance**, vous pouvez configurer les paramètres et limites suivants concernant la performance du serveur XProtect Mobile :

Paramètres de la diffusion vidéo (pour XProtect Expert et XProtect Corporate seulement)

Nom	Description
Activer la diffusion directe	Activez la diffusion en direct dans XProtect Web Client et le client XProtect Mobile (pour XProtect Expert et XProtect Corporate seulement). Cette fonction est activée par défaut.
Activer le flux adaptatif	Activer le flux adaptatif dans XProtect Web Client et le client XProtect Mobile (pour XProtect Expert et XProtect Corporate uniquement). Cette fonction est activée par défaut.
Modes de flux	Après avoir activé la fonctionnalité du flux adaptatif, vous pouvez choisir le type de mode de flux désiré dans la liste :

Nom	Description
	• **Optimiser la qualité de la vidéo (par défaut)** : sélectionne le flux ayant la résolution la plus basse disponible qui est égale ou supérieure à la résolution demandée • **Optimiser les performances du serveur** : réduit la résolution demandée, puis sélectionne le flux ayant la résolution la plus basse disponible qui est égale ou supérieure à la résolution réduite demandée • **Optimiser la résolution pour une bande passante faible** : sélectionne le flux ayant la résolution la plus basse disponible (recommandé si vous utilisez la 3G ou un réseau instable)

Limites des flux vidéo transcodés

Niveau 1

Le **niveau 1** est la limite par défaut affectée au serveur XProtect Mobile. Les limites configurées ici s'appliquent toujours aux flux vidéo transcodés de XProtect Mobile.

Nom	Description
Niveau 1	Cochez la case pour activer le premier niveau de limites à la performance du serveur XProtect Mobile.
FPS maximum	Fixez une limite pour le nombre maximum d'images par seconde (FPS) devant être envoyé du serveur XProtect Mobile aux clients.
Résolution maximale des images	Fixez une limite pour la résolution des images devant être envoyée du serveur XProtect Mobile aux clients.

Niveau 2

Si vous souhaitez exécuter un niveau de limites différent du **Niveau 1** par défaut, cochez la case **Niveau 2**. Vous ne pouvez pas régler les paramètres à un niveau plus élevé que celui fixé au premier niveau. Ainsi, par exemple, si vous avez réglé le FPS max sur 45 au **Niveau 1**, vous ne pouvez régler le FPS max du **Niveau 2** que sur 44 ou moins.

Nom	Description
Niveau 2	Cochez la case pour activer le deuxième niveau de limites à la performance du serveur XProtect Mobile.
Seuil CPU	Fixez un seuil de charge du CPU sur le serveur XProtect Mobile avant que le système n'applique les limites du flux vidéo.
Seuil de bande passante	Fixez un seuil de bande passante sur le serveur XProtect Mobile avant que le système n'applique les limites du flux vidéo.
FPS maximum	Fixez une limite pour le nombre maximum d'images par seconde (FPS) devant être envoyé du serveur XProtect Mobile aux clients.
Résolution maximale des images	Fixez une limite pour la résolution des images devant être envoyée du serveur XProtect Mobile aux clients.

Niveau 3

Vous pouvez également cocher la case **Niveau 3** pour créer un troisième niveau de limites. Vous ne pouvez pas régler les paramètres à un niveau plus élevé que celui fixé aux **Niveau 1** et **Niveau 2**. Ainsi, par exemple, si vous avez réglé le **FPS max** sur 45 au **Niveau 1** et sur 32 au **Niveau 2**, vous ne pouvez régler le **FPS max** du **Niveau 3** que sur 31 ou moins.

Nom	Description
Niveau 3	Cochez la case pour activer le troisième niveau de limites à la performance du serveur XProtect Mobile.
Seuil CPU	Fixez un seuil de charge du CPU sur le serveur XProtect Mobile avant que le système n'applique les limites du flux vidéo.
Seuil de bande passante	Fixez un seuil de bande passante sur le serveur XProtect Mobile avant que le système n'applique les limites du flux vidéo.
FPS maximum	Fixez une limite pour le nombre d'images par seconde (FPS) devant être envoyé du serveur XProtect Mobile aux clients.
Résolution maximale des images	Fixez une limite pour la résolution des images devant être envoyée du serveur XProtect Mobile aux clients.

Le système ne bascule pas instantanément d'un niveau à un autre. Si votre seuil de CPU ou de bande passante dépasse les niveaux indiqués de moins de cinq pour cent, le niveau actuel continue d'être utilisé.

Onglet Enquêtes

Paramètres des enquêtes

Vous pouvez activer les enquêtes de façon à ce que les utilisateurs puissent utiliser le client XProtect Mobile ou XProtect Web Client pour accéder à la vidéo enregistrée et mener des enquêtes sur les incidents, mais aussi préparer et télécharger des preuves vidéo.

Nom	Description
Activer les enquêtes	Cochez cette case pour permettre aux utilisateurs d'accéder aux enquêtes qu'ils n'ont pas créées.
Répertoire Enquêtes	Affiche l'emplacement où vos exportations vidéo sont enregistrées sur votre disque dur.
Activer la limite de la taille du répertoire d'enquêtes	Cochez cette case pour configurer une taille limite du répertoire d'enquêtes et saisissez le nombre maximum de méga-octets que le répertoire d'enquêtes peut contenir. La taille par défaut est 2000 Mo.
Voir les enquêtes créées par d'autres	Cochez cette case pour permettre aux utilisateurs pour accéder aux enquêtes qu'ils n'ont pas créées.
Inclure l'horodatage pour les exports AVI	Cochez cette case pour inclure la date et l'heure auxquelles le fichier AVI a été téléchargé.
Codec utilisé pour les fichiers AVI	Sélectionnez le format de compression à utiliser lors de la préparation de paquets AVI à télécharger. Les codecs que vous pouvez choisir peuvent être différents selon votre système d'exploitation. Si vous ne voyez pas le codec souhaité, vous pouvez l'ajouter à la liste en l'installation sur l'ordinateur exécutant le serveur XProtect

Nom	Description
	Mobile.
Débit binaire audio utilisé pour les exportations AVI	Dans le débit binaire audio approprié dans la liste lorsque votre exportation vidéo inclut l'audio. La valeur par défaut est 160000 Hz.
Conserver ou supprimer les données en cas d'échec de l'export (MKV et AVI)	Indiquez s'il faut conserver ou supprimer les données qui n'ont pas été préparées correctement à des fins de téléchargement dans une enquête.

Enquêtes

Nom	Description
Enquêtes	Affiche la liste des enquêtes qui ont été configurées dans le système jusqu'à maintenant. Utilisez les boutons **Supprimer** ou **Supprimer tout** si vous ne souhaitez plus conserver une enquête. Par exemple, ceci peut s'avérer utile si vous souhaitez libérer plus d'espace disponible sur le serveur.
Détails d'enquête	Pour supprimer des fichiers vidéo individuels qui ont été exportés pour une enquête, mais conserver l'enquête, sélectionnez l'enquête dans la liste. Dans le groupe **Détails de l'enquête**, sélectionnez l'icône Supprimer à droite des champs **Base de données**, **AVI**, ou **MKV** pour les exports.

Onglet Vidéo push

Vous pouvez spécifier les paramètres suivants si vous activez la fonction vidéo push :

Nom	Description
Vidéo push	Activer la vidéo push sur le serveur mobile.
Nombre de canaux	Affiche le nombre de canaux sur lesquels la vidéo push est activée dans votre système XProtect.
Canal	Présente le nombre de canal pour le canal adéquat. Non éditable.
Port	Numéro de port pour le canal video-push adéquat.
Adresse MAC	Adresse MAC pour le canal video-push adéquat.
Nom d'utilisateur	Indiquez le nom d'utilisateur associé au canal vidéo push pertinent.
Nom de la caméra	Affiche le nom de la caméra, si la caméra a été identifiée.

Une fois que vous avez terminé toutes les étapes nécessaires (voir Configuration de vidéo push pour diffuser la vidéo sur la page 55), sélectionnez **Trouver des caméras** pour rechercher la caméra correspondante.

Onglet Notifications

Utilisez l'onglet **Notifications** pour activer ou désactiver les notifications du système et les notifications push.

Si vous activez les notifications et si vous avez configuré un ou plusieurs événements et alarmes, XProtect Mobile informe les utilisateurs de la survenance d'un événement. Lorsque l'application est ouverte, les notifications sont présentées dans XProtect Mobile sur le périphérique portable. Les notifications push informent les utilisateurs qui n'ont pas ouvert XProtect Mobile. Ces notifications sont fournies directement au périphérique portable.

Pour plus d'informations, voir : Activer l'envoi de notifications push à des périphériques portables spécifiques ou à tous les périphériques portables sur la page 52

Le tableau suivant décrit les paramètres de cet onglet.

Nom	Description
Notifications	Cochez la case pour activer les notifications.

Nom	Description
Maintenir l'inscription du périphérique	Cochez cette case pour stocker des informations au sujet des périphériques et des utilisateurs qui se connectent au serveur. Le système envoie des notifications à ces périphériques. En décochant cette case, vous effacez également la liste de périphériques. Pour que les utilisateurs recommencent à recevoir des notifications, vous devez cocher la case et les utilisateurs doivent reconnecter leurs périphériques au serveur.

Périphériques enregistrés

Nom	Description
Activé	Cochez cette case pour commencer à envoyer des notifications au périphérique.
Nom du périphérique	Une liste des périphériques portables qui se sont connectés au serveur. Vous pouvez commencer ou arrêter d'envoyer des notifications à des périphériques spécifiques en cochant ou décochant la case **Activé**.
Utilisateur	Nom de l'utilisateur qui recevra les notifications.

Onglet Vérification en deux étapes

Les fonctions disponibles dépendent du système que vous utilisez. Voir https://www.milestonesys.com/solutions/platform/product-index/ pour plus d'informations.

Utilisez l'onglet **Vérification en deux étapes** pour l'activer et spécifiez une étape de connexion supplémentaire pour les utilisateurs de :

- XProtect Mobile application sur leurs périphériques portables iOS ou Android
- XProtect Web Client

Le premier type de vérification est un mot de passe. Le second type est un code de vérification que vous pouvez configurer de façon à ce qu'il soit envoyé à l'utilisateur par e-mail.

Pour de plus amples informations, voir Configurer des utilisateurs pour une vérification en deux étapes par e-mail sur la page 59.

Les tableaux suivants décrivent les paramètres de cet onglet.

Paramètres du prestataire > **E-mail**

Nom	Description
Serveur SMTP	Saisissez l'adresse IP ou le nom d'hôte du serveur de protocole simple de transfert d'e-mails (SMTP) pour les e-mails de vérification en deux étapes.
Port du serveur SMTP	Spécifiez le port du serveur SMTP pour l'envoi des e-mails. Le numéro de port par défaut est 25 sans SSL et 465 avec SSL.
Utiliser SSL	Cochez cette case si votre serveur SMTP prend en charge le cryptage SSL.
Nom d'utilisateur	Indiquez le nom d'utilisateur requis pour se connecter au serveur SMTP.
Mot de passe	Indiquez le mot de passe requis pour se connecter au serveur SMTP.
Utiliser l'authentification à mot de passe sécurisé (SPA)	Cochez cette case si votre serveur SMTP prend en charge SPA.
Adresse e-mail de l'expéditeur	Indiquez l'adresse e-mail pour l'envoi des codes de vérification.
Objet de l'e-mail	Indiquez le titre (objet) de l'e-mail. Exemple : Votre code de vérification en deux étapes.
Texte de l'e-mail	Saisissez le message que vous souhaitez envoyer. Exemple : Votre code est {0}. Par défaut, si vous oubliez d'inclure la variable {0}, le code est ajouté à la fin du texte.

Paramètres du code de vérification

Nom	Description
Temporisation de reconnexion (0-30 minutes)	Indiquez la période au cours de laquelle les utilisateurs du client XProtect Mobile n'ont pas besoin de revérifier leur connexion en cas de déconnexion du réseau, par exemple. La période par défaut est de trois minutes. Ce paramètre ne s'applique pas à XProtect Web Client.
Le code expire après (1-10 minutes)	Spécifiez la période au cours de laquelle l'utilisateur peut utiliser le code de vérification reçu. Après cette période, le code est invalide et l'utilisateur doit demander un nouveau code. La période par défaut est de cinq minutes.
Tentatives de saisie du code (1-10 tentatives)	Spécifiez le nombre maximum de tentatives de saisie du code avant que le code fourni ne soit plus valide. Le nombre par défaut est trois.
Longueur du code (4-6 caractères)	Spécifiez le nombre de caractères dans le code. La longueur par défaut est de six.
Composition du code	Spécifiez la complexité du code généré par le système. Vous pouvez choisir entre : • **Majuscules latines (A-Z)** • **Minuscules latines (a-z)** • **Chiffres (0-9)** • **Caractères spéciaux (!@#...)**

Paramètres de l'utilisateur

Nom	Description
Utilisateurs et groupes	Affiche la liste des utilisateurs et groupes ajoutés au système XProtect. Si un groupe est configuré dans Active Directory, le serveur mobile utilise des détails, tels que des adresses e-mail, tirés d'Active Directory.

Nom	Description
	Les groupes Windows ne prennent pas la vérification en deux étapes en charge.
Méthode de vérification	Sélectionnez un paramètre de vérification pour chaque utilisateur ou groupe. Vous pouvez choisir entre : • **Aucune connexion** : l'utilisateur ne peut pas se connecter • **Pas de vérification en deux étapes** : l'utilisateur doit saisir un nom d'utilisateur et un mot de passe • **E-mail** : l'utilisateur doit saisir un code de vérification envoyé par e-mail en plus du nom d'utilisateur standard et du mot de passe
Détails utilisateur	Saisissez l'adresse e-mail sur laquelle chaque utilisateur recevra les codes.

Diffusion directe (explications)

XProtect Mobile prend en charge la diffusion directe en mode en direct (pour XProtect Expert et XProtect Corporate uniquement).

La diffusion directe est une technologie de diffusion vidéo qui transfère la vidéo depuis un système XProtect vers les clients directement en code H.264, lequel est pris en charge par la plupart des caméras IP modernes. La diffusion directe ne requiert aucun transcodage pour se produire et supprime ainsi une certaine tension sur le système XProtect.

La technologie de diffusion directe est le contraire du paramètre du transcodage dans XProtect, dans lequel un système XProtect décode la vidéo à partir d'un codec utilisé sur la caméra dans des fichiers JPEG. L'activation de cette fonctionnalité provoque une réduction de l'utilisation du CPU pour la même configuration des caméras et des flux vidéo. La diffusion directe augmente également la performance du matériel : jusqu'à cinq fois plus de flux vidéo simultanés qu'avec le transcodage.

Vous pouvez également utiliser la fonctionnalité de la diffusion directe pour transférer de la vidéo à partir de caméras qui prennent en charge le code H.265 directement vers le client XProtect Mobile.

Dans Management Client, vous pouvez activer ou désactiver la diffusion directe pour les clients (voir Paramètres du serveur mobile sur la page 16).

Le flux vidéo retourne du flux adaptatif au transcodage si :

- La fonctionnalité de la diffusion directe a été désactivée dans Management Client ou si les critères n'ont pas été remplis (voir Configuration de la diffusion directe sur la page 12)
- Le codec de la caméra en diffusion est différent du codec H.264 (pour tous les clients) ou du codec H.265 (pour le client XProtect Mobile uniquement)
- La vidéo ne démarre pas pendant plus de dix secondes
- La fluidité d'image de la caméra en diffusion est configurée à **une** image par seconde (1 FPS)
- La connexion au serveur et à la caméra a été perdue
- Vous utilisez la fonctionnalité de masquage de confidentialité lors de la vidéo en direct

Flux adaptatif (explication)

XProtect Mobile prend en charge le flux adaptatif en mode en direct (pour XProtect Expert et XProtect Corporate uniquement).

Le flux adaptatif est utile lorsque vous visionnez plusieurs flux vidéo en direct dans la même vue de caméras. La fonctionnalité optimise la performance du serveur XProtect Mobile et améliore le décodage et la performance des périphériques exécutant XProtect Mobile client et XProtect Web Client.

Pour tirer le meilleur parti du flux adaptatif, vos caméras doivent avoir plusieurs flux définis avec différentes résolutions. Dans ce cas, la fonctionnalité vous permet de :

- Optimiser la qualité de la vidéo : sélectionne le flux ayant la résolution la plus basse disponible qui est égale ou supérieure à la résolution demandée
- Optimiser les performances du serveur : réduit la résolution demandée, puis sélectionne le flux ayant la résolution la plus basse disponible qui est égale ou supérieure à la résolution réduite demandée
- Optimiser la résolution pour une bande passante faible : sélectionne le flux ayant la résolution la plus basse disponible (recommandé si vous utilisez la 3G ou un réseau instable)

Lorsqu'une vidéo est zoomée, le flux vidéo en direct requis est toujours celui ayant la résolution la plus élevée disponible.

L'utilisation de la bande passante est souvent réduite lorsque l'est la résolution du flux requis. L'utilisation de la bande passante dépend également d'autres paramètres de la configuration des flux définis.

Vous pouvez activer ou désactiver un flux adaptatif et configurer votre mode de diffusion de la fonctionnalité préféré sous l'**onglet Performance** des paramètres du serveur mobile dans Management Client (voir Paramètres du serveur mobile sur la page 16).

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

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

Une autorité de certification (AC) peut émettre des certificats aux services Web sur des serveurs utilisant un certificat de l'AC. 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 désormais utiliser le certificat de serveur public et privé pour échanger une clé secrète et par conséquent, établir une connexion SSL/TLS sécurisée.

Pour plus d'informations sur TLS : https://en.wikipedia.org/wiki/Transport_Layer_Security

Les certificats possèdent une date d'expiration. VMS XProtect 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.

Lorsque vous renouvelez un certificat avec le même nom de sujet, et que vous l'ajoutez à la Windows Certificate Store, les serveurs choisiront automatiquement le nouveau certificat. Cela rend plus facile la rénovation des certificats pour plusieurs serveurs d'enregistrement sans avoir à sélectionner de nouveau le certificat pour chaque serveur d'enregistrement et sans avoir à redémarrer les services.

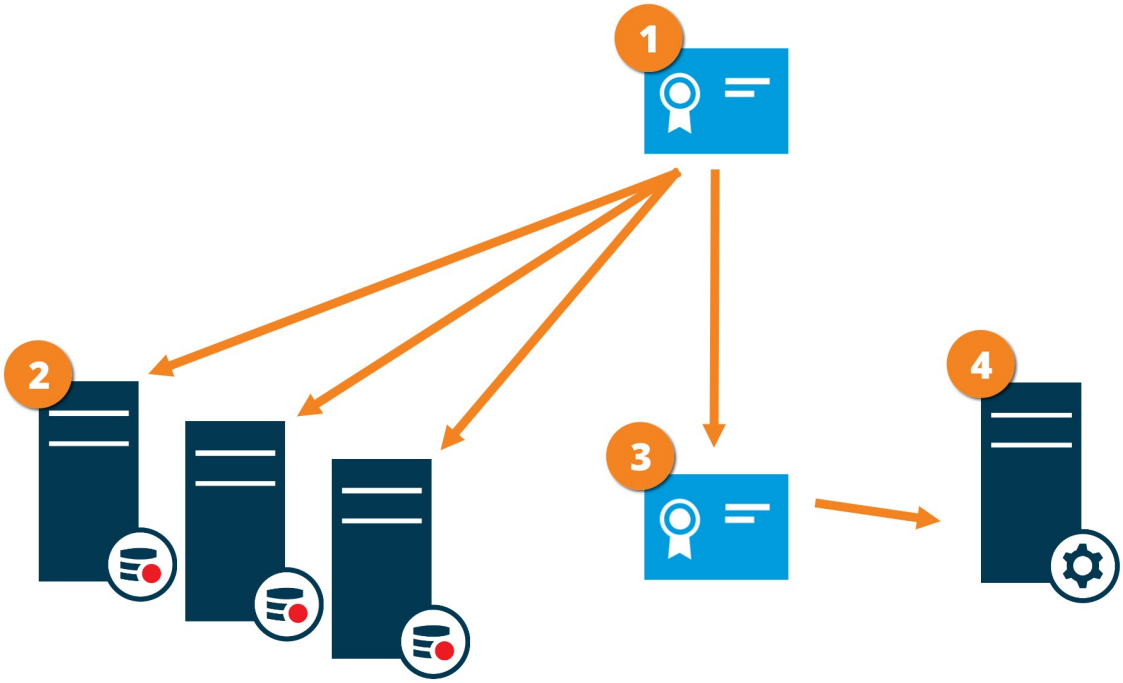
Cryptage du serveur de gestion (explications)

Vous pouvez crypter une connexion bidirectionnelle entre le serveur de gestion et le serveur d'enregistrement. Lorsque vous activez le cryptage sur le serveur de gestion, il s'applique aux connexions depuis les serveurs d'enregistrement se connectant au serveur de gestion. Si vous activez le cryptage sur le serveur de gestion, vous

devez également activer le cryptage sur tous les serveurs d'enregistrement. Avant d'activer le cryptage, vous devez installer des certificats de sécurité sur le serveur de gestion et tous les serveurs d'enregistrement.

Distribution de certificat pour les serveurs de gestion

Le diagramme illustre le concept de base de comment les certificats sont-ils signés, fiables et distribués dans VMS XProtect dans le but de sécuriser la communication vers le serveur de gestion.



❶ Un certificat de l'AC agit en tant que tiers de confiance, jouissant de la confiance du sujet/propriétaire (le serveur de gestion) et de la partie vérifiant le certificat (serveur d'enregistrement)

❷ Le certificat privé de l'AC doit être fiable sur tous les serveurs d'enregistrement. De cette manière, les serveurs d'enregistrement vérifient la validité des certificats émis par l'AC

❸ Le certificat de l'AC est utilisé pour établir une connexion sécurisée entre le serveur de gestion et les services d'enregistrement

❹ Le certificat de l'AC doit être installé sur un ordinateur exécutant le serveur de gestion

Prérequis pour le certificat privé sur le serveur de gestion :

- Émis au serveur de gestion, donc le nom d'hôte du serveur de gestion est inclus dans le nom du certificat, soit en tant qu'objet (propriétaire) ou dans la liste des noms DNS auxquels est émis le certificat
- Fiable sur le serveur de gestion lui-même en utilisant un certificat de l'AC qui a été utilisé pour émettre le

certificat du serveur de gestion

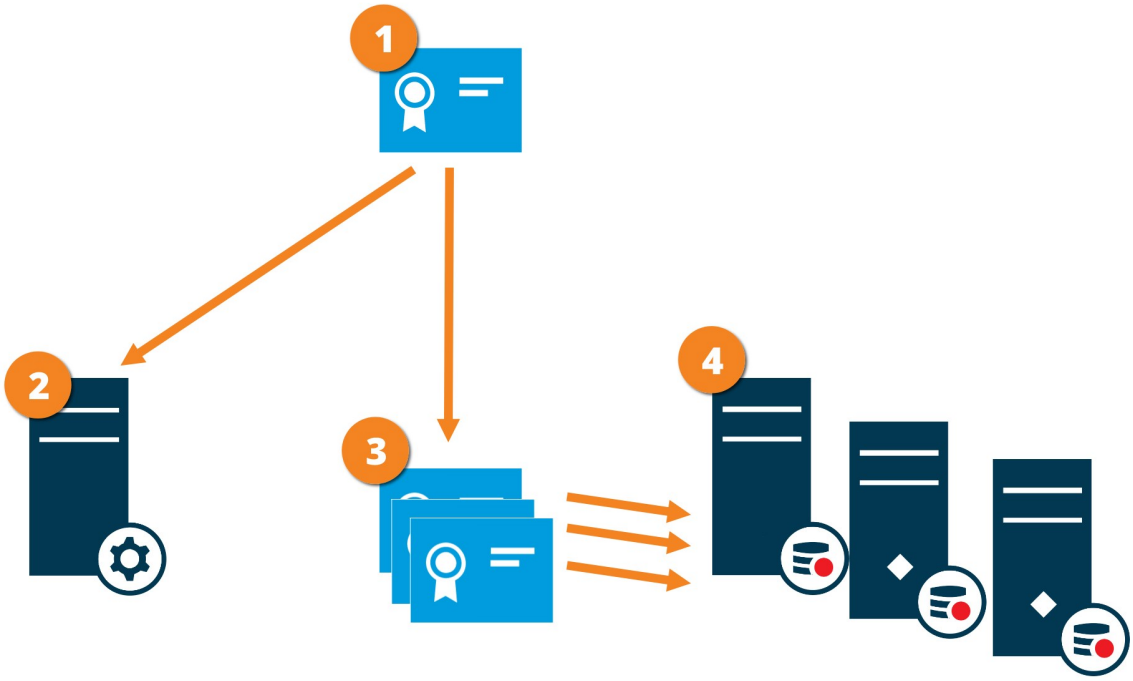
- Fiable sur tous les serveurs d'enregistrement connectés au serveur de gestion de préférence en utilisant un certificat de l'AC qui a été utilisé pour émettre le certificat du serveur de gestion

Cryptage du serveur de gestion vers le serveur d'enregistrement (explications)

Vous pouvez crypter une connexion bidirectionnelle entre le serveur de gestion et le serveur d'enregistrement. Lorsque vous activez le cryptage sur le serveur de gestion, il s'applique aux connexions depuis les serveurs d'enregistrement se connectant au serveur de gestion. Le cryptage de cette communication doit suivre les paramètres de cryptage sur le serveur de gestion. Ainsi, si le cryptage du serveur de gestion est activé, celui-ci doit être également activé sur les serveurs d'enregistrement et vice versa. Avant d'activer le cryptage, vous devez installer des certificats de sécurité sur le serveur de gestion et tous les serveurs d'enregistrement, dont les serveurs d'enregistrement de redondance.

Distribution de certificat

Le diagramme illustre le concept de base de comment les certificats sont-ils signés, fiables et distribués dans VMS XProtect dans le but de sécuriser la communication depuis le serveur de gestion.



❶ Un certificat de l'AC agit en tant que tiers de confiance, jouissant de la confiance du sujet/propriétaire (le serveur d'enregistrement) et de la partie vérifiant le certificat (serveur de gestion)

❷ Le certificat de l'AC doit être fiable sur tous les serveurs de gestion. De cette manière, le serveur de gestion vérifie la validité des certificats émis par l'AC

❸ Le certificat de l'AC est utilisé pour établir une connexion sécurisée entre les serveurs d'enregistrement et le serveur de gestion

❹ Le certificat de l'AC doit être installé sur les ordinateurs exécutant les serveurs d'enregistrement

Prérequis pour le certificat privé sur le serveur d'enregistrement :

- Émis au serveur d'enregistrement, donc le nom d'hôte du serveur d'enregistrement est inclus dans le certificat, soit en tant qu'objet (propriétaire) ou dans la liste des noms DNS auxquels est émis le certificat
- Fiable sur tous les serveurs de gestion connectés au serveur de gestion de préférence en utilisant un certificat de l'AC qui a été utilisé pour émettre le certificat du serveur d'enregistrement

Cryptage entre le serveur de gestion et le Data Collector Server (explications)

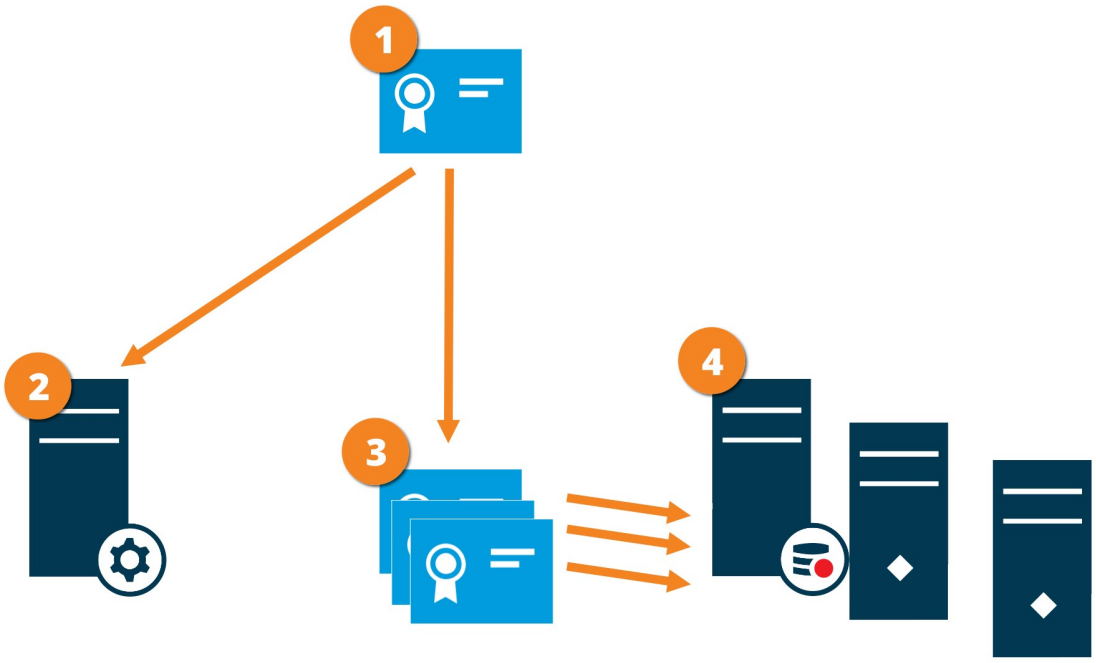
Vous pouvez crypter une connexion bidirectionnelle entre le serveur de gestion et le Data Collector affilié lorsque vous disposez d'un type de serveur distant suivant :

- Recording Server
- Event Server
- Log Server
- LPR Server
- Mobile Server

Lorsque vous activez le cryptage sur le serveur de gestion, il s'applique aux connexions depuis les serveurs Data Collector se connectant au serveur de gestion. Le cryptage de cette communication doit suivre les paramètres de cryptage sur le serveur de gestion. Ainsi, si le cryptage du serveur de gestion est activé, celui-ci doit être également activé sur les serveurs Data Collector affiliés à chacun des serveurs distants et vice versa. Avant d'activer le cryptage, vous devez installer des certificats de sécurité sur le serveur de gestion et tous les serveurs Data Collector affiliés aux serveurs distants.

Distribution de certificat

Le diagramme illustre le concept de base de comment les certificats sont-ils signés, fiables et distribués dans VMS XProtect dans le but de sécuriser la communication depuis le serveur de gestion.



1 Un certificat de l'AC agit en tant que tiers de confiance, jouissant de la confiance du sujet/propriétaire (le serveur de collecteur de données) et de la partie vérifiant le certificat (serveur de gestion)

2 Le certificat de l'AC doit être fiable sur tous les serveurs de gestion. De cette manière, le serveur de gestion vérifie la validité des certificats émis par l'AC

3 Le certificat de l'AC est utilisé pour établir une connexion sécurisée entre les serveurs de collection de données et le serveur d'enregistrement

4 Le certificat de l'AC doit être installé sur les ordinateurs exécutant les serveurs de collection de données

Prérequis pour le certificat privé sur le serveur de collection de données :

- Émis au serveur de collection de données, donc le nom d'hôte du serveur de collection de données est inclus dans le certificat, soit en tant qu'objet (propriétaire) ou dans la liste des noms DNS auxquels est émis le certificat
- Fiable sur tous les serveurs de gestion connectés au serveur de gestion de préférence en utilisant un certificat de l'AC qui a été utilisé pour émettre le certificat du serveur de collection de donnée

Le cryptage s'applique à tous les clients et serveurs recueillant des flux de données depuis le serveur d'enregistrement (explications)

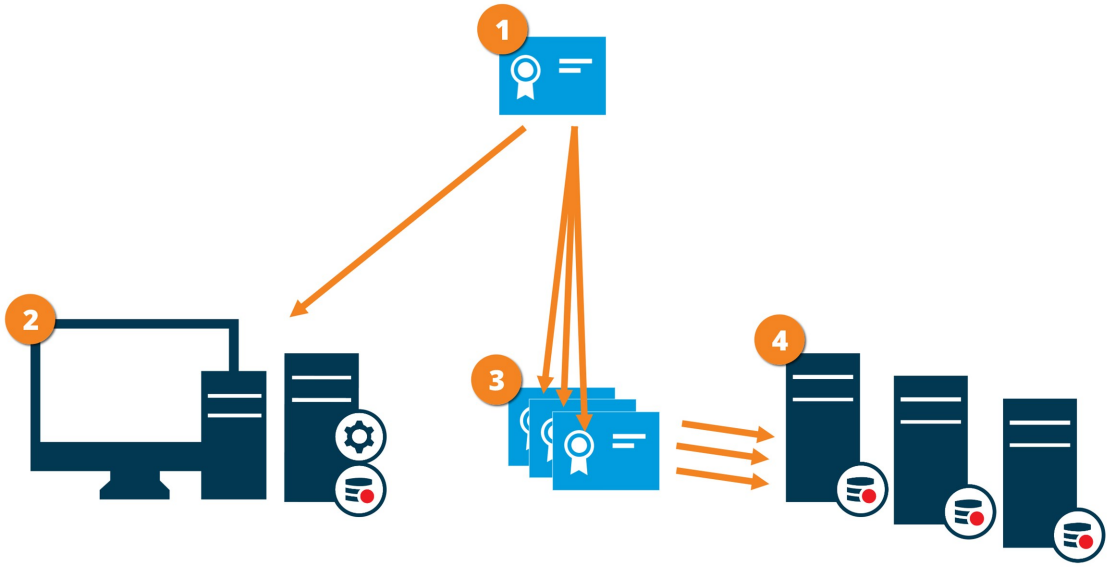
Lorsque vous activez le cryptage sur un serveur d'enregistrement, les communications depuis tous les clients, serveurs et intégrations récoltant des flux de données depuis le serveur d'enregistrement sont cryptées. Dans ce document, dénommé comme « clients » :

- XProtect Smart Client
- Management Client
- Management Server (pour le Système de surveillance et les images ainsi que les vidéos AVI dans les notifications par email)
- Serveur XProtect Mobile
- XProtect Event Server
- XProtect LPR
- Milestone Open Network Bridge
- XProtect DLNA Server
- Les sites collectant des flux de donnée depuis le serveur d'enregistrement par le biais de Milestone Interconnect
- Quelques intégrations tierces de MIP SDK

Pour des solutions intégrant MIP SDK 2018 R3 ou une version plus récente qui accède aux serveurs d'enregistrement : Si les intégrations sont effectuées en utilisant des bibliothèques MIP SDK, elles ont besoin d'être réintégrées avec MIP SDK 2019 R1. Si les intégrations communiquent directement avec les IPA du serveur d'enregistrement sans utiliser les bibliothèques MIP SDK, les intégrateurs doivent alors ajouter le support HTTPS eux-mêmes.

Distribution de certificat

Le diagramme illustre le concept de base de comment les certificats sont-ils signés, fiables et distribués dans VMS XProtect dans le but de sécuriser la communication vers le serveur d'enregistrement.



1 Un certificat de l'AC agit en tant que tiers de confiance, jouissant de la confiance du sujet/propriétaire (le serveur d'enregistrement) et de la partie vérifiant le certificat (tous les clients)

2 Le certificat privé de l'AC doit être fiable sur tous les clients. De cette manière, les clients peuvent vérifier la validité des certificats émis par l'AC

3 Le certificat de l'AC est utilisé pour établir une connexion sécurisée entre les serveurs d'enregistrement et tous les clients et services

4 Le certificat de l'AC doit être installé sur les ordinateurs exécutant les serveurs d'enregistrement

Prérequis pour le certificat privé sur le serveur d'enregistrement :

- Émis au serveur d'enregistrement, donc le nom d'hôte du serveur d'enregistrement est inclus dans le certificat, soit en tant qu'objet (propriétaire) ou dans la liste des noms DNS auxquels est émis le certificat
- Fiable sur tous les ordinateurs exécutant des services qui collectent des flux de données depuis les serveurs d'enregistrement, de préférence en utilisant un certificat de l'AC qui a été utilisé pour émettre le certificat du serveur d'enregistrement
- Le compte du service exécutant le serveur d'enregistrement doit avoir accès à la clé privée du certificat sur le serveur d'enregistrement.

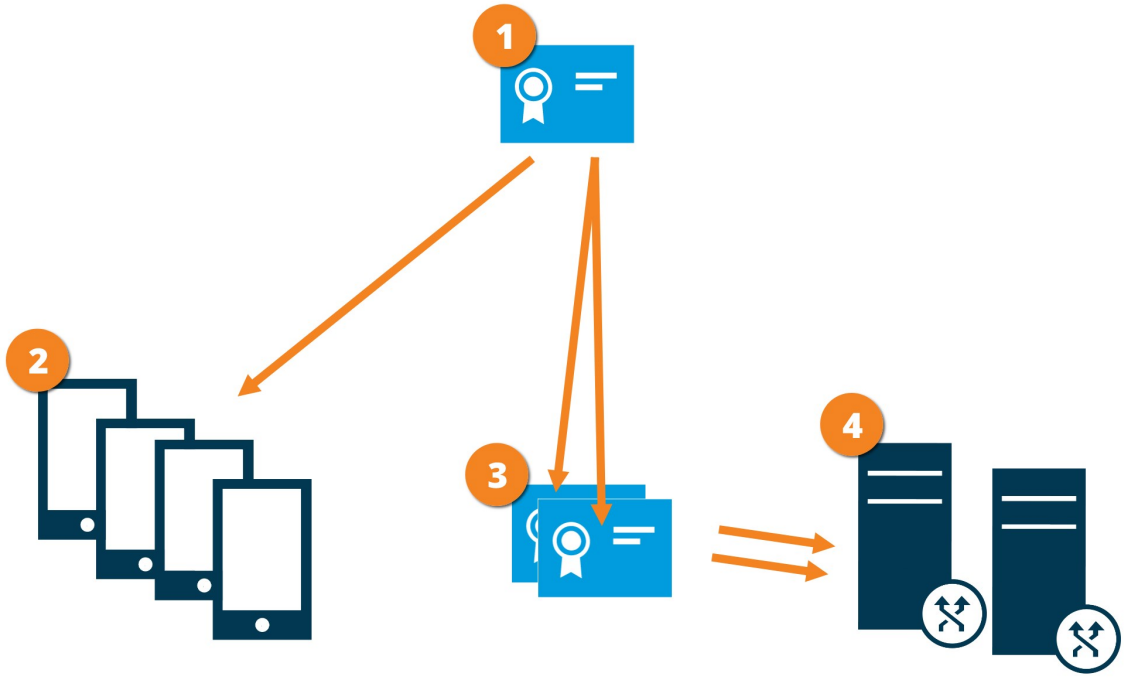
Si vous activez le cryptage sur les serveurs d'enregistrement et que votre système applique des serveurs d'enregistrement de basculement, Milestone vous recommande de préparer également le serveur d'enregistrement de redondance pour le cryptage.

Cryptage des données du serveur mobile (explications)

Sur VMS XProtect, le cryptage est activé ou désactivé par serveur mobile. Lorsque vous activez le cryptage sur un serveur mobile, vous aurez l'option d'utiliser une communication cryptée avec tous les clients, services et intégrations récoltant des flux de données.

Distribution de certificat pour les serveurs mobiles

Le diagramme illustre le concept de base de comment les certificats sont-ils signés, fiables et distribués dans VMS XProtect dans le but de sécuriser la communication avec le serveur mobile.



❶ Un certificat de l'AC agit en tant que tiers de confiance, jouissant de la confiance du sujet/propriétaire (le serveur mobile) et de la partie vérifiant le certificat (tous les clients)

❷ Le certificat privé de l'AC doit être fiable sur tous les clients. De cette manière, les clients vérifient la validité des certificats émis par l'AC

❸ Le certificat de l'AC est utilisé pour établir une connexion sécurisée entre le serveur mobile et les clients et services

❹ Le certificat de l'AC doit être installé sur un ordinateur exécutant le serveur mobile

Prérequis pour le certificat de l'AC :

- Le nom d'hôte du serveur mobile doit être inclus dans le certificat, soit en tant qu'objet/propriétaire ou dans la liste des noms DNS auxquels est émis le certificat
- Un certificat doit être fiable sur tous les périphériques exécutant des services qui collectent des flux de données depuis le serveur mobile
- Le compte du service exécutant le serveur mobile doit avoir accès à la clé privée du certificat de l'AC

Exigences du cryptage du serveur mobile pour les clients

Si vous n'activez pas le cryptage et que vous utilisez une connexion HTTP, la fonctionnalité appuyer pour parler dans XProtect Web Client ne sera pas disponible.

Activer le cryptage

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.

Activer le cryptage depuis et vers le serveur de gestion

Vous pouvez crypter une connexion bidirectionnelle entre le serveur de gestion et le serveur d'enregistrement ou tout autre serveur distant avec le collecteur de données (Event Server, Log Server, LPR Server et Mobile Server).

Si votre système contient plusieurs serveurs d'enregistrement ou serveurs distants, vous devez activer le cryptage sur tous. Pour plus d'informations, voir Cryptage du serveur de gestion (explications) sur la page 33.

Pré-requis :

- Un certificat d'authentification du serveur est fiable sur l'ordinateur hébergeant le serveur de gestion

D'abord, vous devez activer le cryptage sur le serveur de gestion.

Étapes :

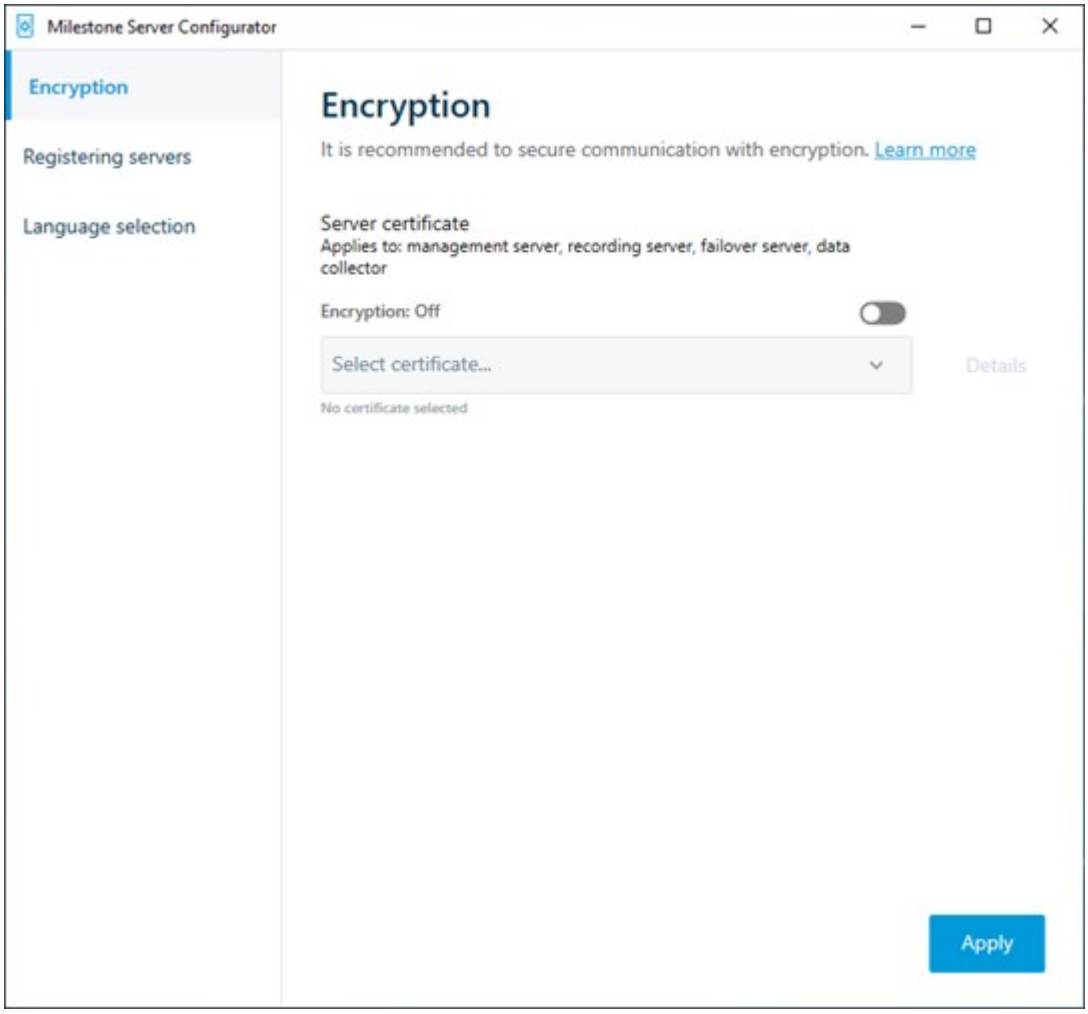
1. Sur un ordinateur où est installé le serveur de gestion, ouvrez le **Server Configurator** à partir de :
   - Le menu Démarrer de Windows

   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 serveur de collection de données.

   Sélectionnez **Détails** pour lire les informations de la Windows Certificate Store sur le certificat sélectionné.



5. Cliquez sur **Appliquer**.

Pour achever l'activation du cryptage, la prochaine étape consiste à mettre à jour les paramètres de cryptage sur chaque serveur d'enregistrement et sur chaque serveur de collecteur de données (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 sur la page 42.

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 avec le collecteur de données (Event Server, Log Server, LPR Server et Mobile Server).

Si votre système contient plusieurs serveurs d'enregistrement ou serveurs distants, vous devez activer le cryptage sur tous. Pour plus d'informations, voir Cryptage du serveur de gestion vers le serveur d'enregistrement (explications) sur la page 35 et Cryptage entre le serveur de gestion et le Data Collector Server (explications) sur la page 36.

Pré-requis :

- Vous avez activé le cryptage sur le serveur de gestion, voir Activer le cryptage sur la page 41

Étapes :

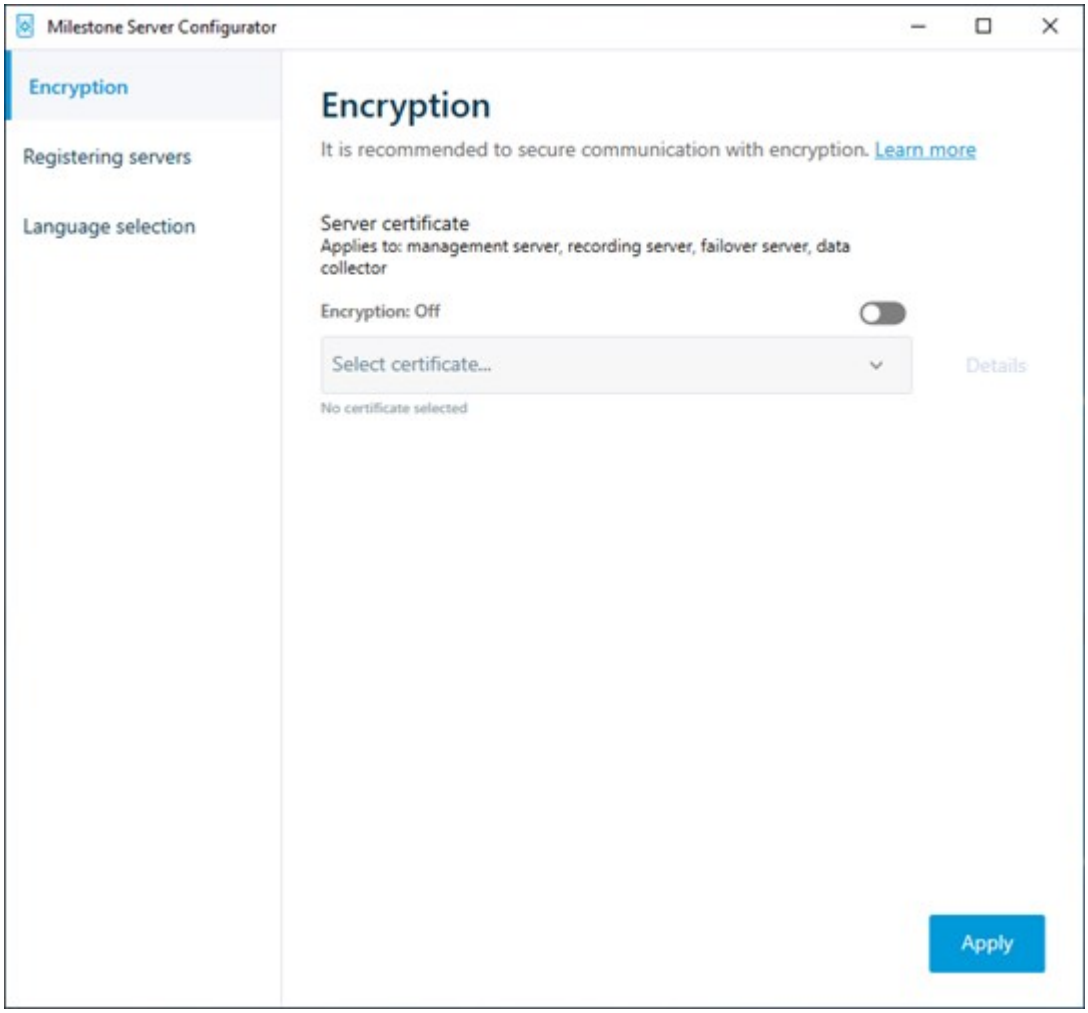
1. Sur un ordinateur où est installé le serveur d'enregistrement, ouvrez le **Server Configurator** à partir de :
   - Le menu Démarrer de Windows

   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 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 sur 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.



2. 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 cryptage pour les clients et les serveurs

Vous pouvez crypter des connexions depuis le serveur d'enregistrement vers les clients et serveurs qui transfèrent des données depuis le serveur d'enregistrement. Pour plus d'informations, voir Le cryptage s'applique à tous les clients et serveurs recueillant des flux de données depuis le serveur d'enregistrement (explications) sur la page 37.

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 :

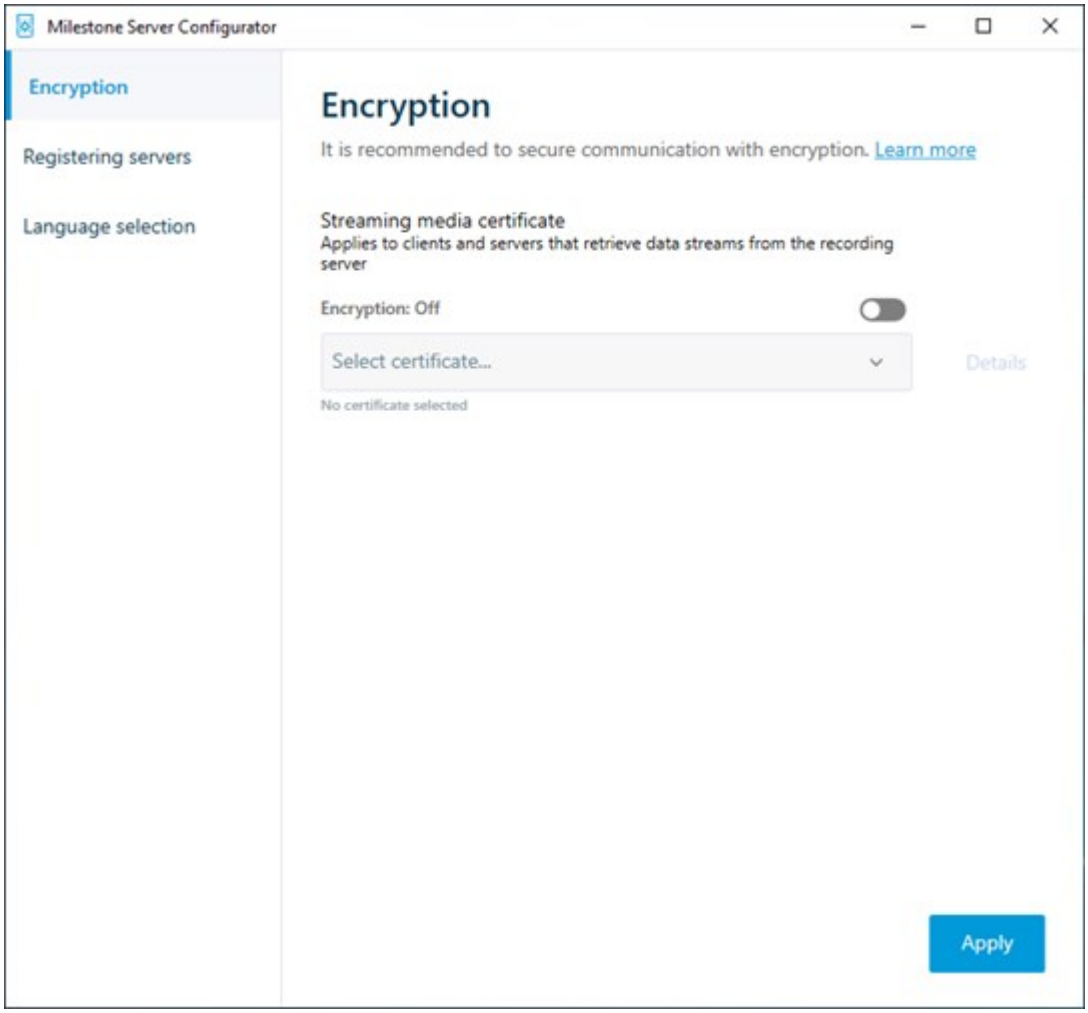
1. Sur un ordinateur où est installé le serveur d'enregistrement, ouvrez le **Server Configurator** à partir de :
   - Le menu Démarrer de Windows

   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 de flux de multimédia**, 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.



2. 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 Cryptage des données du serveur mobile (explications) sur la page 40 et Exigences du cryptage du serveur mobile pour les clients sur la page 41.

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 :

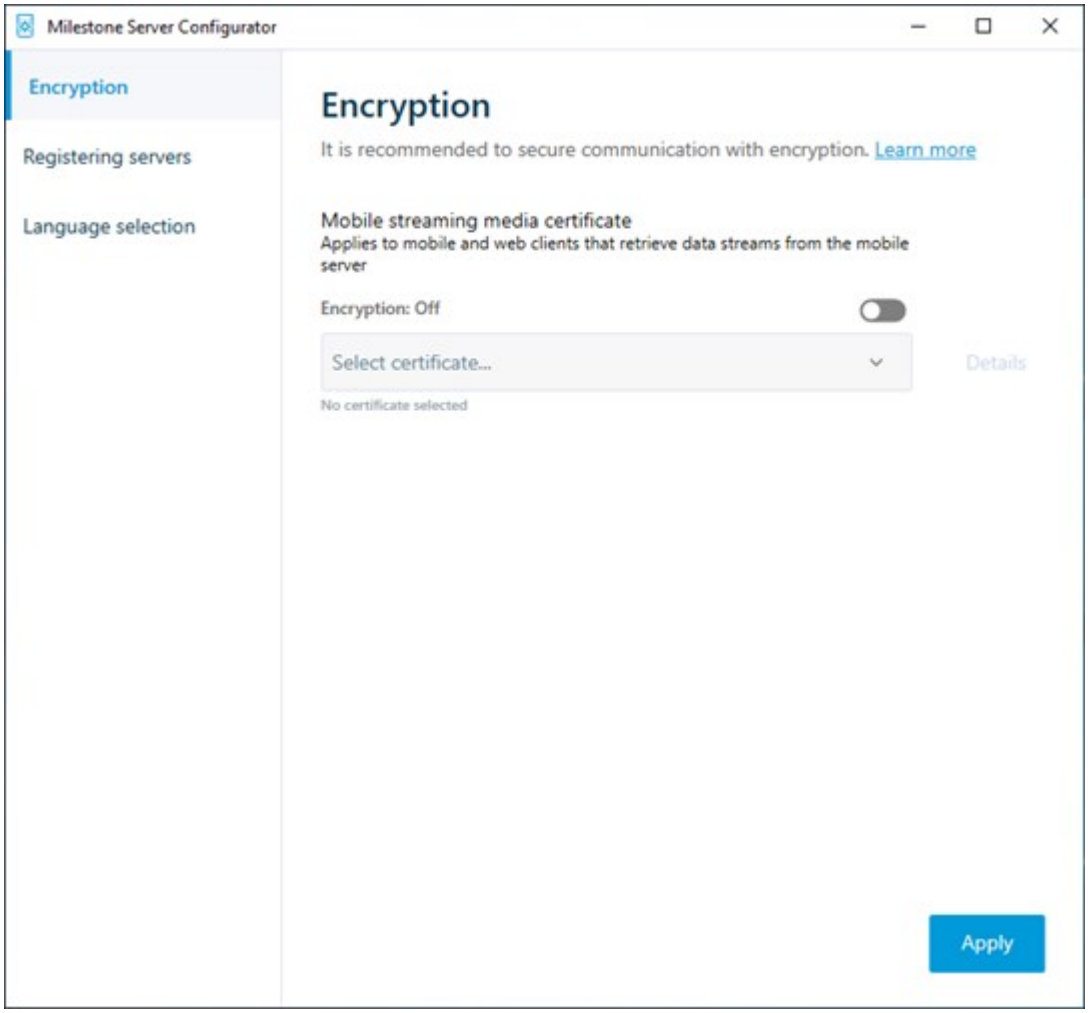
1. Sur un ordinateur où est installé un serveur mobile, ouvrez le **Server Configurator** à partir :
   - Le menu Démarrer de Windows

   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 de flux de multimédia mobile**, 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 la 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.



2. Cliquez sur **Appliquer**.

Lorsque vous appliquez des certificats, le service Mobile Server redémarre.

Milestone Federated Architecture et serveurs maître/asservi (explications)

Si votre système prend en charge Milestone Federated Architecture ou les serveurs en configuration maître/asservi, vous pouvez accéder à ces serveurs à l'aide de votre client XProtect Mobile ou XProtect Web Client. Utilisez cette fonction pour accéder à toutes les caméras de tous les serveurs asservis en vous connectant au serveur maître.

Dans une configuration Milestone Federated Architecture, vous accédez aux sites enfants par le biais du site central. Installez le serveur XProtect Mobile uniquement sur le site central.

Autrement dit, lorsque des utilisateurs du client XProtect Mobile ou XProtect Web Client se connectent à un serveur pour voir les caméras de tous les serveurs de votre système, ils doivent se connecter à l'adresse IP du serveur maître. Les utilisateurs doivent disposer de droits administrateur sur tous les serveurs du système afin que les caméras s'affichent dans le client XProtect Mobile ou XProtect Web Client.

Smart Connect (explications)

Smart Connect vous permet de vérifier que le XProtect Mobile est configuré correctement sans avoir à vous connecter à l'aide d'un périphérique mobile ou d'une tablette à des fins de validation. Cette fonction simplifie également le processus de connexion pour le client XProtect Mobile et les utilisateurs XProtect Web Client.

Cette fonction nécessite que votre serveur XProtect Mobile utilise une adresse IP publique et que votre système soit doté d'une licence avec une formule d'abonnement Milestone Care Plus.

Le système vous donne instantanément des informations dans le Management Client si la configuration de connectivité à distance a bien abouti et confirme que le serveur XProtect Mobile est accessible depuis Internet.

Smart Connect permet au serveur XProtect Mobile de basculer de façon fluide entre des adresses IP internes et externes et de se connecter au XProtect Mobile de partout.

Pour faciliter la configuration des clients mobiles de vos clients, vous pouvez envoyer un e-mail à l'utilisateur final directement depuis le Management Client. L'e-mail inclut un lien ajoutant directement le serveur à XProtect Mobile. Ceci complète la configuration, sans qu'il soit nécessaire de saisir des adresses ou ports de réseau.

Configurer Smart Connect

Pour configurer la fonctionnalité Smart Connect, procédez comme suit :

1. Dans Management Client, dans le volet de navigation, agrandissez **Serveurs** et sélectionnez **Serveurs mobiles**.
2. Sélectionnez le serveur mobile puis cliquez sur l'onglet **Connectivité**.
3. Activez le dispositif de découverte Plug and Play universel sur votre routeur.
4. Configurez les paramètres de connexion.
5. Envoyez un message par e-mail aux utilisateurs.
6. Activez les connexions sur un réseau complexe.

Activez le dispositif de découverte Plug and Play universel sur votre routeur

Pour faciliter la connexion d'appareils mobiles sur les serveurs XProtect Mobile, vous pouvez activer la fonction Plug and Play universelle (UPnP) sur votre routeur. UPnP permet au serveur XProtect Mobile de configuration automatiquement le transfert de port. Cependant, vous pouvez également configurer le transfert de port manuellement sur votre routeur à l'aide de son interface web. Le processus de configuration de cartographie des ports peut varier selon le routeur. Si vous n'êtes pas sûr(e) de savoir comment configurer le transfert de ports sur votre routeur, veuillez consulter la documentation pour ce périphérique.

Toutes les cinq minutes, le service Serveur XProtect Mobile vérifie que le serveur est mis à la disposition des utilisateurs sur Internet. L'état s'affiche dans le coin supérieur gauche du volet **Propriétés** : 

.

Activer les connexions sur un réseau complexe

Si vous avez un réseau complexe doté de paramètres personnalisés, vous pouvez fournir les informations dont les utilisateurs ont besoin pour se connecter.

Sur l'onglet **Connectivité**, dans le groupe **Accès Internet**, spécifiez les éléments suivants :

- Si vous utilisez le mappage de ports UPnP pour diriger les connexions vers une connexion spécifique, cochez la case **Configurer un accès personnalisé à Internet**. Ensuite, saisissez l'**adresse IP ou le nom d'hôte**, ainsi que le port à utiliser pour la connexion. Par exemple, vous devrez peut-être procéder ainsi si votre routeur ne prend pas en charge UPnP ou si vous avez une chaîne de routeurs
- Si vos adresses IP changent souvent, cochez la case **Vérifier pour une récupération dynamique des adresses IP**.

Configurer les paramètres de connexion

1. Dans Management Client, dans le volet de navigation, agrandissez **Serveurs** et sélectionnez **Serveurs mobiles**.
2. Sélectionnez le serveur mobile puis cliquez sur l'onglet **Connectivité**.
3. Utilisez les options du groupe **Général** pour spécifier les éléments suivants :
    - Pour faciliter la connexion du client XProtect Mobile et des utilisateurs XProtect Web Client aux serveurs XProtect Mobile, cochez la case **Activer Smart Connect**.
    - Définissez un délai de fréquence à laquelle le client XProtect Mobile et XProtect Web Client doivent indiquer au serveur mobile qu'ils sont opérationnels
    - Afin de faciliter la découverte du serveur XProtect Mobile sur le réseau au moyen de protocoles UPnP, cochez la case **Activer la découverte UPnP**
    - Pour permettre au serveur XProtect Mobile d'effectuer le mappage du port par lui-même si le routeur est configuré pour cela, cochez la case **Activer le mappage automatique des ports**

Envoyer un message par e-mail aux utilisateurs

Pour faciliter la configuration du client XProtect Mobile et XProtect Web Client, vous pouvez envoyer un e-mail à l'utilisateur final directement depuis le Management Client. L'e-mail inclut un lien ajoutant directement le serveur à XProtect Mobile. Ceci complète la configuration, sans qu'il soit nécessaire de saisir des adresses ou ports de réseau.

1. Dans le champ **Invitation par e-mail à**, saisissez l'adresse e-mail du destinataire de la notification Smart Connect, puis spécifiez une langue.
2. Ensuite, suivez l'une de ces méthodes :
   - Pour envoyer le message, cliquez sur **Envoyer**
   - Copiez les informations vers le programme de messagerie que vous utilisez

Pour plus d'informations, voir :

Exigences pour la configuration Smart Connect sur la page 12

Onglet Connectivité sur la page 18

Envoi de notifications (explications)

Vous pouvez activer XProtect Mobile pour informer les utilisateurs de la survenance d'un événement, tel qu'un déclenchement d'alarme ou un problème au niveau d'un périphérique ou d'un serveur. Les notifications sont toujours livrées, que l'application fonctionne ou non. Lorsque XProtect Mobile est ouvert sur le périphérique portable, l'application fournit la notification. Les notifications du système sont également livrées même lorsque l'application ne fonctionne pas. Les utilisateurs peuvent spécifier les types de notifications qu'ils souhaitent recevoir. Par exemple, un utilisateur peut choisir de recevoir des notifications pour les éléments suivants :

- Toutes les alarmes
- Seules les alarmes qui y sont affectées
- Uniquement les alarmes relatives au système

  Il peut s'agir des alarmes information de la mise hors tension ou du redémarrage d'un serveur.

Vous pouvez également utiliser des notifications push pour informer les utilisateurs qui n'ont pas ouvert XProtect Mobile. Ces notifications sont appelées des notifications push. Les notifications push sont envoyées sur le périphérique portable, et représentent un excellent moyen pour que les utilisateurs restent au courant de la situation pendant leurs déplacements.

Utiliser les notifications push

Pour utiliser les notifications push, votre système doit avoir accès à Internet.

Les notifications push utilisent des services en nuage d'Apple, Microsoft et Google :

- Le service Apple Push Notification (APN)
- Microsoft Azure Notification Hub
- Le service Google Cloud Messaging Push Notification

Il y a une limite quant au nombre de notifications que votre système est autorisé à envoyer au cours d'une période donnée. Si votre système dépasse la limite, il ne peut envoyer qu'une seule notification toutes les 15 minutes au cours de la période suivante. La notification contient un résumé des événements qui se sont produits au cours des 15 minutes. Après la période suivante, les limites sont levées.

Voir également Exigences relatives à la configuration des notifications sur la page 11 et Onglet Notifications sur la page 27.

Configurer les notifications Push sur le serveur XProtect Mobile

Pour configurer les notifications push, suivez ces étapes :

1. Dans Management Client, sélectionnez le serveur mobile, puis cliquez sur l'onglet **Notifications**.
2. Pour envoyer des notifications à tous les appareils mobiles se connectant au serveur, sélectionnez la case à cocher **Notifications**.
3. Pour stocker des informations au sujet des utilisateurs et périphériques mobiles se connectant au serveur, cochez la case **Maintenir l'inscription du périphérique**.

> Le serveur envoie des notifications uniquement aux périphériques portables de cette liste. Si vous décochez la case **Maintenir l'inscription du périphérique** et sauvegardez la modification, le système efface la liste. Pour recevoir les notifications push à nouveau, les utilisateurs doivent reconnecter leur périphérique.

Activer l'envoi de notifications push à des périphériques portables spécifiques ou à tous les périphériques portables

Pour permettre à XProtect Mobile de notifier les utilisateurs lorsqu'un événement se produit en envoyant des notifications push à des périphériques portables spécifiques ou à tous les périphériques portables :

1. Dans Management Client, sélectionnez le serveur mobile, puis cliquez sur l'onglet **Notifications**.
2. Procédez comme suit :
   - Pour des périphériques individuels, cochez la case **Activé** correspondant à chaque périphérique portable indiqué dans le tableau **Périphériques enregistrés**
   - Pour tous les périphériques portables, cochez la case **Notifications**

Arrêter d'envoyer des notifications push à des périphériques portables spécifiques ou à tous les périphériques portables

Il existe plusieurs façons d'arrêter l'envoi de notifications push à des périphériques mobiles spécifiques ou à tous les périphériques portables.

1. Dans Management Client, sélectionnez le serveur mobile, puis cliquez sur l'onglet **Notifications**.
2. Procédez comme suit :
   - Pour les périphériques individuels, décochez la case **Activé** pour chaque périphérique portable. L'utilisateur peut utiliser un autre périphérique pour se connecter au serveur XProtect Mobile
   - Pour tous les périphériques, décochez la case **Notifications**

Pour arrêter temporairement l'envoi vers tous les périphériques, décochez la case **Maintenir l'inscription des périphériques** et sauvegardez votre modification. Le système enverra à nouveau des notifications lorsque les utilisateurs se reconnecteront.

Configurer les enquêtes

Configurez les enquêtes de façon à ce que les gens puissent utiliser XProtect Web Client et XProtect Mobile pour accéder à la vidéo enregistrée et mener des enquêtes sur les incidents, mais aussi préparer et télécharger des preuves vidéo.

Pour configurer les enquêtes, suivez ces étapes :

1. Dans Management Client, cliquez sur le serveur mobile, puis cliquez sur l'onglet **Enquêtes**.
2. Cochez la case **Activer les enquêtes** check box. Par défaut, la case est cochée.
3. Dans le champ **Répertoire d'enquêtes**, spécifiez où vous souhaitez stocker la vidéo aux fins des enquêtes.
4. Cochez la case **Activer la taille limite du répertoire d'enquêtes** pour configurer un nombre maximum de méga-octets que le répertoire d'enquêtes peut contenir.
5. Facultatif : Pour permettre aux utilisateurs d'accéder aux enquêtes créées par d'autres utilisateurs, sélectionnez la case **Voir les enquêtes créées par d'autres utilisateurs**. Si vous ne cochez pas cette case, les utilisateurs ne peuvent voir que leurs propres enquêtes.
6. Facultatif : Pour inclure la date et l'heure de téléchargement d'une vidéo, cochez la case **Inclure l'horodatage pour les exports AVI**.

7. Dans le champ **Codec utilisé pour les exports AVI**, sélectionnez le format de compression à utiliser lors de la préparation de paquets AVI à télécharger.

   Les codecs de la liste peuvent être différents selon votre système d'exploitation. Si vous ne voyez pas le codec que vous souhaitez utiliser, vous pouvez l'installer sur l'ordinateur exécutant Management Client et il s'affichera alors dans cette liste.

   Par ailleurs, les codecs peuvent utiliser différents taux de compression, ce qui peut affecter la qualité de la vidéo. Des taux de compression plus élevés réduisent les exigences de stockage mais peuvent également réduire la qualité de la vidéo. Des taux de compression moins élevés nécessitent plus d'espace de stockage et de capacité du réseau mais accroissent la qualité de la vidéo. Il est conseillé d'effectuer des recherches au sujet des codecs avant d'en sélectionner un.

8. Dans la liste **Débit binaire audio utilisé pour les exportations AVI**, sélectionnez le débit binaire audio approprié lorsque votre exportation vidéo inclut l'audio. La valeur par défaut est 160000 Hz.
9. Dans le champ **Conserver ou supprimer les données en cas d'échec de l'export (MKV et AVI)**, spécifiez s'il faut conserver les données qui ont bien été téléchargées, bien qu'elles puissent être incomplètes, ou s'il faut les supprimer.

   Pour permettre aux utilisateurs de sauvegarder des enquêtes, vous devez accorder la permission **d'exportation** suivante au rôle de sécurité assigné aux utilisateurs.

Nettoyer les enquêtes

Si vous avez des enquêtes ou des exports de vidéo que vous ne souhaitez plus conserver, vous pouvez les supprimer. Par exemple, ceci peut s'avérer utile si vous souhaitez libérer plus d'espace disponible sur le serveur.

- Pour supprimer une enquête et tous les exports de vidéos créés pour celle-ci, sélectionnez l'enquête dans la liste puis cliquez sur **Supprimer**
- Pour supprimer des fichiers vidéo individuels qui ont été exportés pour une enquête, mais conserver l'enquête, sélectionnez l'enquête dans la liste. Dans le groupe **Détails de l'enquête**, cliquez sur l'icône **Supprimer** à droite des champs **Base de données**, **AVI** ou **MKV** pour les exportations.

Utilisation de vidéo push pour diffuser la vidéo (explications)

Vous pouvez configurer vidéo push de façon à ce que les utilisateurs puissent tenir d'autres personnes informées au sujet d'une situation, ou enregistrer une vidéo à des fins d'examen ultérieur, en transmettant la vidéo de la caméra de leur périphérique portable vers votre système de surveillance XProtect. Le flux vidéo peut avoir également l'audio.

Voir également Onglet Vidéo push sur la page 26 et Exigences pour la configuration de vidéo push sur la page 12.

Configuration de vidéo push pour diffuser la vidéo

Pour permettre aux utilisateurs de transmettre la vidéo de leur périphérique portable vers le système XProtect, configurez vidéo push sur le serveur XProtect Mobile.

Dans Management Client, suivez ces étapes dans l'ordre indiqué :

1. Dans l'onglet **Vidéo Push**, cochez la case **Vidéo Push** pour activer la fonctionnalité.
2. Ajouter un canal vidéo push pour la diffusion vidéo.
3. Ajoutez le pilote vidéo push en tant que périphérique au Recording Server. Le pilote simule une caméra afin que vous puissiez transmettre la vidéo au Recording Server.
4. Ajouter le périphérique du pilote vidéo push au canal pour vidéo push.

Ajouter un canal de vidéo push pour la diffusion de la vidéo en continu

Pour ajouter un canal, procédez de la manière suivante :

1. Dans le volet de navigation, sélectionnez **Serveurs mobiles**, puis sélectionnez le serveur mobile.
2. Dans l'onglet **Vidéo Push**, cochez la case **Vidéo Push**.
3. Dans le coin inférieur droit, sous **Application des canaux**, cliquez sur **Ajouter** pour ajouter un canal de push vidéo.
4. Dans la boîte de dialogue qui apparaît, saisissez le nom d'utilisateur du compte utilisateur (ajouté sous **Rôles**) qui utilisera ce canal. Ce compte utilisateur doit être autorisé à accéder au serveur XProtect Mobile et au serveur d'enregistrement (sur l'onglet **Sécurité globale**).

   Pour utiliser vidéo push, les utilisateurs doivent se connecter à XProtect Mobile sur leur périphérique portable à l'aide de l'identifiant et du mot de passe relatifs à ce compte.

   Lorsque vous ajoutez un nouveau canal vidéo push sur le serveur mobile, le système génère le numéro de port et l'adresse MAC du canal qui seront utilisés à l'ajout du canal en tant que périphérique sur le serveur d'enregistrement. Il génère également le mot de passe utilisé pour connecter le Recording Server au Mobile Server. Le mot de passe par défaut est **Milestone**.

5. Notez bien le numéro de port. Vous en aurez besoin lorsque vous ajouterez le pilote vidéo push en tant que périphérique sur le serveur d'enregistrement.

6. Cliquez sur **OK** pour fermer la boîte de dialogue Canal vidéo push.
7. Cliquez sur **Enregistrer** situé dans le coin supérieur gauche du panneau de navigation pour enregistrer le canal.

Modifier un canal de vidéo push

Vous pouvez modifier les informations de configuration d'un canal de vidéo push que vous avez ajouté :

1. Sous **Application des canaux**, sélectionnez le canal à modifier, puis cliquez sur **Modifier**.
2. Une fois vos changements terminés, cliquez sur **OK** pour fermer la boîte de dialogue Canal de vidéo push.
3. Cliquez sur **Enregistrer** situé dans le coin supérieur gauche du panneau de navigation pour enregistrer les changements.

Lorsque vous modifier le numéro de port et l'adresse MAC d'un canal de vidéo push, assurez-vous de remplacer également les informations de configuration du canal vidéo que vous aviez ajoutés sur le serveur d'enregistrement par les nouvelles informations. Sinon, la connexion entre le Recording Server et le Mobile Server sera interrompue.

Supprimer un canal de vidéo push

Vous pouvez supprimer les canaux que vous n'utilisez plus :

1. Sous **Application des canaux**, sélectionnez le canal à supprimer, puis cliquez sur **Supprimer**.
2. Cliquez sur **Enregistrer** situé dans le coin supérieur gauche du panneau de navigation pour enregistrer le changement.

Modifier le mot de passe

Vous pouvez modifier le mot de passe généré automatiquement qui est utilisé pour connecter le Recording Server au Mobile Server :

1. Dans le coin inférieur droit, sous **Application des canaux**, cliquez sur **Modifier le mot de passe**.
2. Dans la boîte de dialogue **Modifier le mot de passe du canal de vidéo push**, saisissez le nouveau mot de passe dans le premier champ, puis à nouveau dans le deuxième champ et cliquez sur **OK**.
3. Cliquez sur **Enregistrer** situé dans le coin supérieur gauche du panneau de navigation pour enregistrer le changement.

La modification du mot de passe du canal de vidéo push s'applique à tous les canaux de vidéo push figurant dans la liste ou qui seront ajoutés par la suite. Le nouveau mot de passe restera actif et s'appliquera aux futurs canaux même si vous supprimez tous les canaux de vidéo push figurant dans la liste.

Une fois le changement enregistré, tous les canaux de vidéo push existants cessent de fonctionner car la connexion entre le Recording Server et Mobile Server est interrompue. Pour restaurer la connexion, vous devez exécuter l'assistant **Remplacer un matériel** en effectuant un clic droit sur l'onglet **Serveurs d'enregistrement** dans le volet de navigation, puis saisir le nouveau mot de passe du canal de vidéo push que vous avez ajouté en tant que périphérique dans le Recording Server.

Ajoutez le pilote vidéo push en tant que périphérique au système Recording Server

1. Dans le volet Navigation sur le site, cliquez sur **Serveurs d'enregistrement**.
2. Effectuez un clic droit sur le serveur auquel vous souhaitez transmettre la vidéo, et cliquez sur **Ajouter matériel** pour ouvrir l'assistant **Ajouter matériel**.
3. Sélectionnez la méthode de détection de matériel **Manuelle**, puis cliquez sur **Suivant**.
4. Saisissez les identifiants de connexion de la caméra comme suit :
   - Nom d'utilisateur : Saisissez les paramètres d'usine par défaut ou le nom d'utilisateur spécifié sur la caméra
   - Mot de passe : Saisissez **Milestone**, le mot de passe généré par le système, ou si vous l'aviez changé lors de l'ajout du canal de vidéo push dans le serveur mobile, saisissez le mot de passe que vous souhaitez utiliser, puis cliquez sur **Suivant**

   Il s'agit des identifiants relatifs au matériel, et non à l'utilisateur. Ils ne sont pas liés au compte utilisateur utilisés pour accéder au canal de vidéo push.

5. Dans la liste de pilotes, développez **Milestone**, cochez la case **Pilote Vidéo Push**, puis cliquez sur **Suivant**.
6. Dans le champ **Adresse**, saisissez l'adresse IP de l'ordinateur sur lequel le serveur XProtect Mobile est installé.

   Nous vous recommandons d'utiliser l'adresse MAC générée par le système. Changez-la uniquement si vous rencontrez des problèmes avec le périphérique du pilote de vidéo push, ou par exemple, si vous avez modifié le numéro de port et l'adresse MAC du canal de vidéo push sur le serveur mobile.

7. Dans le champ **Port**, saisissez le numéro de port pour le canal que vous avez créé pour diffuser la vidéo. Le numéro de port a été assigné au moment de la création du canal.
8. Dans la colonne **Modèle du matériel**, choisissez **Pilote vidéo push**, et cliquez sur **Suivant**.

9. Lorsque le système détecte le nouveau matériel, cliquez sur **Suivant**.
10. Dans le champ **Modèle de nom du matériel**, indiquez s'il faut afficher soit le modèle du matériel soit son adresse IP ou le modèle uniquement.
11. Indiquez s'il faut activer les périphériques associés en cochant la case **Activé**. Vous pouvez ajouter des périphériques associés à la liste pour **Pilote vidéo push**, même s'ils ne sont pas activés. Vous pourrez les activer ultérieurement.

    Si vous souhaitez utiliser les informations géographiques au moment de la diffusion de la vidéo, vous devez activer le port **Métadonnées**.

    Si vous souhaitez lire l'audio alors que vous diffuser la vidéo, vous devez activer le microphone lié à la caméra utilisée pour la diffusion de la vidéo.

12. Sélectionnez les groupes par défaut pour les périphériques associés à gauche, ou sélectionnez un groupe spécifique dans le champ **Ajouter au groupe**. L'ajout de périphériques au groupe peut faciliter l'application simultanée des paramètres à tous les périphériques ou le remplacement de périphériques.

Ajouter le périphérique du pilote vidéo push au canal pour vidéo push

Pour ajouter le périphérique du pilote vidéo push au canal pour vidéo push, suivez ces étapes :

1. Dans le volet de **Navigation sur le site**, cliquez sur **Serveurs portables**, puis cliquez sur l'onglet **Vidéo push**.
2. Cliquez sur **Trouver des caméras**. Si l'opération réussit, le nom de la caméra du pilote vidéo push s'affiche dans le champ **Nom de la caméra**.
3. Enregistrez votre configuration.

Activer l'audio pour le canal de vidéo push existant

Après avoir respecté les prérequis pour activer l'audio dans la vidéo push (voir Exigences pour la configuration de vidéo push sur la page 12), dans Management Client :

1. Dans le panneau **Navigation du site**, développez le nœud **Serveurs** et cliquez sur **Serveurs d'enregistrement**.
2. Dans le panneau de vue d'ensemble, sélectionnez le dossier du serveur d'enregistrement concerné, puis développez le dossier **Pilote Vidéo Push** et effectuez un clic droit sur vidéo push - microphone lié.
3. Sélectionnez **Activé** pour activer le microphone.
4. Toujours dans le même dossier, sélectionnez la vidéo push - caméra liée.
5. Dans le panneau **Propriétés**, cliquez sur l'onglet **Client** (voir Onglet Client (périphériques)).

6. À droite du champ **Microphone lié**, cliquez sur . La fenêtre de dialogue **Périphérique sélectionné** s'ouvre.
7. Dans l'onglet **Serveurs d'enregistrement**, développez le dossier du serveur d'enregistrement et sélectionnez le microphone lié à la vidéo push.
8. Cliquez sur **OK**.

Configurer des utilisateurs pour une vérification en deux étapes par e-mail

Les fonctions disponibles dépendent du système que vous utilisez. Voir https://www.milestonesys.com/solutions/platform/product-index/ pour plus d'informations.

Pour imposer une étape de connexion supplémentaire aux utilisateurs du client XProtect Mobile ou XProtect Web Client, configurez la vérification en deux étapes sur le serveur XProtect Mobile. En plus du nom d'utilisateur standard et du mot de passe, l'utilisateur doit saisir un code de vérification envoyé par e-mail.

Une vérification en deux étapes permet d'augmenter le niveau de protection de votre système de surveillance.

Dans Management Client, suivez ces étapes :

1. Saisissez les informations relatives à votre serveur SMTP sur la page 59.
2. Spécifiez le code de vérification qui sera envoyé aux utilisateurs sur la page 60.
3. Assignez une méthode de connexion aux utilisateurs et aux groupes Active Directory sur la page 60.

Voir également Exigences pour la configuration de la vérification en deux étapes de l'utilisateur sur la page 12 et Onglet Vérification en deux étapes sur la page 28.

Saisissez les informations relatives à votre serveur SMTP

Le prestataire utilise les informations relatives au serveur SMTP :

1. Dans le panneau de navigation, choisissez **Serveurs mobiles** puis sélectionnez le serveur mobile pertinent.
2. Dans l'onglet **Vérification en deux étapes**, cochez la case **Activer la vérification en deux étapes**.
3. Sous les **paramètres du prestataire**, sur l'onglet **e-mail**, saisissez les informations relatives à votre serveur SMTP et spécifiez l'e-mail que le système enverra aux utilisateurs du client lorsqu'ils se connecteront et seront configurés pour une deuxième connexion. Pour obtenir plus d'informations au sujet de chaque paramètre, voir Onglet Vérification en deux étapes sur la page 28.

Pour de plus amples informations, voir l'Onglet Vérification en deux étapes sur la page 28.

Spécifiez le code de vérification qui sera envoyé aux utilisateurs

Pour stipuler la complexité du code de vérification :

1. Sur l'onglet **Vérification en deux étapes**, dans la rubrique **Paramètres du code de vérification**, indiquez la période au cours de laquelle les utilisateurs du client XProtect Mobile n'ont pas besoin de revérifier leur connexion en cas de déconnexion du réseau, par exemple. La période par défaut est de trois minutes.
2. Spécifiez la période au cours de laquelle l'utilisateur peut utiliser le code de vérification reçu. À la fin de cette période, le code est invalide et l'utilisateur doit demander un nouveau code. La période par défaut est de cinq minutes.
3. Spécifiez le nombre maximum de tentatives de saisie du code avant que le code fourni ne soit plus valide. Le nombre par défaut est trois.
4. Spécifiez le nombre de caractères dans le code. La longueur par défaut est de six.
5. Spécifiez la complexité du code généré par le système.

Pour de plus amples informations, voir l'Onglet Vérification en deux étapes sur la page 28.

Assignez une méthode de connexion aux utilisateurs et aux groupes Active Directory

Sur l'onglet **Vérification en deux étapes**, dans la rubrique **Paramètres utilisateur**, la liste des utilisateurs et groupes ajoutés à votre système XProtect s'affiche.

1. Dans la colonne **Méthode de connexion**, sélectionnez une méthode de vérification pour chaque utilisateur ou groupe.
2. Dans le champ **Détails**, ajoutez les détails relatifs à la livraison, tels que les adresses e-mails des utilisateurs individuels. La prochaine fois que l'utilisateur se connectera XProtect Mobile au ou XProtect Web Client à l'application , un identifiant secondaire lui sera demandé.
3. Si un groupe est configuré dans Active Directory, le serveur XProtect Mobile utilise des détails, tels que des adresses e-mail, tirés d'Active Directory.

   Les groupes Windows ne prennent pas la vérification en deux étapes en charge.

4. Enregistrez votre configuration.

Vous avez complété les étapes de configuration de vos utilisateurs pour la vérification en deux étapes par e-mail.

Pour de plus amples informations, voir l'Onglet Vérification en deux étapes sur la page 28.

Actions (explications)

Vous pouvez gérer la disponibilité de l'onglet **Actions** dans le client XProtect Mobile ou dans XProtect Web Client en activant ou désactivant **Actions** dans l'onglet **Généralités**. **Les actions** sont activées par défaut et toutes les actions disponibles pour les périphériques connectés sont affichées ici.

Pour en savoir plus, voir Onglet Généralités sur la page 16.

Nommer une sortie à utiliser dans le client XProtect Mobile et XProtect Web Client (explications)

Pour afficher correctement les actions avec la caméra active, vous devez créer un groupe de sorties qui porte le même nom que la caméra.

Exemple :

Lorsque vous créez un groupe de sorties avec des sorties liées à une caméra nommée « AXIS P3301, P3304 - 10.100.50.110 - Caméra 1 », vous devez saisir le même nom dans le champ **Nom** (dans **Renseignements sur le groupe de périphériques**).

Vous pouvez ajouter une description plus complète dans le champ **Description**, par exemple « AXIS P3301, P3304 - 10.100.50.110 - Caméra 1 - Interrupteur éclairage ».

> ⚠ Si vous ne suivez pas ces conventions, les actions ne seront pas disponibles dans la liste d'actions pour la vue de caméra associée. Au lieu de cela, les actions apparaîtront dans la liste d'autres actions de l'onglet **Actions**.

Pour de plus amples informations, voir Périphériques de sortie (explications).

Maintenance

Mobile Server Manager (explications)

Le Mobile Server Manager est une fonctionnalité contrôlée par barre d'état connectée au serveur mobile. Un clic droit sur l'icône Mobile Server Manager dans la zone de notification ouvre un menu dans lequel vous pouvez accéder aux fonctionnalités du serveur mobile.

Vous pouvez :

- Accès à XProtect Web Client sur la page 62
- Démarrer, arrêter et redémarrer le service Mobile Server sur la page 63
- Saisissez/modifiez l'adresse du serveur de gestion sur la page 63
- Afficher/modifier les numéros de port sur la page 64
- Activer le cryptage sur le serveur mobile sur la page 64 via le **Server Configurator**
- Ouvrez le fichier journal d'aujourd'hui (voir Accès aux journaux et aux enquêtes (explications) sur la page 65)
- Ouvrez le répertoire des journaux (voir Accès aux journaux et aux enquêtes (explications) sur la page 65)
- Ouvrez le répertoire des enquêtes (voir Accès aux journaux et aux enquêtes (explications) sur la page 65)
- Modifier le répertoire d'enquêtes sur la page 66
- Voir le statut de Serveur XProtect Mobile (voir Afficher l'état (explications) sur la page 67)

Accès à XProtect Web Client

Si un serveur XProtect Mobile est installé sur votre ordinateur, vous pouvez utiliser le XProtect Web Client pour accéder à vos caméras et vues. Comme il est inutile d'installer XProtect Web Client, vous pouvez y accéder depuis l'ordinateur sur lequel est installé le serveur XProtect Mobile ou depuis tout ordinateur que vous souhaitez utiliser à cette fin.

1. Configurez le serveur XProtect Mobile dans le Management Client.
2. Si vous utilisez l'ordinateur sur lequel le serveur XProtect Mobile est installé, vous pouvez cliquer avec le bouton droit sur l'icône Mobile Server Manager dans la zone de notification et sélectionner **Ouvrir XProtect Web Client**.
3. Si vous n'utilisez pas l'ordinateur sur lequel le serveur XProtect Mobile est installé, vous pouvez y accéder à partir d'un navigateur. Passez à l'étape 4 de ce processus.
4. Ouvrez un navigateur Internet (Internet Explorer, Mozilla Firefox, Google Chrome ou Safari).

5. Saisissez l'adresse IP externe (c'est-à-dire votre adresse externe et le port du serveur sur lequel le serveur de serveur XProtect Mobile s'exécute).

   Exemple : Le serveur XProtect Mobile est installé sur un serveur dont l'adresse IP est 127.2.3.4. Il est configuré pour accepter les connexions HTTP sur le port 8081 et les connexions HTTPS sur le port 8082 (les valeurs par défaut du programme d'installation).

   Dans la barre d'adresse de votre navigateur, saisissez : **http://127.2.3.4:8081** si vous souhaitez utiliser une connexion HTTP standard ou **https://127.2.3.4:8082** pour utiliser une connexion HTTPS sécurisée. Vous pouvez commencer à utiliser XProtect Web Client.

6. Ajoutez l'adresse en tant que signet dans votre navigateur pour faciliter l'accès à XProtect Web Client ultérieurement. Si vous utilisez XProtect Web Client sur l'ordinateur local sur lequel vous avez installé le serveur XProtect Mobile, vous pouvez également utiliser le raccourci de bureau créé par le programme d'installation. Cliquez sur le raccourci pour lancer votre navigateur par défaut et ouvrir le XProtect Web Client.

Vous devez effacer le cache des navigateurs Internet exécutant le XProtect Web Client avant de pouvoir utiliser une nouvelle version de XProtect Web Client. Les administrateurs système doivent demander à leurs utilisateurs de XProtect Web Client de vider le cache de leur navigateur après la mise à niveau, ou de forcer cette action à distance (vous pouvez effectuer cette action uniquement sur Internet Explorer dans un domaine).

Démarrer, arrêter et redémarrer le service Mobile Server

Si nécessaire, vous pouvez démarrer, arrêter et redémarrer le service Mobile Server du Mobile Server Manager.

- Pour effectuer ces tâches, faites un clic droit sur l'icône Mobile Server Manager et sélectionnez **Démarrer le service Mobile Server**, **Arrêter le service Mobile Server** ou **Redémarrer le service Mobile Server**, respectivement.

Saisissez/modifiez l'adresse du serveur de gestion

1. Effectuez un clic droit sur l'icône Mobile Server Manager et sélectionnez **Adresse du serveur de gestion**.
2. Dans le champ **URL du serveur**, saisissez l'adresse URL du serveur.
3. Cliquez sur **OK**.

Afficher/modifier les numéros de port

1. Faites un clic droit sur l'icône Mobile Server Manager et sélectionnez **Afficher/modifier les numéros de port**.
2. Pour modifier les numéros de port, saisissez le numéro du port concerné. Vous pouvez indiquer un numéro de port standard pour les connexions HTTP, un numéro de port sécurisé pour les connexions HTTPS, ou les deux.
3. Cliquez sur **OK**.

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 Cryptage des données du serveur mobile (explications) sur la page 40 et Exigences du cryptage du serveur mobile pour les clients sur la page 41.

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 :

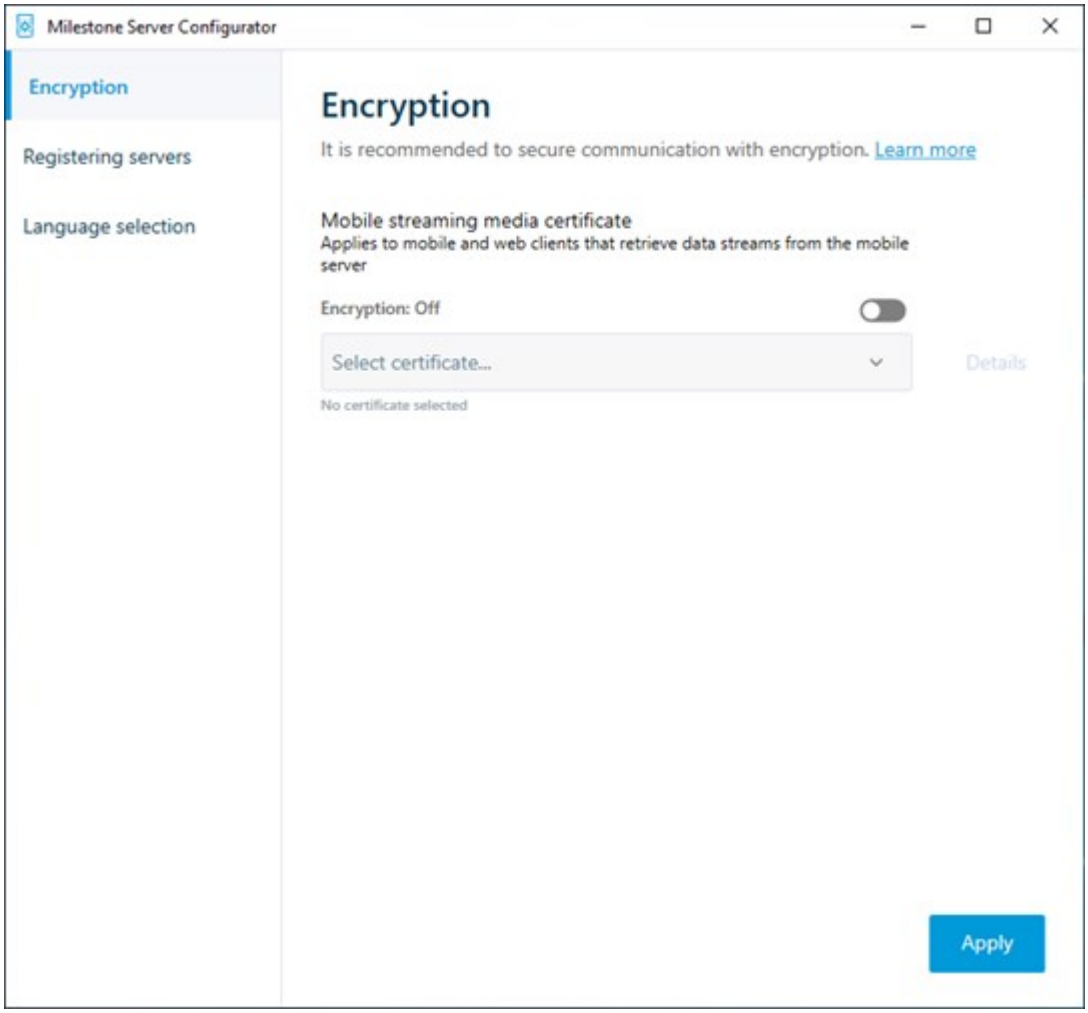
1. Sur un ordinateur où est installé un serveur mobile, ouvrez le **Server Configurator** à partir :
   - Le menu Démarrer de Windows

   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 de flux de multimédia mobile**, 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 la 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.



2. Cliquez sur **Appliquer**.

Lorsque vous appliquez des certificats, le service Mobile Server redémarre.

Accès aux journaux et aux enquêtes (explications)

Le Mobile Server Manager vous permet d'accéder rapidement au fichier journal de la journée, d'ouvrir le répertoire dans lequel les fichiers journaux sont enregistrés, et d'ouvrir le répertoire dans lequel les enquêtes sont enregistrées.

Pour ouvrir l'un de ces répertoires, cliquez avec le bouton droit de la souris sur l'icône Mobile Server Manager et sélectionnez :

- **Ouvrir le journal d'aujourd'hui**
- **Ouvrir un répertoire de journaux**
- **Ouvrir le répertoire d'enquêtes**

> Si vous désinstallez le serveur XProtect Mobile de votre système, ses fichiers journaux ne sont pas supprimés. Les administrateurs disposant des droits d'utilisateur appropriés peuvent accéder à ces fichiers journaux plus tard, ou décider de les supprimer s'ils ne sont plus nécessaires. L'emplacement par défaut des fichiers journaux se trouve dans le répertoire **ProgramData**. Si vous modifiez l'emplacement par défaut des fichiers journaux, les journaux existants ne sont pas copiés vers le nouvel emplacement et ne sont pas supprimés.

Modifier le répertoire d'enquêtes

L'emplacement par défaut des enquêtes se trouve dans le répertoire **ProgramData**. Si vous modifiez l'emplacement par défaut du répertoire d'enquête, les enquêtes existantes ne seront pas automatiquement copiées dans le nouvel emplacement, et ne seront pas supprimées. Pour modifier l'emplacement de sauvegarde des exportations d'enquêtes sur votre disque dur :

1. Cliquez avec le bouton droit de la souris sur l'icône Mobile Server Manager et sélectionnez **Modifier le répertoire d'enquêtes**.

   La fenêtre **Emplacement des enquêtes** s'ouvre.

2. À côté du champ **Répertoire**, lequel indique l'emplacement actuel, cliquez sur l'icône Répertoire pour rechercher ou créer un répertoire > cliquez sur **OK**.

3. Dans la liste **Enquêtes anciennes**, sélectionnez l'action que vous souhaitez appliquer aux enquêtes existantes qui sont stockés dans l'emplacement actuel. Les options sont les suivantes :

   - **Déplacer** : Déplace les enquêtes existantes vers le nouveau répertoire

     > Si vous ne déplacez pas les enquêtes existantes vers le nouveau répertoire, vous ne serez plus en mesure de les voir.

   - **Supprimer** : Supprime les enquêtes existantes
   - **Ne rien faire** : Les enquêtes existantes restent dans l'emplacement de répertoire actuel. Vous ne pourrez plus les voir après avoir changé l'emplacement par défaut du répertoire des enquêtes

4. Cliquez sur **Appliquer** > cliquez sur **OK**.

Afficher l'état (explications)

Faites un clic droit sur l'icône Mobile Server Manager et sélectionnez **Afficher l'état** ou double-cliquez sur l'icône Mobile Server Manager pour ouvrir une fenêtre affichant l'état du serveur XProtect Mobile. Vous pouvez voir les informations suivantes :

Nom	Description
Serveur en cours d'exécution depuis	Heure et date du dernier lancement du serveur XProtect Mobile.
Utilisateurs connectés	Nombre d'utilisateurs actuellement connectés au serveur XProtect Mobile.
Décodage du matériel	Indique si le décodage accéléré du matériel fonctionne sur le serveur XProtect Mobile.
Utilisation unité centrale	Combien de % du processeur est actuellement utilisé par le serveur XProtect Mobile.
Historique de l'utilisation de l'unité centrale	Un graphique détaillant l'historique de l'utilisation du processeur par le serveur XProtect Mobile.

Dépannage

Dépannage XProtect Mobile

Connexions

1. **Pourquoi ne puis-je pas me connecter à mes enregistrements/mon serveur XProtect Mobile à partir de mon client XProtect Mobile** ?

   Pour vous connecter à vos enregistrements, le serveur XProtect Mobile doit être installé sur le serveur exécutant votre système XProtect ou bien sur un serveur dédié. Les paramètres XProtect Mobile pertinents sont également requis dans votre configuration de gestion de la vidéo XProtect. Ceux-ci sont installés soit sous forme de modules d'extension ou dans le cadre d'une installation ou mise à niveau de produit. Pour plus d'informations sur la façon d'obtenir le serveur XProtect Mobile et de l'intégrer aux paramètres du client XProtect Mobile de votre système XProtect, voir la rubrique configuration (voir Paramètres du serveur mobile sur la page 16).

2. **Je viens d'activer mon pare-feu et, maintenant, je ne peux pas connecter de périphérique portable à mon serveur. Pourquoi** ?

   Si votre pare-feu était désactivé au cours de l'installation de votre serveur XProtect Mobile, vous devez activer manuellement les communications TCP et UDP.

3. **Comment puis-je éviter l'avertissement de sécurité lorsque j'exécute XProtect Web Client par le biais d'une connexion HTTPS** ?

   L'avertissement s'affiche parce que les informations du certificat concernant l'adresse du serveur sont incorrectes. La connexion restera cryptée.
   Le certificat auto-signé du serveur XProtect Mobile doit être remplacé par votre propre certificat correspondant à l'adresse du serveur utilisée pour connecter le serveur XProtect Mobile. Ces certificats sont obtenus par le biais d'autorités officielles de signature de certificats, telles que Verisign. Consultez l'autorité de signature de votre choix pour obtenir de plus amples informations.
   XProtect Mobile le serveur n'utilise pas Microsoft IIS. Cela signifie que les instructions fournies pour la production de fichiers de demande de signature d'un certificat (CSR) par l'autorité signataire utilisant IIS ne s'appliquent pas au serveur XProtect Mobile. Vous devez créer un fichier CSR manuellement en utilisant des outils de certification à ligne de commande ou d'autres applications tierces similaires. Ce processus doit être entrepris uniquement par des administrateurs du système ou des utilisateurs avancés.

Qualité d'image

1. **Pourquoi la qualité de l'image est-elle parfois mauvaise lorsque je consulte la vidéo dans le client XProtect Mobile** ?

   Le serveur XProtect Mobile ajuste automatiquement la qualité d'image en fonction de la bande passante disponible entre le serveur et le client. Si vous observez une qualité de l'image inférieure à celle du XProtect® Smart Client, il se peut que votre bande passante soit trop faible pour vous permettre d'obtenir des images de haute résolution par le biais du client XProtect Mobile. Il est possible que cela soit dû à une bande passante trop faible en amont du serveur ou à une bande passante trop faible dans le client. Pour plus d'informations, voir le manuel de l'utilisateur pour XProtect Smart Client.

   Si vous êtes dans une région à bande passante sans fil variable, vous remarquerez peut-être que la qualité de l'image s'améliore lorsque vous entrez dans une zone dotée d'une meilleure bande passante.

2. **Pourquoi la qualité de l'image est-elle mauvaise lorsque je me connecte à mon système de gestion vidéo XProtect à la maison, à partir de la WiFi de mon bureau** ?

   Vérifiez la bande passante de votre connexion Internet personnelle. De nombreuses connexions privées à Internet ont des bandes passantes différentes pour le téléchargement et le chargement, souvent décrites comme suit : 20 Mbit/2 Mbit. En effet, les utilisateurs particuliers ont rarement besoin de charger de grandes quantités de données sur Internet, mais consomment beaucoup de données. Le système de gestion vidéo XProtect a besoin d'envoyer la vidéo au client XProtect Mobile et est limité par la vitesse de chargement de votre connexion. Si vous rencontrez une mauvaise qualité d'image à divers endroits alors que la vitesse de téléchargement du réseau du client XProtect Mobile est bonne, le problème pourrait être résolu en augmentant la vitesse de chargement de votre connexion Internet personnelle.

Décryptage du matériel accéléré

1. **Mon processeur prend-il en charge le décryptage avec accélération matérielle** ?

   Seuls les processeurs les plus récents d'Intel prennent en charge le décryptage avec accélération matérielle. Consultez le site Web d'Intel (https://ark.intel.com/Search/FeatureFilter?productType=processors/) pour savoir si votre processeur est pris en charge.

   Dans le menu, assurez vous que **Technologies** > **Intel Quick Sync Video** est réglé sur **Oui**.

   Si votre processeur est pris en charge, le décryptage avec accélération matérielle est activé par défaut. Vous pouvez voir l'état actuel dans **Afficher l'état** dans le Mobile Server Manager (voir Afficher l'état (explications) sur la page 67).

2. **Mon système d'exploitation prend-il en charge le décryptage avec accélération matérielle** ?

   Tous les systèmes d'exploitation qui prennent en charge XProtect, prennent également en charge l'accélération matérielle.

   Assurez-vous d'installer les pilotes graphiques les plus récents sur votre système à partir du site Web d'Intel. Ces pilotes ne sont pas disponibles à partir de Windows Update.

   Le décryptage avec accélération matérielle n'est pas pris en charge si le serveur mobile est installé dans un environnement virtuel.

3. **Comment puis-je désactiver le cryptage avec accélération matérielle sur le serveur mobile ? (Avancé)**

   Si le processeur du serveur mobile prend en charge le décryptage avec accélération matérielle, celui-ci est activé par défaut. Pour désactiver le décryptage avec accélération matérielle, procédez comme suit :

   1. Trouvez le fichier VideoOS.MobileServer.Service.exe.config. En règle générale, le chemin d'accès est le suivant : C:\Program Files\Milestone\XProtect Mobile Server\VideoOS.MobileServer.Service.exe.config.
   2. Ouvrez le fichier dans Notepad ou un éditeur de texte similaire. Si nécessaire, associez le type de fichier .config à Notepad.
   3. Trouvez le champ <add key="HardwareDecodingMode" value="Auto" />.
   4. Remplacez la valeur « Auto » par « Off ».
   5. Enregistrez et fermez le fichier.

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/.