

MAKE THE  
WORLD SEE

# Milestone Systems

---

XProtect® VMS 2020 R3

Manuel de l'administrateur

XProtect Corporate

XProtect Expert

XProtect Professional+

XProtect Express+



# Table des matières

<b>Copyright, marques et exclusions</b> .....	<b>21</b>
<b>Vue d'ensemble</b> .....	<b>22</b>
Présentation générale du produit .....	22
Composants principaux du système .....	22
Serveur de gestion .....	22
Serveur d'enregistrement .....	23
Serveur d'événements .....	23
Serveur de journaux .....	24
SQL Server et bases de données .....	24
Serveur Mobile .....	24
Active Directory .....	25
Management Client (explications) .....	25
Composants du système en option .....	25
Serveur d'enregistrement de redondance .....	25
Serveur de gestion de redondance .....	26
Clients .....	26
XProtect Smart Client (explications) .....	26
XProtect Mobile client (explications) .....	27
XProtect Web Client (explications) .....	28
Une configuration distribuée du système .....	28
Produits complémentaires .....	29
XProtect Access (explications) .....	29
XProtect LPR (explications) .....	30
XProtect Smart Wall (explications) .....	31
XProtect Transact (explications) .....	32
Milestone Open Network Bridge (explications) .....	32
XProtect DLNA Server (explications) .....	32
Ports utilisés par le système .....	33

Graphique de comparaison des produits .....	46
<b>Licence .....</b>	<b>50</b>
Licences (explications) .....	50
Changer le code de licence du logiciel .....	51
<b>Exigences et considérations .....</b>	<b>52</b>
Heure d'été (explications) .....	52
Serveurs de temps (explications) .....	52
Taille limite de la base de données .....	53
IPv6 et IPv4 (explications) .....	53
Écriture des adresses IPv6 (explications) .....	55
Utiliser les adresses IPv6 dans les URL .....	55
Serveurs virtuels .....	56
Serveurs de gestion multiples (grappes) (explications) .....	56
Conditions préalables à la mise en grappe .....	57
Protection des bases de données d'enregistrement contre la corruption .....	57
Panne de disque dur : protégez vos lecteurs .....	57
Windows Task Manager : attention à la fermeture des processus .....	58
Coupures de courant : utilisation d'un onduleur .....	58
Journal des transactions de la base de données SQL (explications) .....	58
Configuration système minimum .....	59
Avant de commencer l'installation .....	59
Préparation de vos serveurs et du réseau .....	59
Préparer Active Directory .....	60
Méthode d'installation .....	60
Décider d'une édition de SQL Server .....	63
Sélectionner un compte de service .....	64
Authentification Kerberos (explications) .....	64
Exclusions scan antivirus (explications) .....	66
Comment configurer VMS XProtect pour qu'il s'exécute au mode FIPS 140-2 ? .....	68
Avant d'installer VMS XProtect sur un système où est activé le mode FIPS .....	68

Enregistrer le code de licence du logiciel .....	68
Pilotes de périphériques (explications) .....	69
Conditions préalables de l'installation hors ligne .....	69
Communication sécurisée (explications) .....	70
Cryptage du serveur de gestion (explications) .....	70
Cryptage du serveur de gestion vers le serveur d'enregistrement (explications) .....	72
Cryptage entre le serveur de gestion et le Data Collector Server (explications) .....	73
Le cryptage s'applique à tous les clients et serveurs recueillant des flux de données depuis le serveur d'enregistrement (explications) .....	74
Cryptage des données du serveur mobile (explications) .....	77
Exigences du cryptage du serveur mobile pour les clients .....	78
<b>Installation .....</b>	<b>79</b>
Installer un nouveau système XProtect .....	79
Installer le XProtect Essential+ .....	79
Installer votre système - option sur ordinateur unique .....	84
Installer votre système - option personnalisée .....	89
XProtect Installer les nouveaux composants .....	94
Installation via Download Manager (explications) .....	94
Installer le serveur d'enregistrement via Download Manager .....	95
Installer un serveur d'enregistrement de redondance via Download Manager .....	98
Installation silencieuse via un interpréteur de ligne de commande (explications) .....	100
Installation silencieuse d'un serveur d'enregistrement .....	101
Installer XProtect Smart Client silencieusement .....	103
Installation pour les groupes de travail .....	104
Installation dans une grappe .....	105
Download Manager/page web de téléchargement. ....	107
Configuration du Download Manager par défaut .....	109
Installateurs standard du Download Manager (utilisateur) .....	111
Ajouter/publier les composants de l'installateur Download Manager .....	111
Masquer/supprimer les composants de l'installateur Download Manager .....	112

Installateur de pilotes de périphériques - doit être téléchargé .....	113
Fichiers journaux de l'installation et dépannage .....	114
<b>Configuration .....</b>	<b>115</b>
Navigation au sein du Management Client .....	115
Vue d'ensemble de la connexion .....	115
Vue d'ensemble de la fenêtre Management Client .....	117
Vue d'ensemble des volets .....	119
Vue d'ensemble des menus .....	121
Menu Fichier .....	121
Menu Modifier .....	121
Menu Vue .....	121
Menu Action .....	122
Menu Outils .....	122
Menu Aide .....	122
Options de paramétrage pour le système .....	122
Onglet Général (options) .....	123
Onglet Journaux de serveurs (options) .....	126
Onglet Serveur de messagerie (options) .....	127
Onglet Génération AVI (options) .....	128
Onglet Réseau (options) .....	129
Onglet Signet (options) .....	129
Onglet Paramètres utilisateur (options) .....	130
Onglet Customer dashboard (Tableau de bord client) .....	130
Onglet Protection des preuves (options) .....	130
Onglet Messages audio (options) .....	131
Onglet Paramètres de contrôle d'accès (options) .....	132
Onglet Événements analytiques (options) .....	132
Onglet Alarmes et événements (Options) .....	133
Onglet Événements génériques (options) .....	135
Liste des tâches initiales de configuration .....	137

Configuration du système dans le panneau Navigation du site .....	139
Navigation sur le site : Bases .....	139
Informations sur la licence .....	140
Changements apportés aux périphériques sans activation (explications) .....	142
Calcul du nombre de changements apportés aux périphériques sans activation .....	143
Afficher la vue d'ensemble des licences .....	144
Activation automatique des licences (explications) .....	144
Activer l'activation automatique des licences .....	145
Désactiver l'activation automatique des licences .....	145
Activation des licences en ligne .....	145
Activation des licences hors ligne .....	146
Activer des licences après la période de grâce .....	146
Obtenir des licences supplémentaires .....	147
Licences et remplacement de périphériques matériels .....	147
Renseignements sur le site .....	148
Modifier les informations concernant le site .....	148
Navigation sur le site : Serveurs et matériel .....	148
Navigation sur le site : Serveurs et matériel : Serveurs d'enregistrement .....	149
Serveurs d'enregistrement (explications) .....	149
Enregistrer un serveur d'enregistrement .....	150
Changer ou vérifier la configuration de base du serveur d'enregistrement .....	151
Fenêtre Paramètres du serveur d'enregistrement .....	153
Voir le status du cryptage vers les clients .....	154
Icônes d'état du serveur d'enregistrement .....	155
Onglet Info (serveur d'enregistrement) .....	156
Info Propriétés de l'onglet Serveur d'enregistrement .....	157
Onglet Stockage (serveur d'enregistrement) .....	158
Stockage et archivage (explications) .....	159
Spécifier le comportement lorsque le stockage des enregistrements n'est pas disponible .....	163
Ajouter un nouvel emplacement de stockage .....	164

Créer une archive dans un emplacement de stockage .....	165
Relier un périphérique ou un groupe de périphériques à un emplacement de stockage .....	165
Modifier les paramètres d'un emplacement de stockage ou d'une archive sélectionné(e) .....	166
Activer la signature numérique à des fins d'export .....	166
Cryptez vos enregistrements .....	167
Sauvegarde des enregistrements archivés .....	169
Structure des archives (explication) .....	170
Supprimer une archive d'un espace de stockage .....	172
Suppression d'un espace de stockage .....	172
Déplacer les enregistrements non archivés d'un espace de stockage à un autre .....	173
Propriétés des paramètres de stockage et d'enregistrement .....	173
Propriétés des paramètres d'archive .....	175
Onglet Redondance (serveur d'enregistrement) .....	176
Affecter des serveurs d'enregistrement de redondance .....	177
Propriétés de l'onglet Redondance .....	179
Onglet Multicast (serveur d'enregistrement) .....	179
Multicast (explications) .....	181
Activez le multicast pour le serveur d'enregistrement .....	182
Affectation de la plage d'adresses IP .....	183
Spécification des options de datagramme .....	183
Activation du multicast pour des caméras individuelles .....	184
Onglet Réseau (serveur d'enregistrement) .....	184
Pourquoi utiliser une adresse publique ? .....	184
Définition de l'adresse publique et du port .....	185
Affectation de plages IP locales .....	185
Navigation sur le site : Serveurs et matériel : Serveurs de redondance .....	185
Serveurs d'enregistrement de redondance (explications) .....	185
Étapes de redondance (explications) .....	188
Fonctionnalité du serveur d'enregistrement de redondance (explications) .....	189
Configurer et activer des serveurs d'enregistrement de redondance .....	191

Serveurs d'enregistrement de redondance groupes pour une veille à froid .....	192
Lire les icônes d'état du serveur d'enregistrement de redondance .....	192
Onglet Multicast (serveurs de basculement) .....	193
Info Propriétés de l'onglet Serveur de basculement .....	194
Info Propriétés de l'onglet Groupe de basculement .....	196
Propriétés de l'onglet Séquence de groupe de basculement .....	196
Services du serveur d'enregistrement de redondance (explications) .....	196
Voir le cryptage sur un serveur d'enregistrement de redondance .....	197
Voir les messages d'état .....	198
Voir les informations sur la version .....	199
Navigation sur le site : Serveurs et matériel : Matériel .....	199
Matériel (explications) .....	199
Ajouter un matériel .....	199
Configuration matérielle (explications) .....	201
Désactiver/activer le matériel .....	202
Modifier le matériel .....	202
Activer/désactiver des périphériques individuels .....	206
Configurer une connexion sécurisée avec le matériel .....	207
Activer PTZ sur un encodeur vidéo .....	207
Gérer le matériel .....	208
Onglet Info (matériel) .....	208
Onglet Paramètres (matériel) .....	209
Onglet PTZ (encodeurs vidéo) .....	210
Gestion des mots de passe périphériques (explication) .....	210
Modifier les mots de passe sur les périphériques matériels .....	211
Mise à jour du firmware d'un périphérique (explications) .....	212
Mettre à jour le firmware sur les périphériques .....	213
Navigation sur le site : Serveurs et matériel : Gérer les serveurs distants .....	214
Onglet Info (serveur distant) .....	214
Onglet Paramètres (serveur à distance) .....	215



Onglet Événements (serveur distant) .....	215
Onglet Rappel à distance .....	216
Navigation sur le site : Périphériques : Travailler avec des périphériques .....	217
Périphériques (explications) .....	217
Dispositifs de caméra (explications) .....	218
Microphones (explications) .....	218
Périphériques de haut-parleurs (explications) .....	219
Périphériques métadonnées (explications) .....	220
Périphériques d'entrée (explications) .....	221
Activer une entrée manuellement pour la tester .....	222
Périphériques de sortie (explications) .....	223
Activer une sortie manuellement pour la tester .....	223
Activer/désactiver des périphériques par le biais des groupes de périphériques .....	224
Icônes de statut des périphériques .....	225
Navigation sur le site : Périphériques : Travailler avec des groupes de périphériques .....	227
Ajouter un groupe de périphériques .....	228
Spécifier les périphériques à inclure dans un groupe de périphériques .....	228
Spécifier les propriétés communes pour tous les périphériques d'un groupe de périphériques .....	229
Navigation sur le site : Onglet Périphériques .....	230
Onglet Info (périphériques) .....	230
Onglet Infos (explications) .....	230
Propriétés de l'onglet Info .....	231
Onglet Paramètres (périphériques) .....	233
Onglet Paramètres (explications) .....	233
Paramètres de la caméra (explications) .....	234
Onglet Flux (périphériques) .....	234
Onglet Flux (explications) .....	234
Multi-streaming (explications) .....	235
Ajouter un flux .....	236
Onglet Enregistrement (périphériques) .....	237

Onglet Enregistrement (explications) .....	237
Activer/désactiver l'enregistrement .....	239
Activer l'enregistrement sur les périphériques connexes .....	239
Pré-enregistrement (explications) .....	239
Périphériques prenant la mise en mémoire-tampon préalable en charge .....	240
Stockage des enregistrements temporairement en mémoire-tampon .....	240
Gérer la mise en mémoire-tampon préalable .....	240
Gérer l'enregistrement manuel .....	241
Spécifier la fluidité d'image de l'enregistrement .....	242
Activer l'enregistrement des images-clés .....	242
Stockage (explications) .....	242
Transfert de périphériques d'un stockage à un autre .....	244
Enregistrement à distance (explications) .....	244
Onglet Mouvement (périphériques) .....	245
Onglet de mouvement (explications) .....	245
Activer et désactiver la détection du mouvement .....	248
Spécifier les paramètres de détection de mouvement .....	248
Accélération matérielle (explications) .....	248
Activer la sensibilité manuelle .....	250
Spécifier le seuil .....	250
Sélectionner les paramètres des images-clés .....	251
Sélectionner l'intervalle de traitement des images .....	251
Spécifier la résolution de la détection .....	251
Génération des données de mouvement pour la recherche avancée .....	251
Spécifier l'exclusion de zones .....	252
Onglet Préréglages (périphériques) .....	253
Onglet Préréglages (explications) .....	253
Ajouter une position prédéfinie (type 1) .....	255
Utiliser les positions prédéfinies de la caméra (type 2) .....	257
Assigner une position prédéfinie par défaut .....	257

Modifier une position prédéfinie (type 1 seulement) .....	257
Renommer une position prédéfinie (type 2 seulement) .....	259
Verrouiller une position prédéfinie .....	259
Tester une position prédéfinie (type 1 seulement) .....	260
Sessions PTZ réservées (explication) .....	260
Libérer la session PTZ .....	260
Spécifier les périodes d'expiration des sessions PTZ .....	260
Propriétés des sessions PTZ .....	261
Onglet Patrouilles (périphériques) .....	262
Onglet Patrouille (explications) .....	262
Ajouter un profil de patrouille .....	265
Spécifier des positions prédéfinies dans un profil de patrouille .....	265
Spécifier la durée à chaque position prédéfinie .....	266
Personnaliser les transitions (PTZ) .....	266
Spécifier une position de fin .....	267
Patrouille manuelle (explications) .....	267
Propriétés des patrouilles manuelles .....	268
Onglet Lentille fisheye (périphériques) .....	268
Onglet Lentille Fisheye (explications) .....	268
Activer et désactiver la prise en charge fisheye .....	269
Spécifier les paramètres de la lentille fisheye .....	269
Onglet Événements (périphériques) .....	270
Onglet Événements (explications) .....	270
Ajout d'un événement .....	271
Spécifier les propriétés des événements .....	271
Utiliser plusieurs instances d'un événement .....	271
Onglet événement (propriétés) .....	272
Onglet Client (périphériques) .....	272
Onglet Client (explications) .....	272
Propriétés de l'onglet Client .....	273

Onglet Masquage de confidentialité (périphériques) .....	275
Onglet masquage de confidentialité (explications) .....	275
Masquage de confidentialité (explications) .....	277
Activer/désactiver le masquage de confidentialité .....	279
Définir les masques de confidentialité .....	279
Donner aux utilisateurs l'autorisation d'enlever les masques de confidentialité .....	280
Changez le délai d'expiration des masques de confidentialité .....	281
Créer un rapport de configuration de votre configuration du masquage de confidentialité .....	282
Onglet Masquage de confidentialité (propriétés) .....	283
Navigation sur le site : Clients .....	285
Clients (explications) .....	285
Navigation sur le site : Clients : En cours de configuration de Smart Wall .....	286
Licences XProtect Smart Wall .....	286
Configurer les Smart Wall .....	286
Configurer des droits d'utilisateur pour XProtect Smart Wall .....	288
Utilisation de règles avec des préréglages Smart Wall (explications) .....	289
Propriétés de Smart Wall .....	290
Onglet Info (propriétés du Smart Wall) .....	290
Onglet Préréglages (propriétés du Smart Wall) .....	290
Onglet Disposition (propriétés du Smart Wall) .....	291
Propriétés du moniteur .....	292
Onglet Info (propriétés du moniteur) .....	292
Onglet Positions prédéfinies (propriétés du moniteur) .....	293
Navigation sur le site : Clients : Groupes de vues .....	293
Groupes de vues et rôles (explications) .....	294
Ajouter un groupe de vues .....	294
Navigation sur le site : Clients : Profils Smart Client .....	295
Ajouter et configurer un profil Smart Client .....	295
Copier un profil Smart Client .....	295
Créer et configurer des profils Smart Client, rôles et profils de temps .....	296

Définir le mode simplifié comme le mode par défaut .....	297
Empêcher des opérateurs de permuter entre mode simple et avancé .....	299
Propriétés du profil Smart Client .....	300
Onglet Info (profils Smart Client) .....	300
Onglet Général (profils Smart Client) .....	300
Onglet Avancé (profils Smart Client) .....	301
Onglet En direct (profils Smart Client) .....	302
Onglet Relecture (profils Smart Client) .....	302
Onglet Configuration (profils Smart Client) .....	302
Onglet Exportations (profils Smart Client) .....	303
Onglet Chronologie (profils Smart Client) .....	303
Onglet Contrôle d'accès (profils Smart Client) .....	303
Onglet Gestionnaire d'alarme (profils Smart Client) .....	304
Onglet Smart Map (profils Smart Client) .....	304
Onglet Disposition des vues (profils Smart Client) .....	305
Navigation sur le site : Clients : Profils Management Client .....	305
Ajouter et configurer un profil Management Client .....	306
Copier un profil Management Client .....	306
Propriétés du profil Management Client .....	306
Info tab (Onglet Info (Profils Management Client) .....	306
Onglet Profil (Profils Management Client) .....	307
Navigation sur le site : Clients : En cours de configuration de Matrix .....	310
Ajouter des destinataires Matrix .....	310
Définir les règles d'envoi de vidéos aux destinataires Matrix .....	311
Envoyer la même vidéo à plusieurs vues XProtect Smart Client .....	311
Navigation sur le site : Règles et événements .....	312
Règles et événements (explications) .....	312
Actions et actions d'arrêt (explications) .....	314
Vue d'ensemble des événements .....	326
Règles .....	338

Règles (explications) .....	338
Règles par défaut (explications) .....	339
Complexité de la règle (explications) .....	343
Valider les règles (explications) .....	344
Ajouter une règle .....	345
Modifier, copier et renommer une règle .....	346
Désactiver et activer une règle .....	346
Temps récurrent .....	347
Profils temporels .....	347
Spécifier un profil de temps .....	348
Modifier un profil de temps .....	350
Profils de temps toute la journée (explications) .....	350
Créer un profil de temps toute la journée .....	351
Propriétés du profil de temps journalier .....	351
Profils de notification .....	352
Profils de notification (explications) .....	352
Conditions préalables à la création des profils de notification .....	352
Ajouter des profils de notification .....	352
Utiliser des règles pour déclencher des notifications par e-mail .....	354
Profils de notification (propriétés) .....	354
Événements définis par l'utilisateur .....	356
Événements définis par l'utilisateur (explications) .....	356
Ajouter un événement défini par l'utilisateur .....	358
Renommer un événement défini par l'utilisateur .....	358
Événements analytiques .....	358
Événements analytiques (explications) .....	358
Ajouter et modifier un événement analytique .....	359
Tester un événement analytique .....	359
Événement analytique test (propriétés) .....	360
Modifier les paramètres des événements analytiques .....	363

Événements génériques .....	363
Événements génériques (explications) .....	363
Ajouter un événement générique .....	364
Événements génériques (propriétés) .....	364
Source de données d'un événement générique (propriétés) .....	366
Navigation sur le site : Sécurité .....	368
Rôles (explications) .....	369
Droits d'un rôle (explications) .....	369
Utilisateurs (explications) .....	370
Ajouter et gérer un rôle .....	372
Copier, renommer ou supprimer un rôle .....	372
Assigner et supprimer des utilisateurs et groupes aux/des rôles .....	373
Afficher les rôles effectifs .....	374
Paramètres des rôles .....	374
Onglet Info (rôles) .....	374
Onglet Utilisateur et Groupes (rôles) .....	376
Onglet Sécurité globale (rôles) .....	377
Onglet Périphériques (rôles) .....	405
Onglet PTZ (rôles) .....	413
Onglet Audio (rôles) .....	415
Onglet Enregistrements à distance (rôles) .....	415
Onglet Smart Wall (rôles) .....	415
Onglet Événement externe (rôles) .....	416
Onglet Groupe de vues (rôles) .....	416
Onglet Serveurs (rôles) .....	417
Onglet Matrix (rôles) .....	417
Onglet alarmes (rôles) .....	418
Onglet Contrôle d'accès (rôles) .....	418
Onglet LPR (rôles) .....	419
Onglet MIP (rôles) .....	419

Utilisateurs basiques (explications) .....	420
Créer des utilisateurs de base .....	420
Navigation sur le site : Tableau de bord système .....	420
Tableau de bord du système (explications) .....	420
Moniteur système (explication) .....	421
Personnaliser le tableau de bord .....	422
Détails du moniteur système (explications) .....	423
Seuils du Moniteur système (explication) .....	425
Définir les seuils du moniteur système .....	427
Protection des preuves (explications) .....	428
Tâches actuelles (explications) .....	431
Rapports de configuration (explications) .....	431
Créer un rapport de configuration .....	431
Configurer les détails du rapport .....	431
Navigation sur le site : Journaux des serveurs .....	432
Journaux (explications) .....	432
Filtrer les journaux .....	433
Exporter les journaux .....	434
Autoriser la version 2018 R2 et les composants antérieurs à écrire dans les journaux .....	434
Journaux système (propriétés) .....	435
Journaux d'activité (propriétés) .....	436
Journaux déclenchés par les règles (propriétés) .....	437
Navigation sur le site : utilisation des métadonnées .....	437
Définition des métadonnées .....	437
Recherche de métadonnées (explications) .....	438
Critères de la recherche de métadonnées .....	438
Afficher ou masquer les catégories et les filtres de recherche de métadonnées dans XProtect Smart Client .....	438
Navigation sur le site : Alarmes .....	439
Alarmes (explications) .....	439
Configuration des alarmes (explications) .....	440



Définitions des alarmes .....	441
Ajout d'une alarme .....	442
Définitions d'alarmes (Propriétés) .....	443
Paramètres des données de l'alarme .....	445
Paramètres sons .....	447
Activer le cryptage .....	448
Activer le cryptage depuis et vers le serveur de gestion .....	448
Activer le cryptage du serveur pour les serveurs d'enregistrement ou les serveurs distants .....	449
Activer le cryptage pour les clients et les serveurs .....	451
Activer le cryptage sur le serveur mobile .....	453
Voir le status du cryptage vers les clients .....	455
En cours de configuration de Milestone Federated Architecture .....	456
Configurer votre système pour exécuter des sites fédérés .....	460
Ajouter un site à la hiérarchie .....	462
Accepter les ajouts dans la hiérarchie .....	462
Définir les propriétés du site .....	463
Actualiser la hiérarchie des sites .....	464
Connexion à d'autres sites de la hiérarchie .....	464
Détacher un site de la hiérarchie .....	464
Propriétés des sites fédérés .....	465
Onglet Généralités .....	465
Onglet Site parent .....	465
En cours de configuration de Milestone Interconnect .....	466
Sélectionner Milestone Interconnect ou Milestone Federated Architecture (explications) .....	466
Milestone Interconnect et les licences .....	467
Milestone Interconnect (explications) .....	467
Configurations Milestone Interconnect (explications) .....	469
Ajouter un site distant à votre site Milestone Interconnect central .....	470
Attribuer des droits d'utilisateur .....	472
Mise à jour du matériel du site distant .....	472

Établir une connexion à distance entre le bureau et un système à distance .....	472
Activer la lecture directe à partir de la caméra du site distant .....	473
Rappeler les enregistrements à distance de la caméra du site distant .....	473
Configurer votre site central pour répondre aux événements des sites distants .....	474
Configuration des services de connexion à distance .....	475
Installer un environnement STS pour une connexion à la caméra One-click .....	476
Ajouter/Modifier des STS .....	476
Enregistrer une nouvelle caméra Axis One-Click .....	477
Propriété de connexion à la caméra Axis One-Click .....	477
Configuration de Smart Map .....	478
Arrière-plans géographiques (explications) .....	479
Acquérir une clé API pour Google Maps ou Bing Maps .....	479
Google Maps .....	479
Bing Maps .....	480
Activer Bing Maps ou Google Maps dans Management Client .....	480
Activer Bing Maps ou Google Maps dans XProtect Smart Client .....	480
Spécifier le serveur de tuile OpenStreetMap .....	481
Fichiers smart map en cache supprimés (explications) .....	482
Activer la modification de la smart map .....	483
Activer l'édition des caméras sur smart map .....	484
Définissez la position de la caméra, la direction, le champ de visualisation et la profondeur (smart map) .....	484
Configuration d'une Smart Map avec Milestone Federated Architecture .....	486
<b>Maintenance .....</b>	<b>488</b>
Sauvegarde et restauration de la configuration système .....	488
Sauvegarde et de la restauration de la configuration de votre système (explications) .....	488
Sélectionner le fichier de sauvegarde partagé .....	489
Sauvegarde manuelle de la configuration système .....	489
Restauration d'une configuration système à partir d'une sauvegarde manuelle .....	489
Mot de passe de configuration système (explications) .....	491
Paramètres du mot de passe de configuration système .....	491

Modifier les paramètres du mot de passe de configuration système .....	492
Entrer les paramètres du mot de passe de configuration système (récupération) .....	493
Sauvegarde manuelle de la configuration de votre système (explications) .....	493
Sauvegarde et restauration de la configuration du serveur d'événements (explications) .....	494
Sauvegarde et restauration programmées de la configuration du système (explications) .....	494
Sauvegarder la configuration du système avec une sauvegarde programmée .....	495
Restauration d'une configuration système à partir d'une sauvegarde programmée .....	495
Sauvegarder la base de données SQL du serveur de journaux .....	496
Scénarios de problèmes et d'échecs de sauvegarde/restauration (explications) .....	496
Déplacer le serveur de gestion .....	497
Serveurs de gestion indisponibles (explications) .....	498
Déplacer la configuration du système .....	499
Remplacer un serveur d'enregistrement .....	499
Déplacer le matériel .....	500
Déplacer du matériel (Assistant) .....	501
Remplacer le matériel .....	504
Gérer le SQL Server et les bases de données .....	507
Modifier les adresses du SQL Server et de la base de données (explications) .....	507
Modifier le SQL Server et la base de données du serveur des journaux .....	508
Modifier les adresses de la base de données SQL du serveur de gestion et du serveur d'événements .....	508
Services du serveur de gestion .....	509
Icônes de la barre des tâches du serveur de gestion (explication) .....	509
Démarrer ou arrêter le service Management Server .....	511
Démarrer ou arrêter le service Recording Server .....	512
Consulter les messages d'état relatifs au serveur de gestion ou au serveur d'enregistrement .....	513
Gérer le cryptage avec le Server Configurator .....	513
Démarrer, arrêter ou redémarrer le service Event Server .....	514
Arrêt du service Event Server .....	515
Consulter le Event Server ou les journaux MIP .....	515
Gérer les services enregistrés .....	516

Ajouter et modifier des services enregistrés .....	517
Gérer la configuration du réseau .....	517
Propriétés des services enregistrés .....	517
Supprimer des pilotes de périphériques (explications) .....	518
Supprimer un serveur d'enregistrement .....	519
Supprimer tous les périphériques matériels sur un serveur d'enregistrement .....	519
<b>Dépannage .....</b>	<b>520</b>
Problème : Le changement des adresses de SQL Server et de la base de données empêche l'accès à la base de données ..	520
Problème : Le démarrage du serveur d'enregistrement échoue en raison d'un conflit de port .....	520
Problème : Recording Server est mis hors tension lors du basculement du nœud en grappe de Management Server .....	521
<b>Mise à niveau .....</b>	<b>522</b>
Mise à niveau (explications) .....	522
Conditions préalables de mise à niveau .....	523
Mettre à jour VMS XProtect pour un fonctionnement conforme au mode FIPS 140-2 .....	524
Mise à jour des meilleures pratiques .....	526
Mise à niveau dans une configuration de groupe de travail .....	528
Mise à jour dans une grappe .....	528

# Copyright, marques et exclusions

Copyright © 2020 Milestone Systems A/S

## 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

## Présentation générale du produit

Les produits VMS XProtect constituent un logiciel de gestion de vidéo conçu pour les installations de toutes formes et de toutes tailles. Que vous souhaitiez protéger votre magasin contre le vandalisme ou gérer une installation de haute sécurité sur plusieurs sites, XProtect vous permet d'y parvenir. Les solutions apportent une administration centralisée de tous les périphériques, serveurs et utilisateurs et permet d'utiliser un système basé sur des règles extrêmement flexibles et contrôlé par des programmes et des événements.

Votre système comprend les principaux composants suivants :

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

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

Vous pouvez installer votre système sur les serveurs virtualisés ou sur plusieurs serveurs physiques dans une configuration distribuée. Voir également Une configuration distribuée du système sur la page 28.

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

Grâce aux produits les plus riches en fonctionnalités (voir Graphique de comparaison des produits sur la page 46), votre système peut gérer, sur plusieurs sites, si cela est nécessaire, un nombre illimité de caméras, de serveurs et d'utilisateurs. Votre système peut supporter IPv4 ainsi que IPv6.

## Composants principaux du système

### Serveur de gestion

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

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

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

## Serveur d'enregistrement

Le serveur d'enregistrement est chargé de communiquer avec les caméras réseau et les encodeurs vidéo, d'enregistrer l'audio et la vidéo récupérés ainsi que de garantir l'accès du client à la fois à l'audio et à la vidéo enregistrés et en direct. En outre, le serveur d'enregistrement est chargé de communiquer avec d'autres produits Milestone connectés via la technologie Milestone Interconnect.

### Pilotes de périphériques

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

### Base de données Multimédia

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

## Serveur d'événements

Le serveur d'événements gère différentes tâches liées à des événements, des alarmes, des cartes et des intégrations tierces via le MIP SDK.

### Événements

- Tous les événements du système sont regroupés dans le serveur d'événements afin d'avoir un seul

endroit et une seule interface pour que les partenaires effectuent des intégrations qui utilisent les événements du système

- En outre, le serveur d'événements offre un accès tiers à l'envoi d'événements au système via les événements génériques ou l'interface d'analyse d'événements

### Alarmes

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

### Plans

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

### MIP SDK

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

## Serveur de journaux

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

## SQL Server et bases de données

Le serveur de gestion, le serveur d'événements et le serveur stockent la configuration du système, les alarmes, les événements et les messages de journaux, entre autres, dans les bases de données SQL sur une ou plusieurs installations SQL Server. Le serveur de gestion et le serveur d'événements partagent la même base de données SQL, alors que le serveur de journaux possède sa propre base de données SQL. L'installateur de système inclut Microsoft SQL Server Express qui est une version gratuite de SQL Server.

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

## Serveur Mobile

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



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

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

## Active Directory

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

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

## Management Client (explications)

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

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

Pour un aperçu détaillé de Management Client, voir la Navigation au sein du Management Client sur la page 115.

## Composants du système en option

L'utilisation des composants suivants n'est pas obligatoire, mais vous pouvez les ajouter pour répondre à différents besoins.

### Serveur d'enregistrement de redondance

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

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

- Veille à froid - pour la surveillance de plusieurs serveurs d'enregistrement
- Veille à chaud - pour la surveillance d'un serveur d'enregistrement unique

La différence entre le mode de redondance à froid et le mode de veille à chaud est que pour le mode de redondance à froid, le serveur d'enregistrement de redondance ne sait pas quel serveur prendre en charge, il ne peut donc pas commencer avant qu'un serveur d'enregistrement ne tombe en panne. En mode de veille à chaud, le temps de basculement est beaucoup plus court, comme le serveur d'enregistrement de redondance sait déjà quel serveur d'enregistrement il doit prendre en charge et peut donc pré-charger la configuration et le démarrage complètement - sauf pour la dernière étape de connexion aux caméras.

## Serveur de gestion de redondance

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

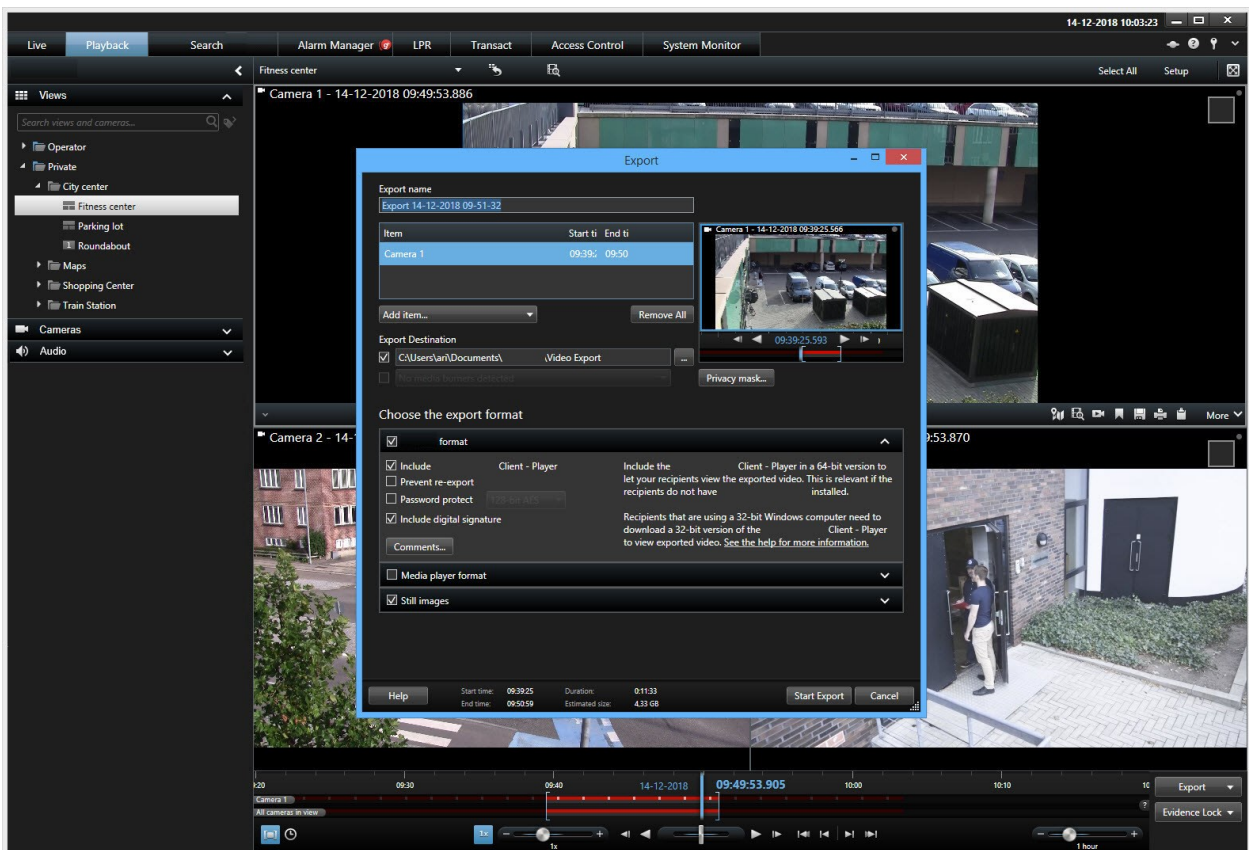
## Clients

Introductions aux différents clients utilisés par les opérateurs d'une système.

### XProtect Smart Client (explications)

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

Disponible dans de nombreuses langues, XProtect Smart Client est une interface utilisateur flexible pouvant être optimisée pour les tâches de chaque opérateur et réglée en fonction de ses compétences et niveaux d'autorité spécifiques.



L'interface vous permet de personnaliser votre visualisation afin de spécifier votre environnement de travail en sélectionnant un thème clair ou sombre. Elle dispose également d'onglets travail optimisés et d'une chronologie de la vidéo intégrée pour une opération de surveillance aisée.

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

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

## XProtect Mobile client (explications)

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

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

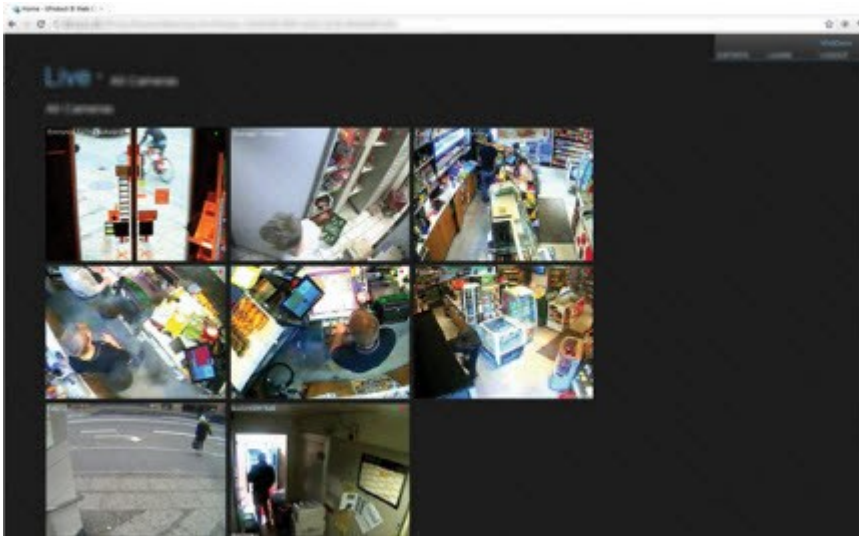


Si vous souhaitez utiliser le client XProtect Mobile avec votre système, vous devez disposer d'un serveur XProtect Mobile afin d'établir la connexion entre le client XProtect Mobile et votre système. Une fois que le serveur XProtect Mobile est configuré, téléchargez le client XProtect Mobile gratuitement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

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

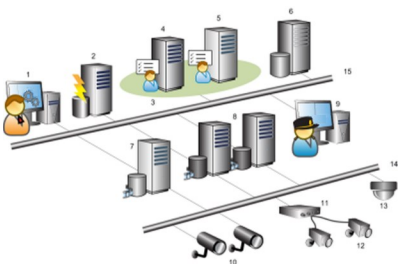
## XProtect Web Client (explications)

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



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

## Une configuration distribuée du système



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

Légende :

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

## Produits complémentaires

Milestone a mis au point des produits complémentaires qui s'intègrent pleinement aux XProtect pour vous offrir plus de fonctionnalités. L'accès à des produits complémentaires est contrôlé par votre code de licence du logiciel (SLC).

### XProtect Access (explications)



L'utilisation de XProtect Access nécessite l'achat d'une licence de base qui vous permet d'accéder à cette fonctionnalité au sein de votre système XProtect. Vous avez également besoin d'une licence de porte à contrôle d'accès pour chaque porte que vous souhaitez contrôler.



Vous pouvez utiliser XProtect Access avec les systèmes de contrôle d'accès des fournisseurs lorsqu'il existe un module d'extension spécifique au fournisseur pour XProtect Access.

La fonction d'intégration du contrôle d'accès contient une nouvelle fonctionnalité qui facilite l'intégration des systèmes de contrôle d'accès des clients avec XProtect. Vous obtenez ainsi :

- Une interface utilisateur commune destinée aux opérateurs pour de multiples systèmes de contrôle d'accès dans XProtect Smart Client
- Une intégration plus rapide et plus puissante des systèmes de contrôle d'accès
- Plus de fonctions pour l'opérateur (voir ci-dessous)

Dans XProtect Smart Client, l'opérateur obtient :

- La surveillance en direct des événements et des points d'accès
- Un passage autorisé par un opérateur pour les demandes d'accès
- L'intégration du plan
- Des définitions d'alarmes pour les événements de contrôle d'accès
- Une enquête sur les événements et les points d'accès
- Une vue d'ensemble centralisée et un contrôle de l'état des portes
- Des informations sur les détenteurs de carte et la gestion de ces derniers

Le **Journal d'activité** enregistre toutes les commandes effectuées par chaque utilisateur dans le système de contrôle d'accès à partir de XProtect Smart Client.

Hormis la licence de base XProtect Access, vous devez installer un module d'extension d'intégration spécifique au fournisseur sur le serveur d'événements avant de pouvoir débiter une intégration .

## XProtect LPR (explications)

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

XProtect LPR propose une fonction d'analyse du contenu et de reconnaissance des plaques d'immatriculation de véhicules basée sur la vidéo (VCA) en interaction avec votre système de surveillance et votre XProtect Smart Client.

Pour lire les caractères d'une plaque, XProtect LPR utilise une fonction de reconnaissance optique de caractères sur des images, à l'aide de paramètres de caméra spécialisés.

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

Exemples d'événements dans XProtect LPR :

- Déclencher des enregistrements d'une qualité particulière dans le système de surveillance
- Activer des alarmes
- Faire la correspondance avec des éléments des listes de correspondance positive/négative des plaques d'immatriculation
- Ouvrir des barrières
- Allumer la lumière
- Transmission de type push de la vidéo d'incidents sur les écrans d'ordinateurs de certains membres du personnel de sécurité
- Envoyer des SMS sur téléphone mobile

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

## XProtect Smart Wall (explications)



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

XProtect Smart Wall est un produit complémentaire qui permet aux entreprises de créer des murs vidéo qui répondent à leurs besoins spécifiques en matière de sécurité. Smart Wall fournit un aperçu de toutes les données vidéo dans le système VMS<sup>1</sup> et il peut être partagé entre plusieurs opérateurs.

Avec XProtect Smart Wall, les opérateurs peuvent partager presque tout type de contenu disponible dans XProtect Smart Client, comme de la vidéo, des images, du texte, des alarmes et des Smart Maps, par exemple.



XProtect Smart Wall est initialement configuré par un administrateur du système dans XProtect Management Client. Cela inclut les préférences contrôlant la disposition de l'affichage du Smart Wall et la distribution des caméras dans les différents moniteurs. Dans XProtect Smart Client, les opérateurs peuvent modifier le contenu affiché sur le Smart Wall en appliquant différents préférences. Les changements d'affichage peuvent être également contrôlés par des règles qui changent automatiquement les préférences.

---

<sup>1</sup>Abréviation pour "Logiciel de gestion des vidéos".

Avec la vue d'ensemble Smart Wall, les opérateurs peuvent ajouter du contenu spécifique ou des vues complètes aux moniteurs Smart Wall par de simples glisser-déposer.

## XProtect Transact (explications)



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

XProtect Transact est un produit complémentaire aux solutions de vidéosurveillance IP de Milestone.

XProtect Transact est un outil servant à observer les transactions en cours et à enquêter sur des transactions antérieures. Les transactions sont connectées aux systèmes de surveillance vidéo numériques contrôlant les transactions. Cela permet par exemple d'apporter des preuves en cas de fraude ou de vol. Il existe une relation directe entre les lignes de transaction et les images vidéo.

Les données de transaction peuvent provenir de différents types de sources. La plupart du temps, ces sources sont des systèmes de points de vente ou des distributeurs automatiques de billets.

## Milestone Open Network Bridge (explications)

ONVIF est un forum mondial ouvert qui œuvre pour standardiser et sécuriser la communication des produits de vidéosurveillance IP. Le but est de faciliter l'échange de données vidéo. Par exemple, pour permettre aux autorités, centres de surveillance ou organisations similaires d'accéder rapidement à des flux vidéo en direct et enregistrés dans tout système de surveillance IP.

Milestone Systems souhaite soutenir cet objectif et a développé Milestone Open Network Bridge dans ce but. Milestone Open Network Bridge fait partie de la plateforme ouverte Milestone et offre une interface prenant en charge les parties de la norme ONVIF liées à la récupération des vidéos en direct et enregistrées depuis n'importe quel produit Milestone VMS.

Ce document fournit les informations suivantes :

- Informations sur la norme ONVIF et liens vers les matériels de référence
- Instructions pour installer et configurer le Milestone Open Network Bridge dans votre produit VMS XProtect.
- Exemples de la manière de mettre en œuvre différents types de clients ONVIF pour diffuser de la vidéo en direct et enregistrée depuis les produits VMS XProtect

## XProtect DLNA Server (explications)

DLNA (Digital Living Network Alliance) est une norme de connexion pour plusieurs appareils. Les fabricants d'électronique obtiennent la certification DLNA de leurs produits afin de garantir l'interopérabilité entre les différents fournisseurs et appareils. Ils peuvent ainsi distribuer un contenu multimédia audio, vidéo et photo.



Les TVs et affichages publics disposent souvent de la norme DLNA et sont connectés à un réseau. Ils peuvent ainsi scanner le réseau à la recherche de contenu multimédia, se connecter au périphérique et demander l'envoi d'un flux média vers leur lecteur intégré. Le XProtect DLNA Server peut être détecté par certains périphériques certifiés DLNA et fournir des flux vidéo en direct à partir de caméras sélectionnées vers des périphériques certifiés DLNA avec un lecteur média.



Les périphériques DLNA ont un délai d'affichage de la vidéo en direct de 1 à 10 secondes. Cela est dû aux différentes tailles de tampon dans les périphériques.

Le XProtect DLNA Server doit être connecté au même réseau que le système XProtect et le périphérique DLNA doit être connecté au même réseau que le XProtect DLNA Server.

## Ports utilisés par le système

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

Ceux-ci sont classés en deux groupes :

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

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

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

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

### Composants du serveur (connexions entrantes)

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

### Service Management Server et processus connexes

Numéro de port	Protocole	Processus	Connexions de...	Objectif
80	HTTP	IIS	Tous les composants XProtect  Le service Management Server et les services Recording Server	Communication principale, par exemple : authentification et configurations.  Enregistrement des serveurs d'enregistrement et des serveurs de gestion par le pôle d'applications Identity Server (IDP).
443	HTTPS	IIS	XProtect Smart Client et les Management Client	Authentification des utilisateurs de base.
6473	TCP	Service Management Server	Icône de la barre d'état Management Server Manager, connexion locale uniquement.	Affichage de l'état et gestion du service.
8080	TCP	Serveur de gestion	Connexion locale uniquement.	La communication entre les processus internes du serveur.
9000	HTTP	Serveur de gestion	Services Recording Server	Service Web pour une communication interne entre les serveurs.
12345	TCP	Service Management Server	XProtect Smart Client	Communication entre le système et les bénéficiaires Matrix.  En cas de besoin, vous pouvez modifier le numéro de port dans le Management Client.
12974	TCP	Service Management Server	Service SNMP Windows	Communication avec l'agent d'extension SNMP.  N'utilisez pas le port à d'autres fins, même si votre système n'applique pas SNMP.  Dans les systèmes XProtect 2014 ou plus anciens, le numéro de port était

Numéro de port	Protocole	Processus	Connexions de...	Objectif
				6475.  Dans les système XProtect 2019 R2 et plus anciens, le numéro de port était 7475.

### Service SQL Server

Numéro de port	Protocole	Processus	Connexions de...	Objectif
1433	TCP	SQL Server	Service Management Server	Enregistrement et récupération des configurations.
1433	TCP	SQL Server	Service Event Server	Enregistrement et récupération des événements.
1433	TCP	SQL Server	Service Log Server	Enregistrement et récupération des entrées de journaux.

### Service Data Collector

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

### Service Event Server

Numéro de port	Protocole	Processus	Connexions de...	Objectif
1234	TCP/UDP	Service Event Server	Tout serveur envoyant des événements génériques à votre système XProtect.	Écouter des événements génériques de systèmes ou de périphériques externes.  Uniquement si la source de données pertinente est activée.
1235	TCP	Service Event Server	Tout serveur envoyant des événements génériques à votre système XProtect.	Écouter des événements génériques de systèmes ou de périphériques externes.  Uniquement si la source de données pertinente est activée.
9090	TCP	Service Event Server	Tout système ou périphérique envoyant des événements analytiques à votre système XProtect.	Écouter les événements analytiques des systèmes ou des dispositifs externes.  Pertinent uniquement si la fonction Événements analytiques est activée.
22331	TCP	Service Event Server	XProtect Smart Client et les Management Client	Configuration, événements, alarmes, et données de plan.
22333	TCP	Service Event Server	Modules d'extension et applications MIP.	Messagerie MIP.

### Service Recording Server

Numéro de port	Protocole	Processus	Connexions de...	Objectif
25	SMTP	Service Recording Server	Caméras, encodeurs et périphériques E/S.	Écouter des messages d'événements à partir des périphériques. Le port est désactivé par défaut.
5210	TCP	Service Recording Server	Serveurs d'enregistrement de redondance.	Fusion des bases de données après l'exécution d'un serveur d'enregistrement de basculement.
5432	TCP	Service Recording Server	Caméras, encodeurs et périphériques E/S.	Écouter des messages d'événements à partir des périphériques. Le port est désactivé par défaut.
7563	TCP	Service Recording Server	XProtect Smart Client, Management Client	Récupération des flux vidéo et audio, commandes PTZ.
8966	TCP	Service Recording Server	Icône de la barre d'état Recording Server Manager, connexion locale uniquement.	Affichage de l'état et gestion du service.
9001	HTTP	Service Recording Server	Serveur de gestion	Service Web pour une communication interne entre les serveurs. Si plusieurs instances du serveur d'enregistrement sont en cours d'utilisation, chaque instance doit avoir son propre port. Les ports supplémentaires seront 9002, 9003, etc.
11000	TCP	Service Recording Server	Serveurs d'enregistrement	Interrogation de l'état des serveurs d'enregistrement.

Numéro de port	Protocole	Processus	Connexions de...	Objectif
		Server	de redondance	
12975	TCP	Service Recording Server	Service SNMP Windows	<p>Communication avec l'agent d'extension SNMP.</p> <p>N'utilisez pas le port à d'autres fins, même si votre système n'applique pas SNMP.</p> <p>Dans les systèmes XProtect 2014 ou plus anciens, le numéro de port était 6474.</p> <p>Dans les système XProtect 2019 R2 et plus anciens, le numéro de port était 7474.</p>
65101	UDP	Service Recording Server	Connexion locale uniquement	Écouter des notifications d'événements des pilotes.



Outre les connexions entrantes vers le service Recording Server susmentionné, le service Recording Server établit des connexions sortantes vers les caméras, NVR et les sites interconnectés distants (Milestone Interconnect ICP).

### Service Failover Server et service Failover Recording Server

Numéro de port	Protocole	Processus	Connexions de...	Objectif
25	SMTP	Service Failover Recording Server	Caméras, encodeurs et périphériques E/S.	<p>Écouter des messages d'événements à partir des périphériques.</p> <p>Le port est désactivé par défaut.</p>

Numéro de port	Protocole	Processus	Connexions de...	Objectif
5210	TCP	Service Failover Recording Server	Serveurs d'enregistrement de redondance	Fusion des bases de données après l'exécution d'un serveur d'enregistrement de basculement.
5432	TCP	Service Failover Recording Server	Caméras, encodeurs et périphériques E/S.	Écouter des messages d'événements à partir des périphériques. Le port est désactivé par défaut.
7474	TCP	Service Failover Recording Server	Service SNMP Windows	Communication avec l'agent d'extension SNMP. N'utilisez pas le port à d'autres fins, même si votre système n'applique pas SNMP.
7563	TCP	Service Failover Recording Server	XProtect Smart Client	Récupération des flux vidéo et audio, commandes PTZ.
8844	UDP	Service Failover Recording Server	Connexion locale uniquement.	La communication entre les serveurs.
8966	TCP	Service Failover Recording Server	Icône de la barre d'état Failover Recording Server Manager, connexion locale uniquement.	Affichage de l'état et gestion du service.
8967	TCP	Service Failover Server	Icône de la barre d'état Failover Server Manager, connexion locale uniquement.	Affichage de l'état et gestion du service.
8990	TCP	Service Failover	Service Management Server	Suivi de l'état du service Failover Server.

Numéro de port	Protocole	Processus	Connexions de...	Objectif
		Server		
9001	HTTP	Service Failover Server	Serveur de gestion	Service Web pour une communication interne entre les serveurs.



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

### Service Log Server

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

### Service Mobile Server

Numéro de port	Protocole	Processus	Connexions de...	Objectif
8000	TCP	Service Mobile Server	Icône de la barre d'état Mobile Server Manager, connexion locale uniquement.	Application SysTray.
8081	HTTP	Service	Clients mobiles, clients Web, et	Envoi de flux de



Numéro de port	Protocole	Processus	Connexions de...	Objectif
		Mobile Server	Management Client.	données, vidéo et audio.
8082	HTTPS	Service Mobile Server	Clients mobiles et clients Web.	Envoi de flux de données, vidéo et audio.
40001 - 40099	HTTP	Service Mobile Server	Service Recording Server	Mobile Server Vidéo Push. Cette plage de port est désactivée par défaut.

#### Service LPR Server

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

#### Service Milestone Open Network Bridge

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

### Service XProtect DLNA Server

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

### Service XProtect Screen Recorder

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

### Composants du serveur (connexions sortantes)

#### Service Management Server

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

### Service du serveur

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

### Service Failover Server et service Failover Recording Server

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

### Service Event Server

Numéro de port	Protocole	Connexions à...	Objectif
443	HTTPS	Milestone Customer Dashboard par <a href="https://service.milestonesys.com/">https://service.milestonesys.com/</a>	Envoyer l'état, les événements et les messages d'erreur depuis le système XProtect vers Milestone Customer Dashboard.

### Service Log Server

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

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

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

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

Numéro de port	Protocole	Connexions à...	Objectif
25	SMTP	Serveurs d'enregistrement et serveurs d'enregistrement de basculement	Envoi de notifications d'événements (obsolète).
5432	TCP	Serveurs d'enregistrement et serveurs d'enregistrement de basculement	Envoi de notifications d'événements. Le port est désactivé par défaut.
22337	HTTP	Serveur de journaux	Transmettre les messages au serveur de journaux.



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

**Composants du client (connexions sortantes)**

XProtect Smart Client, XProtect Management Client, serveur XProtect Mobile

Numéro de port	Protocole	Connexions à...	Objectif
80	HTTP	Service Management Server	Authentification
443	HTTPS	Service Management Server	Authentification des utilisateurs de base.
7563	TCP	Service Recording Server	Récupération des flux vidéo et audio, commandes PTZ.
22331	TCP	Service Event Server	Alarmes.

**XProtect Web Client, client XProtect Mobile**

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

## 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	Site distant	Site distant	Site

Nom	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
		distant			central/distant
Milestone Federated Architecture™	-	-	-	Site distant	Site central/distant
Basculement sur serveur d'enregistrement	-	-	-	Affectation multiple et affectation unique	Affectation multiple et affectation 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)	-	-	-	✓	✓

Nom	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
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)	-	-	-	✓	✓
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	✓



Nom	XProtect Essential+	XProtect Express+	XProtect Professional+	XProtect Expert	XProtect Corporate
Moniteur système	-	-	-	✓	✓
Smart Map	-	-	-	✓	✓
Vérification en deux étapes	-	-	-	-	✓
Assistance DLNA	-	✓	✓	✓	✓
Masquage de confidentialité	-	✓	✓	✓	✓
Gestion des mots de passe périphériques			✓	✓	✓

# Licence

## Licences (explications)

Si vous avez installé un système XProtect Essential+, vous pouvez exécuter le système et huit licences de périphérique matériel gratuitement. Une activation automatique de la licence est autorisée et le matériel est activé au fur et à mesure que vous l'ajoutez au système.

Ce n'est que lorsque vous serez passé à un produit XProtect plus avancé (voir [Changer le code de licence du logiciel sur la page 51](#)), que le reste de cette rubrique et les autres rubriques relatives aux licences présentées dans ces documents deviendront pertinentes.

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

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

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

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

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

Pour commencer, téléchargez le logiciel sur notre site Web (<https://www.milestonesys.com/downloads/>). Lors de l'installation du logiciel (voir [Installer un nouveau système XProtect sur la page 79](#)), il vous sera demandé de fournir un fichier de licence logicielle.

Au terme de l'installation et une fois vos licences activées, vous pourrez afficher une vue d'ensemble de vos licences pour toutes les installations sous le même SLC sur la page **Bases > Renseignements sur la licence**.

Vous avez acheté au moins deux types de licences :

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

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

Pour plus d'informations, consultez la liste des périphériques pris en charge sur le site Web de Milestone (<https://www.milestonesys.com/supported-devices/>). Si vous souhaitez utiliser la fonction vidéo push dans XProtect Mobile, vous aurez besoin d'une licence de périphérique pour chaque portable ou tablette pouvant utiliser cette fonction dans votre système. Si vous êtes à court de licences de périphérique matériel, vous pouvez désactiver (voir Désactiver/activer le matériel sur la page 202) les périphériques moins importants pour permettre à de nouveaux périphériques de fonctionner.

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

La plupart des produits complémentaires XProtect nécessitent des types de licences supplémentaires. Le fichier de licence logicielle comprend également des informations relatives aux licences pour les produits complémentaires. Certains produits complémentaires possèdent leurs propres fichiers de licence du logiciel.

## Changer le code de licence du logiciel

Si votre installation fonctionne avec un code de licence du logiciel (SLC) temporaire pendant la première période, ou si vous avez mis à niveau votre système vers un produit XProtect plus avancé, vous pouvez le changer au profit d'un SLC permanent sans avoir besoin de désinstaller ni de réinstaller quoi que ce soit lorsque vous recevez votre nouveau fichier de licence logicielle.



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

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



2. Cliquez avec le bouton droit sur l'icône **Serveur de gestion** et sélectionnez **Changer de licence**.
3. Cliquez sur **Importer une licence**.
4. Ensuite, sélectionnez le fichier de licence du logiciel sauvegardé à cette fin. Lorsque vous avez terminé, l'emplacement du fichier de licence du logiciel sélectionné est ajouté juste en-dessous du bouton **Importer une licence**.
5. Cliquez sur **OK**. Vous êtes maintenant prêt à enregistrer le SLC. Voir Enregistrer le code de licence du logiciel sur la page 68.

## Exigences et considérations

### Heure d'été (explications)

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

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



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

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

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

Exemple :

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

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

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

Exemple :

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

Pour éviter qu'une telle situation ne se produise, votre système archive la vidéo en cours au cas où l'heure du système changerait de plus de cinq minutes. Vous ne pouvez pas consulter la première instance de l'heure 01h00 directement dans l'un de nos clients, mais les données sont enregistrées et conservées en sécurité. Vous pouvez parcourir cette vidéo dans XProtect Smart Client en ouvrant directement la base de données archivée.

### Serveurs de temps (explications)

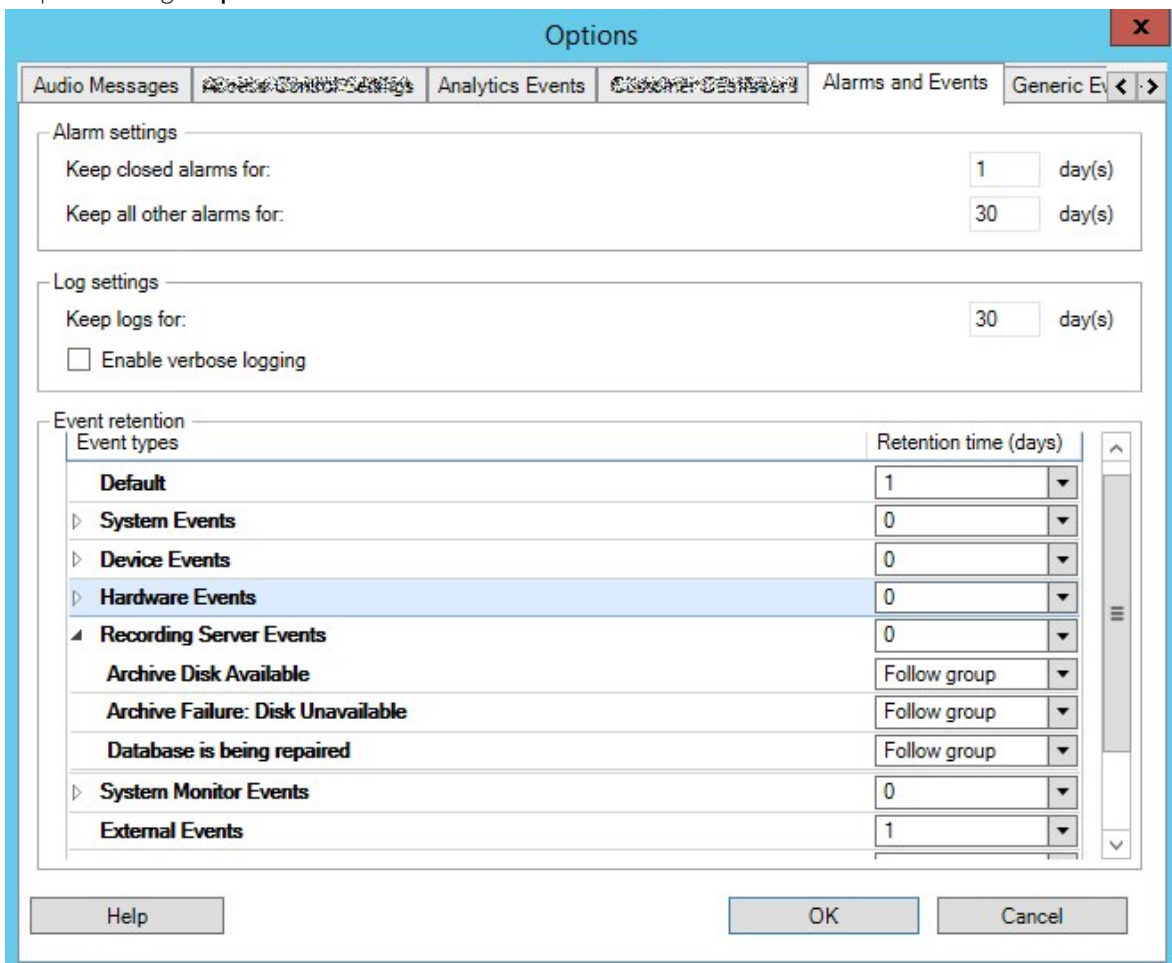
Dès que votre système reçoit les images, elles sont immédiatement horodatées. Les caméras sont des unités distinctes qui peuvent avoir des périphériques de réglage de l'heure distincts. L'heure de la caméra et l'heure de votre système peuvent par conséquent ne pas correspondre exactement. Cela peut parfois prêter à confusion. Si les horodateurs sont pris en charge par vos caméras, Milestone vous recommande de synchroniser automatiquement l'heure de la caméra et du système via un serveur de temps pour une synchronisation cohérente.

Pour de plus amples informations sur la configuration d'un serveur de temps, effectuez des recherches sur le site Web de Microsoft (<https://www.microsoft.com/>) en saisissant les mots-clés « **serveur de temps** », « **service de temps** » ou d'autres termes similaires.

## Taille limite de la base de données

Pour empêcher la base de données SQL (voir SQL Server et bases de données sur la page 24) d'atteindre une taille qui compromet la performance du système, vous pouvez indiquer le nombre de jours pendant lesquels les différents types d'événements et d'alarmes y sont stockés.

1. Ouvrez le menu **Outils**.
2. Cliquez sur l'onglet **Options > Alarmes et événements**.



3. Appliquez les paramètres nécessaires. Pour plus d'informations, voir Onglet Alarmes et événements (Options) sur la page 133.

## IPv6 et IPv4 (explications)

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

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

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

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

### Utilisation du système avec IPv6 (explications)

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

#### Serveurs

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

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

#### Périphériques

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

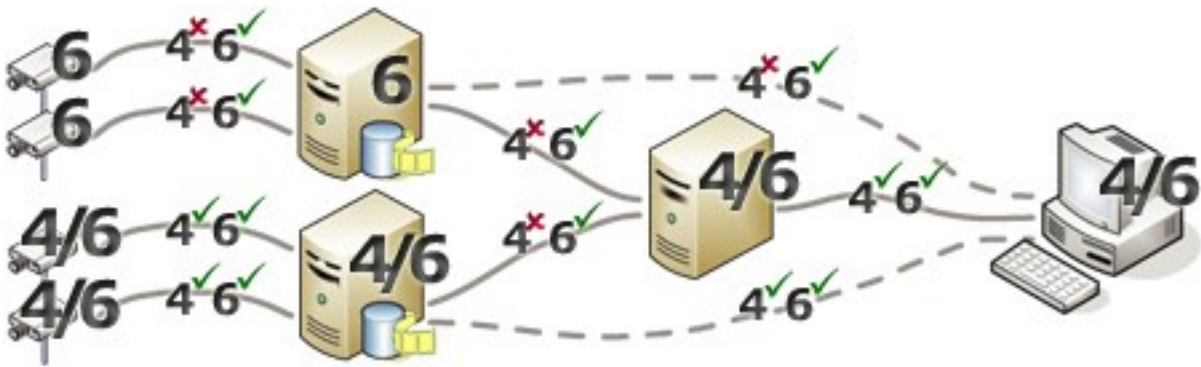
#### Clients

Si votre système utilise IPv6, les utilisateurs doivent se connecter avec le XProtect Smart Client. Le XProtect Smart Client prend en charge IPv6 et IPv4.

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

Cependant, les utilisateurs XProtect Smart Client n'ont pas à être eux-mêmes sur le réseau IPv6, pourvu que votre équipement réseau supporte la communication entre les différentes versions IP, et qu'ils ont installé le protocole IPv6 sur leurs ordinateurs. Voir également l'illustration. Pour installer IPv6 sur un ordinateur client, ouvrez une invite de commande, saisissez **installer ipv6**, et appuyez sur **ENTRÉE**.

#### Illustration en exemple



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

**Aucune compatibilité Matrix Monitor**

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

**Écriture des adresses IPv6 (explications)**

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

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

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

**Exemple :**

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

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

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

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

**Utiliser les adresses IPv6 dans les URL**

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

**Exemple** d'une URL avec une adresse IPv6 :

`http://[2001:0B80:0000:0000:0000:0F80:3FA8:18AB]`, qui peut être évidemment abrégé, par exemple, `http://[2001:B80::F80:3FA8:18AB]`

**Exemple** d'une URL avec une adresse IPv6 et un numéro de port :

*http://[2001:0B80:0000:0000:0F80:3FA8:18AB]:1234*, qui peut être évidemment abrégé, par exemple, *http://[2001:B80::F80:3FA8:18AB]:1234*

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

## Serveurs virtuels

Vous pouvez exécuter tous les composants du système dans des serveurs Windows® virtuels, tels que VMware® et Microsoft® Hyper-V®.

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

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

## Serveurs de gestion multiples (grappes) (explications)

Le serveur de gestion peut être installé sur de multiples serveurs au sein d'une grappe de serveurs. Ceci permet de garantir un temps d'arrêt limité du système. Si un serveur dans une grappe devient indisponible, un autre serveur de cette grappe prend automatiquement le relais du serveur défaillant et continue d'exécuter le serveur de gestion. Le processus automatique de basculement entre les services du serveur de gestion et un autre serveur de la grappe ne demande que 30 secondes.

Il n'est possible d'avoir qu'un seul serveur de gestion actif par configuration de surveillance, mais d'autres serveurs de gestion peuvent être configurés pour prendre le relais en cas de défaillance.





Le nombre de redondances permis est limité à deux pour toute période de six heures. En cas de dépassement de ce seuil, le service de regroupement ne démarre pas automatiquement les services du serveur de gestion. Le nombre de redondances permises peut être modifié pour mieux correspondre à vos besoins.

## Conditions préalables à la mise en grappe

- Deux machines avec Microsoft Windows Server 2012 ou une version plus récente. Assurez-vous que :
  - Tous les serveurs que vous souhaitez ajouter en tant que nœuds de grappe exécutent la même version de Windows Server
  - Tous les serveurs que vous souhaitez ajouter en tant que nœuds de grappe sont regroupés sous le même domaine
  - Vous pouvez vous connecter au compte Windows en tant qu'administrateur local

Pour en savoir plus sur les grappes dans Microsoft Windows Servers, voir Grappes de redondance <https://docs.microsoft.com/en-us/windows-server/failover-clustering/create-failover-cluster>.

- Une installation de Microsoft SQL Server

**Soit** un SQL Server externe et une base de données installée **en dehors** de la grappe du serveur **ou** un service SQL Server **interne** au sein de la grappe du serveur (la création d'un service SQL Server interne nécessite l'utilisation de l'édition de Microsoft® SQL Server® Standard ou de Microsoft® SQL Server® Enterprise, laquelle peut travailler en tant que SQL Server regroupé en grappes).



Selon vos paramètres de mot de passe de configuration système, vous pourriez être invité à saisir le mot de passe de configuration système actuel lorsque vous connectez le serveur de gestion à la base de données. Voir Mot de passe de configuration système (explications) sur la page 491.

## Protection des bases de données d'enregistrement contre la corruption

Les bases de données des caméras peuvent devenir corrompues. Plusieurs options de réparation des bases de données existent pour résoudre un tel problème. Mais Milestone vous recommande de prendre des mesures pour vous assurer que les bases de données de votre caméra ne deviennent pas corrompues.

### Panne de disque dur : protégez vos lecteurs

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

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

## Windows Task Manager : attention à la fermeture des processus

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

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

## Coupures de courant : utilisation d'un onduleur

La raison la plus courante de corruption des bases de données est l'arrêt brutal du serveur d'enregistrement, sans sauvegarde des fichiers et sans fermeture correcte du système d'exploitation. Ceci peut arriver en raison de pannes d'alimentation, dues à un débranchement accidentel du câble d'alimentation du serveur ou autre.

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

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

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

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

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

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

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

## Configuration système minimum

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/>).

## Avant de commencer l'installation

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

## Préparation de vos serveurs et du réseau

### Systeme d'exploitation

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

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

### Microsoft® .NET Framework

Vérifiez que Microsoft .NET Framework 4.7 ou ultérieur est installé sur tous les serveurs.

### Réseau

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

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

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

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

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

## Préparer Active Directory

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

Pour une gestion plus facile des utilisateurs et des groupes, Milestone recommande d'avoir Microsoft Active Directory® d'installé et de configuré avant d'installer votre système XProtect. Si vous ajoutez le serveur de gestion à Active Directory après l'installation de votre système, vous devrez réinstaller le serveur de gestion et remplacer des utilisateurs par de nouveaux utilisateurs Windows définis dans Active Directory.

Les utilisateurs basiques ne sont pas pris en charge dans les systèmes Milestone Federated Architecture, donc si vous pensez utiliser Milestone Federated Architecture, vous devez ajouter les utilisateurs en tant qu'utilisateurs de Windows via le service Active Directory. Si vous n'installez pas Active Directory, suivez les étapes Installation pour les groupes de travail sur la page 104 lors de l'installation.

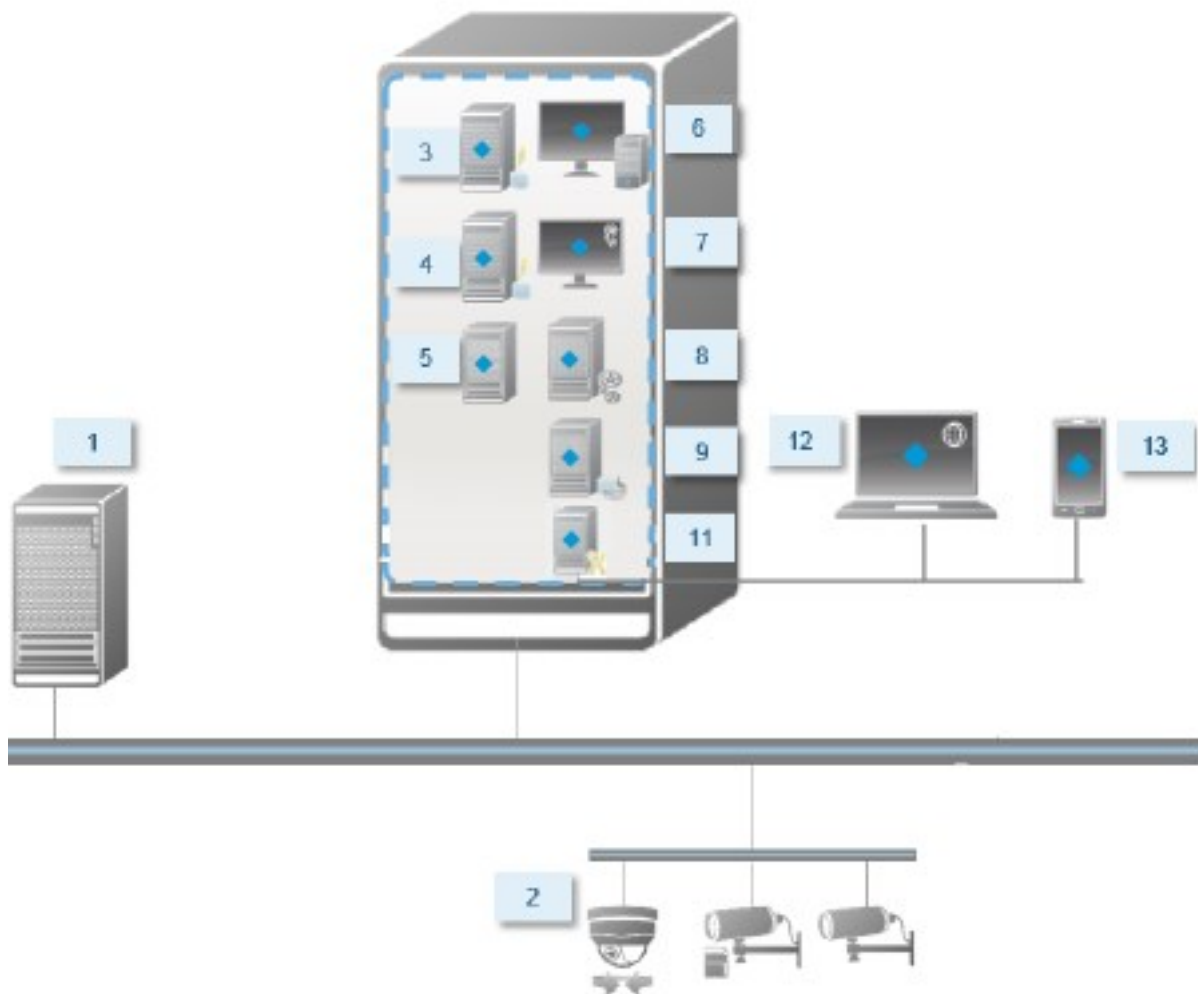
## Méthode d'installation

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

Options	Description
<b>Ordinateur</b>	Installe l'ensemble des composants liés au serveur et au client, ainsi que le SQL Server sur

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

## Installation sur un seul ordinateur

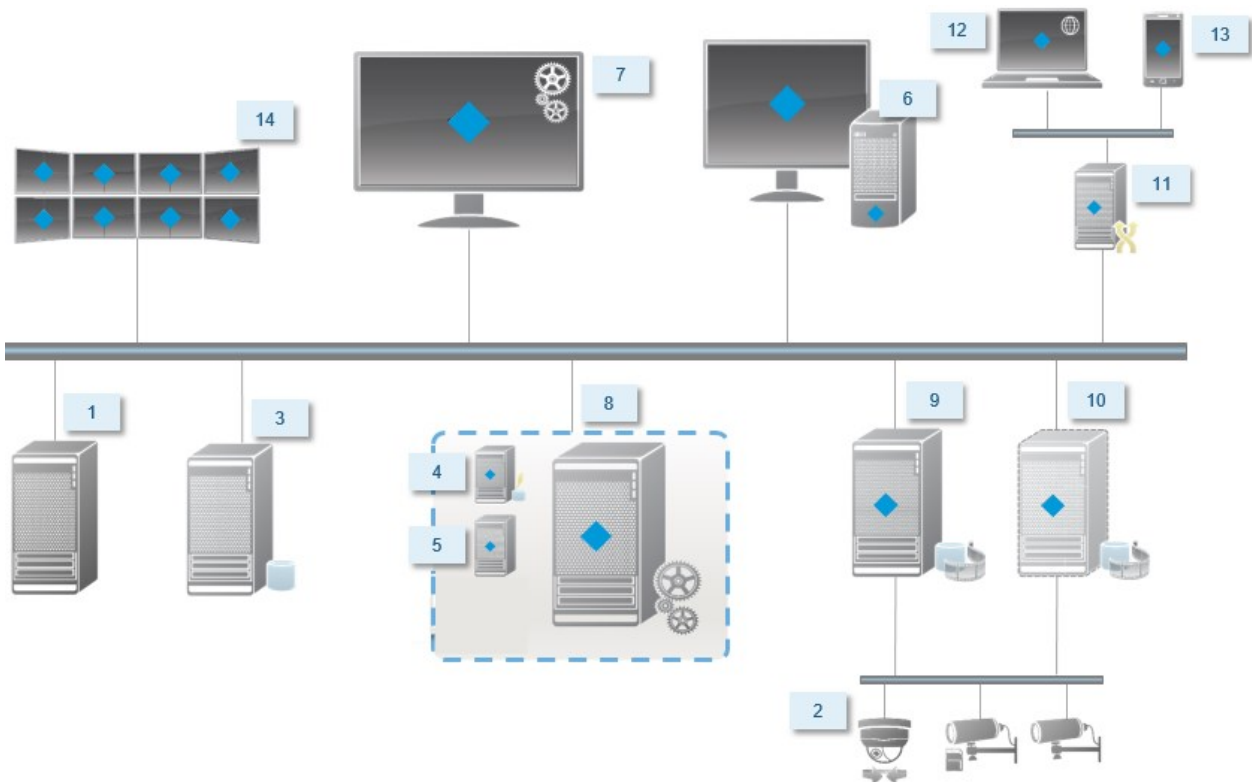


Composants typiques d'un système :

1. **Active Directory**
2. **Périphériques**
3. **Serveur avec SQL Server**
4. **Serveur d'événements**
5. **Serveur de journaux**
6. **XProtect Smart Client**
7. **Management Client**
8. **Serveur de gestion**

9. **Serveur d'enregistrement**
10. **Serveur d'enregistrement de redondance**
11. **Serveur XProtect Mobile**
12. **XProtect Web Client**
13. **Client XProtect Mobile**
14. **XProtect Smart Client avec XProtect Smart Wall**

### Installation personnalisée - exemple des composants du système distribués



### Décider d'une édition de SQL Server

Microsoft® SQL Server® Express est une édition gratuite de SQL Server et est facile à installer et prête à l'utilisation en comparaison des autres éditions de SQL Server. Lors de l'installation d'un **Ordinateur unique**, Microsoft SQL Server Express est installé à moins que SQL Server ne soit déjà installé sur l'ordinateur.

L'installation de VMS XProtect inclut la version 2019 de Microsoft SQL Server Express. Certains systèmes d'exploitation de Windows ne sont pas compatibles avec cette édition de SQL Server. Avant d'installer VMS XProtect, assurez-vous que votre système d'exploitation prend en charge SQL Server 2019. Si ce n'est pas le cas,

installez une édition compatible de SQL Server avant de commencer l'installation de VMS XProtect. Pour plus d'informations sur les éditions de SQL Server prises en charge, voir <https://www.milestonesys.com/systemrequirements/>.

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

## Sélectionner un compte de service

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

Vous pouvez sélectionner un compte prédéfini ou un compte utilisateur. Basez votre décision sur l'environnement sur lequel vous souhaitez installer votre système :

### Environnement de domaine

Dans un domaine de domaine :

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

### Environnement de groupe de travail

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



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

## Authentification Kerberos (explications)

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



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

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

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

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

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



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

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

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

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

```
VideoOS/[Nom d'hôte DNS]:[Port]  
VideoOS/[Nom de domaine entièrement qualifié]:[Port]
```

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

```
Nom d'hôte : Record-Server1  
Domaine : Surveillance.com
```

SPN à enregistrer :

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

## Exclusions scan antivirus (explications)

Comme avec tout autre logiciel de base de données, si un programme antivirus est installé sur un ordinateur exécutant le logiciel XProtect, il est important d'exclure certains types de fichiers et emplacements, ainsi que trafic du réseau. Sans appliquer ces exceptions, la détection de virus utilise une quantité considérable de ressources système. De plus, le processus de numérisation peut verrouiller temporairement des fichiers, ce qui peut engendrer une interruption du processus d'enregistrement et même la corruption des bases de données.

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

Créer les exclusions supplémentaires suivantes :

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

Produit	Ports TCP
<b>VMS XProtect</b>	80, 8080, 7563, 25, 21, 9000
<b>XProtect Mobile</b>	8081

ou

- Exclure l'analyse en réseau des processus suivants :

Produit	Processus
<b>VMS XProtect</b>	VideoOS.Recorder.Service.exe, VideoOS.Server.Service.exe, VideoOS.Administration.exe
<b>XProtect Mobile</b>	VideoOS.MobileServer.Service.exe

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

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

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

- Exécuter le système d'exploitation de Windows en mode FIPS 140-2. Voir le [site](#) de Microsoft pour plus d'informations sur l'activation du mode FIPS.
- Vous assurer que les intégrations autonomes tierces peuvent s'exécuter dans un système d'exploitation Windows où est activé le mode FIPS.
- Vous connecter aux périphériques tout en garantissant que leur exécution est conforme aux normes FIPS 140-2
- Vous assurer que les données des bases de données multimédia sont cryptées avec un cryptage conforme aux normes FIPS 140-2

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

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

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

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

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

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

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

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

## Enregistrer le code de licence du logiciel

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

Vous pouvez installer une version gratuite de XProtect Essential+. Cette version vous offre des possibilités limitées de VMS XProtect pour un nombre limité de caméras. Vous devez disposer d'une connexion Internet pour installer XProtect Essential+.

Le code de licence du logiciel (SLC) est imprimé sur la confirmation de commande et le nom du fichier de licence logicielle est lié à votre SLC.

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

## Pilotes de périphériques (explications)

Votre système utilise les pilotes de périphériques vidéo pour contrôler et communiquer avec les périphériques de type caméra connectés à un serveur d'enregistrement. Vous devez installer les pilotes de périphériques sur chaque serveur d'enregistrement de votre système.

À partir de la version 2018 R1, les pilotes de périphériques sont répartis en deux device packs : le device pack classique équipé des pilotes plus récents et un périphérique d'ancienne génération doté de pilotes plus anciens.

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

L'ancien Device Pack ne peut être installé que si un device pack classique est installé dans le système. Les pilotes relevant de l'ancien Device Pack sont installés automatiquement si une version précédente est déjà installée sur votre système. Il peut être téléchargé et installé manuellement sur la page de téléchargement du logiciel (<https://www.milestonesys.com/downloads/>).

Arrêtez le service Recording Server avant de procéder à l'installation, sinon vous devrez redémarrer l'ordinateur.

Nous vous recommandons de toujours utiliser la dernière version des pilotes de périphériques pour garantir des performances optimales.

## Conditions préalables de l'installation hors ligne

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

- Le fichier `Milestone XProtect Produits VMS 2020 R3 Système Installer.exe`
- Le fichier de licence logicielle (SLC) de votre système XProtect
- Média d'installation du système d'exploitation incluant la version .NET requise (<https://www.milestonesys.com/systemrequirements/>)

## Communication sécurisée (explications)

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

Dans 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](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 ledits 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.

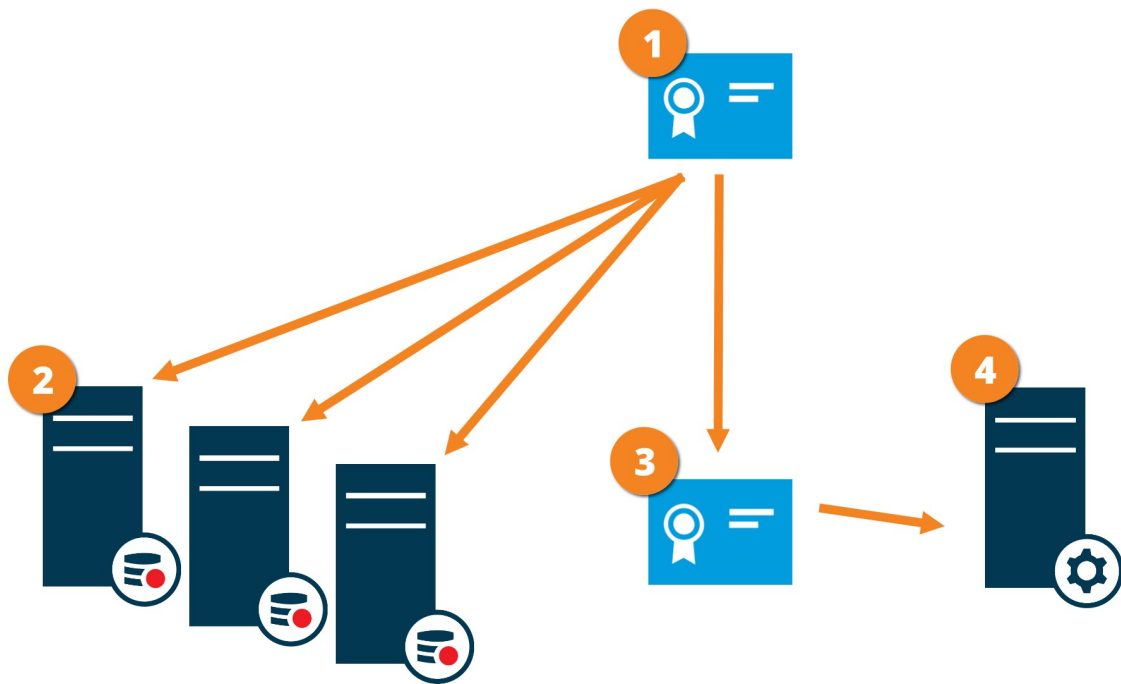
## Cryptage du serveur de gestion (explications)

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.



- 1 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)
- 2 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
- 3 Le certificat de l'AC est utilisé pour établir une connexion sécurisée entre le serveur de gestion et les services d'enregistrement
- 4 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

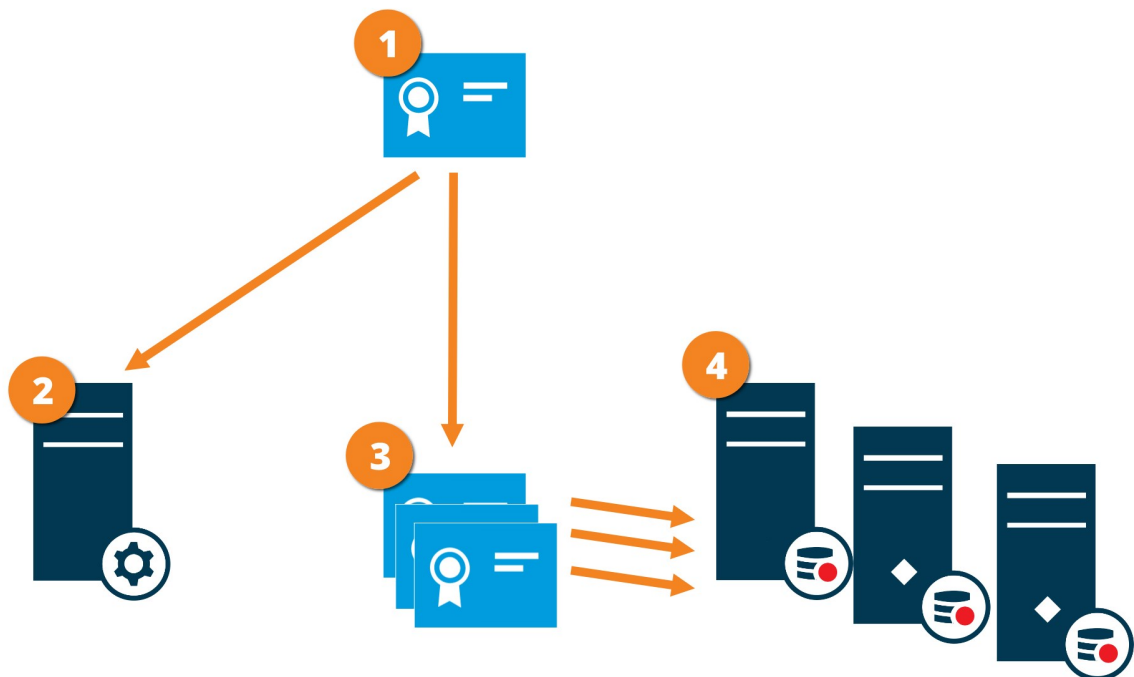
- Fiable sur tous les serveurs d'enregistrement connectés au serveur de gestion de préférence en utilisant un certificat de l'AC qui a été utilisé pour émettre le certificat du serveur de gestion

## 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.



- 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 (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 d'enregistrement et le serveur de gestion

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 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)

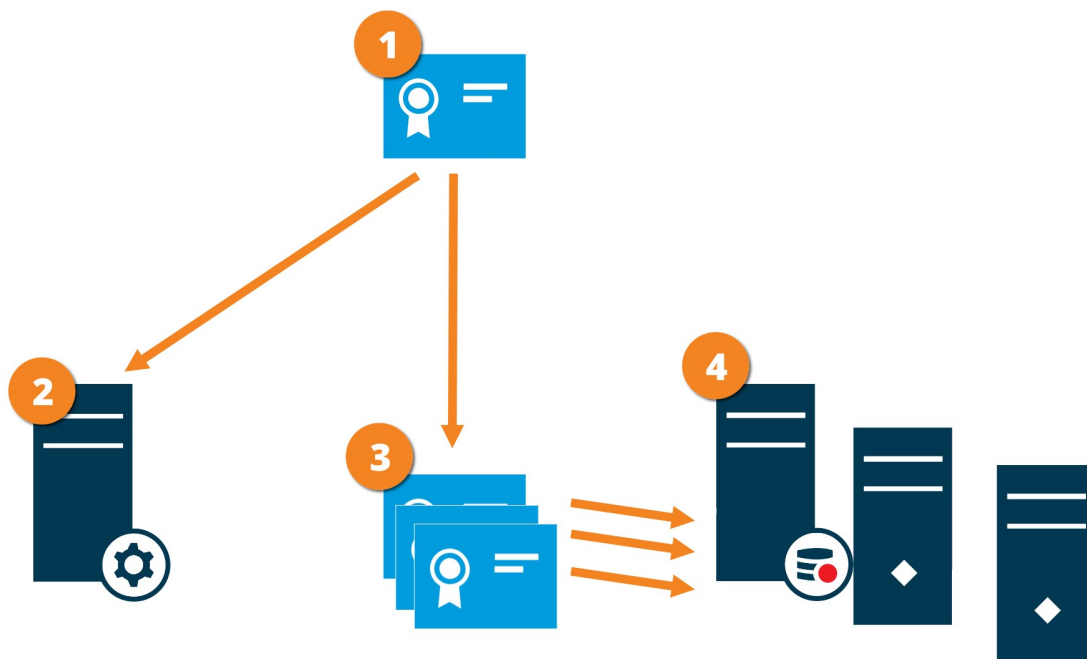
Vous pouvez crypter une connexion bidirectionnelle entre le serveur de gestion et le Data Collector affilié lorsque vous disposez d'un type de serveur distant suivant :

- 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.



- ❶ 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)
- 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 de collection de données et le serveur d'enregistrement
- ❹ 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 » :

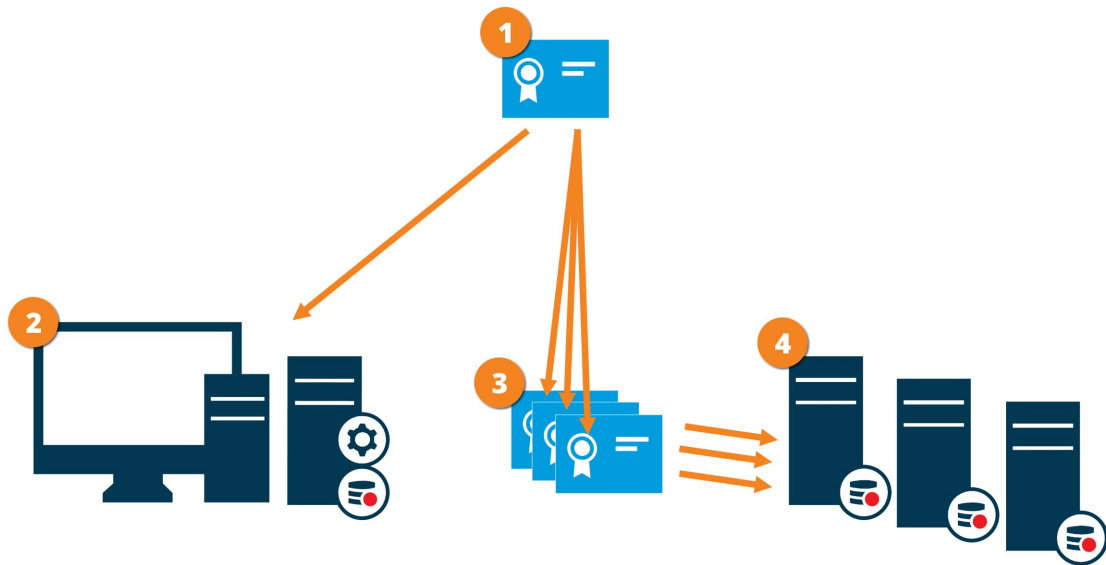
- XProtect Smart Client
- Management Client
- Management Server (pour le Système de surveillance et les images ainsi que les vidéos AVI dans les notifications par email)
- Serveur XProtect Mobile
- XProtect Event Server
- XProtect LPR
- Milestone Open Network Bridge
- XProtect DLNA Server
- Les sites 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.



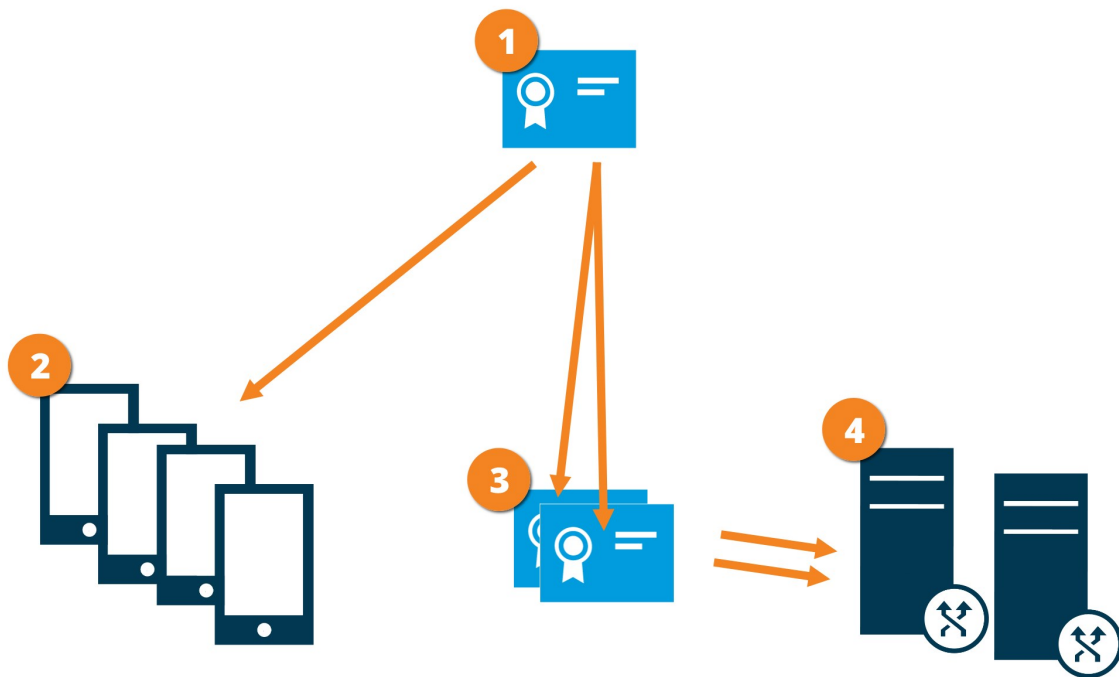
Si vous activez le cryptage sur les serveurs d'enregistrement et que votre système applique des serveurs d'enregistrement de basculement, Milestone vous recommande de préparer également le serveur d'enregistrement de redondance pour le cryptage.

## 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.



- 1 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)
- 2 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
- 3 Le certificat de l'AC est utilisé pour établir une connexion sécurisée entre le serveur mobile et les clients et services
- 4 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.

# Installation

## Installer un nouveau système XProtect

### Installer le XProtect Essential+

Vous pouvez installer une version gratuite de XProtect Essential+. Cette version vous offre des possibilités limitées de VMS XProtect pour un nombre limité de caméras. Vous devez disposer d'une connexion Internet pour installer XProtect Essential+.

Cette version est installée sur un ordinateur unique à l'aide de l'option d'installation sur un **ordinateur unique**. L'option **Ordinateur unique** installe l'ensemble des composants liés au serveur et au client sur l'ordinateur actuel.



Milestone vous recommande de lire avec attention la section suivante avant de procéder à l'installation : Avant de commencer l'installation sur la page 59.



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

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

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



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

1. Télécharger le programme depuis Internet (<https://www.milestonesys.com/downloads/>) et exécuter le fichier `Milestone XProtect Produits VMS 2020 R3 Système Installer.exe`.
2. La décompression des fichiers d'installation débute. Un ou plusieurs messages d'avertissement Windows® s'afficheront en fonction des paramètres de sécurités. Acceptez-les afin de poursuivre la décompression.
3. Lorsque vous avez terminé, l'assistant d'installation **VMS Milestone XProtect** s'affiche.
  1. Sélectionnez la **Langue** à utiliser au cours de l'installation (il ne s'agit pas de la langue que votre système utilise une fois qu'il est installé, celle-ci est sélectionnée par la suite). Cliquez sur **Continuer**.
  2. Lisez le *Contrat de licence utilisateur final Milestone*. Cochez la case **J'accepte les termes du contrat de licence**, puis cliquez sur **Continuer**.
  3. Cliquez sur le lien **XProtect Essential+** pour télécharger un fichier de licence gratuit.

La licence gratuite est téléchargée et s'affiche dans le champ **Saisir ou rechercher l'emplacement du fichier de licence**. Cliquez sur **Continuer**.
4. Sélectionnez **Ordinateur unique**.

Une liste de composants à installer apparaît (vous ne pouvez pas modifier cette liste). Cliquez sur **Continuer**.
5. Sur la page **Assigner un mot de passe de configuration système**, saisissez un mot de passe qui protégera votre configuration système. Vous en aurez besoin lorsque vous souhaitez restaurer votre système ou bien l'étendre, par exemple, avec l'ajout de grappes.



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

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

Cliquez sur **Continuer**.



6. Sur la page **Spécifier les paramètres du serveur d'enregistrement**, spécifiez les paramètres du serveur d'enregistrement :
  1. Dans le champ **Nom du serveur d'enregistrement**, saisissez le nom du serveur d'enregistrement. Le nom par défaut est celui de l'ordinateur.
  2. Le champ **Adresse du serveur de gestion** indique l'adresse et le numéro du port du serveur de gestion : localhost:80.
  3. Dans le champ **Sélectionner l'emplacement de votre base de données médias**, sélectionnez l'emplacement où vous voulez sauvegarder votre enregistrement vidéo. Milestone vous recommande de sauvegarder vos enregistrements vidéo dans un emplacement différent de celui où vous avez installé le logiciel, et non sur le lecteur système. L'emplacement par défaut est le lecteur qui dispose du plus grand espace disponible.
  4. Dans le champ **Durée de rétention des enregistrements vidéo**, définissez la durée pendant laquelle vous voulez conserver les enregistrements vidéo. Vous pouvez saisir entre 1 et 999 jours dans lesquels 7 jours correspondent à la durée de rétention par défaut.
  5. Cliquez sur **Continuer**.

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

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

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



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

- Entre les serveurs d'enregistrement et les clients

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

- Entre le serveur mobile et les clients

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

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

Pour plus d'informations sur la préparation de votre système pour une communication sécurisée, voir Communication sécurisée (explications) sur la page 70 et le [Milestone guide sur les certificats](#).

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

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

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



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

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

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

9. Vous serez invité à redémarrer votre ordinateur. Après avoir redémarré votre ordinateur, un ou plusieurs messages d'avertissement Windows s'afficheront en fonction des paramètres de sécurité. Acceptez-les afin de terminer l'installation.
10. Une fois l'installation terminée, une liste s'affiche pour indiquer les composants installés sur l'ordinateur. Cliquez sur **Continuer** pour ajouter un matériel et des utilisateurs au système.



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

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

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

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

12. Sur la page **Sélectionner le matériel à ajouter au système**, sélectionnez le matériel que vous souhaitez ajouter au système. Cliquez sur **Continuer** et patientez pendant que le système ajoute le matériel.
13. Sur la page **Configurer les périphériques**, vous pouvez attribuer des noms descriptifs au matériel en cliquant sur l'icône Modifier située en regard du nom du matériel. Ce nom est ensuite préfixé aux périphériques.

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



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

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

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

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

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

15. Lorsque l'installation et la configuration initiale sont terminées, la page **La configuration est terminée** s'ouvre et affiche :
  - Une liste de périphériques qui sont ajoutés au système
  - Une liste d'utilisateurs qui sont ajoutés au système
  - Les adresses vers le XProtect Web Client et le client XProtect Mobile que vous pouvez partager avec vos utilisateurs

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

## Installer votre système - option sur ordinateur unique

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



Milestone vous recommande de lire avec attention la section suivante avant de procéder à l'installation : Avant de commencer l'installation sur la page 59.



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

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

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



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

1. Télécharger le programme depuis Internet (<https://www.milestonesys.com/downloads/>) et exécuter le fichier `Milestone XProtect Produits VMS 2020 R3 Système Installer.exe`.
2. La décompression des fichiers d'installation débute. Un ou plusieurs messages d'avertissement Windows® s'afficheront en fonction des paramètres de sécurités. Acceptez-les afin de poursuivre la décompression.
3. Lorsque vous avez terminé, l'assistant d'installation **VMS Milestone XProtect** s'affiche.
  1. Sélectionnez la **Langue** à utiliser au cours de l'installation (il ne s'agit pas de la langue que votre système utilise une fois qu'il est installé, celle-ci est sélectionnée par la suite). Cliquez sur **Continuer**.
  2. Lisez le *Contrat de licence utilisateur final Milestone*. Cochez la case **J'accepte les termes du contrat de licence**, puis cliquez sur **Continuer**.
  3. Dans **Saisir ou rechercher l'emplacement du fichier de licence**, saisissez le fichier de licence envoyé par votre prestataire XProtect. Alternativement, naviguez jusqu'à l'emplacement du fichier ou cliquez sur le lien **XProtect Essential+** pour télécharger un fichier de licence gratuit. Pour consulter les limitations du produit gratuit XProtect Essential+, voir le Graphique de comparaison des produits sur la page 46. Le système vérifie votre fichier de licence avant que vous puissiez poursuivre. Cliquez sur **Continuer**.
4. Sélectionnez **Ordinateur unique**.

Une liste de composants à installer apparaît (vous ne pouvez pas modifier cette liste). Cliquez sur **Continuer**.
5. Sur la page **Assigner un mot de passe de configuration système**, saisissez un mot de passe qui protégera votre configuration système. Vous en aurez besoin lorsque vous souhaitez restaurer votre système ou bien l'étendre, par exemple, avec l'ajout de grappes.



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

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

Cliquez sur **Continuer**.

6. Sur la page **Spécifier les paramètres du serveur d'enregistrement**, spécifiez les paramètres du serveur d'enregistrement :
  1. Dans le champ **Nom du serveur d'enregistrement**, saisissez le nom du serveur d'enregistrement. Le nom par défaut est celui de l'ordinateur.
  2. Le champ **Adresse du serveur de gestion** indique l'adresse et le numéro du port du serveur de gestion : localhost:80.
  3. Dans le champ **Sélectionner l'emplacement de votre base de données médias**, sélectionnez l'emplacement où vous voulez sauvegarder votre enregistrement vidéo. Milestone vous recommande de sauvegarder vos enregistrements vidéo dans un emplacement différent de celui où vous avez installé le logiciel, et non sur le lecteur système. L'emplacement par défaut est le lecteur qui dispose du plus grand espace disponible.
  4. Dans le champ **Durée de rétention des enregistrements vidéo**, définissez la durée pendant laquelle vous voulez conserver les enregistrements vidéo. Vous pouvez saisir entre 1 et 999 jours dans lesquels 7 jours correspondent à la durée de rétention par défaut.
  5. Cliquez sur **Continuer**.

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

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

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



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

- Entre les serveurs d'enregistrement et les clients

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

- Entre le serveur mobile et les clients

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

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

Pour plus d'informations sur la préparation de votre système pour une communication sécurisée, voir Communication sécurisée (explications) sur la page 70 et le [Milestone guide sur les certificats](#).

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

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

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



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

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

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

9. Vous serez invité à redémarrer votre ordinateur. Après avoir redémarré votre ordinateur, un ou plusieurs messages d'avertissement Windows s'afficheront en fonction des paramètres de sécurité. Acceptez-les afin de terminer l'installation.
10. Une fois l'installation terminée, une liste s'affiche pour indiquer les composants installés sur l'ordinateur. Cliquez sur **Continuer** pour ajouter un matériel et des utilisateurs au système.



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

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

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

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

12. Sur la page **Sélectionner le matériel à ajouter au système**, sélectionnez le matériel que vous souhaitez ajouter au système. Cliquez sur **Continuer** et patientez pendant que le système ajoute le matériel.
13. Sur la page **Configurer les périphériques**, vous pouvez attribuer des noms descriptifs au matériel en cliquant sur l'icône Modifier située en regard du nom du matériel. Ce nom est ensuite préfixé aux périphériques.

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



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

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

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

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

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



15. Lorsque l'installation et la configuration initiale sont terminées, la page **La configuration est terminée** s'ouvre et affiche :
  - Une liste de périphériques qui sont ajoutés au système
  - Une liste d'utilisateurs qui sont ajoutés au système
  - Les adresses vers le XProtect Web Client et le client XProtect Mobile que vous pouvez partager avec vos utilisateurs

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

## Installer votre système - option personnalisée

L'option **Personnalisée** installe le serveur de gestion, mais vous pouvez sélectionner quels autres composants du client et du serveur vous souhaitez installer sur l'ordinateur actuel. Par défaut, la case du serveur d'enregistrement est décochée dans la liste de composants. En fonction de vos choix, vous pouvez installer les composants du système non sélectionnés sur d'autres ordinateurs par la suite. Pour plus d'informations concernant chaque composant du système et leur rôle, voir Composants principaux du système sur la page 22. L'installation sur d'autres ordinateurs se fait par le biais de la page Web de téléchargement du serveur de gestion intitulée Download Manager. Pour plus d'informations concernant l'installation via le Download Manager, voir XProtect Installer les nouveaux composants sur la page 94.



Milestone vous recommande de lire avec attention la section suivante avant de procéder à l'installation : Avant de commencer l'installation sur la page 59.



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

1. Télécharger le programme depuis Internet (<https://www.milestone.com/downloads/>) et exécuter le fichier `Milestone XProtect Produits VMS 2020 R3 Système Installer.exe`.
2. La décompression des fichiers d'installation débute. Un ou plusieurs messages d'avertissement Windows® s'afficheront en fonction des paramètres de sécurité. Acceptez-les afin de poursuivre la décompression.
3. Lorsque vous avez terminé, l'assistant d'installation **VMS Milestone XProtect** s'affiche.

1. Sélectionnez la **Langue** à utiliser au cours de l'installation (il ne s'agit pas de la langue que votre système utilise une fois qu'il est installé, celle-ci est sélectionnée par la suite). Cliquez sur **Continuer**.
2. Lisez le *Contrat de licence utilisateur final Milestone*. Cochez la case **J'accepte les termes du contrat de licence**, puis cliquez sur **Continuer**.
3. Dans **Saisir ou rechercher l'emplacement du fichier de licence**, saisissez le fichier de licence envoyé par votre prestataire XProtect. Alternativement, naviguez jusqu'à l'emplacement du fichier ou cliquez sur le lien **XProtect Essential+** pour télécharger un fichier de licence gratuit. Pour consulter les limitations du produit gratuit XProtect Essential+, voir le Graphique de comparaison des produits sur la page 46. Le système vérifie votre fichier de licence avant que vous puissiez poursuivre. Cliquez sur **Continuer**.
4. Sélectionnez **Personnaliser**. Une liste de composants à installer apparaît. Hormis le serveur de gestion, tous les composants de la liste sont facultatifs. Par défaut, la case du serveur d'enregistrement est décochée. Cliquez sur **Continuer**.



Dans les étapes ci-dessous, tous les composants du système sont installés. Pour un système encore plus distribué, n'installez que quelques composants du système sur cet ordinateur et les composants restants sur les autres ordinateurs. Si vous ne reconnaissez pas une étape de l'installation, c'est sûrement dû au fait que vous n'avez pas choisi d'installer le composant du système auquel appartient cette page. Dans ce cas, passez à l'étape suivante. Voir également XProtect Installer les nouveaux composants sur la page 94, XProtect Installer les nouveaux composants sur la page 94 et XProtect Installer les nouveaux composants sur la page 94.

5. La page **Sélectionnez un site Web IIS à utiliser avec le système XProtect** ne s'affiche que si vous avez plus d'un site Web IIS disponibles sur cet ordinateur. Vous devez sélectionner le site Web à utiliser avec votre système XProtect. Si possible, sélectionnez un site Web doté d'une liaison HTTPS, car ce protocole est une version plus avancée et sécurisée de HTTP. Cliquez sur **Continuer**.

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

6. Sur la page **Sélectionner Microsoft SQL Server**, sélectionnez le SQL Server que vous souhaitez utiliser. Voir également SQL Server options lors de l'installation personnalisée sur la page 94. Cliquez sur **Continuer**.



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

7. Sur la page **Sélectionner une base de données** (ne s'affiche que si vous avez sélectionné un SQL Server existant), sélectionnez ou créez une base de données SQL pour y stocker votre configuration système. Si vous choisissez une base de données SQL existante, choisissez **Conserver** ou **Remplacer** les données existantes. Si vous procédez à une mise à niveau, choisissez de conserver les données existantes afin de ne pas perdre votre configuration système. Voir également SQL Server options lors de l'installation personnalisée sur la page 94. Cliquez sur **Continuer**.
8. Sur la page **Assigner un mot de passe de configuration système**, saisissez un mot de passe qui protégera votre configuration système. Vous en aurez besoin lorsque vous souhaitez restaurer votre système ou bien l'étendre, par exemple, avec l'ajout de grappes.



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

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

Cliquez sur **Continuer**.

9. Sur la page **Sélectionner le compte de service**, sélectionnez soit **Ce compte prédéfini**, soit **Ce compte** pour sélectionner le compte de service pour tous les composants du système à l'exception du serveur d'enregistrement. Si nécessaire, saisissez un mot de passe. Cliquez sur **Continuer**.
10. Dans la fenêtre **Sélectionner le compte de service pour le serveur d'enregistrement**, sélectionnez soit **Ce compte prédéfini**, soit **Ce compte** pour sélectionner le compte de service pour le serveur d'enregistrement.

Si nécessaire, saisissez un mot de passe.



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

Cliquez sur **Continuer**.

11. Sur la page **Spécifier les paramètres du serveur d'enregistrement**, spécifiez les paramètres du serveur d'enregistrement :
  1. Dans le champ **Nom du serveur d'enregistrement**, saisissez le nom du serveur d'enregistrement. Le nom par défaut est celui de l'ordinateur.
  2. Le champ **Adresse du serveur de gestion** indique l'adresse et le numéro du port du serveur de gestion : localhost:80.
  3. Dans le champ **Sélectionner l'emplacement de votre base de données médias**, sélectionnez l'emplacement où vous voulez sauvegarder votre enregistrement vidéo. Milestone vous recommande de sauvegarder vos enregistrements vidéo dans un emplacement différent de celui où vous avez installé le logiciel, et non sur le lecteur système. L'emplacement par défaut est le lecteur qui dispose du plus grand espace disponible.
  4. Dans le champ **Durée de rétention des enregistrements vidéo**, définissez la durée pendant laquelle vous voulez conserver les enregistrements vidéo. Vous pouvez saisir entre 1 et 999 jours dans lesquels 7 jours correspondent à la durée de rétention par défaut.
  5. Cliquez sur **Continuer**.

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

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

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



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

- Entre les serveurs d'enregistrement et les clients

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

- Entre le serveur mobile et les clients

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

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

Pour plus d'informations sur la préparation de votre système pour une communication sécurisée, voir Communication sécurisée (explications) sur la page 70 et le [Milestone guide sur les certificats](#).

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

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



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

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

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

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

16. Configuration de votre système dans Management Client. Voir Liste des tâches initiales de configuration sur la page 137.
17. En fonction de vos choix, installez les composants du système restants sur les autres ordinateurs par le biais du Download Manager. Voir XProtect Installer les nouveaux composants sur la page 94.

### SQL Server options lors de l'installation personnalisée

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

SQL Server options :

- **Installer Microsoft® SQL Server® Express sur cet ordinateur** : Cette option ne s'affiche que si vous n'avez pas un SQL Server installé sur l'ordinateur
- **Utiliser le SQL Server sur cet ordinateur** : Cette option ne s'affiche que si un SQL Server est déjà installé sur l'ordinateur
- **Sélectionner un SQL Server sur votre réseau par le biais de la recherche** : Vous permet de chercher tous les SQL Server découverts sur le sous-réseau de votre réseau
- **Sélectionner un SQL Server sur votre réseau** : Vous permet de saisir l'adresse (nom d'hôte ou adresse IP) d'un SQL Server que la recherche ne trouve pas

Options de la base de données SQL :

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

## XProtect Installer les nouveaux composants

### Installation via Download Manager (explications)

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

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

- Recording Server (voir également Installer le serveur d'enregistrement via Download Manager sur la page 95 ou Installation silencieuse d'un serveur d'enregistrement sur la page 101)
- Management Client
- Smart Client
- Event Server



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

- Log Server
  - Mobile Server
3. Ouvrez un navigateur Internet, saisissez l'adresse de la page Web de téléchargement du Management Server dans le champ d'adresse et téléchargez l'assistant d'installation en question.
  4. Exécutez l'installateur.

Voir Installer votre système - option personnalisée sur la page 89 en cas de doute concernant les sélections à faire et les paramètres dans les différentes étapes d'installation.

## Installer le serveur d'enregistrement via Download Manager

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



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



Voir XProtect Installer les nouveaux composants sur la page 94, si vous souhaitez installer un serveur d'enregistrement de redondance.

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

3. Ouvrez un navigateur Internet, saisissez l'adresse de la page web de téléchargement du Management Server dans le champ d'adresse et appuyez sur Entrée.
4. Télécharger l'assistant d'installation du serveur d'enregistrement en sélectionnant **Toutes les langues** sous **L'Assistant d'installation du serveur d'enregistrement**. Sauvegardez l'installateur ou exécutez-le directement à partir de la page web.
5. Sélectionnez la **Langue** que vous souhaitez utiliser pendant l'installation. Cliquez sur **Continuer**.
6. Sur la page **Sélectionner un type d'installation**, sélectionnez :
  - Typique** : pour installer un serveur d'enregistrement avec des valeurs par défaut, ou
  - Personnalisé** : pour installer un serveur d'enregistrement avec des valeurs personnalisées.
7. Sur la page **Spécifier les paramètres du serveur d'enregistrement**, spécifiez les paramètres du serveur d'enregistrement :
  1. Dans le champ **Nom du serveur d'enregistrement**, saisissez le nom du serveur d'enregistrement. Le nom par défaut est celui de l'ordinateur.
  2. Le champ **Adresse du serveur de gestion** indique l'adresse et le numéro du port du serveur de gestion : localhost:80.
  3. Dans le champ **Sélectionner l'emplacement de votre base de données médias**, sélectionnez l'emplacement où vous voulez sauvegarder votre enregistrement vidéo. Milestone vous recommande de sauvegarder vos enregistrements vidéo dans un emplacement différent de celui où vous avez installé le logiciel, et non sur le lecteur système. L'emplacement par défaut est le lecteur qui dispose du plus grand espace disponible.
  4. Dans le champ **Durée de rétention des enregistrements vidéo**, définissez la durée pendant laquelle vous voulez conserver les enregistrements vidéo. Vous pouvez saisir entre 1 et 999 jours dans lesquels 7 jours correspondent à la durée de rétention par défaut.
  5. Cliquez sur **Continuer**.
8. La page **Adresse IP des serveurs d'enregistrement** ne s'affiche que si vous choisissez **Personnalisée**. Précisez le nombre de serveurs d'enregistrement que vous souhaitez installer sur cet ordinateur. Cliquez sur **Continuer**.



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

Si nécessaire, saisissez un mot de passe.



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

Cliquez sur **Continuer**.

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

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

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



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

- Entre les serveurs d'enregistrement et les clients

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

- Entre le serveur mobile et les clients

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

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

Pour plus d'informations sur la préparation de votre système pour une communication sécurisée, voir Communication sécurisée (explications) sur la page 70 et le [Milestone guide sur les certificats](#).

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

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



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

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

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

13. Une fois que vous avez installé le serveur d'enregistrement, vous pouvez vérifier son état à partir de l'icône de Recording Server Manager et le configurer dans Management Client. Pour plus d'informations, voir Liste des tâches initiales de configuration sur la page 137.

## Installer un serveur d'enregistrement de redondance via Download Manager



Si vous gérez des groupes de travail, vous devrez utiliser la méthode alternative d'installation pour les serveurs d'enregistrement de redondance (voir Installation pour les groupes de travail sur la page 104).

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

7. Sur la page **Spécifier les paramètres du serveur d'enregistrement**, spécifiez les paramètres du serveur d'enregistrement. Le nom du serveur d'enregistrement de redondance, l'adresse du serveur de gestion et le chemin vers la base de données multimédia. Cliquez sur **Continuer**.
8. Sur la page **Sélectionner un compte de service pour le serveur d'enregistrement** et lors de l'installation d'un serveur d'enregistrement de redondance, vous devez utiliser le compte d'utilisateur particulier appelé **Ce compte**. Cela crée le compte d'utilisateur de redondance. Si nécessaire, saisissez un mot de passe et confirmez-le. Cliquez sur **Continuer**.
9. Vous pouvez sécuriser les flux de communication sur la page **Choisir le cryptage** :

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

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



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

- Entre les serveurs d'enregistrement et les clients

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

- Entre le serveur mobile et les clients

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

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

Pour plus d'informations sur la préparation de votre système pour une communication sécurisée, voir Communication sécurisée (explications) sur la page 70 et le [Milestone guide sur les certificats](#).

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

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



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

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

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

12. Une fois que vous avez installé le serveur d'enregistrement de redondance, vous pouvez vérifier son état à partir de l'icône Service de Failover Server et le configurer dans Management Client. Pour plus d'informations, voir Liste des tâches initiales de configuration sur la page 137.

## Installation silencieuse via un interpréteur de ligne de commande (explications)

Avec l'installation silencieuse, les administrateurs de système peuvent installer et mettre à jour le logiciel Recording Server et le logiciel Smart Client sur un large réseau sans interaction de la part des utilisateurs et avec le moins de perturbations possibles pour les utilisateurs finaux.

Les programmes d'installation Recording Server et Smart Client (fichiers .exe) ont différents arguments de ligne de commande. Ils ont chacun leur propre ensemble de paramètres de ligne de commande, lesquels peuvent être invoqués directement dans un interpréteur de ligne de commande ou par le biais d'un fichier Arguments. Vous pouvez également utiliser les options de ligne de commande avec les programmes d'installation dans l'interpréteur de ligne de commande.

Vous pouvez combiner les programmes d'installation de XProtect, ainsi que ses paramètres de ligne de commande et les options de ligne de commande avec les outils pour une distribution et une installation silencieuses de logiciel, tel que Microsoft System Center Configuration Manager (SCCM, également connu sous ConfigMgr). Pour plus d'informations concernant ces outils, rendez-vous sur le site Web du fabricant. Vous pouvez également utiliser Milestone Software Manager pour installer et mettre à jour à distance Recording Server, les pilotes de périphériques et Smart Client. Pour plus d'informations, voir la documentation relative à Milestone Software Manager.

### Paramètres de ligne de commande et fichiers d'arguments

Lors de l'installation silencieuse, vous pouvez préciser les paramètres qui sont étroitement liés aux différents composants du système VMS, ainsi que leur communication interne avec les paramètres de la commande de ligne et des fichiers d'arguments. Les paramètres de la ligne de commande et les fichiers d'arguments ne doivent être utilisés uniquement pour les nouvelles installations car vous ne pouvez pas modifier les paramètres que les paramètres de la commande de ligne représentent lors d'une mise à jour.

Rendez-vous dans le répertoire où se trouve le programme d'installation et saisissez la commande suivante pour voir les paramètres de ligne de commande disponibles et pour générer un fichier Arguments pour un programme d'installation :

```
[NameOfExeFile].exe --generateargsfile=[path]
```

Exemple :

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=c:\temp
```

Dans le fichier des arguments enregistrés (Arguments.xml), chaque paramètre de ligne de commande est accompagné d'une description indiquant son but. Vous pouvez modifier et enregistrer le fichier d'arguments afin que les valeurs des paramètres de la ligne de commande s'adaptent aux besoins de votre installation.

Lorsque vous souhaitez utiliser un fichier d'arguments, ainsi que son programme d'installation, utilisez l'option de ligne de commande `--arguments` en saisissant la commande suivante :

```
[NameOfExeFile].exe --quiet --arguments=[path]\[filename]
```

Exemple :

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
--arguments=C:\temp\arguments.xml
```

### Options de ligne de commande

Vous pouvez également combiner les programmes d'installation aux options de ligne de commande dans l'interpréteur de ligne de commande. En général, les options de ligne de commande modifient le comportement d'une commande.

Rendez-vous au répertoire où se situe le programme d'installation et saisissez `[NameOfExeFile].exe --help` dans l'interpréteur de ligne de commande pour afficher la liste complète des options de la ligne de commande. Vous devez préciser une valeur pour les options de ligne de commande nécessitant une valeur afin de réussir l'installation.

Vous pouvez utiliser à la fois les paramètres de ligne de commande et les options de ligne de commande au sein d'une même commande. Utilisez l'option de ligne de commande `--parameters` et divisez chaque paramètre de ligne de commande avec deux-points (:). Dans l'exemple ci-dessous, `--quiet`, `--showconsole` et `--parameters` représentent les options de ligne de commande, et `ISFAILOVER` et `RECORDERNAME` sont les paramètres de ligne de commande :

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --showconsole
--parameters=ISFAILOVER:true:RECORDERNAME:Failover1
```

## Installation silencieuse d'un serveur d'enregistrement

Lors d'une installation silencieuse, vous ne recevez pas de notifications une fois l'installation terminée. Pour recevoir des notifications, incluez l'option de ligne de commande `--showconsole` dans la commande. L'icône de la barre d'état Milestone XProtect Recording Server apparaît une fois terminée l'installation.

Dans les exemples de commandes ci-dessous, le texte figurant entre les crochets ([ ]) et les crochets eux-mêmes doivent être remplacés par des valeurs réelles. Exemple : au lieu de « [path] », vous pourriez saisir "**d:\program files\, d:\record\, ou \\network-storage-02\surveillance**". Utilisez l'option de ligne de commande `--help` pour en lire plus sur les formats légaux de chaque valeur d'option de ligne de commande.

1. Connectez-vous sur l'ordinateur où vous souhaitez installer le composant Recording Server.
2. Ouvrez un navigateur Internet, saisissez l'adresse de la page Web de téléchargement du Management Server destinée aux administrateurs dans le champ d'adresse et appuyez sur Entrée.  
L'adresse est généralement la suivante : `http://[management server address]:[port]/installation/Admin/default-en-US.htm`.
3. Téléchargez l'assistant d'installation du serveur d'enregistrement en sélectionnant **Toutes les langues** sous **Assistant d'installation du Recording Server**.
4. Ouvrez votre interpréteur de ligne de commande préférée. Pour ouvrir Invite de commande Windows, ouvrez le menu Démarrer de Windows et saisissez **cmd**.
5. Naviguez jusqu'au répertoire contenant le fichier d'installation téléchargé.
6. Poursuivez l'installation selon l'un des deux scénarios ci-dessous :

#### Scénario 1 : Mettre à jour une installation existante ou en installer une sur un serveur avec le composant Management Server avec des valeurs par défaut

- Saisissez la commande suivant pour démarrer l'installation.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet
```

#### Scénario 2 : Installer dans un système distribué

1. Saisissez la commande suivante pour générer un fichier d'arguments avec des paramètres de ligne de commande.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --generateargsfile=[chemin d'accès]
```

2. Ouvrez le fichier d'arguments (Arguments.xml) à partir du chemin spécifié et modifiez les valeurs des paramètres de la ligne de commande si nécessaire.



Assurez-vous de donner aux paramètres de ligne de commande `SERVERHOSTNAME` et `SERVERPORT` des valeurs valides. Sinon, l'installation ne pas se terminer.

4. Enregistrez le fichier Arguments.

- Retournez à l'interpréteur de ligne de commande et entrez la commande ci-dessous pour installer les valeurs de paramétrage de la ligne de commande spécifiées dans le fichier Arguments.

```
MilestoneXProtectRecordingServerInstaller_x64.exe --quiet --arguments=[chemin d'accès]\[nom du fichier]
```

## Installer XProtect Smart Client silencieusement

Lors d'une installation silencieuse, vous ne recevez pas de notifications une fois l'installation terminée. Pour recevoir des notifications, incluez l'option de ligne de commande `--showconsole` dans la commande. Un raccourci vers XProtect Smart Client apparaît sur le bureau une fois terminée l'installation.

Dans les exemples de commandes ci-dessous, le texte figurant entre les crochets ([ ]) et les crochets eux-mêmes doivent être remplacés par des valeurs réelles. Exemple : au lieu de « [path] », vous pourriez saisir "**d:\program files\**", **d:\record\**, ou **\\network-storage-02\surveillance**. Utilisez l'option de ligne de commande `--help` pour en lire plus sur les formats légaux de chaque valeur d'option de ligne de commande.

- Ouvrez un navigateur Internet, saisissez l'adresse de la page Web de téléchargement du Management Server destinée aux utilisateurs finaux dans le champ d'adresse et appuyez sur Entrée.

L'adresse est généralement la suivante : `http://[management server address]:[port]/installation/default-en-US.htm`.

- Téléchargez le programme d'installation XProtect Smart Client en sélectionnant **Toutes les langues** sous **Programme d'installation XProtect Smart Client**.
- Ouvrez votre interpréteur de ligne de commande préféré. Pour ouvrir Invite de commande Windows, ouvrez le menu Démarrer de Windows et saisissez **cmd**.
- Naviguez jusqu'au répertoire contenant le fichier d'installation téléchargé.
- Poursuivez l'installation selon l'un des deux scénarios ci-dessous :

### Scénario 1 : Mettre à jour une installation existante ou en installer une avec des valeurs de paramètres de ligne de commande par défaut

- Saisissez la commande suivant pour démarrer l'installation.

```
XProtect Smart Client 2020 R3 Installer.exe --quiet
```

## Scénario 2 : Installer des valeurs de paramètres de ligne de commande personnalisées à l'aide d'un fichier d'arguments xml comme entrée

1. Saisissez la commande suivante pour générer un fichier d'arguments xml avec des paramètres de ligne de commande.

```
XProtect Smart Client 2020 R3 Installer.exe --generateargsfile=[chemin d'accès]
```

2. Ouvrez le fichier d'arguments (Arguments.xml) à partir du chemin spécifié et modifiez les valeurs des paramètres de la ligne de commande si nécessaire.
3. Enregistrez le fichier Arguments.
4. Retournez à l'interpréteur de ligne de commande et entrez la commande ci-dessous pour installer les valeurs de paramétrage de la ligne de commande spécifiées dans le fichier Arguments.

```
XProtect Smart Client 2020 R3 Installer.exe --quiet --arguments=[path] \ [filename]
```

## Installation pour les groupes de travail

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

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



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

2. Selon vos besoins, démarrez l'installation du serveur de gestion ou d'enregistrement et cliquez sur **Personnaliser**.
3. Selon votre sélection lors de la 2e étape, choisissez d'installer le service Management Server ou Recording Server à l'aide d'un compte administrateur commun.
4. Terminez l'installation.
5. Répétez les étapes 1 à 4 pour installer tous les autres systèmes que vous souhaitez connecter. Ils doivent tous être installés en utilisant un compte administrateur commun.

Vous ne pouvez pas utiliser cette méthode lorsque vous mettez à jour les installations de groupe de travail. Consultez la rubrique Mise à niveau dans une configuration de groupe de travail sur la page 528.



## Installation dans une grappe

Avant de procéder à l'installation dans une grappe, voir Serveurs de gestion multiples (grappes) (explications) sur la page 56 et Conditions préalables à la mise en grappe sur la page 57.



Les descriptions et illustrations présentées peuvent être différentes de ce que vous voyez à l'écran.

### Installation et modification de l'adresse URL :

1. Installer le serveur de gestion et tous ses sous-composants sur le premier serveur de la grappe.

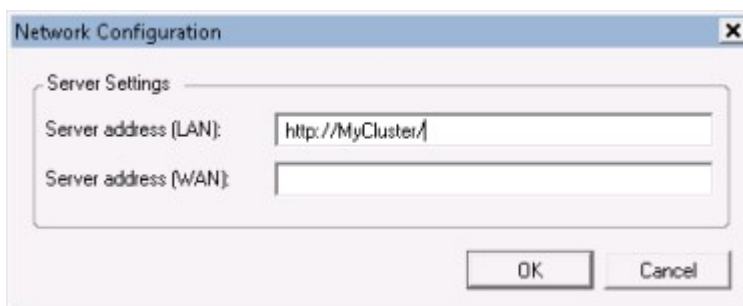


Le serveur de gestion doit être installé avec un utilisateur spécifique, et non en tant que service de réseau. Pour ce faire, vous devez utiliser l'option d'installation **Personnalisée**. De plus, l'utilisateur spécifique doit avoir accès au disque de réseau partagé et à un mot de passe sans expiration de préférence.

2. Après avoir installé le serveur de gestion et le Management Client sur le premier serveur de la grappe, ouvrez le Management Client, puis, à partir du menu **Outils**, sélectionnez **Services enregistrés**.
  1. Dans la fenêtre **Ajouter/supprimer des services enregistrés**, sélectionnez **Service de journal** dans la liste, puis cliquez sur **Modifier**.
  2. Dans la fenêtre **Modifier le service enregistré**, remplacez l'adresse URL du service de journal par l'adresse URL de la grappe.



3. Répétez ces étapes pour tous les services listés dans la fenêtre **Ajouter/supprimer des services enregistrés**. Cliquez sur **Réseau**.
4. Dans la fenêtre **Configuration du réseau**, remplacez l'adresse URL du serveur par l'adresse URL de la grappe. (Cette étape s'applique uniquement au premier serveur de la grappe.) Cliquez sur **OK**.



5. Dans la fenêtre **Ajouter/supprimer des services enregistrés**, cliquez sur **Fermer**. Quittez le Management Client.
6. Arrêtez le service Management Server ainsi qu'IIS. Obtenez de plus amples informations sur la façon d'arrêter IIS sur le site Web de Microsoft ([https://technet.microsoft.com/library/cc732317\(WS.10\).aspx](https://technet.microsoft.com/library/cc732317(WS.10).aspx)).
7. Répétez ces étapes pour tous les serveurs suivants de la grappe, en les orientant cette fois-ci vers SQL Server et la base de données existant. Cependant, pour le dernier serveur de la grappe sur lequel vous installez le serveur de gestion, n'arrêtez pas le service Management Server.

**Configurez le service Management Server en tant que service générique dans la grappe de redondance :**

1. Sur le dernier serveur sur lequel vous avez installé le serveur de gestion, allez dans **Démarrer > Outils d'administration**, ouvrez le module de **Gestion de la grappe de redondance** de Windows. Dans la fenêtre **Gestion de la grappe de redondance**, agrandissez votre grappe, cliquez sur **Services et applications** à l'aide du bouton droit de votre souris et sélectionnez **Configurer un service ou une application**.



2. Dans la boîte de dialogue **Haute disponibilité**, cliquez sur **Suivant**.
3. sélectionnez **Service générique** et cliquez sur **Suivant**.
4. Ne spécifiez rien sur la troisième page de la boîte de dialogue et cliquez sur **Suivant**.
5. Choisissez le service **Milestone XProtect Management Server**, puis cliquez sur **Suivant**. Spécifiez le nom (nom de l'hôte de la grappe), que les clients utilisent pour accéder au service, cliquez sur **Suivant**.
6. Aucun espace de stockage n'est requis pour ce service, puis cliquez sur **Suivant**. Aucun paramètre de registre ne doit être répliqué ; cliquez sur **Suivant**. Vérifiez que le service regroupé est configuré selon vos besoins, puis cliquez sur **Suivant**. Le serveur de gestion est maintenant configuré en tant que service générique dans la grappe de redondance. Cliquez sur **Terminer**.
7. Dans la configuration de la grappe, le serveur d'événements et le Data Collector doivent être configurés comme service dépendant du serveur de gestion pour que le serveur d'événements s'arrête lorsque le serveur de gestion s'arrêtera.

8. Pour ajouter le service **Milestone XProtect Event Server** en tant que ressource pour le service **Milestone XProtect Management Server Cluster**, cliquez sur le service de grappe à l'aide du bouton droit de votre souris et cliquez sur **Ajouter une ressource > 4 - Service générique** et sélectionnez **Milestone XProtect Event Server**.

### Modifiez les paramètres de configuration suivants :

Dans les nœuds Management Server :

- Dans C:\ProgramData\Milestone\XProtectManagement Server\ServerConfig.xml :

```
<AuthorizationServerUri>http://ClusterRoleAddress/IDP</AuthorizationServerUri>
```

- Dans C:\Program Files\Milestone\XProtectManagement Server\IIS\IDP\appsettings.json :

```
« Authority » : « http://ClusterRoleAddress/IDP »
```

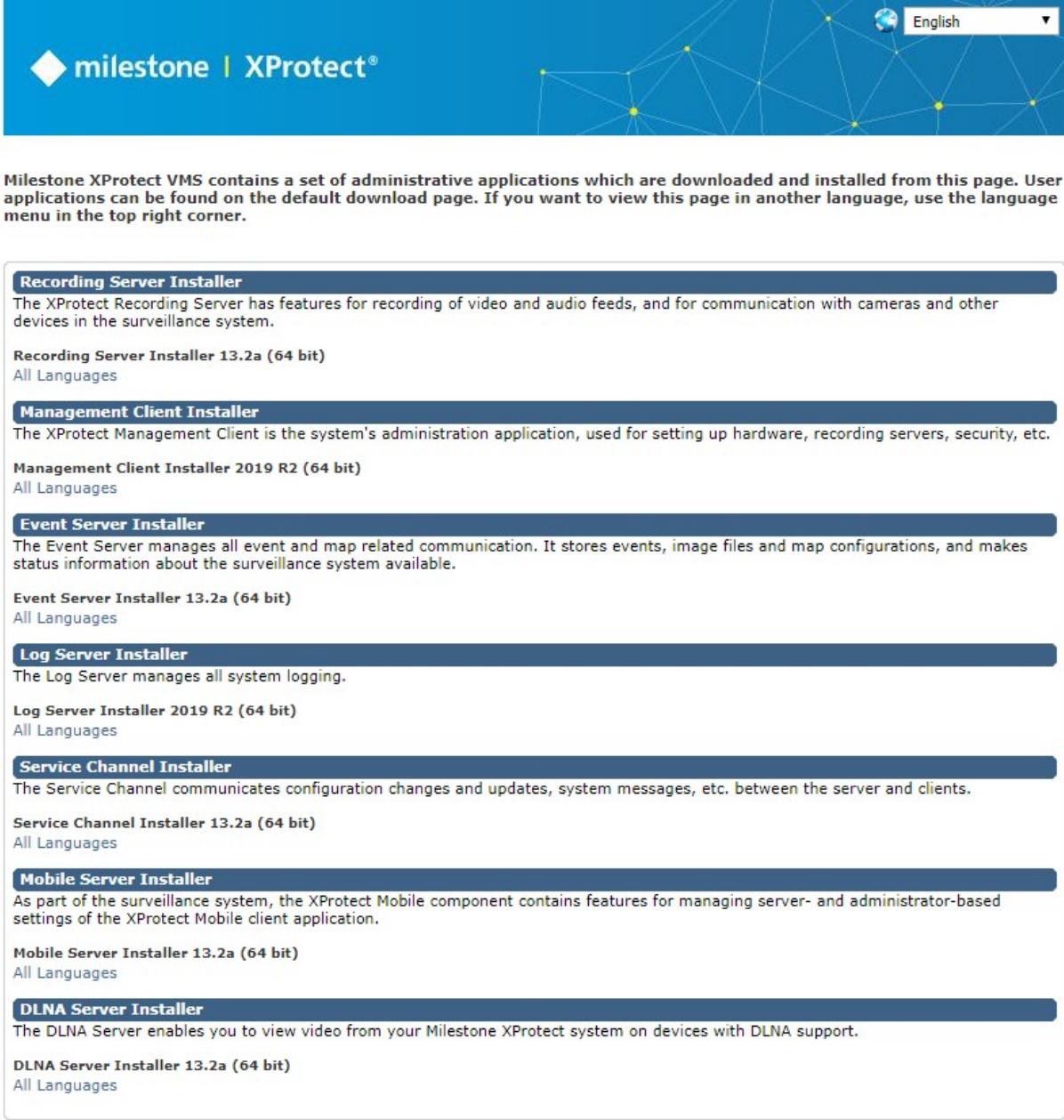
Dans les Recording Server, vérifiez que l'adresse du serveur d'autorisation est également configurée sur l'adresse du rôle en grappe :

Dans C:\ProgramData\Milestone\XProtectRecording Server\RecorderConfig.xml :

```
<authorizationserveraddress>http://ClusterRoleAddress/IDP</authorizationserveraddress>
```

## Download Manager/page web de téléchargement.

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



**Milestone XProtect VMS contains a set of administrative applications which are downloaded and installed from this page. User applications can be found on the default download page. If you want to view this page in another language, use the language menu in the top right corner.**

**Recording Server Installer**  
The XProtect Recording Server has features for recording of video and audio feeds, and for communication with cameras and other devices in the surveillance system.  
**Recording Server Installer 13.2a (64 bit)**  
All Languages

**Management Client Installer**  
The XProtect Management Client is the system's administration application, used for setting up hardware, recording servers, security, etc.  
**Management Client Installer 2019 R2 (64 bit)**  
All Languages

**Event Server Installer**  
The Event Server manages all event and map related communication. It stores events, image files and map configurations, and makes status information about the surveillance system available.  
**Event Server Installer 13.2a (64 bit)**  
All Languages

**Log Server Installer**  
The Log Server manages all system logging.  
**Log Server Installer 2019 R2 (64 bit)**  
All Languages

**Service Channel Installer**  
The Service Channel communicates configuration changes and updates, system messages, etc. between the server and clients.  
**Service Channel Installer 13.2a (64 bit)**  
All Languages

**Mobile Server Installer**  
As part of the surveillance system, the XProtect Mobile component contains features for managing server- and administrator-based settings of the XProtect Mobile client application.  
**Mobile Server Installer 13.2a (64 bit)**  
All Languages

**DLNA Server Installer**  
The DLNA Server enables you to view video from your Milestone XProtect system on devices with DLNA support.  
**DLNA Server Installer 13.2a (64 bit)**  
All Languages

© Milestone Systems A/S

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

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

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

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

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

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

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

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

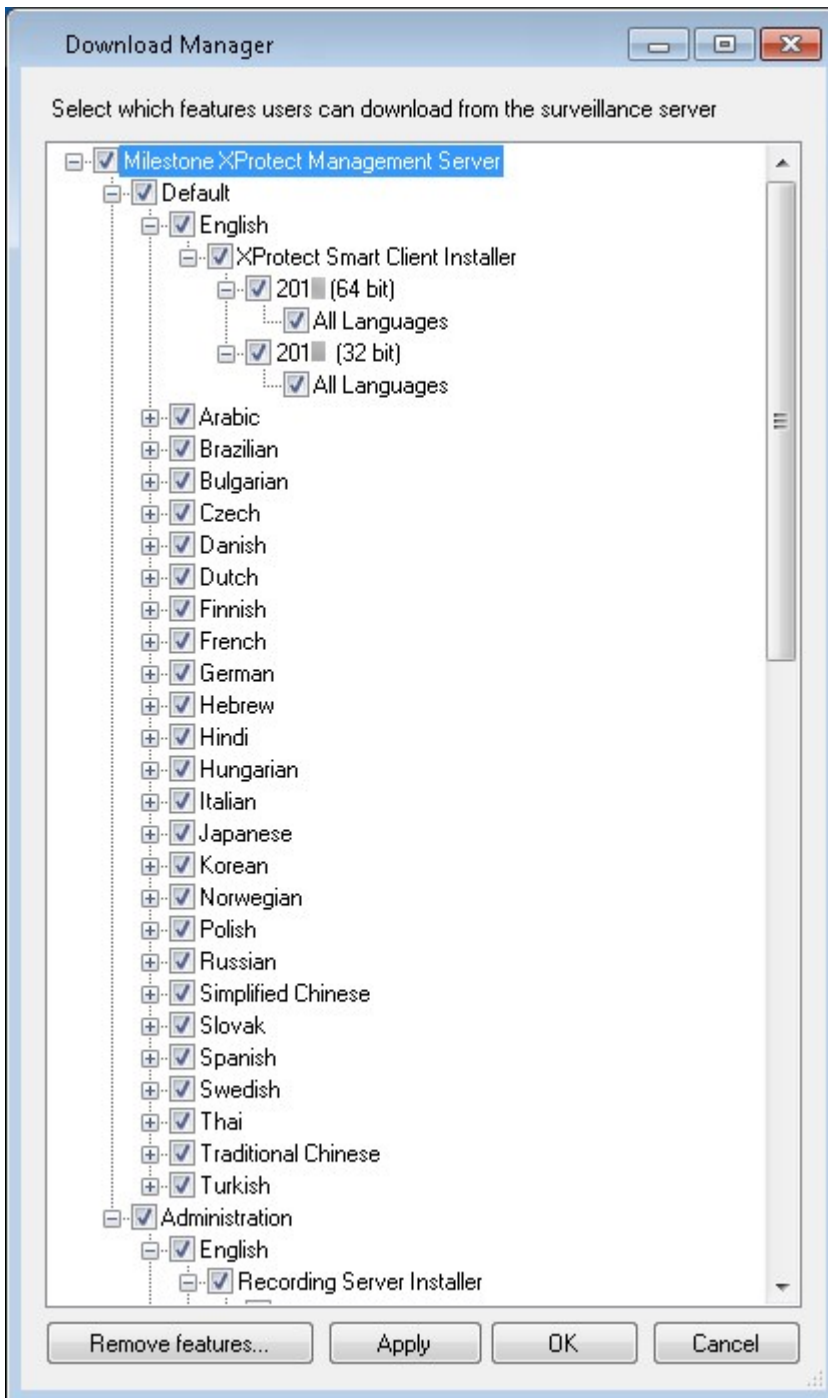
Même si le Download Manager vous permet de contrôler les composants que les utilisateurs peuvent télécharger et installer, vous ne pouvez pas l'utiliser en tant qu'outil de gestion des droits d'utilisateurs. Ces droits sont déterminés par les rôles définis dans le Management Client.

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

## Configuration du Download Manager par défaut

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

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



- Le premier niveau : Se rapporte à votre produit XProtect
- Le deuxième niveau : Se rapporte aux deux versions ciblées de la page web. **Par défaut** se rapporte à la version de la page web visualisée par les utilisateurs finaux. **Administration** se rapporte à la version de la page web visualisée par les administrateurs du système
- Le troisième niveau : Se rapporte aux langues dans lesquelles la page web est disponible

- Le quatrième niveau : Se rapporte aux composants qui sont (ou peuvent être mis) à la disposition des utilisateurs
- Le cinquième niveau : Se rapporte aux versions particulières de chaque composant qui sont (ou peuvent être mises) à la disposition des utilisateurs
- Le sixième niveau : Se rapporte aux versions linguistiques des composants qui sont (ou peuvent être mises) à la disposition des utilisateurs

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

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

## Installeurs standard du Download Manager (utilisateur)

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

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

Pour l'installation des pilotes de périphériques, voir Installateur de pilotes de périphériques - doit être téléchargé sur la page 113.

## Ajouter/publier les composants de l'installateur Download Manager

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

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

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

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

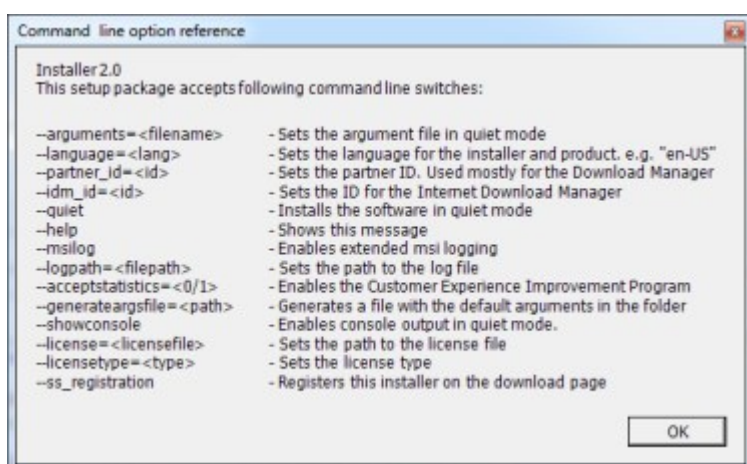
1. Sur l'ordinateur où vous avez téléchargé le(s) composant(s), allez sur le menu **Démarrer** de Windows et saisissez *Invite de commande*
2. Dans l'*Invite de commande*, exécutez le nom du fichier (.exe) avec : [espace]--ss\_registration

Exemple : *MilestoneXProtectRecordingServerInstaller\_x64.exe --ss\_registration*

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



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



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

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

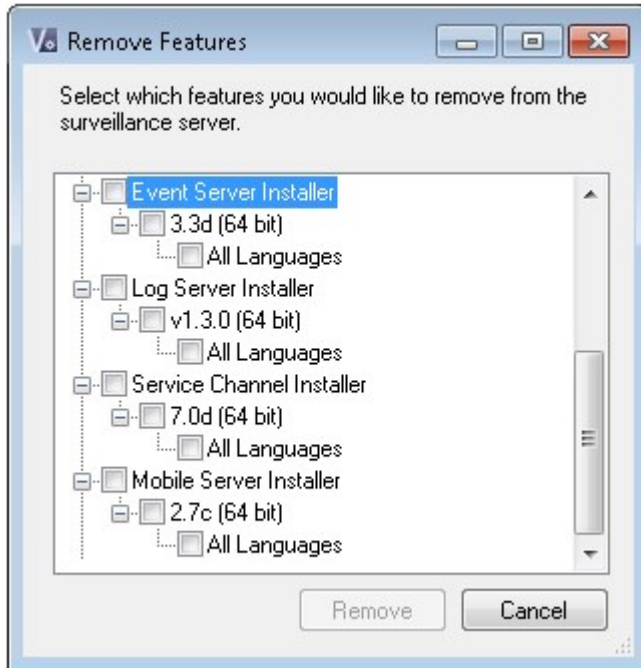
### Masquer/supprimer les composants de l'installateur Download Manager

Trois options s'offrent à vous :

- **Masquer des composants** depuis la page Web en décochant des cases de l'arborescence de Download Manager. Les composants sont tout de même installés sur le serveur de gestion, mais en cochant des cases de l'arborescence du Download Manager, vous pourrez rapidement rendre les composants à nouveau disponibles



- **Supprimer l'installation des composants** sur le serveur de gestion. Les composants disparaissent du Download Manager, mais les fichiers d'installation des composants restent sur *C:\Program Files (x86)\Milestone\XProtect Download Manager*. Vous pourrez donc les réinstaller ultérieurement si nécessaire
  1. Dans le Download Manager, cliquez sur **Supprimer des fonctionnalités**.
  2. Dans la fenêtre **Supprimer fonctions**, sélectionnez la ou les fonction(s) à supprimer.



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

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

## Installateur de pilotes de périphériques - doit être téléchargé

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

1. Profitez du tout dernier pack classique de pilotes de périphériques sur la page de téléchargement du site Web Milestone (<https://www.milestonesys.com/downloads/>).
2. Vous pourrez également y télécharger le pack de pilotes de périphérique avec des pilotes plus anciens. Pour vérifier si vos caméras utilisent des pilotes de l'ancien Device Pack, rendez-vous sur ce site Web (<https://www.milestonesys.com/community/business-partner-tools/device-packs/>).
3. Ajoutez/Publiez-le sur le Download Manager en l'appelant à l'aide de la commande `--ss_registration`.

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

## Fichiers journaux de l'installation et dépannage

Lors d'une installation, mise à jour ou désinstallation, les entrées de journal sont écrites dans plusieurs fichiers journaux de l'installation : Dans le fichier journal de l'installation principal `install.log` et dans les fichiers journaux appartenant aux différents composants du système que vous installez. Toutes les entrées de journal ont un horodatage et les entrées de journal les plus récentes se situent à la fin des fichiers journaux.

Vous pouvez localiser toutes les entrées des journaux de l'installation dans le dossier `C:\ProgramData\Milestone\Installer\`. Les fichiers journaux nommés `*I.log` ou `*I[integer].log` concernent les nouvelles installations ou mises à jour, alors que les fichiers journaux nommés `*U.log` ou `*U[integer].log` portent sur les installations. Si vous avez acheté un serveur avec un système XProtect déjà installé via un partenaire Milestone, il se peut qu'il en contienne aucun fichier journal de l'installation.

Les fichiers journaux contiennent des informations concernant les paramètres de ligne de commande et les options de ligne de commande, ainsi que leurs valeurs utilisées lors d'une installation, mise à jour ou désinstallation. Pour localiser les paramètres de ligne de commande figurant dans les fichiers journaux, recherchez **Ligne de commande** : ou **Paramètre** ' selon le fichier journal.

Pour le dépannage, le fichier journal d'installation principal est le premier endroit où chercher. Les exceptions, erreurs ou avertissements survenant au cours de l'installation sont journalisées. Essayez de rechercher une **exception**, **erreur**, ou un **avertissement**. « Code de sortie : 0 » signifie que l'installation a réussi et Code de sortie : 1 », son échec. Vos trouvailles dans les fichiers journaux peuvent vous permettre de trouver une solution dans [https://supportcommunity.milestonesys.com/s/knowledgebase?language=en\\_US/](https://supportcommunity.milestonesys.com/s/knowledgebase?language=en_US/). Sinon, contactez votre partenaire Milestone et partagez-lui les fichiers journaux de l'installation concernés.

# Configuration

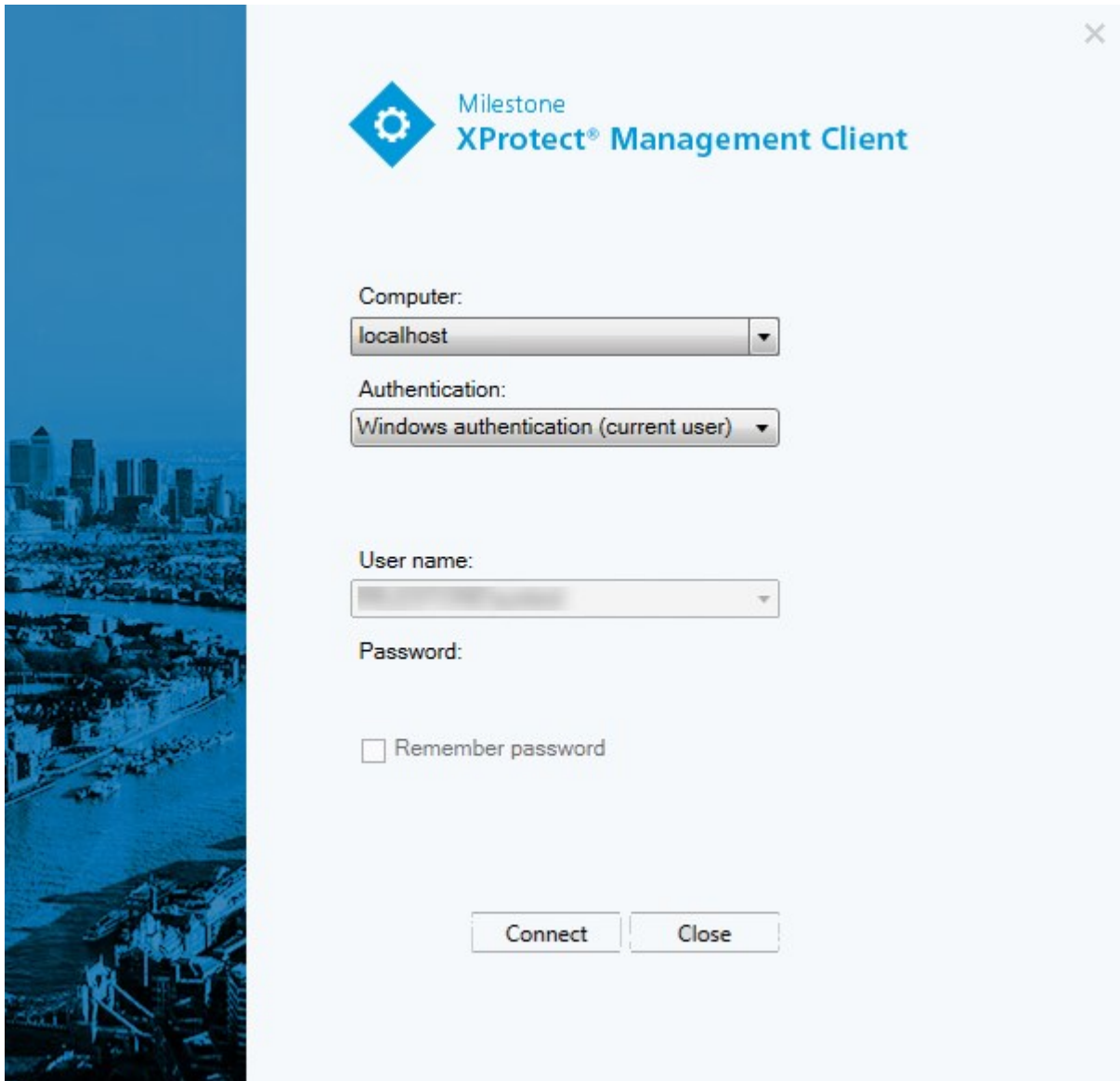
## Navigation au sein du Management Client

Cette section fournit une introduction à l'interface utilisateur de Management Client.

### Vue d'ensemble de la connexion

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

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



### Autorisation de connexion (explications)

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

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

Pour associer l'autorisation de connexion à un rôle :

- Définissez l'**Autorisation de connexion requise** pour le rôle sélectionné dans l'onglet **Info** (voir Paramètres des rôles sur la page 374) dans **Rôles**, de façon à ce que l'utilisateur reçoive une demande d'autorisation supplémentaire au cours de la connexion
- Définissez **Autoriser des utilisateurs** pour le rôle sélectionné dans l'onglet **Sécurité globale** (voir Paramètres des rôles sur la page 374) dans **Rôles**, de sorte que l'utilisateur puisse autoriser les connexions d'autres utilisateurs

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

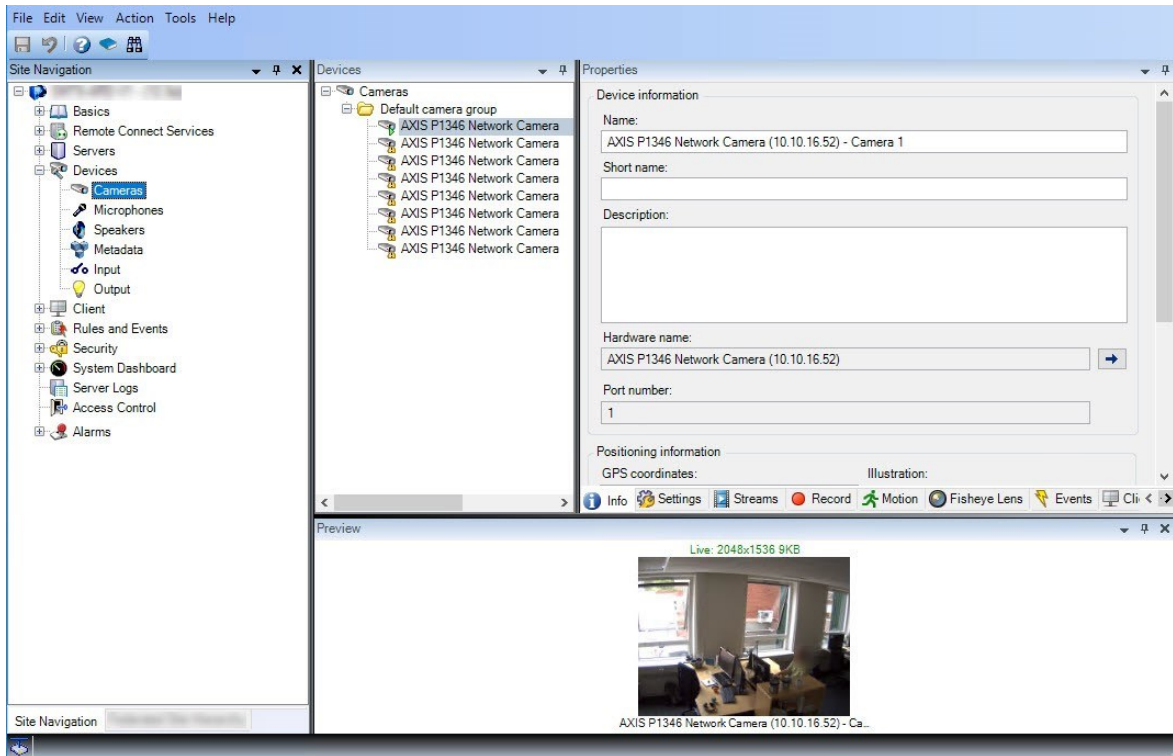
## Vue d'ensemble de la fenêtre Management Client

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

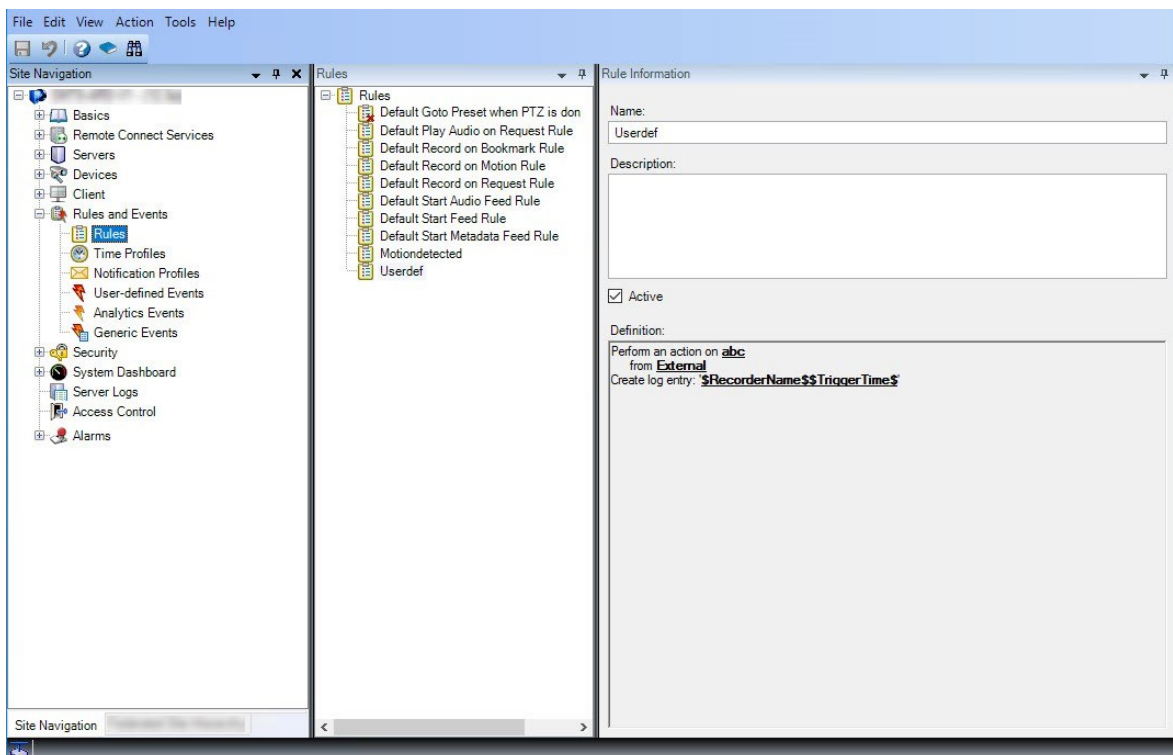
- Configuration système
- Tâche
- Fonctions disponibles

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

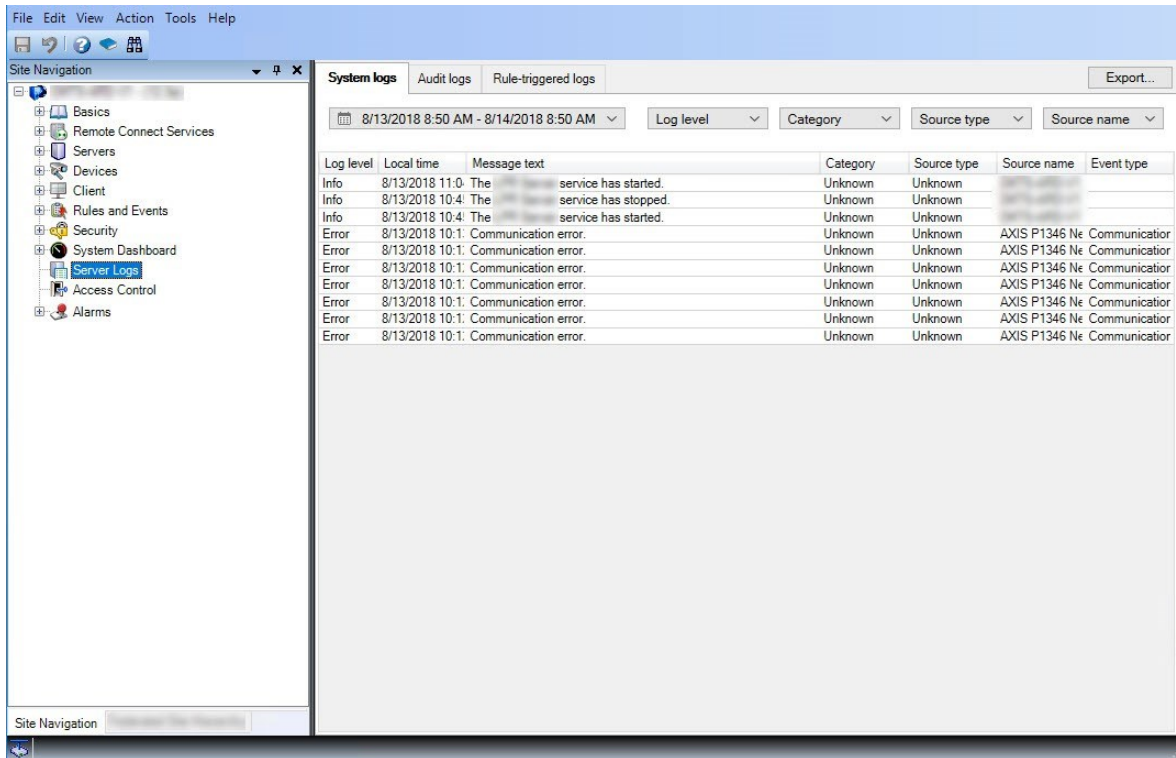
- Lorsque vous travaillez avec des serveurs d'enregistrement et des périphériques :



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



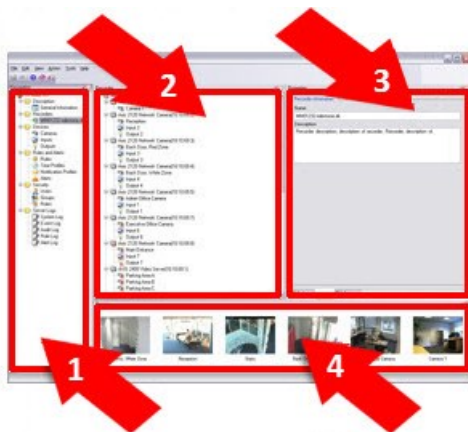
- Lorsque vous affichez des journaux :



## Vue d'ensemble des volets



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



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

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

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

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

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

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



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

Live: 640x480 88kB



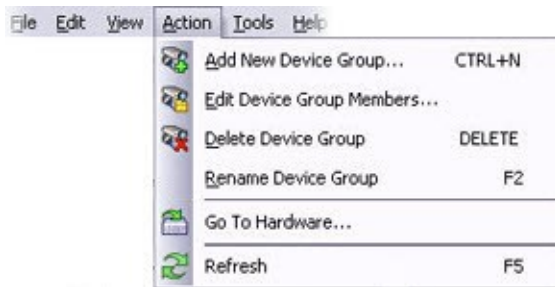
Camera 5

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

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



## Vue d'ensemble des menus



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

### Menu Fichier

Vous pouvez enregistrer les modifications apportées à la configuration et quitter l'application. Vous pouvez également sauvegarder votre configuration, voir Sauvegarde et de la restauration de la configuration de votre système (explications) sur la page 488.

### Menu Modifier

Vous pouvez annuler les modifications.

### Menu Vue

Nom	Description
<b>Réinitialiser la présentation de l'application</b>	Réinitialisez la présentation des différents volets du Management Client à leurs paramètres par défaut.
<b>Fenêtre Aperçu</b>	Activez ou désactivez le volet <b>Aperçu</b> lorsque vous travaillez avec des serveurs d'enregistrement et des périphériques.
<b>Afficher les flux d'enregistrement</b>	Par défaut, les informations affichées avec les images d'aperçu dans le volet <b>Aperçu</b> se rapportent aux flux en direct des caméras. Si vous souhaitez plutôt obtenir de plus amples informations sur les flux d'enregistrement, sélectionnez <b>Afficher flux d'enregistrement</b> .
<b>Hiérarchie des sites fédérés</b>	Par défaut, le volet <b>Hiérarchie des sites fédérés</b> est activé.
<b>Navigation sur le site</b>	Par défaut, le volet <b>Navigation sur le site</b> est activé.

## Menu Action

Le contenu du menu **Action** dépend de l'élément sélectionné dans le volet **Navigation sur le site**. Les actions disponibles sont identiques lorsque vous cliquez avec le bouton droit de la souris sur l'élément. Les éléments sont décrits dans Configuration du système dans le panneau Navigation du site sur la page 139.

La période pré-enregistrement pour chaque caméra, voir Périphériques prenant la mise en mémoire-tampon préalable en charge sur la page 240

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

## Menu Outils

Nom	Description
<b>Services enregistrés</b>	Gérez les services enregistrés. Voir Gérer les services enregistrés sur la page 516.
<b>Rôles effectifs</b>	Affichez tous les rôles d'un utilisateur ou groupe sélectionné.
<b>Options</b>	Ouvre la boîte de dialogue Options, qui vous permet de définir et de modifier les paramètres généraux du système.

## Menu Aide

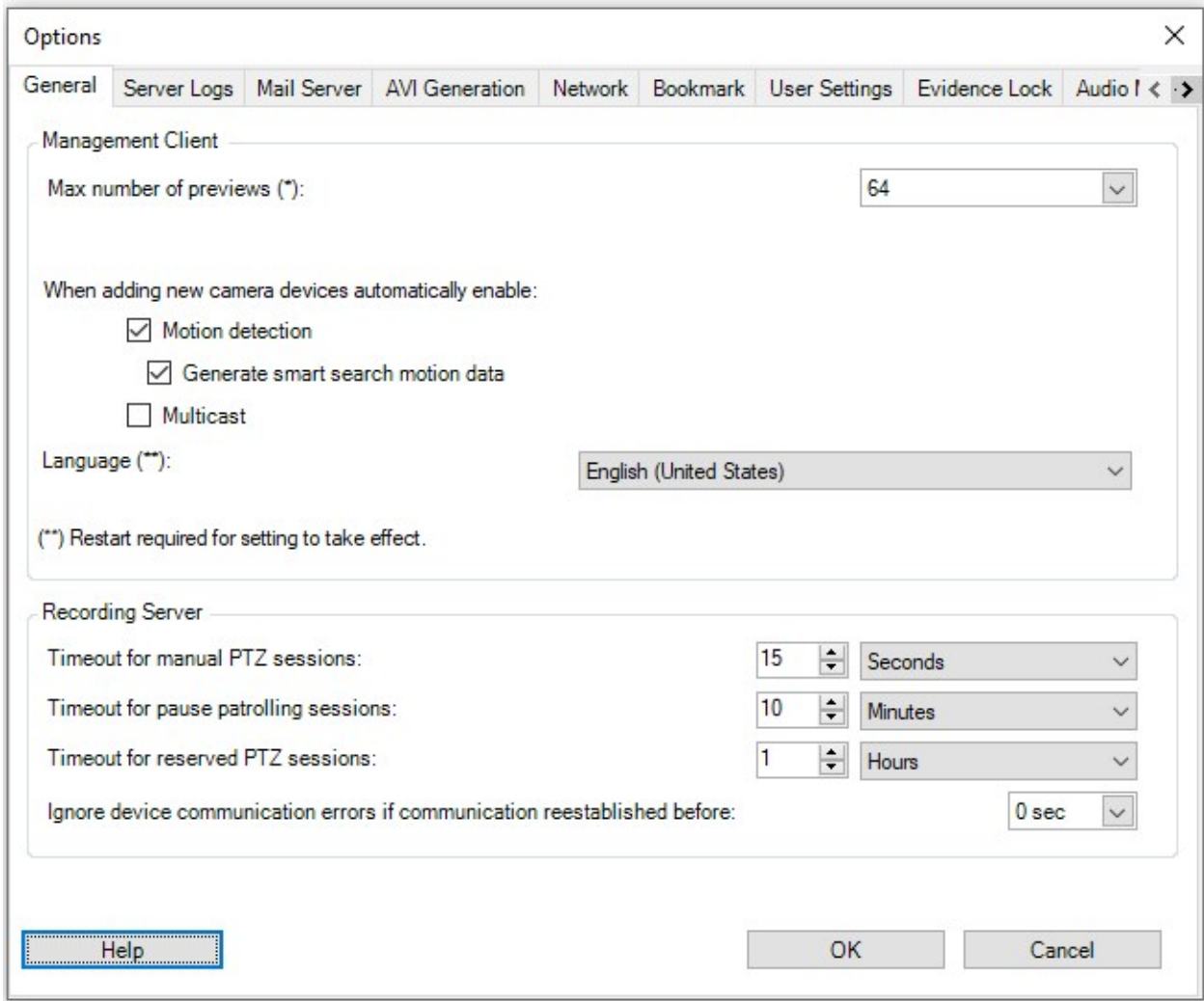
Vous pouvez accéder au système d'aide et aux informations relatives à la version du Management Client.

## Options de paramétrage pour le système

Dans la boîte de dialogue **Options**, vous pouvez spécifier un certain nombre de paramètres en relation avec l'aspect général et la fonctionnalité du système.

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

Pour accéder à la boîte de dialogue, sélectionnez **Outils > Options**.



## Onglet Général (options)

Dans l'onglet Général, vous pouvez préciser les paramètres d'ordre général pour le Management Client et le serveur d'enregistrement.

### Management Client

Nom	Description
Nombre max. d'aperçus	Sélectionnez le nombre maximum d'images miniatures affichées dans le volet <b>Aperçu</b> . Par défaut, le nombre

Nom	Description
	<p>d'images miniatures est de 64.</p> <p>Sélectionnez <b>Action</b> &gt; <b>Rafraîchir</b> dans le menu pour confirmer la modification.</p> <p>Une grande quantité d'images miniatures combinée à une fluidité d'image élevée peut ralentir le système.</p>
<p><b>Lors de l'ajout de nouveaux périphériques de type caméra, activer automatiquement :</b> <b>Détection des mouvements</b></p>	<p>Cochez la case pour activer la détection de mouvement pour les nouvelles caméras lorsque vous les ajoutez au système à l'aide de l'assistant <b>Ajouter du matériel</b>.</p> <p>Ce paramètre n'influence pas les paramètres de détection du mouvement des caméras existantes.</p> <p>Vous activez et désactivez la détection du mouvement pour une caméra dans l'onglet <b>Mouvement</b> pour le périphérique de type caméra.</p>
<p><b>Lors de l'ajout de nouveaux périphériques de type caméra, activer automatiquement :</b> <b>Générer des données de mouvement pour la recherche intelligente</b></p>	<p>La génération de données de mouvement pour la recherche intelligente exige que la détection du mouvement soit activée pour la caméra.</p> <p>Cochez la case pour activer la génération de données mouvement pour la recherche avancée sur les nouvelles caméras lorsque vous les ajoutez au système à l'aide de l'assistant <b>Ajouter du matériel</b>.</p> <p>Ce paramètre n'influence pas les paramètres de détection du mouvement des caméras existantes.</p> <p>Vous activez et désactivez la génération de données de recherche intelligente pour une caméra dans l'onglet <b>Mouvement</b> pour le périphérique de type caméra.</p>
<p><b>Lors de l'ajout de nouveaux périphériques de type caméra, activer automatiquement :</b> <b>Multicast</b></p>	<p>Cochez la case pour activer la diffusion multflux pour les nouvelles caméras lorsque vous les ajoutez au système à l'aide de l'assistant <b>Ajouter du matériel</b>.</p> <p>Ce paramètre n'influence pas les paramètres de diffusion multflux des caméras existantes.</p> <p>Vous activez et désactivez le multicast en direct pour une</p>

Nom	Description
	caméra dans l'onglet <b>Client</b> pour le périphérique de type caméra.
<b>Langue</b>	Sélectionnez la langue du Management Client. Redémarrez le Management Client pour activer la nouvelle langue.

### Serveur d'enregistrement

Nom	Description
<b>Période d'inactivité pour les sessions PTZ manuelles</b>	Les utilisateurs du client dotés des droits d'utilisateurs nécessaires peuvent interrompre manuellement la patrouille des caméras PTZ. Sélectionnez la durée qui doit s'écouler avant que le programme de patrouille habituel reprenne suite à une interruption manuelle. Ce paramètre s'applique à toutes les caméras PTZ de votre système. Le paramètre par défaut est de 15 secondes.  Si vous souhaitez appliquer des délais individuels aux caméras, spécifiez ceux-ci dans l'onglet <b>Préréglages</b> de la caméra.
<b>Période d'inactivité pour la mise en pause des sessions PTZ</b>	Les utilisateurs du client disposant d'une priorité PTZ suffisante peuvent mettre des patrouilles en pause sur les caméras PTZ. Sélectionnez la durée qui doit s'écouler avant que le programme de patrouille habituel reprenne suite à une pause. Ce paramètre s'applique à toutes les caméras PTZ de votre système. La limite de temps par défaut est de 10 minutes.  Si vous souhaitez appliquer des délais individuels aux caméras, spécifiez ceux-ci dans l'onglet <b>Préréglages</b> de la caméra.
<b>Période d'inactivité pour les sessions PTZ réservées</b>	Réglez la période d'inactivité par défaut pour les sessions PTZ réservées. Lorsqu'un utilisateur exécute une session PTZ réservée, la caméra PTZ ne peut pas être utilisée par d'autres personnes tant qu'elle n'est pas libérée manuellement ou que la période d'inactivité n'a pas pris fin. Le paramètre par défaut est de 1 heure.  Si vous souhaitez appliquer des délais individuels aux caméras, spécifiez ceux-ci dans l'onglet <b>Préréglages</b> de la caméra.

Nom	Description
<b>Ignorer les erreurs de communication avec le périphérique si la communication est rétablie avant</b>	Le système note toutes les erreurs de communication sur le matériel et les périphériques, mais vous sélectionnez ici combien de temps doit exister une erreur de communication avant que le moteur des règles ne déclenche l'événement <b>Erreur de communication</b> .

## Onglet Journaux de serveurs (options)

Dans l'onglet **Journaux de serveurs**, vous pouvez spécifier les paramètres pour les journaux des serveurs de gestion du système.

Pour en savoir plus, voir Journaux (explications) sur la page 432.

Nom	Description
<b>Journaux</b>	<p>Sélectionnez le type de journal que vous souhaitez configurer :</p> <ul style="list-style-type: none"> <li>• Journaux système</li> <li>• Journaux d'audit</li> <li>• Journaux déclenchés par les règles</li> </ul>
<b>Paramètres</b>	<p>Désactivez ou activez les journaux et spécifiez la durée de rétention.</p> <p>Autorisez la version 2018 R2 et les composants antérieurs à écrire dans les journaux. Pour plus d'informations, voir Autoriser la version 2018 R2 et les composants antérieurs à écrire dans les journaux sur la page 434</p> <p>Pour les journaux <b>Système</b>, indiquez le niveau des messages que vous souhaitez consigner :</p> <ul style="list-style-type: none"> <li>• Tous les messages (y compris les messages indéfinis)</li> <li>• Informations, avertissements et erreurs</li> <li>• Avertissements et erreurs</li> <li>• Erreurs (paramètre par défaut)</li> </ul>

Nom	Description
	<p>Pour les journaux <b>Audit</b>, activez le protocole des accès utilisateur si vous souhaitez que le système consigne toutes les actions des utilisateurs dans XProtect Smart Client. Il s'agit par exemple des exportations, de l'activation des sorties, ainsi que du visionnage de caméras en direct ou en mode lecture.</p> <p>Précisez :</p> <ul style="list-style-type: none"> <li>La durée d'une séquence de lecture</li> </ul> <p>Cela signifie qu'à condition que l'utilisateur procède à la lecture pendant cette période, le système ne génère qu'une entrée du journal. Lors d'une lecture en dehors de la période, le système crée une nouvelle entrée du journal.</p> <ul style="list-style-type: none"> <li>Le nombre d'enregistrements (images) qu'un utilisateur a vu avant que le système ne crée une entrée au journal</li> </ul>

## Onglet Serveur de messagerie (options)

L'onglet **Serveur de messagerie** vous permet de préciser les paramètres du serveur de messagerie sortant de votre système.

Voir Profils de notification sur la page 352 pour de plus amples informations.

Nom	Description
<b>Adresse e-mail de l'expéditeur</b>	Saisissez l'adresse e-mail à afficher en tant qu'expéditeur des notifications par e-mail pour tous les profils de notifications. Exemple : <b>expéditeur@entreprise.org</b> .
<b>Adresse du serveur de messagerie</b>	Saisissez l'adresse du serveur de messagerie SMTP procédant à l'envoi des notifications par e-mail. Exemple : <b>serveurmessagerie.entreprise.org</b> .
<b>Port du serveur de messagerie</b>	Le port TCP utilisé pour la connexion au serveur de messagerie. Le port par défaut est 25 pour les connexions non cryptées. Les connexions cryptées utilisent généralement le port 465 ou 587.

Nom	Description
<b>Crypter la connexion au serveur</b>	<p>Si vous souhaitez sécuriser la communication entre le serveur de gestion et le serveur de messagerie SMTP, sélectionnez cette case à cocher.</p> <p>La connexion est sécurisée grâce à la commande du protocole de messagerie STARTTLS. Dans ce mode, la session commence sur une connexion non-cryptée, puis une commande STARTTLS est fournie par le serveur de messagerie SMTP au serveur de gestion pour basculer vers une communication sécurisée qui utilise SSL.</p>
<b>Connexion au serveur requise</b>	<p>Si activée, vous devez indiquer un identifiant et mot de passe pour les utilisateurs qui se connectent au serveur de messagerie.</p>

## Onlet Génération AVI (options)

L'onglet **Génération AVI** vous permet de spécifier les paramètres de compression pour la génération de fichiers de clip vidéo AVI. La spécification de ces paramètres est requise si vous désirez inclure des fichiers AVI dans les notifications par e-mail envoyées par les profils de notification déclenchés par les règles.

Reportez-vous également à la section Profils de notification sur la page 352.

Nom	Description
<b>Logiciel de compression</b>	<p>Sélectionnez le codec (technologie de compression/décompression) à appliquer. Pour disposer de plusieurs codecs sur la liste, installez-les sur le serveur de gestion.</p> <p>Toutes les caméras ne prennent pas tous les codecs en charge.</p>
<b>Qualité de compression</b>	<p>(N'est pas disponible pour tous les codecs). À l'aide du curseur, sélectionnez le niveau de compression (<b>0-100</b>) que le codec doit exécuter.</p> <p><b>0</b> signifie aucune compression, entraînant généralement une haute qualité d'image et une taille de fichier importante. <b>100</b> signifie compression maximum, entraînant généralement une faible qualité d'image et une petite taille de fichier.</p> <p>Si le curseur n'est pas accessible, la qualité de compression est intégralement déterminée par le codec sélectionné.</p>



Nom	Description
<b>Image-clé toutes les</b>	<p>(N'est pas disponible pour tous les codecs). Si vous souhaitez utiliser les images-clés, cochez la case et spécifiez le nombre requis d'images entre les images-clés.</p> <p>Une image-clé est une seule image stockée à intervalles définis. L'image-clé contient l'intégralité de la vue de la caméra, alors que les images suivantes ne contiennent que les pixels qui changent. Cela permet de réduire considérablement la taille des fichiers.</p> <p>Si la case à cocher n'est pas accessible, ou non sélectionnée, chaque image contient l'intégralité de la vue de la caméra.</p>
<b>Débit</b>	<p>(N'est pas disponible pour tous les codecs). Si vous souhaitez utiliser un débit spécifique, cochez la case et spécifiez le nombre de kilooctets par seconde requis.</p> <p>Le débit indique la taille du fichier AVI joint.</p> <p>Si la case à cocher n'est pas accessible, ou non sélectionnée, le débit est déterminé par le codec sélectionné.</p>

## Onglet Réseau (options)

L'onglet **Réseau** vous permet de préciser les adresses IP des clients locaux si les clients doivent se connecter au serveur d'enregistrement via Internet. Le système de surveillance les reconnaît comme venant du réseau local.

Vous pouvez également préciser la version IP du système : IPv4 ou IPv6. La valeur par défaut est IPv4.

## Onglet Signet (options)



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

L'onglet **Signets** vous permet de préciser les paramètres des signets, leur ID et leur fonction dans XProtect Smart Client.

Nom	Description
<b>Préfixe d'ID de</b>	Indiquez un préfixe pour tous les signets créés par les utilisateurs de XProtect Smart

Nom	Description
signet	Client.
Durée du signet par défaut	Indiquez le début et la fin par défaut d'un signet défini dans XProtect Smart Client. Ce paramètre doit être aligné avec : <ul style="list-style-type: none"> <li>• Pour la règle de signet par défaut, voir Règles sur la page 338</li> <li>• La période pré-enregistrement pour chaque caméra, voir Périphériques prenant la mise en mémoire-tampon préalable en charge sur la page 240</li> </ul>

Pour indiquer les droits de signet d'un rôle, voir Onglet Périphériques (rôles) sur la page 405.

### Onglet Paramètres utilisateur (options)

L'onglet **Paramètres utilisateur** vous permet de préciser les paramètres de préférence, par exemple le fait d'afficher un message lorsque l'enregistrement à distance est activé.

### Onglet Customer dashboard (Tableau de bord client)

Dans l'onglet **Tableau de bord client**, vous pouvez activer ou désactiver Milestone Customer Dashboard.

Le tableau de bord client est un service de surveillance en ligne qui fournit une représentation graphique de l'état actuel de votre système, y compris d'éventuels problèmes techniques, comme les défaillances de la caméra, aux administrateurs système ou à d'autres personnes qui ont eu accès aux informations sur l'installation de votre système.

Vous pouvez cocher ou décocher la case pour modifier les paramètres du tableau de bord client.

### Onglet Protection des preuves (options)



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

Dans l'onglet **Protection des preuves** vous définissez et modifiez les profils de protection des preuves et la durée que vos utilisateurs du client peuvent choisir pour conserver les données protégées.

Nom	Description
<b>Profils de verrouillage des preuves</b>	<p>Une liste de profils de protection des preuves définis.</p> <p>Vous pouvez ajouter et supprimer des profils de protection des preuves existants. Vous ne pouvez pas supprimer le profil de protection des preuves par défaut, mais vous pouvez modifier ses options de durée et son nom.</p>
<b>Options de durée de verrouillage</b>	<p>La durée que les utilisateurs du client peuvent choisir pour la protection des preuves.</p> <p>Les options de durée disponibles sont : heure(s), jour(s), semaine(s), mois(s), année(s), indéterminés ou définis par l'utilisateur.</p>

Pour indiquer les droits d'accès à la protection des preuves d'un rôle, voir l'Onglet Périphériques (rôles) sur la page 405) pour les paramètres de rôle.

## Onglet Messages audio (options)

L'onglet **Messages audio** vous permet de charger des fichiers contenant des messages audio utilisés pour la diffusion des messages, déclenchés par des règles.

Le nombre maximum de fichiers chargés s'élève à 50 et la taille maximale autorisée pour chaque fichier est égale à 1 Mo.

Nom	Description
<b>Nom</b>	Indique le nom du message. Vous saisissez le nom lorsque vous ajoutez un message. Pour charger un message dans le système, cliquez sur <b>Ajouter</b> .
<b>Description</b>	<p>Indique une description du message.</p> <p>Vous saisissez la description lorsque vous ajoutez un message. Vous pouvez utiliser le champ de description pour décrire le but ou le message proprement dit.</p>
<b>Ajouter</b>	<p>Permet de charger des messages audio dans le système.</p> <p>Les formats pris en charge sont les formats de fichier audio Windows standard :</p> <ul style="list-style-type: none"> <li>• .wav</li> <li>• .wma</li> </ul>

Nom	Description
	<ul style="list-style-type: none"> <li>.flac</li> </ul>
<b>Modifier</b>	Permet de modifier le nom et la description ou de remplacer le fichier proprement dit.
<b>Supprimer</b>	Permet de supprimer le message audio de la liste.
<b>Lire</b>	Cliquez sur ce bouton pour écouter le message sur l'ordinateur qui exécute le Management Client.

Pour créer une règle qui déclenche la lecture des messages audio, voir Règles sur la page 338.

Pour en savoir plus au sujet des actions en général que vous pouvez utiliser dans les règles, voir Actions et actions d'arrêt (explications) sur la page 314.

## Onglet Paramètres de contrôle d'accès (options)



L'utilisation de XProtect Access nécessite l'achat d'une licence de base qui vous permet d'accéder à cette fonctionnalité.

Nom	Description
<b>Afficher le volet des propriétés de développement</b>	<p>Si elles sont sélectionnées, les informations de développeur supplémentaire apparaissent pour <b>Contrôle d'accès &gt; Paramètres généraux</b>.</p> <p>Ce paramètre est uniquement destiné aux développeurs d'intégrations de systèmes de contrôle d'accès.</p>

## Onglet Événements analytiques (options)



L'onglet **Événements analytiques** vous permet d'activer et de spécifier la fonction d'événements analytiques.

Nom	Description
<b>Activer</b>	Spécifiez si vous souhaitez utiliser les événements analytiques. Par défaut, la fonction est désactivée.
<b>Port</b>	Indiquez le port utilisé par cette fonction. Port par défaut : 9090.  Veillez à ce que les fournisseurs de l'outil VCA concernés utilisent également ce numéro de port. Si vous modifiez le numéro de port, rappelez-vous d'également modifier le numéro de port des fournisseurs.
<b>Toutes les adresses du réseau ou Adresses réseau spécifiée</b>	Indiquez si l'autorisation porte sur les événements de toutes les adresses IP ou/et noms d'hôtes ou seulement sur les événements des adresses IP ou/et noms d'hôte spécifiés dans la <b>liste des adresses</b> (voir ci-dessous).
<b>Liste des adresses</b>	Saisissez une liste des adresses IP ou noms d'hôte de confiance. La liste filtre les données entrantes de sorte que seuls les événements de certaines adresses IP ou noms d'hôtes soient autorisés. Vous pouvez utiliser les deux formats d'adresse pour le système de nom de domaine (DNS), IPv4 et IPv6.  Vous pouvez ajouter des adresses à votre liste en entrant manuellement chaque adresse IP ou nom d'hôte, ou en important une liste d'adresses externe. <ul style="list-style-type: none"> <li>• <b>Saisie manuelle</b> : Saisissez l'adresse IP ou le nom d'hôte dans la liste d'adresses. Répétez l'opération pour chaque adresse désirée</li> <li>• <b>Importer</b> : Cliquez sur le bouton <b>Importer</b> pour parcourir la liste d'adresses externe. La liste externe doit être un fichier .txt et chaque adresse IP ou nom d'hôte doit être sur une ligne séparée</li> </ul>

## Onglet Alarmes et événements (Options)

Dans l'onglet **Alarmes et événements**, vous pouvez spécifier les paramètres des alarmes, des événements et des journaux. Également en lien avec ces paramètres, voir Taille limite de la base de données sur la page 53.

Nom	Description
<p><b>Désactiver les alarmes pendant</b></p>	<p>Indiquez le nombre de jours pour le stockage des alarmes avec l'état <b>Fermé</b> dans la base de données. Si vous définissez la valeur sur <b>0</b>, l'alarme est supprimée après avoir été fermée.</p> <div data-bbox="419 454 1385 960" style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;"> <p> Des horodateurs sont toujours associés aux alarmes. Si l'alarme est déclenchée par une caméra, l'horodateur dispose d'une image de l'heure de la caméra. Les informations sur l'alarme elle-même sont stockées sur le serveur d'événements, alors que les enregistrements vidéo correspondant à l'image attachée sont sauvegardés sur le serveur du système de surveillance concerné.</p> <p>Pour voir les images de vos alarmes, conservez les enregistrements vidéo pendant une durée au moins égale à celle pendant laquelle vous souhaitez conserver les alarmes sur le serveur d'événements.</p> </div>
<p><b>Activer toutes les autres alarmes pendant</b></p>	<p>Indiquez le nombre de jour permettant de stocker des alarmes avec l'état <b>Nouveau, En cours</b> ou <b>En attente</b>. Si vous définissez la valeur sur 0, l'alarme s'affiche dans le système, mais elle ne sera pas mémorisée.</p> <div data-bbox="419 1137 1385 1644" style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;"> <p> Des horodateurs sont toujours associés aux alarmes. Si l'alarme est déclenchée par une caméra, l'horodateur dispose d'une image de l'heure de la caméra. Les informations sur l'alarme elle-même sont stockées sur le serveur d'événements, alors que les enregistrements vidéo correspondant à l'image attachée sont sauvegardés sur le serveur du système de surveillance concerné.</p> <p>Pour voir les images de vos alarmes, conservez les enregistrements vidéo pendant une durée au moins égale à celle pendant laquelle vous souhaitez conserver les alarmes sur le serveur d'événements.</p> </div>
<p><b>Activer les journaux pendant</b></p>	<p>Précisez le nombre de jours pour la conservation des journaux du serveur d'événements. Si vous conservez les journaux pendant des périodes plus longues, vérifiez que la machine sur laquelle est installé le serveur d'événements possède un</p>

Nom	Description
	espace disque suffisant.
<b>Activer la journalisation détaillée</b>	Pour conserver un journal plus détaillé pour la communication du serveur d'événements, cochez la case. Il sera stocké pendant le nombre de jours indiqués dans le champ <b>Conserver les journaux pendant</b> .
<b>Types d'événement</b>	<p>Indiquez le nombre de jours pour le stockage des événements dans la base de données. Il existe deux possibilités pour le faire :</p> <ul style="list-style-type: none"> <li>• Vous pouvez spécifier la durée de conservation d'un groupe d'événements entier. Les types d'événements comportant la valeur <b>Suivre le groupe</b> peuvent hériter de la valeur du groupe d'événements</li> <li>• Même si vous définissez une valeur pour un groupe d'événements, vous pouvez spécifier la durée de conservation des différents types d'événements.</li> </ul> <div data-bbox="419 875 1386 1003" style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;"> <p> Si la valeur est <b>0</b>, les événements seront pas enregistrés dans la base de données.</p> </div> <div data-bbox="419 1055 1386 1335" style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;"> <p> Les événements externes (événements définis par l'utilisateur, événements génériques et événements d'entrée) sont définis sur <b>0</b> par défaut ; par ailleurs, vous ne pouvez pas modifier cette valeur. Ces types d'événements se produisent de manière si fréquente que le fait de les stocker dans la base de données peut entraîner des problèmes au niveau de la performance.</p> </div>

## Onglet Événements génériques (options)

L'onglet **Événements génériques** vous permet de spécifier les paramètres associés aux sources de données et aux événements génériques.

Pour de plus amples informations sur la façon de configurer les événements génériques réels, voir Événements génériques sur la page 363.

Nom	Description
<b>Source de données</b>	<p>Vous pouvez choisir entre deux sources de données par défaut et définir une source de données personnalisée. Votre choix dépend du type de votre programme tiers et/ou du type de matériel ou logiciel à partir duquel vous souhaitez établir une interface :</p> <p><b>Compatible</b> : Les propriétés par défaut sont activées, écho de tous les octets, TCP et UDP, IPv4 uniquement, port 1234, aucun séparateur, hôte local uniquement, encodage de pages de codes actuel (ANSI).</p> <p><b>International</b> : Les propriétés par défaut sont activées, écho des statistiques uniquement, TCP uniquement, IPv4+6, port 1235, &lt;CR&gt;&lt;LF&gt; comme séparateur, hôte local uniquement, encodage UTF-8. (&lt;CR&gt;&lt;LF&gt; = 13,10).</p> <p>[Source de données A]</p> <p>[Source de données B]</p> <p>etc.</p>
<b>Nouveau</b>	Cliquez pour définir une nouvelle source de données.
<b>Nom</b>	Nom de la source de données.
<b>Activé</b>	Par défaut, les sources de données sont activées. Décochez la case pour désactiver la source de données.
<b>Réinitialiser</b>	Cliquez pour réinitialiser tous les paramètres de la source de données sélectionnée. Le nom saisi dans le champ <b>Nom</b> est conservé.
<b>Port</b>	Le numéro de port de la source de données.
<b>Sélecteur type de protocole</b>	<p>Les protocoles que le système doit écouter et analyser en vue de détecter les événements génériques :</p> <p><b>Tout</b> : TCP aussi bien que UDP.</p> <p><b>TCP</b> : TCP uniquement.</p> <p><b>UDP</b> : UDP uniquement.</p> <p>Les paquets TCP et UDP utilisés pour les événements génériques peuvent contenir des caractères spéciaux, tels que @, #, +, ~, etc.</p>
<b>Sélecteur</b>	Types d'adresses IP à sélectionner : IPv4, IPv6 ou les deux.



Nom	Description
type IP	
Octets de séparation	Sélectionnez les octets séparateurs utilisés pour séparer les enregistrements d'événements génériques individuels. Le type de source de données <b>International</b> par défaut (consultez <b>Sources de données</b> plus haut) est <b>13,10</b> . (13,10 = <CR><IF>).
Sélecteur type d'écho	Formats de retour d'écho disponibles : <ul style="list-style-type: none"> <li>• <b>Statistiques d'écho</b> : Renvoie le format suivant : <b>[X],[Y],[Z],[Nom de l'événement générique]</b>  <b>[X]</b> = numéro de demande.  <b>[Y]</b> = nombre de caractères.  <b>[Z]</b> = nombre de concordances avec un événement générique.  <b>[Nom de l'événement générique]</b> = nom saisi dans le champ <b>Nom</b>.</li> <li>• <b>Écho de tous les octets</b> : Produit un écho de tous les octets</li> <li>• <b>Pas d'écho</b> : Supprime tous les échos</li> </ul>
Sélecteur type d'encodage	Par défaut, la liste affiche uniquement les options les plus pertinentes. Cochez la case <b>Afficher tout</b> pour afficher tous les codages à disposition.
Adresses IPv4 externes autorisées	Spécifiez les adresses IP avec lesquelles le serveur de gestion doit pouvoir communiquer afin de gérer les événements externes. Vous pouvez également utiliser cette fonction pour exclure les adresses IP dont vous ne souhaitez pas recevoir de données.
Adresses IPv6 externes autorisées	Spécifiez les adresses IP avec lesquelles le serveur de gestion doit pouvoir communiquer afin de gérer les événements externes. Vous pouvez également utiliser cette fonction pour exclure les adresses IP dont vous ne souhaitez pas recevoir de données.

## Liste des tâches initiales de configuration

La liste de contrôle ci-dessous répertorie les tâches initiales pour la configuration de votre système. Vous pouvez avoir déjà terminé certaines d'entre elles lors de l'installation.

Effectuer tous ces contrôles ne garantit pas en soi que le système soit parfaitement adapté aux besoins de votre organisation. Pour que le système soit adapté aux besoins de votre organisation, Milestone vous recommande de contrôler et d'ajuster le système de façon continue.

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

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

Étape	Description
<input checked="" type="checkbox"/>	Vous avez terminé l'installation initiale de votre système. Voir Installer un nouveau système XProtect sur la page 79.
<input checked="" type="checkbox"/>	Changer le SLC d'essai au profit d'un SLC permanent (si nécessaire). Voir Changer le code de licence du logiciel sur la page 51.
<input checked="" type="checkbox"/>	Connectez-vous au Management Client. Voir Vue d'ensemble de la connexion sur la page 115.
<input type="checkbox"/>	Vérifier que les paramètres de stockage de chaque serveur d'enregistrement répondent à vos besoins. Voir Onglet Stockage (serveur d'enregistrement) sur la page 158.
<input type="checkbox"/>	Vérifier que les paramètres d'archivage de chaque serveur d'enregistrement répondent à vos besoins. Voir Onglet Stockage (serveur d'enregistrement) sur la page 158.
<input type="checkbox"/>	Détecter les périphériques, caméras et encodeurs vidéo, qui peuvent être ajoutés à chaque serveur d'enregistrement. Voir Ajouter un matériel sur la page 199.
<input type="checkbox"/>	Configurer les caméras individuelles de chaque serveur d'enregistrement. Voir Dispositifs de caméra (explications) sur la page 218.

Étape	Description
<input type="checkbox"/>	Activer le stockage et l'archivage pour des caméras individuelles ou pour un groupe de caméras. Cette opération peut être effectuée à partir des caméras individuelles ou à partir du groupe de périphériques.  Voir Onglet Stockage (serveur d'enregistrement) sur la page 158.
<input type="checkbox"/>	Activer et configurer des périphériques.  Voir Navigation sur le site : Périphériques : Travailler avec des périphériques sur la page 217.
<input type="checkbox"/>	Les règles déterminent largement le comportement du système. Vous créez des règles pour définir à quel moment les caméras doivent enregistrer, à quel moment les caméras PTZ (pan-tilt-zoom) doivent patrouiller et à quel moment les notifications doivent être envoyées.  Créer des règles.  Voir Règles et événements (explications) sur la page 312.
<input type="checkbox"/>	Ajouter des rôles au système.  Voir Rôles (explications) sur la page 369.
<input type="checkbox"/>	Ajouter des utilisateurs ou des groupes d'utilisateurs à chacun des rôles.  Voir Assigner et supprimer des utilisateurs et groupes aux/des rôles sur la page 373.
<input type="checkbox"/>	Activer des licences.  Voir Informations sur la licence sur la page 140 ou Informations sur la licence sur la page 140.

Voir également Configuration du système dans le panneau Navigation du site sur la page 139.

## Configuration du système dans le panneau Navigation du site

Dans le panneau **Navigation du site**, vous pouvez configurer et gérer votre système pour qu'il corresponde à vos besoins. Si votre système n'est pas un système mono-site, mais qu'il comprend des sites fédérés, vous pourrez gérer ces sites sur le panneau **Hiérarchie des sites fédérés**.

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

## Navigation sur le site : Bases

Cet article décrit comment voir et gérer des licences et comment ajouter des informations sur le site.

## Informations sur la licence

Vous pouvez suivre les licences qui partagent les mêmes fichiers de licence du logiciel sur ce site et tous les autres sites, faire un suivi de vos abonnements Milestone Care et décider comment activer vos licences. Pour obtenir des informations de base à propos des différentes licences XProtect, voir Licences (explications) sur la page 50.

### Licence attribuée à

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

### Milestone Care

Vous trouverez ici des informations relatives au niveau actuel de Milestone Care™. Lors de l'achat de votre système, vous avez également pris un abonnement Milestone Care Plus de deux ans. Votre installation est toujours couverte par Milestone Care Basic qui vous donne accès à différents types de documents d'assistance autonome tels que des articles de base de connaissances, des guides et des tutoriels sur notre site Web d'assistance (<https://www.milestonesys.com/support/>). La date d'expiration de votre abonnement Milestone Care Plus est visible dans le tableau **Produits installés**. Si vous décidez d'acheter ou de renouveler un abonnement Milestone Care après l'installation de votre système, vous devrez activer vos licences pour que les bonnes informations Milestone Care apparaissent.

Un abonnement Milestone Care Plus vous donne accès à des mises à jour. Vous avez également accès au service Customer dashboard (Tableau de bord client), à la fonction Smart Connect et à toutes les notifications push. Si vous disposez d'un abonnement Milestone Care Premium, vous pouvez également contacter l'assistance Milestone pour demander de l'aide. Lorsque vous contactez l'assistance Milestone, n'oubliez pas de préciser les informations concernant votre identifiant Milestone Care. La date d'expiration de votre abonnement Milestone Care Premium est visible. Pour en savoir plus sur Milestone Care, suivez les liens.

### Produits installés

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

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



Certaines licences, telles que XProtect Essential+, sont installées au moyen d'une activation automatique des licences autorisée, et il est impossible de désactiver ce paramètre.

**Installed Products**

Product Version	Software License Code	Expiration Date	Milestone Care Plus	Milestone Care Premium
XProtect Corporate 2016	M01-C01-100-01-BC4288	Unlimited	01-10-2016	01-10-2016
Milestone XProtect Smart Wall	M01-P03-023-01-BC4284	Unlimited	Unlimited	
Milestone XProtect Access 2016 v10.0a	M01-P01-011-01-BC428F	Unlimited	Unlimited	
Milestone XProtect Transact 2016	M01-P08-100-01-BC42E1	Unlimited	Unlimited	

**Vue d'ensemble des licences - Tous les sites**

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

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

**License Overview - All sites**[License Details - All Sites...](#)

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

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

**Détails de la licence - Site actuel**

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

Vous pouvez également afficher le nombre de changements apportés aux périphériques sans activation utilisés (voir Changements apportés aux périphériques sans activation (explications) sur la page 142) et combien vous en possédez par an dans la colonne **Changements sans activation**.

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

Si vous oubliez d'activer les licences avant la fin de la période de grâce, vous ne recevrez plus de vidéo dans le système. Ces licences s'affichent dans la colonne **Période de grâce expirée**. Voir Activer des licences après la période de grâce sur la page 146 pour de plus amples informations.

Si vous utilisez plus de licences que vous ne possédez, elles s'afficheront dans la colonne **Sans licence** et vous ne pourrez pas les utiliser dans votre système. Pour plus d'informations, voir Obtenir des licences supplémentaires sur la page 147.

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

#### License Details - Current Site: SYS TESTS VM

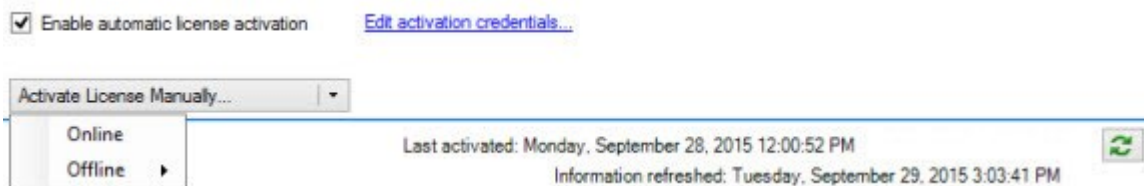
License Type	Activated	Changes without activation	In Grace Period	Grace Period Expired	Without License
Hardware Device	32	0 out of 10	0	0	0
Milestone Interconnect Camera	11	N/A	0	0	0
Access control door	9	N/A	0	0	0
Transaction source	1	N/A	0	0	0

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

### Fonctions pour activer les licences

Sous les trois tableaux, vous trouverez :

- Une case à cocher pour activer l'activation automatique des licences et un lien pour modifier les identifiants utilisateur pour l'activation automatique. Pour plus d'informations, voir Activation automatique des licences (explications) sur la page 144 et Activer l'activation automatique des licences sur la page 145. Si l'activation automatique échoue, un message apparaîtra en rouge. Pour plus d'information, veuillez cliquer sur le lien **Détails**
- Liste déroulante pour activer manuellement les licences en ligne ou hors ligne. Pour plus d'informations, voir Activation des licences en ligne sur la page 145 et Activation des licences hors ligne sur la page 146
- Dans le coin en bas à gauche, vous pouvez voir la date de la dernière activation de vos licences (automatique ou manuelle) et la date d'actualisation des informations de la page. Les données d'horodatage proviennent du serveur et non pas de l'ordinateur local



### Changements apportés aux périphériques sans activation (explications)

Sur la page **Bases > Renseignements sur la licence**, la colonne **Changements sans activation** affiche le nombre de périphériques pouvant être remplacés ou ajoutés sans avoir à activer la licence et le nombre de changements apportés depuis la dernière activation. Les périphériques ajoutés dans le cadre de vos changements sans activation fonctionnent comme avec des licences entièrement activées.

Un an après la dernière activation de votre licence, le nombre de **changements apportés aux périphériques sans activation** est automatiquement remis à zéro. Après cette remise à zéro, vous pouvez continuer d'ajouter et remplacer des périphériques sans en activer les licences.

Le nombre de changements apportés aux périphériques sans activation varie d'une installation à l'autre et est calculé d'après plusieurs variables. Pour une description plus détaillée, voir Informations sur la licence sur la page 140.

Si votre système de surveillance reste hors ligne pendant des périodes prolongées, par exemple à bord d'un bateau en croisière ou dans un endroit reculé sans accès à internet, vous pouvez contacter votre revendeur Milestone et lui demander un nombre plus élevé de changements apportés aux périphériques sans activation.

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

### Calcul du nombre de changements apportés aux périphériques sans activation

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

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

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

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

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

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

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

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

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

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

Un client achète 115 licences de périphériques. Il ajoute 100 caméras à son système et active ses licences. Il dispose désormais de 15 changements sans activation. Il ajoute 15 caméras de plus sans les activer et utilise la totalité des 15 sur 15 changements sans activation. Il supprime 50 caméras du système et le nombre de changements sans activation passe à 7. Cela signifie que 8 de ses caméras ajoutées dans le cadre des 15 changements sans activation passent en période de grâce. Le client ajoute alors 50 nouvelles caméras. Vu que le client a activé 100 caméras sur son système lors de l'activation de ses licences, le nombre de changements sans activation repasse à 15 et les 8 caméras en période de grâce sont à nouveau considérées comme des changements sans activation. Les 50 nouvelles caméras passent en période de grâce.

### Afficher la vue d'ensemble des licences

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

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

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

### Activation automatique des licences (explications)

Pour une maintenance plus aisée et une meilleure flexibilité, Milestone vous recommande d'activer l'activation automatique des licences (voir Activer l'activation automatique des licences sur la page 145) pour vous faciliter la tâche. L'activation automatique des licences nécessite la mise en ligne du serveur de gestion.

Une fois ces conditions préalables remplies, le système active vos périphériques ou autres licences quelques minutes après l'ajout, la suppression ou le remplacement des périphériques, ou toute autre modification ayant affecté l'utilisation de vos licences. Ainsi, vous n'avez jamais besoin de lancer une activation des licences manuellement. Le nombre de changements de périphériques utilisés sans activation est toujours égal à zéro. Aucun de vos périphériques ne se trouvera en période d'évaluation, avec des licences risquant d'expirer. Par mesure de précaution, si l'une de vos licences de base expire au bout de 14 jours, votre système XProtect tentera automatiquement d'activer votre licence toutes les nuits.

Vos licences ne doivent être activées manuellement que dans les cas suivants :



- Acheter des licences supplémentaires (voir Obtenir des licences supplémentaires sur la page 147)
- Réalisation d'une mise à niveau (voir Conditions préalables de mise à niveau sur la page 523)
- Acheter ou renouveler un abonnement Milestone Care (voir Activation automatique des licences (explications))
- Réception d'une indemnité pour davantage de changements apportés aux périphériques sans activation (voir Changements apportés aux périphériques sans activation (explications) sur la page 142)

### Activer l'activation automatique des licences

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

Les identifiants sont enregistrés dans un fichier sur le serveur de gestion.
3. Cliquez sur **OK**.

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

### Désactiver l'activation automatique des licences

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

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

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

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

### Activation des licences en ligne

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

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

Si vous recevez un message d'erreur pendant l'activation en ligne, suivez les instructions à l'écran pour résoudre le problème ou contactez l'assistance Milestone.

### Activation des licences hors ligne

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

1. Sur le nœud **Renseignements sur la licence**, sélectionnez **Activer votre licence manuellement > Hors ligne > Exporter une licence pour activation** pour exporter un fichier de demande de licence (.lrg) contenant des informations sur vos périphériques ajoutés.
2. Le nom du fichier de demande de licence (.lrg) est le même que votre SLC. Si vous disposez de plusieurs sites, n'oubliez pas de choisir un nom unique de façon à pouvoir identifier facilement le fichier appartenant à chaque site.
3. Copiez le fichier de demande de licence sur un ordinateur avec connexion Internet et connectez-vous à notre site Internet (<https://online.milestonesys.com/>) pour obtenir le fichier de licence logicielle activé (.lic).
4. Copiez sur votre ordinateur le fichier .lic avec le même nom que votre fichier de demande de licence avec Management Client.
5. Dans le Management Client, sur la page **Renseignements sur la licence**, sélectionnez **Activer licence hors ligne > Importer une licence activée**, et sélectionnez le fichier de licence logicielle activé pour l'importer et ainsi activer vos licences.
6. Cliquez sur **Terminer** pour conclure le processus d'activation.

### Activer des licences après la période de grâce

Si vous n'activez pas une licence au cours de la période d'évaluation (licences de périphérique, de caméra Milestone Interconnect ou de porte), le périphérique devient indisponible et ne peut pas être utilisé dans le système de surveillance :

- La configuration de la caméra et des autres paramètres ne sont pas supprimés du Management Client
- La licence n'est pas supprimée de la configuration système
- Pour réactiver les périphériques indisponibles, activez les licences comme à l'accoutumée. Pour plus d'informations, voir Activation des licences hors ligne sur la page 146 ou Activation des licences en ligne sur la page 145

### Obtenir des licences supplémentaires

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

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

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

- Il vous suffit d'activer vos licences manuellement pour accéder aux nouvelles licences. Pour plus d'informations, voir Activation des licences hors ligne sur la page 146 ou Activation des licences en ligne sur la page 145

Nouvelles licences pour une version mise à niveau du système de surveillance :

- Vous recevrez un fichier de licence logicielle mis à jour (**.lic**) (voir Licences (explications) sur la page 50) avec de nouvelles licences et une nouvelle version. Vous devez utiliser le nouveau fichier de licence logicielle au cours de l'installation de la nouvelle version. Pour plus d'informations, voir Conditions préalables de mise à niveau sur la page 523

### Licences et remplacement de périphériques matériels

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

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

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

Si vous remplacez un périphérique par un modèle différent, vous devez utiliser l'assistant **Remplacer le matériel** (voir Remplacer le matériel sur la page 504) pour cartographier toutes les bases de données pertinentes des caméras, microphones, entrées, sorties et paramètres.

Si vous avez activé l'activation automatique des licences (voir Activer l'activation automatique des licences sur la page 145), le nouveau périphérique sera automatiquement activé.

Si vous avez utilisé tous vos changements apportés aux périphériques sans activation (voir Changements apportés aux périphériques sans activation (explications) sur la page 142), vous devrez activer manuellement vos licences. Pour plus d'informations à propos de l'activation des licences, voir Activation des licences hors ligne sur la page 146 ou Activation des licences en ligne sur la page 145.

## Renseignements sur le site

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

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

### Modifier les informations concernant le site

Pour mettre à jour les renseignements sur le site :

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

## Navigation sur le site : Serveurs et matériel

Cette section décrit comment installer et configurer les serveurs d'enregistrement et les serveurs d'enregistrement de redondance. Vous apprendrez également comment ajouter un nouveau matériel au système et l'interconnecter à d'autres sites.

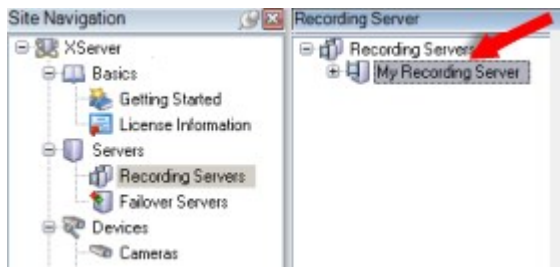
- Navigation sur le site : Serveurs et matériel : Serveurs d'enregistrement sur la page 149
- Navigation sur le site : Serveurs et matériel : Serveurs de redondance sur la page 185
- Navigation sur le site : Serveurs et matériel : Matériel sur la page 199
- Navigation sur le site : Serveurs et matériel : Gérer les serveurs distants sur la page 214

## Navigation sur le site : Serveurs et matériel : Serveurs d'enregistrement

### Serveurs d'enregistrement (explications)

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

Les serveurs d'enregistrement sont des ordinateurs où vous avez installé le programme Recording Server, et où vous l'avez configuré pour communiquer avec le serveur de gestion. Vous pouvez consulter vos serveurs d'enregistrement dans le volet **Vue d'ensemble** lorsque vous développez le dossier **Serveurs** et sélectionnez **Serveurs d'enregistrement**.



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

Le serveur d'enregistrement supporte un cryptage des flux de données vers les clients et services. Pour plus d'informations, voir Avant de commencer l'installation sur la page 59 :

- Activer le cryptage pour les clients et les serveurs sur la page 451
- Voir le status du cryptage vers les clients sur la page 154

Le serveur d'enregistrement prend également en charge le cryptage de la connexion avec le serveur de gestion. Pour plus d'informations, voir Avant de commencer l'installation sur la page 59 :

- Activer le cryptage sur la page 448
- Activer le cryptage du serveur pour les serveurs d'enregistrement ou les serveurs distants sur la page 449

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

- Ajouter un matériel sur la page 199
- Déplacer le matériel sur la page 500
- Supprimer tous les périphériques matériels sur un serveur d'enregistrement sur la page 519

- Supprimer un serveur d'enregistrement sur la page 519



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

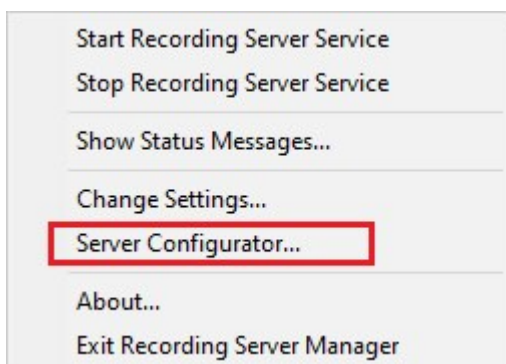
## Enregistrer un serveur d'enregistrement

Lors de l'installation d'un serveur d'enregistrement, cet enregistrement est automatiquement accordé la plupart du temps. Toutefois, vous avez besoin de procéder à l'enregistrement manuellement, si :

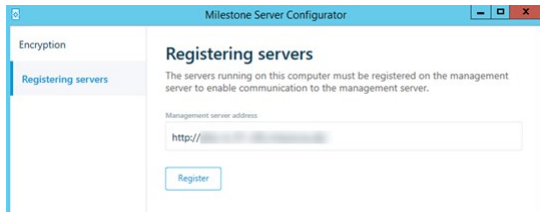
- Vous avez remplacé un serveur d'enregistrement
- Le serveur d'enregistrement a été installé hors ligne, puis ajouté par la suite au serveur de gestion
- Votre serveur de gestion n'utilise pas les ports par défaut. Les numéros de ports dépendent de la configuration du cryptage. Pour plus d'informations, voir Ports utilisés par le système sur la page 33
- Un enregistrement automatique a échoué, par exemple, après avoir changé l'adresser du serveur de gestion ou bien après avoir activé ou désactivé les paramètres du cryptage des communications

Lorsque vous enregistrez un serveur d'enregistrement, vous le configurez pour qu'il se connecte à votre serveur de gestion. La partie du serveur de gestion qui prend en charge l'enregistrement est le service Authorization Server.

1. Ouvrez le Server Configurator depuis le menu Démarrer de Windows ou depuis l'icône de la barre des tâches du serveur d'enregistrement.



2. Dans le Server Configurator, sélectionnez **Enregistrement des serveurs**.



3. Vérifiez l'adresse du serveur de gestion et le modèle (http ou https) que vous souhaitez connecter aux serveurs de l'ordinateur, puis cliquez sur **Enregistrer**.

Un message de confirmation s'affiche, indiquant le succès de l'enregistrement sur le serveur de gestion.

Voir également Remplacer un serveur d'enregistrement sur la page 499.

## Changer ou vérifier la configuration de base du serveur d'enregistrement

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

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

1. Sur l'ordinateur hébergeant le serveur d'enregistrement, cliquez sur l'icône **Serveur d'enregistrement** avec le bouton droit de votre souris dans la zone de notification.
2. Sélectionnez **Arrêter le service Recording Server**.

3. Cliquez avec le bouton droit à nouveau sur l'icône **Serveur d'enregistrement** et sélectionnez **Modifier les paramètres**.

La fenêtre **Paramètres du serveur d'enregistrement** s'affiche.

4. Vérifiez ou changez, par exemple, les paramètres suivants :
  - **Serveur de gestion : Adresse** : Spécifiez l'adresse IP ou le nom d'hôte du serveur de gestion auquel le serveur d'enregistrement devrait être connecté.
  - **Serveur de gestion : Port** : Spécifiez le numéro de port à utiliser lors de la communication avec le serveur de gestion. Vous pouvez le modifier si nécessaire, mais le numéro de port doit toujours correspondre au numéro de port configuré sur le serveur de gestion. Voir Ports utilisés par le système sur la page 33.
  - **Serveur d'enregistrement : Port du serveur Web** : Spécifiez le numéro de port à utiliser lors de la communication avec le serveur Web du serveur d'enregistrement. Voir Ports utilisés par le système sur la page 33.
  - **Serveur d'enregistrement : Port du serveur d'alerte** : Activez et spécifiez le numéro de port à utiliser lors de la communication avec le serveur d'alerte du serveur d'enregistrement, qui détecte les messages d'événements des périphériques. Voir Ports utilisés par le système sur la page 33.
  - **Serveur SMTP : Port** : Activez ou spécifiez le numéro de port à utiliser lors de la communication avec le service Simple Mail Transfer Protocol (SMTP) du serveur d'enregistrement. Voir Ports utilisés par le système sur la page 33.



5. Cliquez sur **OK**.
6. Pour redémarrer le service Recording Server, cliquez sur l'icône **Serveur d'enregistrement** avec le bouton droit de la souris et sélectionnez **Démarrer le service Recording Server**.



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

## Fenêtre Paramètres du serveur d'enregistrement

Lorsque vous effectuez un clic droit sur l'icône Recording Server Manager de la barre d'état et que vous sélectionnez **Modifier les paramètres**, vous pouvez spécifier ce qui suit :

Nom	Description
<b>Adresse</b>	Adresse IP (exemple : 123.123.123.123) ou nom d'hôte (exemple : notreserveur) du serveur de gestion auquel le serveur d'enregistrement devrait être connecté. Cette information est nécessaire pour assurer la communication entre le serveur d'enregistrement et le serveur de gestion.
<b>Port</b>	Numéro de port à utiliser lors de la communication avec le serveur de gestion. Le port par défaut est 9000. Vous pouvez le modifier si nécessaire.
<b>Port du serveur Web</b>	Numéro de port à utiliser pour gérer les demandes du serveur Web, par exemple, pour gérer les commandes de contrôles des caméra PTZ et pour gérer les recherches et les demandes en direct depuis XProtect Smart Client. Le port par défaut est 7563. Vous pouvez le modifier si nécessaire.
<b>Port du serveur d'alerte</b>	Numéro de port à utiliser lorsque le serveur d'enregistrement détecte des données TCP (certains périphériques utilisent un port TCP pour envoyer des messages d'événements). Le port par défaut est 5432 (désactivé par défaut). Vous pouvez le modifier si nécessaire.
<b>Port du serveur SMTP</b>	Numéro de port à utiliser lorsque le serveur d'enregistrement détecte des informations du Simple Mail Transfer Protocol (SMTP). SMTP est la norme utilisée par les serveurs pour s'envoyer des messages par e-mail. Certains périphériques utilisent le SMTP pour envoyer des messages d'événements ou des images au serveur du système de surveillance via des e-mails. Le port par défaut est 25, que vous pouvez activer ou

Nom	Description
	désactiver. Vous pouvez modifier le numéro de port si nécessaire.
<b>Crypter les connexions du serveur de gestion au serveur d'enregistrement</b>	<p>Avant d'activer le cryptage et de sélectionner le certificat d'authentification du serveur dans la liste, assurez-vous d'activer en premier le cryptage sur le serveur de gestion et que le certificat du serveur de gestion est de confiance sur le serveur d'enregistrement.</p> <p>Pour plus d'informations, voir Avant de commencer l'installation sur la page 59</p>
<b>Crypter les connexions des clients et services transférant des données</b>	<p>Avant d'activer le cryptage et de sélectionner un certificat d'authentification du serveur de la liste, assurez-vous que le certificat est de confiance sur tous les ordinateurs exécutant les services qui collectent les flux de données depuis le serveur d'enregistrement.</p> <p>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.</p> <p>Pour plus d'informations, voir Avant de commencer l'installation sur la page 59.</p> <p>Pour vérifier si le serveur d'enregistrement utilise le cryptage, voir Voir le status du cryptage vers les clients sur la page 154.</p>
<b>Détails</b>	Lire les informations de la Windows Certificate Store sur le certificat sélectionné.

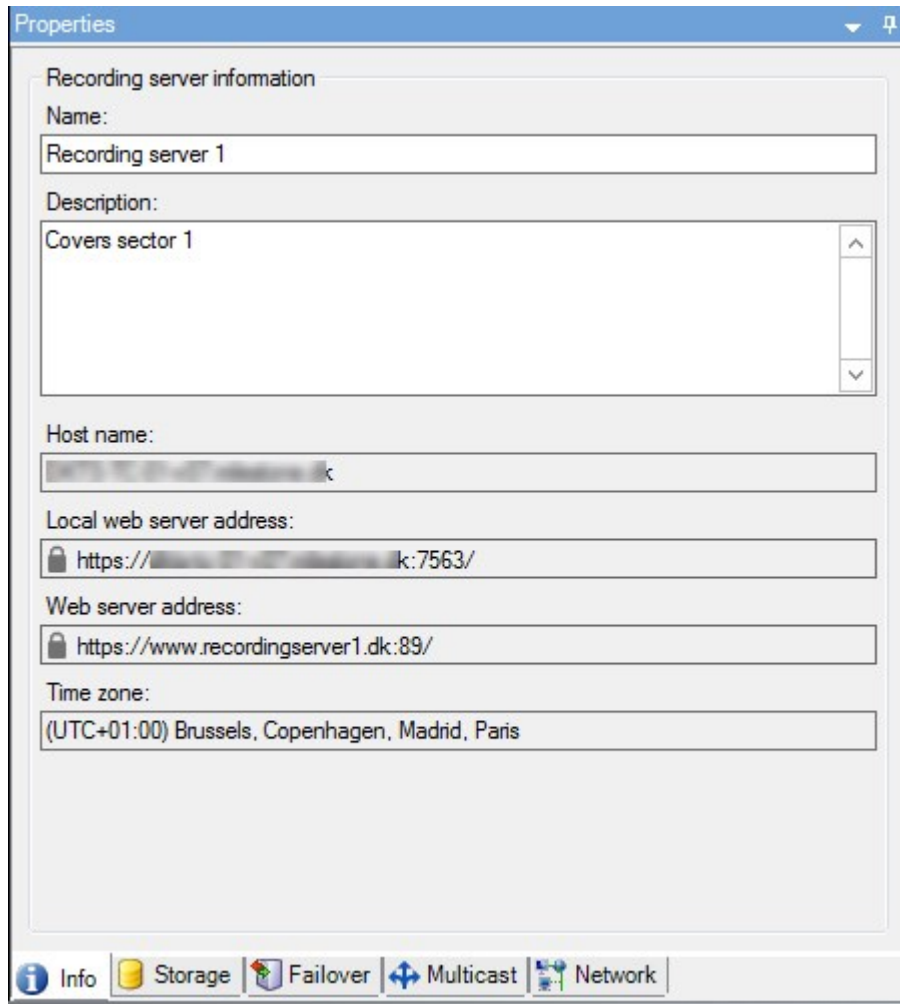
## Voir le status du cryptage vers les clients

Pour vérifier si votre serveur d'enregistrement crypte les connexions :

1. Ouvrez le Management Client.
2. Dans le panneau **Navigation du site**, sélectionnez **Serveurs > Serveurs d'enregistrement**. Cette commande ouvre une liste de serveurs d'enregistrement.






3. Dans le volet **Vue d'ensemble**, sélectionnez le serveur d'enregistrement concerné, puis allez sur l'onglet **Info**.

Si le cryptage est activé vers les clients et serveurs récupérant des flux de données depuis le serveur d'enregistrement, une icône représentant un cadenas apparaîtra devant l'adresse du serveur Web local et l'adresse du serveur Web optionnel.



## Icônes d'état du serveur d'enregistrement

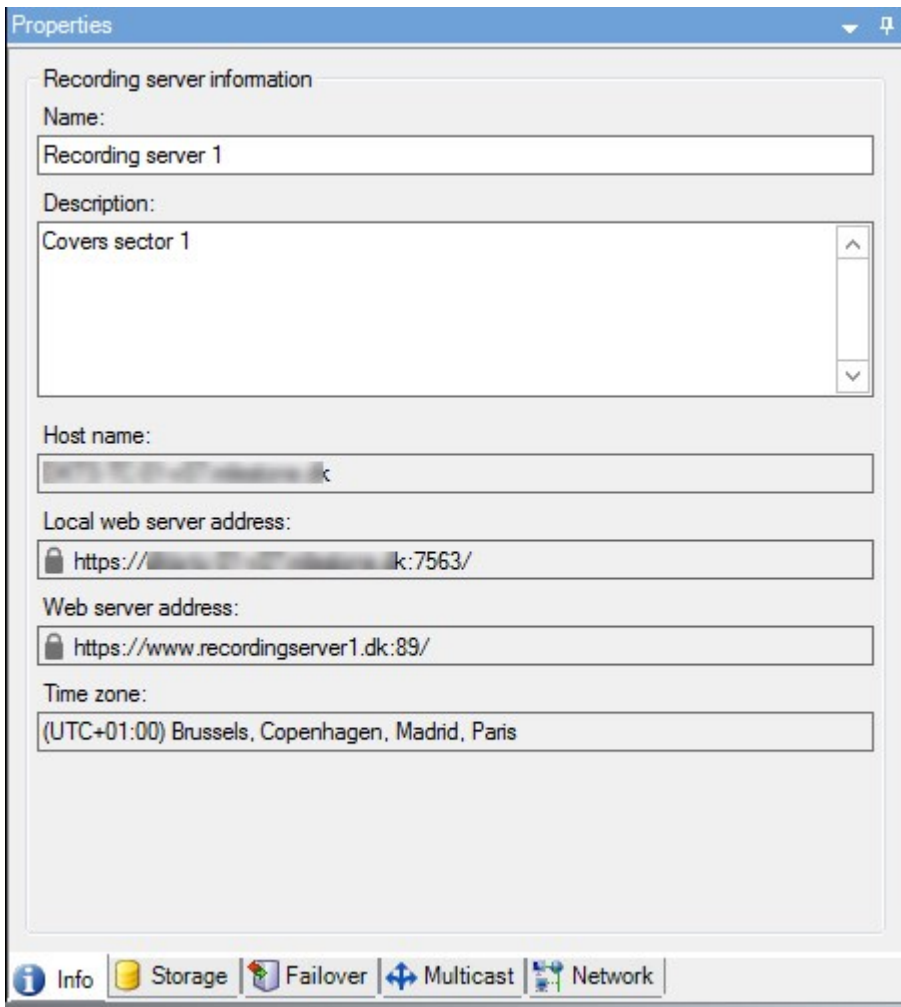
Management Client utilise les icônes suivantes pour indiquer l'état des serveurs d'enregistrement individuels :

Icône	Description
	<p><b>Le serveur d'enregistrement est en cours de fonctionnement</b></p>
	<p><b>Le serveur d'enregistrement requiert votre attention</b> : Soit le serveur d'enregistrement ne fonctionne pas, soit il fonctionne avec des erreurs.</p> <ol style="list-style-type: none"> <li>1. Passez la souris sur le serveur d'enregistrement pour voir le message d'état.</li> <li>2. Si vous devez redémarrer ou arrêter le serveur d'enregistrement, cliquez droit sur l'icône du Recording Server Manager dans la barre d'état.</li> </ol>
	<p><b>Réparation de la base de données en cours</b> : S'affiche lorsque les bases de données sont corrompues, par exemple en raison d'une panne de courant, et que le serveur d'enregistrement les répare. Le processus de réparation peut prendre un certain temps si les bases de données sont de grande taille.</p> <p>Reportez-vous à la section Protection des bases de données d'enregistrement contre la corruption sur la page 57 pour savoir comment éviter les bases de données corrompues.</p> <div data-bbox="280 936 1385 1106" style="background-color: #f9e79f; padding: 10px; border: 1px solid #ccc;"> <p> Pendant la réparation d'une base de données au démarrage, vous ne pouvez pas enregistrer une vidéo à partir des caméras connectées au serveur d'enregistrement. Seul le visionnage en direct est disponible.</p> </div> <div data-bbox="280 1155 1385 1283" style="background-color: #d9e1f2; padding: 10px; border: 1px solid #ccc;"> <p> Une réparation de base de données pendant le fonctionnement normal n'affecte pas les enregistrements.</p> </div>

## Onglet Info (serveur d'enregistrement)

Dans l'onglet **Info**, vous pouvez vérifier ou éditer le nom et la description du serveur d'enregistrement.

Vous pouvez voir le nom d'hôte et les adresses. L'icône en forme de cadenas située devant l'adresse du serveur Web indique que la communication est cryptée entre les clients et les services récupérant les flux de données depuis ce serveur d'enregistrement.



### Info Propriétés de l'onglet Serveur d'enregistrement

Nom	Description
<b>Nom</b>	<p>Vous pouvez choisir d'entrer un nom pour le serveur d'enregistrement. Le nom est utilisé partout où le périphérique apparaît dans une liste sur le système et les clients. Le nom ne doit pas nécessairement être unique.</p> <p>Lorsque vous renommez un serveur d'enregistrement, son nom est modifié de manière globale dans le Management Client.</p>
<b>Description</b>	<p>Vous pouvez choisir d'entrer une description qui apparaît dans plusieurs listes au sein du</p>

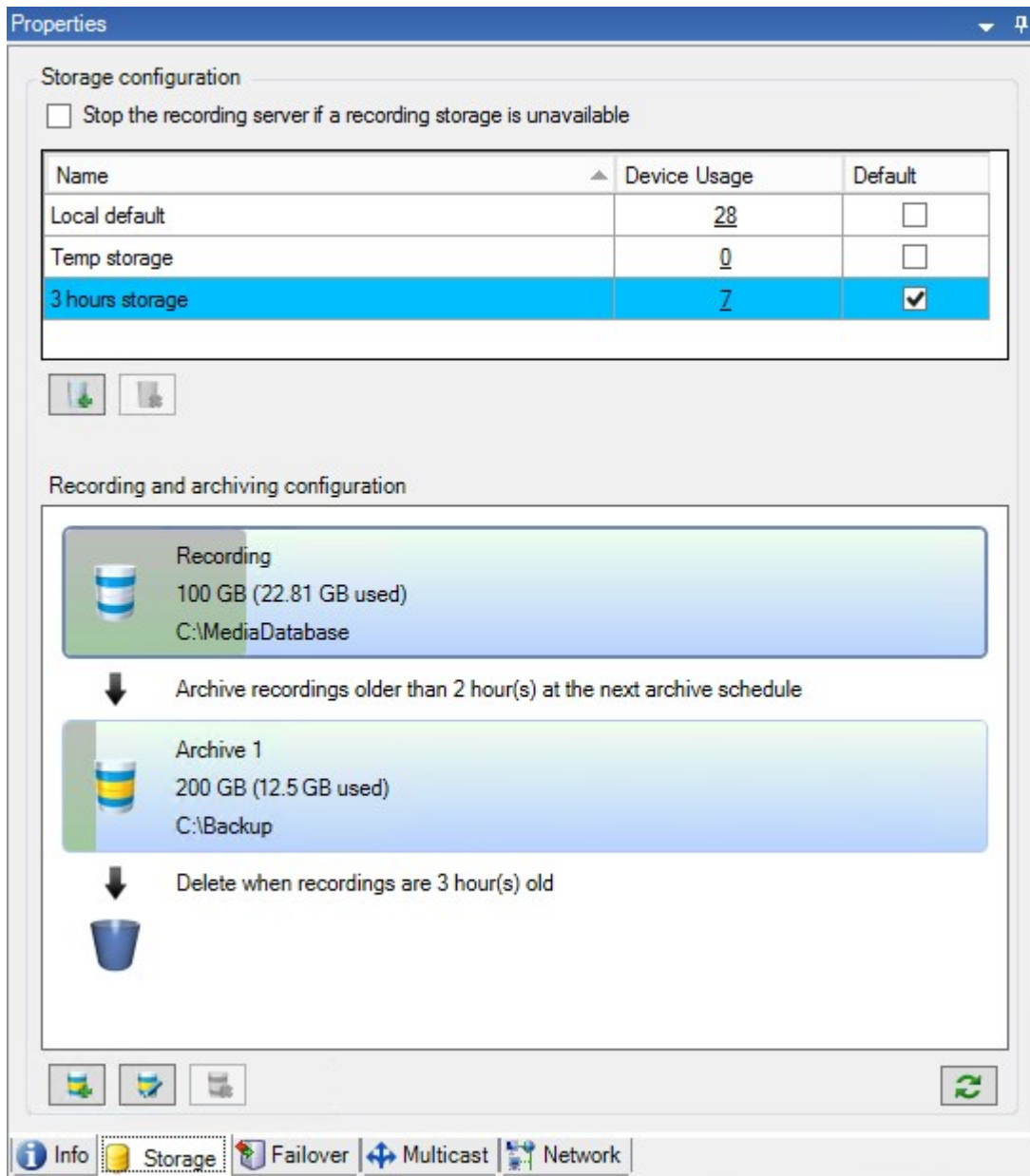
Nom	Description
	système. Il n'est pas obligatoire de saisir une description.
<b>Nom de l'hôte</b>	Affiche le nom de l'hôte du serveur d'enregistrement.
<b>Adresse locale du serveur Web</b>	<p>Affiche l'adresse locale du serveur Web du serveur d'enregistrement de redondance. Vous utilisez l'adresse locale, par exemple, pour gérer les commandes de contrôle des caméras PTZ, et pour gérer les recherches et les demandes en direct depuis XProtect Smart Client.</p> <p>L'adresse inclue le numéro de port utilisé pour la communication du serveur Web (habituellement, le port 7563).</p> <p>Si vous activez le cryptage des clients et serveurs récupérant les flux de données du serveur d'enregistrement, une icône représentant un cadenas apparaît, ainsi qu'une adresse affichant <b>https</b> au lieu de <b>http</b>.</p>
<b>Adresse du serveur Web</b>	<p>Affiche l'adresse publique du serveur Web du serveur d'enregistrement sur Internet.</p> <p>Si votre installation utilise un pare-feu ou du routeur NAT, entrez l'adresse du pare-feu ou du routeur NAT pour que les clients qui accèdent au système de surveillance depuis Internet puissent se connecter aux serveur d'enregistrement de redondance.</p> <p>Vous spécifiez l'adresse publique et le numéro de port dans l'onglet <b>Réseau</b>.</p> <p>Si vous activez le cryptage des clients et serveurs récupérant les flux de données du serveur d'enregistrement, une icône représentant un cadenas apparaît, ainsi qu'une adresse affichant <b>https</b> au lieu de <b>http</b>.</p>
<b>Fuseau horaire</b>	Affiche le fuseau horaire sur lequel se trouve le serveur d'enregistrement.

## Onglet Stockage (serveur d'enregistrement)

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

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

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



### Stockage et archivage (explications)

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

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

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



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

Vous configurez le stockage et l'archivage sur chaque serveur d'enregistrement.

À condition que vous stockiez les enregistrements archivés localement ou sur des disques réseau accessibles, vous pouvez utiliser XProtect Smart Client pour les visualiser.

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

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



Milestone vous recommande d'utiliser un disque dur dédié pour le stockage et l'archivage d'enregistrements afin d'éviter toute mauvaise performances du disque. Lors du formatage du disque dur, il est important de changer son paramètre **Taille d'unité d'allocation** de 4 à 64 kilo-octets. Ceci permet d'améliorer de façon significative les performances d'enregistrement du disque dur. Vous pouvez obtenir de plus amples informations sur les tailles d'unités d'allocation sur le site web de Microsoft (<https://support.microsoft.com/help/140365/default-cluster-size-for-ntfs-fat-and-exfat>).





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



Pour les systèmes conformes aux normes FIPS 140-2 comportant des exportations et des bases de données multimédias archivées à partir des versions de VMS XProtect antérieures à 2017 R3 qui sont cryptées avec un cryptage non-conforme aux normes FIPS, il est nécessaire d'archiver les données dans un emplacement auquel il est possible d'accéder après l'activation du mode FIPS. Pour de plus amples informations sur comment configurer votre VMS XProtect pour qu'il s'exécute conformément au mode FIPS 140-2, voir la section de conformité aux normes FIPS 140-2 dans le [guide de durcissement](#).

### Relier des périphériques à un emplacement de stockage

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

#### Archivage efficace

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

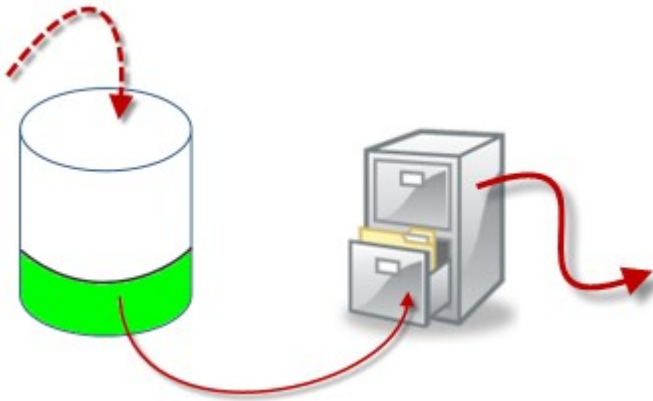
Selon vos exigences, vous pouvez configurer une ou plusieurs archives pour chacun de vos stockages. Les archives peuvent être situées soit sur l'ordinateur du serveur d'enregistrement, soit dans un autre emplacement que le système peut atteindre, comme par exemple un disque réseau.

En configurant votre archivage de manière efficace, vous pouvez optimiser vos besoins de stockage. Bien souvent, vous souhaitez minimiser la taille des enregistrements archivés afin qu'ils prennent le moins de place possible, tout spécialement à long terme où il est même possible de diminuer un peu la qualité de l'image. Vous configurerez un archivage efficace à partir de l'onglet **Stockage** d'un serveur d'enregistrement en réglant plusieurs paramètres interdépendants :

- Conservation du stockage d'enregistrements
- Taille du stockage des enregistrements
- Durée de rétention des archives
- Taille de l'archive

- Calendrier d'archivage
- Cryptage
- Images par seconde (Frames per second - FPS).

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



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

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

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

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

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

**Exemple** : Ces emplacements de stockage (image à gauche) ont une durée de rétention de 4 jours alors que l'archive suivante (image à droite) a une durée de rétention de 10 jours. L'archivage est réglé de façon à se produire tous les jours à 10h30, permettant un archivage des données bien plus fréquent que la durée de rétention.

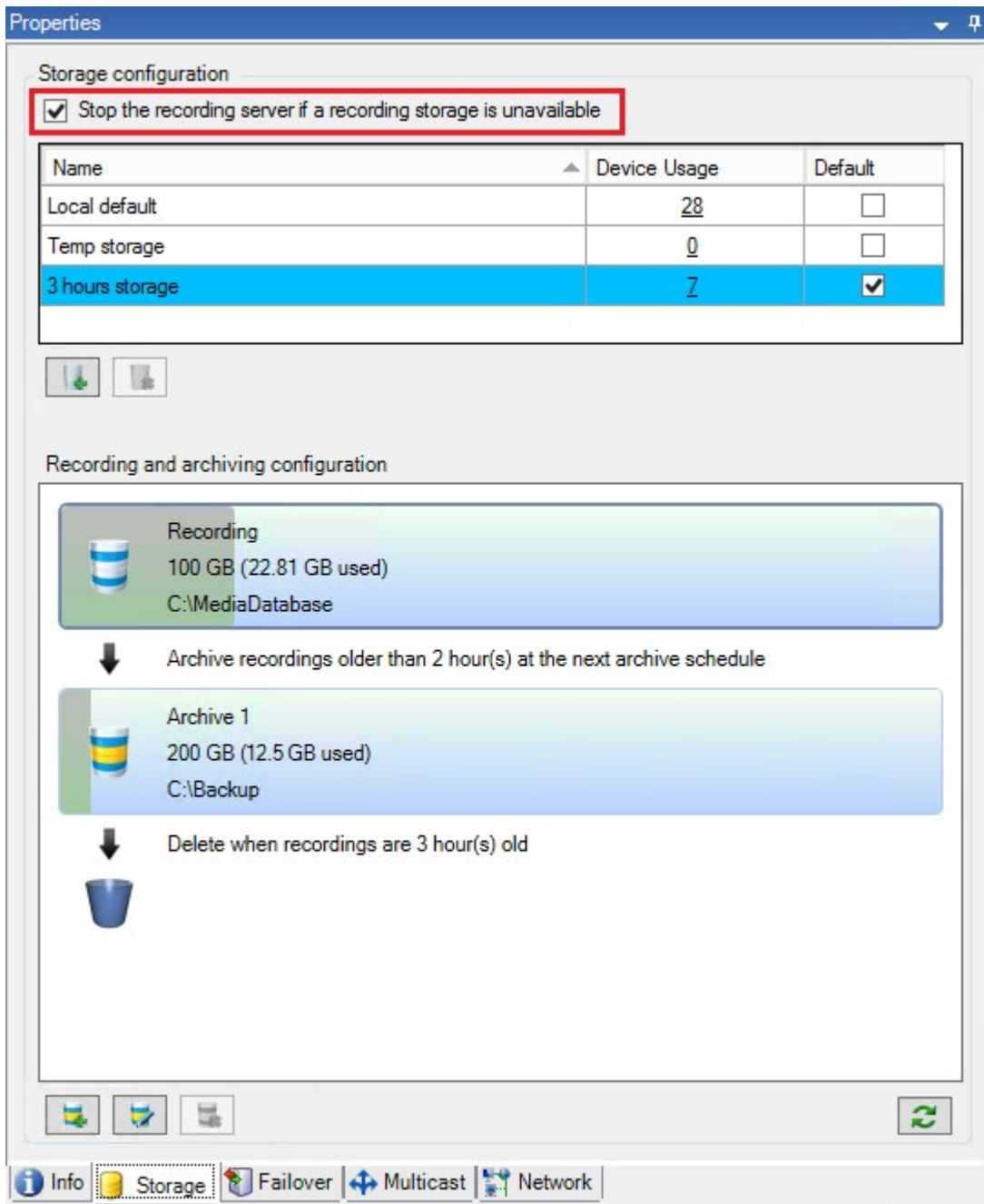


Vous pouvez également contrôler l'archivage au moyen de règles et d'événements.

### Spécifier le comportement lorsque le stockage des enregistrements n'est pas disponible


Par défaut, le serveur d'enregistrement continue de fonctionner si le stockage des enregistrements n'est plus disponible. Si votre système est configuré avec des serveurs d'enregistrement de redondance, vous pouvez spécifier le serveur d'enregistrement pour arrêter l'exécution, pour que les serveurs de basculement prennent le relais :

1. Sur le serveur d'enregistrement concerné, allez sur l'onglet **Stockage**.
2. Sélectionnez l'option **Arrêter le serveur d'enregistrement en cas d'indisponibilité d'un stockage d'enregistrement**.



### Ajouter un nouvel emplacement de stockage


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

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

Si besoin, vous êtes maintenant prêt à créer une ou des archive(s) à l'intérieur de votre nouvel emplacement de stockage.

### Créer une archive dans un emplacement de stockage

Un emplacement de stockage n'a pas d'archive(s) par défaut, mais vous pouvez les créer.

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


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

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

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

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

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

1. Pour modifier un emplacement de stockage, sélectionnez sa base de données d'enregistrement dans la liste **Configuration d'enregistrement et d'archivage**. Pour modifier une archive, sélectionnez la base de données de l'archive.
2. Cliquez sur le bouton **Modifier stockage d'enregistrement**  situé sous la liste **Configuration d'enregistrement et d'archivage**.
3. Modifiez une base de données d'enregistrement ou modifiez une archive.



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

### Activer la signature numérique à des fins d'export



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

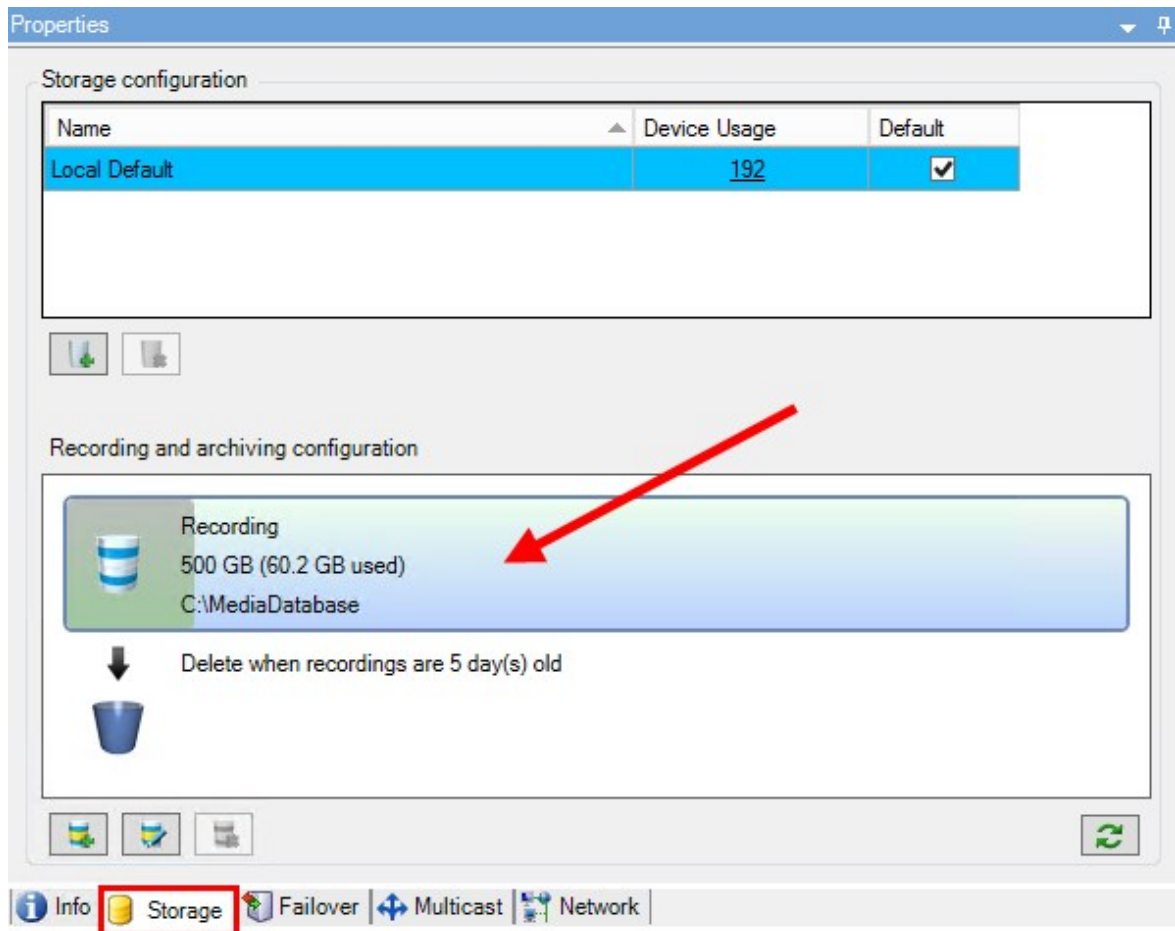
Vous pouvez activer la signature numérique pour la vidéo enregistrée, de sorte que les utilisateurs du client puissent vérifier que la vidéo enregistrée n'a pas été falsifiée depuis son enregistrement. La vérification de l'authenticité de la vidéo est une tâche que l'utilisateur peut effectuer dans XProtect Smart Client – Player une fois que la vidéo a été exportée.



La signature doit également être activée dans XProtect Smart Client, dans la boîte de dialogue **Exporter**. Autrement, le bouton **Vérifier les signatures** dans XProtect Smart Client – Player ne s'affiche pas.

1. Dans le panneau **Navigation du site**, développez le nœud **Serveurs**.
2. Cliquez sur **Serveurs d'enregistrement**.
3. Dans le volet de vue d'ensemble, cliquez sur le serveur d'enregistrement sur lequel vous souhaitez activer la signature.

- En bas du panneau **Propriétés**, cliquez sur l'onglet **Stockage**.



- Dans la rubrique **Configuration de l'enregistrement et de l'archivage**, double-cliquez sur la barre horizontale représentant la base de données d'enregistrement. La fenêtre **Paramètres de stockage et d'enregistrement** apparaît.
- Cochez la case **Signature**.
- Cliquez sur **OK**.

### Cryptez vos enregistrements



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

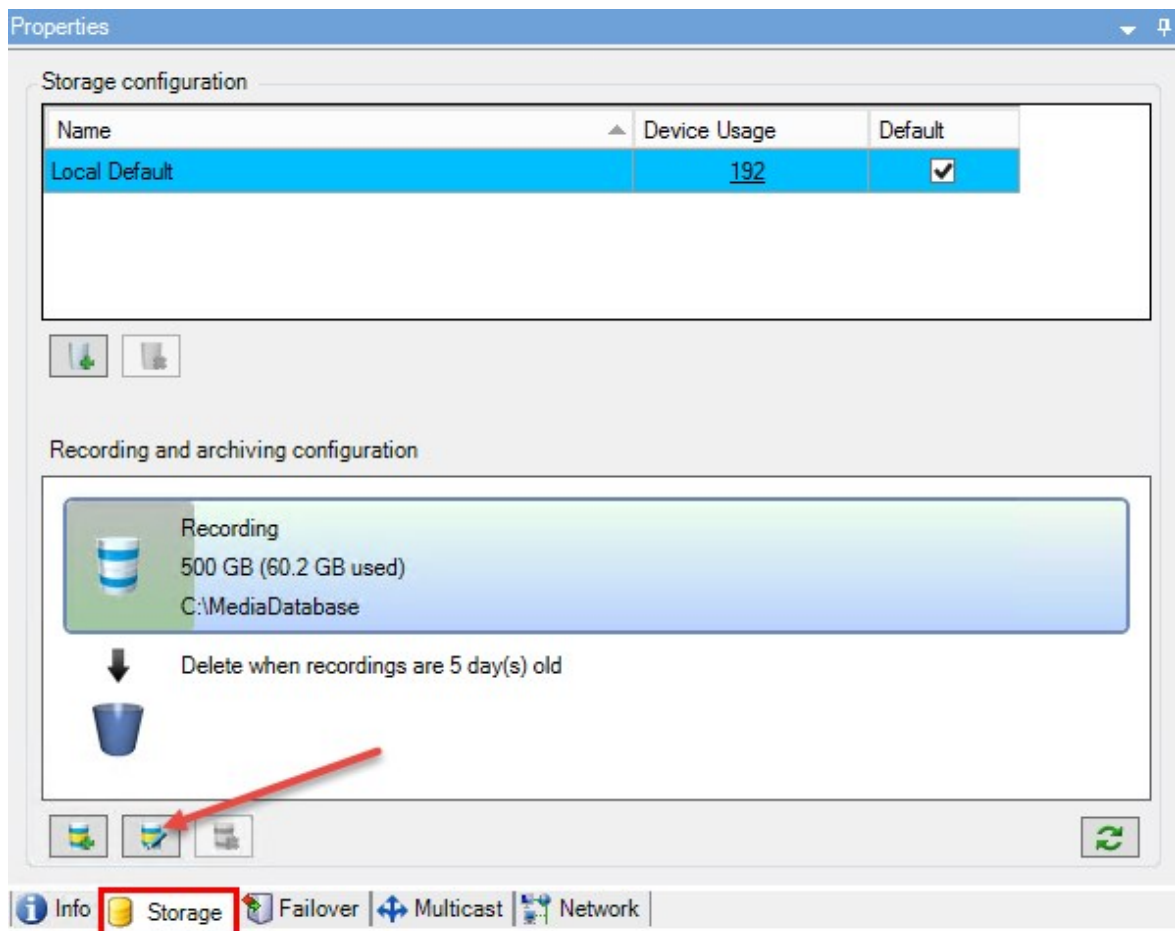
Vous avez la possibilité de sécuriser vos enregistrements en activant le cryptage dans l'option stockage et archives de vos serveurs d'enregistrement. Vous pouvez choisir entre un cryptage faible et un cryptage fort. En activant le cryptage, vous devez également spécifier un mot de passe ci-dessous.



Le fait d'activer ou de modifier les paramètres de cryptage ou le mot de passe peut éventuellement prendre du temps, en fonction de la taille de la base de données et de la performance du lecteur. Vous pouvez suivre le progrès dans **Tâches en cours**.

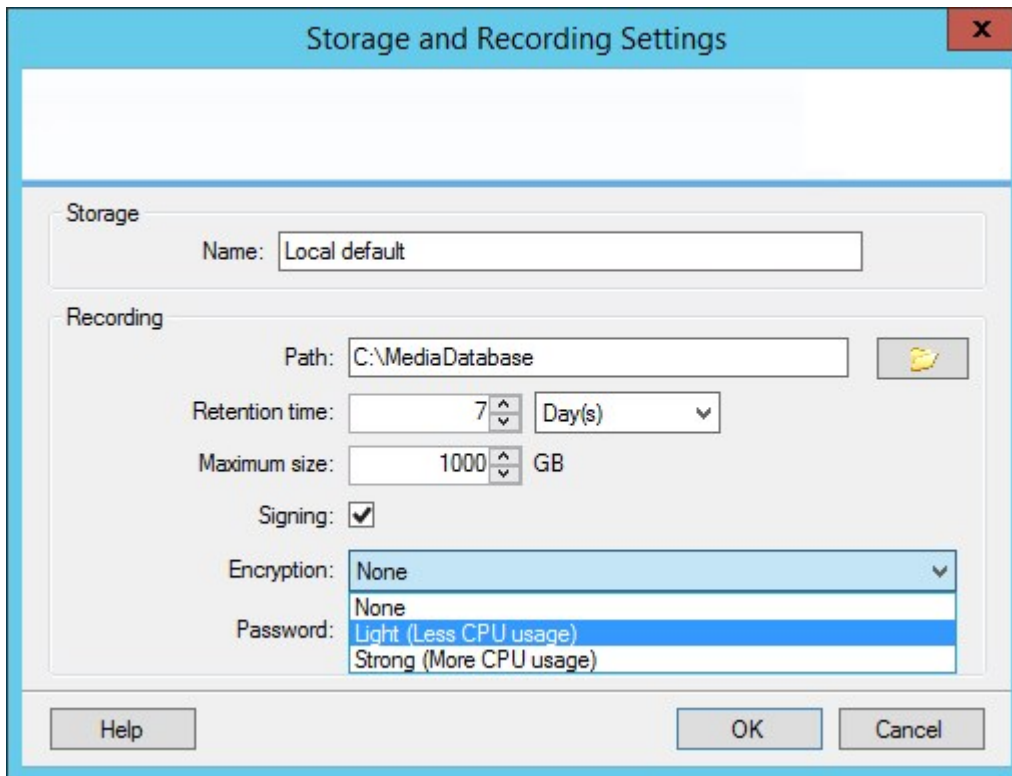
**N'arrêtez pas** l'enregistrement du serveur d'enregistrement lorsque cette tâche est en cours.

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





2. Dans la fenêtre de dialogue qui s'affiche, indiquez le niveau de cryptage.



3. Vous êtes automatiquement redirigé vers la boîte de dialogue **Définir un mot de passe**. Saisissez un mot de passe et cliquez sur **OK**.

### Sauvegarde des enregistrements archivés

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

#### **Sauvegardez les archives plutôt que les bases de données des caméras**

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

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

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

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

Dans le cadre d'une utilisation ordinaire de votre système, la structure de sous-répertoires est entièrement transparente aux utilisateurs du système lorsqu'ils parcourent tous les enregistrements avec le XProtect Smart Client. Ceci est valable pour les enregistrements archivés et non archivés. Il est judicieux de connaître la structure de sous-répertoires (voir [Structure des archives \(explications\)](#)) si vous souhaitez sauvegarder vos enregistrements archivés (voir Sauvegarde et restauration de la configuration système sur la page 488).

### Structure des archives (explication)

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



Dans le cadre d'une utilisation ordinaire de votre système, la structure de sous-répertoires est entièrement transparente aux utilisateurs du système lorsqu'ils parcourent tous les enregistrements avec le XProtect Smart Client, que ces enregistrements soient archivés ou non. Une bonne connaissance de votre structure de sous-répertoires est particulièrement intéressante si vous souhaitez sauvegarder vos enregistrements archivés.

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

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

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

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

#### Structure de désignation

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

Si les données proviennent de la caméra locale :

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

Si les données proviennent de SMTP :

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

### Exemple réel

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

### Sous-répertoires

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

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

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

### Exemples de sauvegarde

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

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

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

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

### Supprimer une archive d'un espace de stockage

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



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

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



Si l'archive n'est pas disponible, par exemple, en mode hors ligne, vous devez restaurer la connexion avant de pouvoir effacer l'archive.

### Suppression d'un espace de stockage

Vous ne pouvez pas supprimer le ou les stockages par défaut utilisés par les dispositifs comme stockage des enregistrements pour les enregistrements en direct.

Cela signifie que vous devrez peut-être déplacer des périphériques (voir [Déplacer le matériel sur la page 500](#)) et tout enregistrement pas encore archivé vers un autre emplacement de stockage avant de supprimer l'emplacement de stockage.

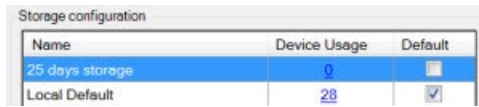
1. Pour consulter la liste des périphériques qui utilisent cet emplacement de stockage, cliquez sur le numéro d'utilisation du périphérique.




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

2. Suivez les étapes présentées dans [Déplacer les enregistrements non archivés d'un emplacement de stockage à un autre](#).
3. Continuez jusqu'à ce que vous ayez déplacé tous les périphériques.

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



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

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

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


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

### Propriétés des paramètres de stockage et d'enregistrement

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

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

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


Nom	Description
<b>Durée de rétention</b>	<p>Précisez la durée pendant laquelle les enregistrements doivent demeurer dans l'archive avant d'être supprimés ou déplacés dans l'archive suivante (en fonction des paramètres de l'archive).</p> <p>La durée de rétention doit toujours être plus longue que la durée de rétention de l'archive précédente ou de la base de données d'enregistrement par défaut. En effet, le nombre de jours de rétention indiqué pour une archive inclut toutes les périodes de rétention mentionnées précédemment dans le processus.</p>
<b>Taille maximum</b>	<p>Sélectionnez le nombre maximum de giga-octets de données d'enregistrement à enregistrer dans la base de données d'enregistrement.</p> <p>Les données d'enregistrement supérieures au nombre de giga-octets spécifié seront déplacées automatiquement dans la première archive de la liste - si des archives sont spécifiées - ou supprimées.</p> <div style="border: 1px solid #c00000; padding: 10px; background-color: #fff9e6;"> <p> S'il y a moins de 5 Go d'espace libre, le système archive toujours automatiquement (ou supprime si aucune archive suivante n'est définie) les plus anciennes données d'une base de données. S'il y a moins de 1 Go d'espace libre, les données seront supprimées. Une base de données a toujours besoin de 250 Mo d'espace libre. Si vous atteignez cette limite (si les données ne sont pas supprimées assez rapidement), aucune autre donnée ne sera ajoutée à la base de données tant que vous n'aurez pas libéré suffisamment d'espace. La taille maximum réelle de votre base de données est la quantité de giga-octets que vous spécifiez, moins 5 Go.</p> </div>
<b>Signature</b>	<p>Active une signature numérique pour les enregistrements. Par exemple, cela signifie que le système confirme qu'une vidéo exportée n'a pas été modifiée ou manipulée lors de la lecture.</p> <p>Le système utilise l'algorithme SHA-2 pour la signature numérique.</p>
<b>Cryptage</b>	<p>Sélectionnez le niveau de cryptage des enregistrements :</p> <ul style="list-style-type: none"> <li>• Aucun</li> <li>• Faible (utilisation du processeur moindre)</li> <li>• Fort (utilisation du processeur supérieure)</li> </ul> <p>Le système utilise l'algorithme AES-256 pour le cryptage.</p>

Nom	Description
	<p>Si vous sélectionnez <b>Faible</b>, une partie de l'enregistrement sera cryptée. Si vous sélectionnez <b>Fort</b>, tout l'enregistrement sera crypté.</p> <p>Si vous choisissez d'activer le cryptage, vous devez également spécifier un mot de passe ci-dessous.</p>
<b>Mot de passe</b>	<p>Saisissez un mot de passe pour les utilisateurs autorisés à consulter les données cryptées.</p> <p>Milestone vous recommande d'utiliser des mots de passe forts. Les mots de passe forts ne contiennent pas de mots qui peuvent se trouver dans un dictionnaire ou qui font partie du nom de l'utilisateur. Ils comportent huit ou plusieurs caractères alphanumériques, des majuscules ou minuscules et des caractères spéciaux.</p>

### Propriétés des paramètres d'archive

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

Nom	Description
<b>Nom</b>	Renommez l'emplacement de stockage si nécessaire. Les noms doivent être uniques.
<b>Chemin</b>	<p>Spécifiez le chemin jusqu'au répertoire dans lequel vous sauvegardez les enregistrements dans cet emplacement de stockage. L'emplacement de stockage ne doit pas nécessairement être situé sur l'ordinateur du serveur d'enregistrement.</p> <p>Si le répertoire n'existe pas, vous pouvez le créer. Les disques réseau doivent être indiqués à l'aide du format UNC (Universal Naming Convention), par exemple : <code>\\server\volume\directory\</code>.</p>
<b>Durée de rétention</b>	<p>Précisez la durée pendant laquelle les enregistrements doivent demeurer dans l'archive avant d'être supprimés ou déplacés dans l'archive suivante (en fonction des paramètres de l'archive).</p> <p>La durée de rétention doit toujours être plus longue que la durée de rétention de l'archive précédente ou de la base de données d'enregistrement par défaut. En effet, le nombre de jours de rétention indiqué pour une archive inclut toutes les périodes de rétention mentionnées précédemment dans le processus.</p>

Nom	Description
<b>Taille maximum</b>	<p>Sélectionnez le nombre maximum de giga-octets de données d'enregistrement à enregistrer dans la base de données d'enregistrement.</p> <p>Les données d'enregistrement supérieures au nombre de giga-octets spécifié seront déplacées automatiquement dans la première archive de la liste - si des archives sont spécifiées - ou supprimées.</p> <div style="border: 1px solid #c00; padding: 10px; background-color: #fff9e6;"> <p> S'il y a moins de 5 Go d'espace libre, le système archive toujours automatiquement (ou supprime si aucune archive suivante n'est définie) les plus anciennes données d'une base de données. S'il y a moins de 1 Go d'espace libre, les données seront supprimées. Une base de données a toujours besoin de 250 Mo d'espace libre. Si vous atteignez cette limite (si les données ne sont pas supprimées assez rapidement), aucune autre donnée ne sera ajoutée à la base de données tant que vous n'aurez pas libéré suffisamment d'espace. La taille maximum réelle de votre base de données est la quantité de giga-octets que vous spécifiez, moins 5 Go.</p> </div>
<b>Calendrier</b>	<p>Spécifiez un calendrier d'archivage qui définit les intervalles dans lesquels le processus d'archivage doit commencer. Vous pouvez archiver très fréquemment (en principe chaque heure toute l'année) ou très rarement (par exemple, chaque premier lundi tous les 36 mois).</p>
<b>Réduire la fluidité d'image</b>	<p>Pour réduire le FPS lors de l'archivage, sélectionnez la case à cocher <b>Réduire la fluidité d'image</b> et configurez un nombre d'images par seconde (FPS).</p> <p>La réduction de la fluidité d'image d'un nombre d'images par seconde sélectionné permet de faire en sorte que vos enregistrements prennent moins de place dans l'archive, mais réduit également la qualité de votre archive.</p> <p>MPEG-4/H.264/H.265 réduit automatiquement aux images clés comme minimum.</p> <p>0,1 = 1 image par 10 secondes.</p>

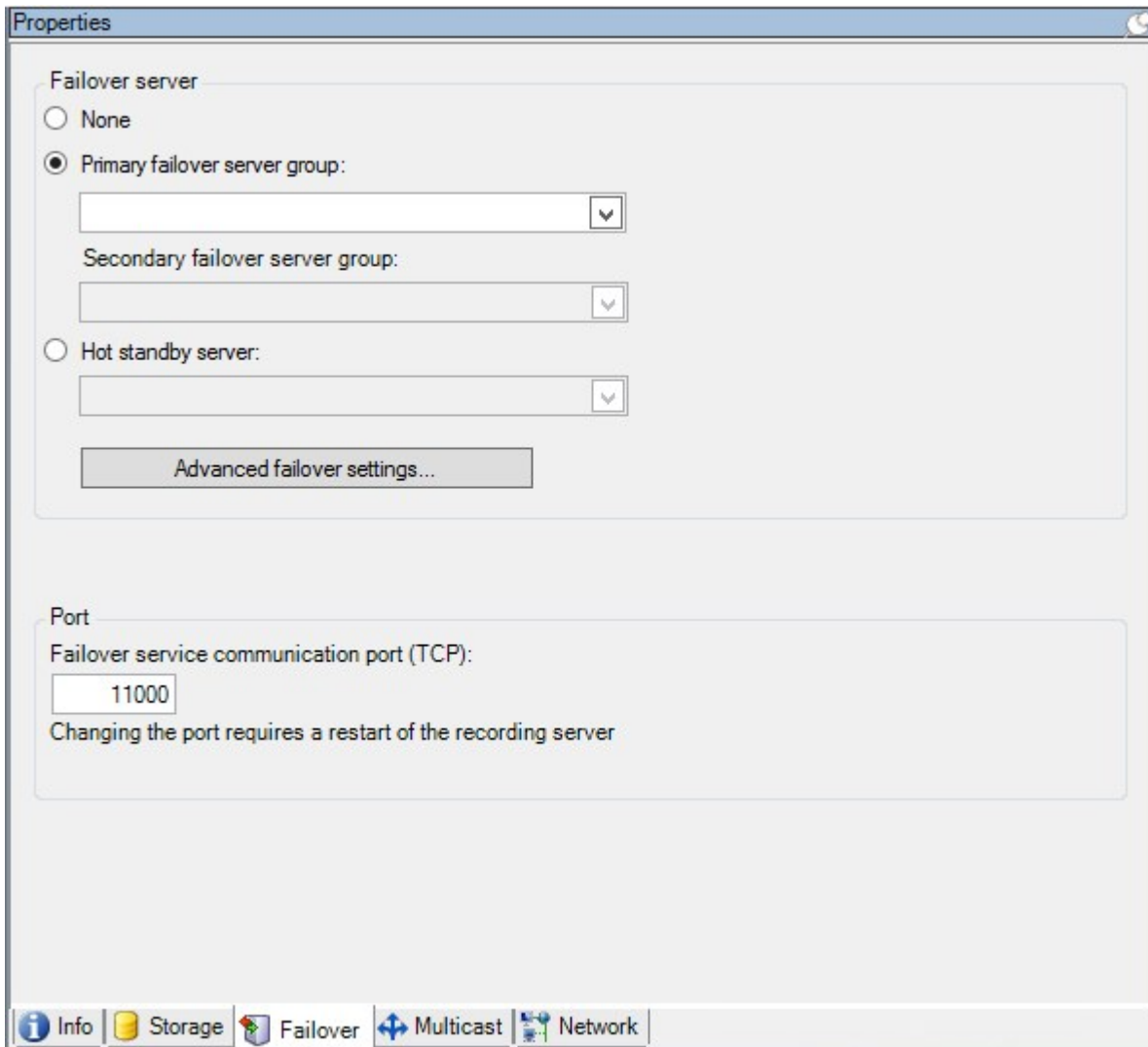
## Onglet Redondance (serveur d'enregistrement)



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



Si votre organisation utilise des serveurs d'enregistrement de redondance, utilisez l'onglet **Redondance** pour affecter des serveurs de basculement aux serveurs d'enregistrement, voir [Propriétés de l'onglet Redondance](#).



Pour obtenir des informations plus détaillées sur les serveurs d'enregistrement de redondance, l'installation et les paramètres, les groupes de redondance et leurs paramètres, reportez-vous au paragraphe Serveurs d'enregistrement de redondance (explications) sur la page 185.

### Affecter des serveurs d'enregistrement de redondance

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

- Pas de configuration de redondance
- Une configuration de redondance primaire/secondaire (veille à froid)
- Une configuration à affectation unique

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

1. Dans le panneau **Navigation du site**, sélectionnez **Serveurs > Serveurs d'enregistrement**. Cette commande ouvre une liste de serveurs d'enregistrement.
2. Dans le volet **Vue d'ensemble**, sélectionnez le serveur d'enregistrement souhaité puis allez sur l'onglet **Redondance**.
3. Pour choisir le type de configuration de redondance, faites votre choix parmi :
  - **Aucun**
  - **Groupe de serveurs de redondance primaire/groupe de serveurs de redondance secondaire**
  - **Serveur de redondance à affectation unique**

Vous ne pouvez pas choisir le même groupe de redondance comme groupe de redondance primaire et secondaire ni sélectionner des serveurs de redondance ordinaires qui font déjà partie d'un groupe de redondance en tant que serveurs de redondance à affectation unique.

4. Ensuite, cliquez sur **Paramètres de redondance avancés**. Ceci ouvre la fenêtre **Paramètres de redondance avancés**, qui répertorie tous les périphériques rattachés au serveur d'enregistrement sélectionné. Si vous avez sélectionné **Aucun**, les Paramètres de redondance avancés sont disponibles. Toute sélection est conservée pour toute configuration de redondance ultérieure.
5. Afin de spécifier le niveau de soutien de redondance, sélectionnez **Soutien complet, Uniquement en direct** ou **Désactivé** pour chaque périphérique de la liste. Cliquez sur **OK**.
6. Dans le champ **Port de communication avec le support de redondance (TCP)**, modifiez le numéro de port si nécessaire.



Si vous activez la prise en charge du support de redondance et que le serveur est configuré pour continuer à fonctionner en cas d'indisponibilité d'un stockage d'enregistrement, le serveur d'enregistrement redondant ne prendra pas le relais. Pour que le support de redondance fonctionne, vous devez sélectionner l'option **Arrêter le serveur d'enregistrement en cas d'indisponibilité d'un stockage d'enregistrement** sous l'onglet **Stockage**.

## Propriétés de l'onglet Redondance

Nom	Description
Aucun	Sélectionnez une configuration sans serveur d'enregistrement de redondance.
Groupe de serveurs de basculement primaire / Groupe de serveurs de basculement secondaire	Sélectionnez une configuration de redondance ordinaire avec un groupe de serveurs de redondance primaire, et potentiellement un groupe secondaire.
Serveur de redondance à affectation unique	Sélectionnez une configuration à affectation unique dotée d'un serveur d'enregistrement dédié en tant que serveur de redondance à affectation unique.
Paramètres de redondance avancés	Ouvre la fenêtre <b>Paramètres de redondance avancés</b> : <ul style="list-style-type: none"> <li>• <b>Soutien complet</b> : Active un soutien de redondance complète pour le périphérique</li> <li>• <b>Uniquement en direct</b> : Active un soutien de redondance complète pour les flux en direct sur le périphérique</li> <li>• <b>Désactivé</b> : Désactive le soutien de redondance pour le périphérique</li> </ul>
Port de communication avec le service de redondance (TCP)	Par défaut, le numéro de port est 11000. Vous utilisez ce port pour les communications entre les serveurs d'enregistrement et les serveurs d'enregistrement de redondance. Si vous modifiez le port, le serveur d'enregistrement <b>doit</b> être en cours de fonctionnement et <b>doit</b> être connecté au serveur de gestion.

## Onglet Multicast (serveur d'enregistrement)

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

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



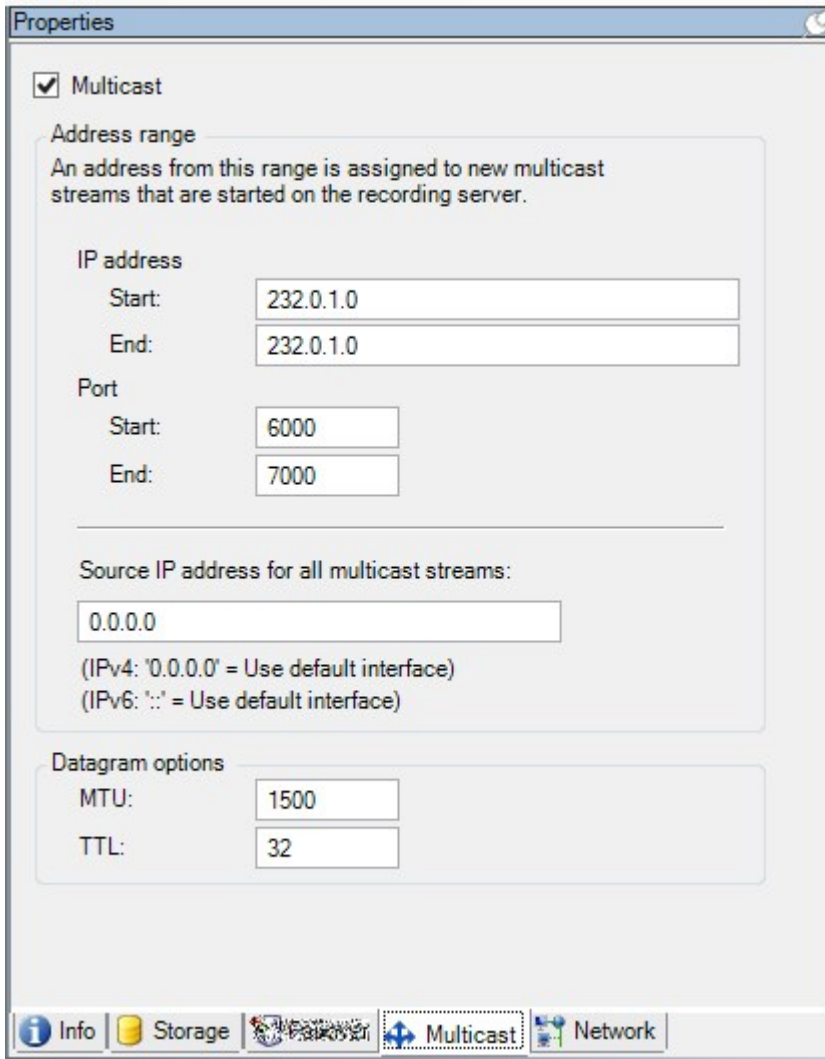
Si un serveur d'enregistrement possède plus d'une carte d'interface réseau, il est uniquement possible de procéder à un multicast sur l'une d'entre elles. Vous pouvez spécifier laquelle utiliser par le biais du Management Client.



Si vous utilisez des serveurs de basculement, pensez également à indiquer l'adresse IP de la carte d'interface réseau sur les serveurs de basculement (voir Onglet Multicast (serveurs de basculement) sur la page 193).



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



### Multicast (explications)

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

- Lorsque vous utilisez l'**unicast**, la source doit transmettre un flux de données pour chaque destinataire
- Lorsque vous utilisez le **multicast**, un seul flux de données suffit sur chaque segment du réseau

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

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



Les flux de multidiffusion ne sont pas cryptés, même si le serveur d'enregistrement utilise le cryptage.

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

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

### Activez le multicast pour le serveur d'enregistrement

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

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

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



Les flux de multidiffusion ne sont pas cryptés, même si le serveur d'enregistrement utilise le cryptage.

## Affectation de la plage d'adresses IP

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

Pour chaque envoi de la caméra en multicast, la combinaison d'adresse IP et de port doit être unique (exemple IPv4 : 232.0.1.0:6000). Vous pouvez utiliser une adresse IP et de nombreux ports, ou de nombreuses adresses IP et moins de ports. Par défaut, le système suggère une seule adresse IP et une plage de 1000 ports, mais vous pouvez le modifier selon les besoins.

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

Nom	Description
Adresse IP	Dans le champ <b>Début</b> , indiquez la première adresse IP de la plage désirée. Ensuite, indiquez la dernière adresse IP de la plage dans le champ <b>Fin</b> .
Port	Dans le champ <b>Début</b> , indiquez le premier numéro de port de la plage désirée. Ensuite, indiquez le dernier numéro de port de la plage dans le champ <b>Fin</b> .
Adresse IP source pour tous les flux multicast	<p>Vous pouvez uniquement multidiffuser sur une carte d'interface réseau, donc ce champ est pertinent si votre serveur d'enregistrement possède plus d'une carte d'interface réseau ou s'il possède une carte d'interface réseau comptant plus d'une adresse IP.</p> <p>Pour utiliser l'interface par défaut du serveur d'enregistrement, laissez la valeur 0.0.0.0 (IPv4) ou :: (IPv6) dans le champ. Si vous souhaitez utiliser une autre carte d'interface réseau, ou une adresse IP différente sur la même carte d'interface réseau, indiquez l'adresse IP de l'interface désirée.</p> <ul style="list-style-type: none"> <li>• IPv4 : 224.0.0.0 à 239.255.255.255.</li> <li>• IPv6, la plage est décrite sur le site Web IANA (<a href="https://www.iana.org/">https://www.iana.org/</a>).</li> </ul>

## Spécification des options de datagramme

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

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

### Activation du multicast pour des caméras individuelles

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

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



Les flux de multidiffusion ne sont pas cryptés, même si le serveur d'enregistrement utilise le cryptage.

### Onglet Réseau (serveur d'enregistrement)

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

#### Pourquoi utiliser une adresse publique ?

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

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



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

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

### Définition de l'adresse publique et du port

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



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

### Affectation de plages IP locales

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

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

## Navigation sur le site : Serveurs et matériel : Serveurs de redondance

### Serveurs d'enregistrement de redondance (explications)



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

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

Les serveurs d'enregistrement de redondance sont installés comme les serveurs d'enregistrement standard (voir XProtect Installer les nouveaux composants sur la page 94). Une fois que vous avez installé les serveurs d'enregistrement de redondance, ils sont visibles dans le Management Client. Milestone vous recommande d'installer tous les serveurs d'enregistrement de redondance sur des ordinateurs séparés. Assurez-vous de configurer les serveurs d'enregistrement de redondance avec la bonne adresse IP ou le bon nom d'hôte du serveur de gestion. Les droits d'utilisateur du compte d'utilisateur sous lequel s'exécute le service du serveur de redondance sont fournis lors de l'installation. Il s'agit des :

- Permissions Démarrer/Arrêter pour démarrer et arrêter le serveur d'enregistrement de redondance
- Permissions d'accès Lire et Modifier pour lire ou modifier le fichier RecorderConfig.xml

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



Si le serveur d'enregistrement de redondance prend le contrôle depuis le serveur d'enregistrement utilisant le cryptage, Milestone recommande de préparer également le serveur d'enregistrement de redondance pour qu'il utilise le cryptage. Pour plus d'informations, voir Avant de commencer l'installation sur la page 59 et XProtect Installer les nouveaux composants sur la page 94.

Vous pouvez spécifier quel type d'assistance de redondance vous souhaitez pour chaque périphérique. Pour chaque périphérique d'un serveur d'enregistrement, vous pouvez sélectionner une assistance complète, uniquement en direct ou aucune assistance de redondance. Ceci vous aide à accorder une priorité à vos ressources de redondance et, par exemple, à ne configurer de système de redondance que pour la vidéo et non pour l'audio, ou encore à n'avoir de système de redondance que pour les caméras essentielles et non pour les caméras de moindre importance.



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

### Serveurs d'enregistrement de redondance à froid

Dans une configuration de serveur de redondance à froid, vous regroupez plusieurs serveurs d'enregistrement de redondance dans un groupe de redondance. L'ensemble du groupe de redondance se consacre à prendre le

relais de plusieurs serveurs d'enregistrement présélectionnés au cas où l'un d'entre eux ne serait plus disponible. Vous pouvez créer autant de groupes que vous le souhaitez (voir [Serveurs d'enregistrement de redondance groupes pour une veille à froid](#)).

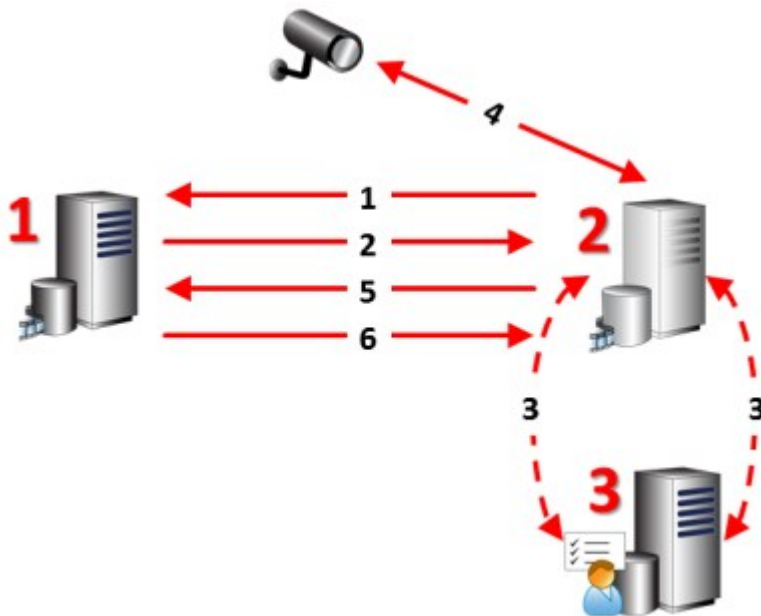
Le regroupement a un avantage évident : par la suite, lorsque vous spécifiez les serveurs d'enregistrement de redondance devant prendre le relais d'un serveur d'enregistrement, vous sélectionnez un groupe de serveurs d'enregistrement de redondance. Si le groupe choisi contient plus d'un serveur d'enregistrement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

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

### **Serveurs d'enregistrement de redondance à affectation unique**

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

## Étapes de redondance (explications)



### Description

Serveurs impliqués (numéros en rouge) :

1. Recording Server
2. Failover Recording Server
3. Management Server

Étapes de redondance pour les configurations **à veille à froid** :

1. Pour vérifier si elle fonctionne ou non, un serveur d'enregistrement de redondance dispose d'une connexion TCP permanente avec le serveur d'enregistrement.
2. Cette connexion est interrompue.
3. Le serveur d'enregistrement de redondance demande la configuration actuelle du serveur d'enregistrement à partir du serveur de gestion. Le serveur de gestion envoie la configuration requise, le serveur d'enregistrement de redondance reçoit la configuration, démarre et commence à enregistrer pour le compte du serveur d'enregistrement.
4. Le serveur d'enregistrement de redondance et la/les caméra(s) échangent des données vidéo.

Description
<ol style="list-style-type: none"> <li>5. Le serveur d'enregistrement de redondance essaie continuellement de rétablir la connexion avec le serveur d'enregistrement.</li> <li>6. Lorsque la connexion au serveur d'enregistrement est rétablie, le serveur d'enregistrement de redondance s'éteint et le serveur d'enregistrement recherche les données vidéo (le cas échéant) enregistrées pendant sa coupure et les données vidéo sont fusionnées dans la base de données du serveur d'enregistrement.</li> </ol>
<p>Étapes de redondance pour les configurations <b>à affectation unique</b> :</p> <ol style="list-style-type: none"> <li>1. Pour vérifier si elle fonctionne ou non, un serveur de redondance à affectation unique dispose d'une connexion TCP permanente avec le serveur d'enregistrement auquel il est assigné.</li> <li>2. Cette connexion est interrompue.</li> <li>3. À partir du serveur de gestion, le serveur de redondance à affectation unique connaît déjà la configuration actuelle de son serveur d'enregistrement assigné et commence à enregistrer pour son compte.</li> <li>4. Le serveur de redondance à affectation unique et la ou les caméra(s) pertinente(s) échangent des données vidéo.</li> <li>5. Le serveur de redondance à affectation unique essaie continuellement de rétablir la connexion avec le serveur d'enregistrement.</li> <li>6. Lorsque la connexion au serveur d'enregistrement est rétablie et que le serveur de redondance à affectation unique retourne en mode veille, le serveur d'enregistrement récupère les données vidéo (le cas échéant) enregistrées pendant sa coupure et les données vidéo sont fusionnées dans la base de données du serveur d'enregistrement.</li> </ol>

## Fonctionnalité du serveur d'enregistrement de redondance (explications)

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

- Un serveur d'enregistrement de redondance à froid prend le relais du serveur d'enregistrement qui est devenu indisponible après cinq secondes plus le temps qu'il faut au service Recording Server du serveur d'enregistrement de redondance pour démarrer, plus le temps nécessaire à la connexion aux caméras. Par contre, un serveur d'enregistrement de redondance à affectation unique prend le relais plus rapidement car le service Recording Server fonctionne déjà avec la bonne configuration et n'a qu'à démarrer ses caméras pour diffuser les flux. Pendant la période de démarrage, vous ne pouvez pas stocker d'enregistrements ni visionner des vidéos en direct à partir des caméras concernées
- Lorsqu'un serveur d'enregistrement redevient disponible, il prend automatiquement le relais du serveur d'enregistrement de redondance. Les enregistrements stockés par le serveur d'enregistrement de redondance sont automatiquement fusionnés dans les bases de données du serveur d'enregistrement standard. Le temps requis par le processus de fusion dépend de la quantité d'enregistrements à fusionner, de la capacité du réseau, etc. Pendant le processus de fusion, vous ne pouvez pas parcourir les enregistrements à partir de la période pendant laquelle le serveur d'enregistrement de redondance a pris le relais
- Si un serveur d'enregistrement de redondance doit prendre le relais d'un autre serveur d'enregistrement pendant le processus de fusion dans une configuration de serveur d'enregistrement de redondance à froid, il reporte le processus de fusion avec le serveur d'enregistrement A, et prend le relais du serveur d'enregistrement B. Lorsque le serveur d'enregistrement B redevient disponible, le serveur d'enregistrement de redondance reprend le processus de fusion avec le serveur d'enregistrement A, après quoi il commence la fusion avec le serveur d'enregistrement B.
- Dans une configuration à affectation unique, un serveur de redondance à affectation unique ne peut pas prendre le relais d'un autre serveur d'enregistrement car il n'est affecté qu'à un seul serveur d'enregistrement. Mais si ce serveur d'enregistrement subit une nouvelle défaillance, le serveur à affectation unique prend à nouveau le relais et conserve les enregistrements de la période précédente. Le serveur d'enregistrement conserve les enregistrements jusqu'à leur fusion avec l'enregistreur primaire ou jusqu'à ce que le serveur d'enregistrement de redondance n'ait plus d'espace disponible sur le disque
- Une solution de redondance n'offre pas une redondance intégrale. Elle peut uniquement servir de moyen fiable pour minimiser les temps d'arrêt. Si un serveur d'enregistrement redevient disponible, le service Failover Server s'assure que le serveur d'enregistrement est prêt à sauvegarder de nouveau les enregistrements. Alors seulement la responsabilité de sauvegarder les enregistrements revient au serveur d'enregistrement standard. Par conséquent, la perte des enregistrements à ce stade du processus est très improbable

- Les utilisateurs clients remarquent à peine qu'un serveur d'enregistrement de redondance prend le relais. Une brève coupure se produit, généralement pendant quelques secondes seulement, au moment où le serveur d'enregistrement de redondance prend le relais. Au cours de cette interruption, les utilisateurs n'ont pas accès à la vidéo du serveur d'enregistrement concerné. Les utilisateurs clients peuvent reprendre le visionnage des vidéos en direct dès que le serveur d'enregistrement de redondance a pris le relais. Comme les enregistrements récents sont stockés sur le serveur d'enregistrement de redondance, ils peuvent lire les enregistrements effectués après la prise de relais par le serveur d'enregistrement de redondance. Les clients ne peuvent pas lire les enregistrements plus anciens sauvegardés uniquement sur le serveur d'enregistrement touché tant que ce serveur d'enregistrement ne fonctionne pas de nouveau, et a pris le relais du serveur d'enregistrement de redondance. Vous ne pouvez pas accéder aux enregistrements archivés. Lorsque le serveur d'enregistrement fonctionne de nouveau, un processus de fusion a lieu. Au cours de ce processus, les enregistrements du serveur de redondance sont fusionnés dans la base de données du serveur d'enregistrement. Pendant ce processus, vous ne pouvez pas lire les enregistrements de la période pendant laquelle le serveur d'enregistrement de redondance a pris le relais
- Dans une configuration de redondance à froid, la configuration d'un serveur d'enregistrement de redondance en soutien d'un autre serveur d'enregistrement de redondance n'est pas nécessaire. La raison est que vous attribuez des groupes de redondance et non des serveurs d'enregistrement de redondance particuliers pour prendre le relais des serveurs d'enregistrement spécifiques. Un groupe de redondance doit comprendre au moins un serveur d'enregistrement de redondance, mais vous pouvez ajouter autant de serveurs d'enregistrement de redondance que nécessaire. Si un groupe de redondance contient plusieurs serveurs d'enregistrement de redondance, plusieurs serveurs d'enregistrement de redondance peuvent prendre le relais.
- Dans une configuration à affectation unique, vous ne pouvez pas configurer des serveurs d'enregistrement de redondance ou des serveurs à affectation unique en tant que serveur de redondance à affectation unique

## Configurer et activer des serveurs d'enregistrement de redondance



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

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

1. Dans le panneau **Navigation du site**, sélectionnez **Serveurs > Serveurs de basculement**. Ceci ouvre une liste des serveurs d'enregistrement de redondance et des groupes de redondance installés.
2. Dans le volet **Vue d'ensemble**, sélectionnez le serveur d'enregistrement de redondance requis.
3. Faites un clic droit et sélectionnez **Activé**. Le serveur d'enregistrement de redondance est maintenant activé.
4. Pour modifier les propriétés du serveur d'enregistrement de redondance, allez dans l'onglet **Info**.

- Une fois que vous avez terminé, allez dans l'onglet **Réseau**. Ici, vous pouvez entre autres définir l'adresse IP publique du serveur d'enregistrement de redondance. Cela vous concerne si vous utilisez NAT (Network Address Translation) et la redirection du port. Reportez-vous à l'onglet **Réseau** du serveur d'enregistrement standard pour de plus amples informations.
- Dans le panneau **Navigation du site**, sélectionnez **Serveurs** > **Serveurs d'enregistrement**. Sélectionnez le serveur d'enregistrement pour lequel vous voulez le support de redondance et attribuez-lui les serveurs d'enregistrement de redondance (voir Onglet Redondance (serveur d'enregistrement) sur la page 176).

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



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




## Serveurs d'enregistrement de redondance groupes pour une veille à froid

- Sélectionnez **Serveurs** > **Serveurs de redondance**. Ceci ouvre une liste des serveurs d'enregistrement de redondance et des groupes de redondance installés.
- Dans le volet **Vue d'ensemble**, faites un clic droit sur le nœud supérieur **Groupes de redondance** et sélectionnez **Ajouter groupe**.
- Spécifiez un nom (dans cet exemple *Groupe de redondance 1*) et une description (facultative) de votre nouveau groupe. Cliquez sur **OK**.
- Faites un clic droit sur le groupe (*Groupe de redondance 1*) que vous venez de créer. Sélectionnez **Modifier les membres du groupe**. La fenêtre **Sélectionner les membres du groupe** s'ouvre.
- Utilisez les boutons ou votre souris pour déplacer le(s) serveur(s) d'enregistrement de redondance du côté gauche au côté droit. Cliquez sur **OK**. Le(s) serveur(s) d'enregistrement de redondance appartient maintenant au groupe (*Groupe de redondance 1*) que vous venez de créer.
- Allez dans l'onglet **Séquence**. Cliquez sur **Haut** et **Bas** pour configurer la séquence interne des serveurs d'enregistrement de redondance ordinaires dans le groupe.

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

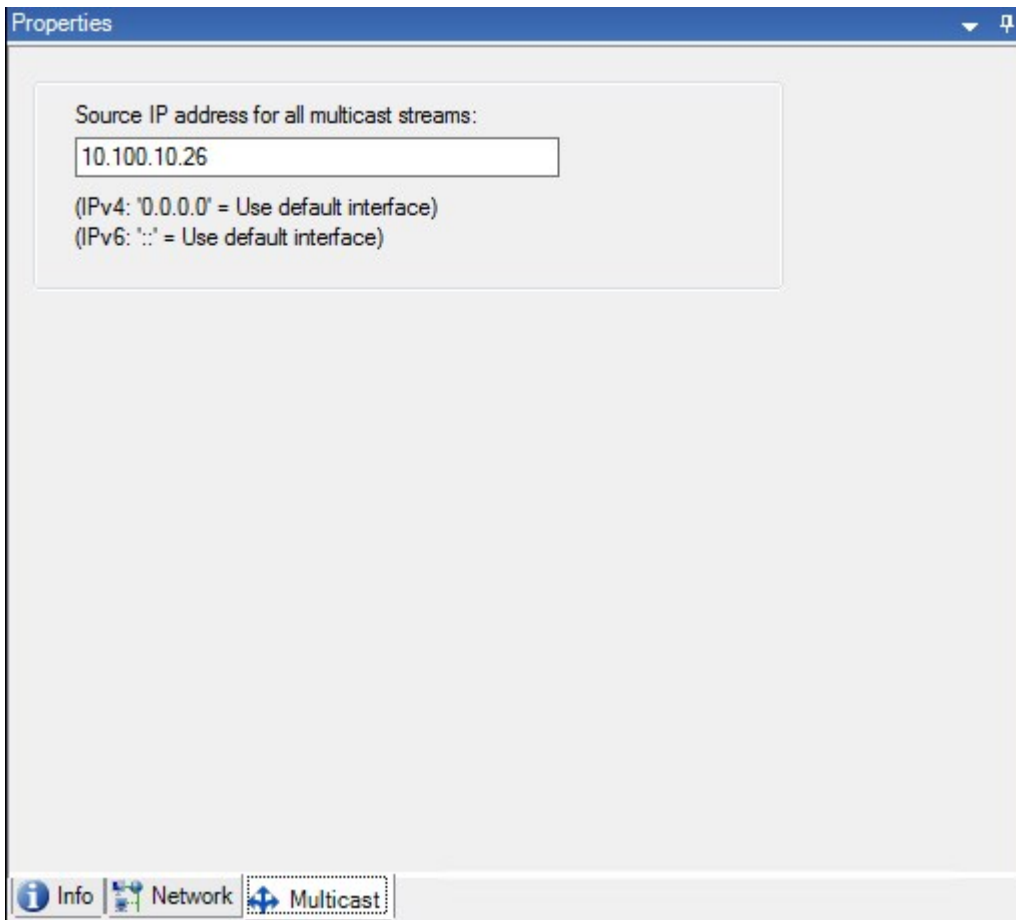
Les icônes suivantes représentent l'état des serveurs d'enregistrement de redondance (les icônes sont visibles dans le volet **Vue d'ensemble**) :



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

## Onglet Multicast (serveurs de basculement)

Si vous utilisez des serveurs de basculement et que vous avez activé le multicast de la diffusion en direct, vous devez préciser l'adresse IP de la carte d'interface réseau que vous utilisez - à la fois sur les serveurs d'enregistrement et les serveurs de redondance.



Pour plus d'informations sur le multicast, voir Onglet Multicast (serveur d'enregistrement) sur la page 179 ou Onglet Multicast (serveur d'enregistrement) sur la page 179.

## Info Propriétés de l'onglet Serveur de basculement

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

Nom	Description
Nom	Le nom du serveur d'enregistrement de redondance tel qu'il apparaît dans le Management Client, les journaux et autres.
Description	Un champ facultatif que vous pouvez utiliser pour décrire le serveur d'enregistrement de

Nom	Description
	redondance, par exemple de quel serveur d'enregistrement il prend le relais.
<b>Nom de l'hôte</b>	Affiche le nom de l'hôte du serveur d'enregistrement de redondance. Vous ne pouvez pas le modifier.
<b>Adresse locale du serveur Web</b>	<p>Affiche l'adresse locale du serveur Web du serveur d'enregistrement de redondance. Vous utilisez l'adresse locale, par exemple, pour gérer les commandes de contrôle des caméras PTZ, et pour gérer les recherches et les demandes en direct depuis XProtect Smart Client.</p> <p>L'adresse inclue le numéro de port utilisé pour la communication du serveur Web (habituellement, le port 7563).</p> <p>Si le serveur d'enregistrement de redondance prend le contrôle depuis le serveur d'enregistrement utilisant le cryptage, vous aurez également besoin de préparer le serveur d'enregistrement de redondance pour qu'il utilise le cryptage.</p> <p>Si vous activez le cryptage des clients et serveurs récupérant les flux de données du serveur d'enregistrement, une icône représentant un cadenas apparaît, ainsi qu'une adresse affichant <b>https</b> au lieu de <b>http</b>.</p>
<b>Adresse du serveur Web</b>	<p>Affiche l'adresse publique du Serveur Web du serveur d'enregistrement de redondance sur Internet.</p> <p>Si votre installation utilise un pare-feu ou du routeur NAT, entrez l'adresse du pare-feu ou du routeur NAT pour que les clients qui accèdent au système de surveillance depuis Internet puissent se connecter aux serveur d'enregistrement de redondance.</p> <p>Vous spécifiez l'adresse publique et le numéro de port dans l'onglet <b>Réseau</b>.</p> <p>Si vous activez le cryptage des clients et serveurs récupérant les flux de données du serveur d'enregistrement, une icône représentant un cadenas apparaît, ainsi qu'une adresse affichant <b>https</b> au lieu de <b>http</b>.</p>
<b>Port UDP</b>	Le numéro de port utilisé pour la communication entre les serveurs d'enregistrement de redondance. Le port par défaut est 8844.
<b>Emplacement de la base de données</b>	<p>Spécifiez le chemin conduisant à la base de données utilisée par le serveur d'enregistrement de redondance pour le stockage des enregistrements.</p> <p>Vous ne pouvez pas modifier le chemin de la base de données lorsque le serveur d'enregistrement de redondance prend le relais d'un serveur d'enregistrement. Le système applique les modifications lorsque le serveur d'enregistrement de redondance ne prend</p>

Nom	Description
	plus le relais du serveur d'enregistrement.
<b>Activer ce serveur de redondance</b>	Décochez la case pour désactiver le serveur d'enregistrement de redondance (cochée par défaut). Vous devez désactiver les serveurs d'enregistrement de redondance avant qu'ils puissent prendre le relais des serveurs d'enregistrement.

## Info Propriétés de l'onglet Groupe de basculement

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

## Propriétés de l'onglet Séquence de groupe de basculement

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

## Services du serveur d'enregistrement de redondance (explications)

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

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

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

Dans une configuration à affectation unique, ce service fonctionne en permanence et permet au serveur de redondance à affectation unique de prendre le relais plus rapidement que le serveur d'enregistrement de redondance à froid.

## Voir le cryptage sur un serveur d'enregistrement de redondance

Pour vérifier si votre serveur d'enregistrement de redondance utilise le cryptage, suivez les étapes suivantes :

1. Dans le panneau **Navigation du site**, sélectionnez **Serveurs > Serveurs de basculement**. Cette commande ouvre une liste de serveurs d'enregistrement.
2. Dans le volet **Vue d'ensemble**, sélectionnez le serveur d'enregistrement concerné, puis allez sur l'onglet **Info**.

Si le cryptage est activé vers les clients et serveurs récupérant des flux de données depuis le serveur d'enregistrement, une icône représentant un cadenas apparaîtra devant l'adresse du serveur Web local et

l'adresse du serveur Web optionnel.

**Properties**

Failover server information

Name:  
Failover recording server 1

Description:  
Failover for Recording server 1

Host name:  
192.168.1.101.local

Local web server address:  
https://192.168.1.101.local:7563/

Web server address:  
https://www.failoverrecordingserver1:89/

UDP port:  
8844

Database location:  
C:\MediaDatabase

Enable this failover server

Info Network Multicast

## Voir les messages d'état

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

## Voir les informations sur la version

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

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

## Navigation sur le site : Serveurs et matériel : Matériel

### Matériel (explications)

Le matériel représente :

- L'unité physique qui se connecte directement au serveur d'enregistrement du système de surveillance via IP, par exemple une caméra, un encodeur vidéo ou un module E/S.
- Un serveur d'enregistrement sur un site distant dans une configuration Milestone Interconnect

Pour plus d'informations sur l'ajout d'un matériel à votre système, voir [Ajouter un matériel](#) sur la page 199.

### Ajouter un matériel

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




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

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

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



Certains matériels doivent être préconfigurés lorsque vous ajoutez le matériel pour la première fois. Un assistant **Préconfigurer les périphériques matériels** apparaîtra lorsque vous ajouterez ledit matériel. Pour plus d'informations, voir Configuration matérielle (explications) sur la page 201.

Nom	Description
<p><b>Rapide</b> (recommandé)</p>	<p>Le système recherche automatiquement les nouveaux matériels disponibles sur le réseau local du serveur d'enregistrement.</p> <p>Cochez la case <b>Afficher le matériel exécuté sur d'autres serveurs d'enregistrement</b> pour voir si le matériel détecté fonctionne sur d'autres serveurs d'enregistrement.</p> <p>Vous pouvez sélectionner cette option chaque fois que vous ajoutez un nouveau matériel sur votre réseau et souhaitez l'utiliser dans votre système.</p> <p>Vous ne pouvez pas utiliser cette option pour ajouter des systèmes à distance dans les configurations Milestone Interconnect.</p> <div style="background-color: #e1f5fe; padding: 10px; border: 1px solid #ccc;"> <p> Pour ajouter les matériels HTTP et HTTPS, exécutez la détection <b>Express</b> en ayant coché l'option <b>HTTPS (Sécurisé)</b>, puis en ayant coché l'option <b>HTTP (Non sécurisé)</b>.</p> </div>
<p><b>Analyse de la plage d'adresses</b></p>	<p>Le système recherche les matériels et les systèmes à distance Milestone Interconnect pertinents sur votre réseau en fonction de vos spécifications de :</p> <ul style="list-style-type: none"> <li>• noms d'utilisateur et mots de passe des matériels. Ceci n'est pas nécessaire si votre matériel utilise les noms d'utilisateur et mots de passe par défaut configurés en usine</li> <li>• pilotes</li> <li>• Plages IP (IPv4 uniquement)</li> <li>• numéro de port (port par défaut 80)</li> </ul> <p>Vous pouvez sélectionner cette option lorsque vous souhaitez seulement analyser une partie de votre réseau, par exemple lors d'une expansion de votre système.</p>
<p><b>Manuel</b></p>	<p>Précisez les détails concernant chaque matériel et système à distance Milestone Interconnect séparément. Il peut s'agir d'un choix judicieux si vous souhaitez ajouter uniquement quelques matériels et que vous connaissez leurs adresses IP, les noms</p>



Nom	Description
	d'utilisateur et mots de passe concernés ou si une caméra ne prend pas en charge la fonction de détection automatique.
<b>Matériel de connexion à distance</b>	<p>Le système recherche les matériels connectés au moyen d'un serveur connecté à distance.</p> <p>Vous pouvez utiliser cette option si vous avez installé des serveurs pour, par exemple, la Connexion à la caméra Axis One-click.</p> <p>Vous ne pouvez pas utiliser cette option pour ajouter des systèmes à distance dans les configurations Milestone Interconnect.</p>

## Configuration matérielle (explications)

Certains fabricants exigent que les identifiants soient configurés dans le matériel dès sa sortie de la boîte, soit avant d'ajouter le matériel à un système VMS pour la première fois. Il s'agit de la préconfiguration matérielle qui s'effectue via l'assistant **Préconfigurer le matériel**, lequel apparaît lorsque ledit matériel est détecté par l'assistant Ajouter un matériel sur la page 199.

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

- Un matériel qui requiert des identifiants de base avant son ajout dans un système VMS ne peut être ajouté via les identifiants par défaut habituels. Il doit être configuré via l'assistant ou en vous connectant directement au matériel
- Les identifiants (nom d'utilisateur et mot de passe) peuvent être ajoutés uniquement dans les champs marqués comme **non configuré**
- Une fois que l'**état** du matériel est paramétré sur **configuré**, vous ne pouvez plus changer les identifiants de connexion (nom d'utilisateur ou mot de passe)
- La préconfiguration s'applique aux matériels prêts à l'emploi et ne doit être faite qu'une seule fois. Une fois préconfiguré, le matériel peut être géré comme n'importe quel autre matériel dans Management Client
- Après la fermeture de l'assistant **Préconfigurer le matériel**, le matériel préconfiguré apparaîtra dans l'assistant Ajouter un matériel sur la page 199 et il peut être ajouté à votre système



Nous vous recommandons fortement d'ajouter le matériel préconfiguré à votre système via l'assistant Ajouter un matériel sur la page 199 une fois que vous fermez l'assistant **Préconfigurer un matériel**. Management Client ne conservera pas les identifiants préconfigurés si vous n'ajoutez pas le matériel à votre système.

## Désactiver/activer le matériel

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

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



activé



Désactivé

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

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

## Modifier le matériel




Effectuez un clic droit avec votre souris sur le matériel ajouté, puis sélectionnez **Modifier le matériel** pour modifier la configuration du réseau et les paramètres d'authentification des utilisateurs du matériel dans Management Client.




Pour certains matériels, la boîte de dialogue **Modifier le matériel** vous permet également d'appliquer les paramètres directement sur le matériel.

Si le bouton radio **Modifier les paramètres de Management Client** est sélectionné, la boîte de dialogue **Modifier le matériel** affiche les paramètres qu'utilisent Management Client pour se connecter au matériel. Pour vous assurer que le matériel est correctement ajouté au système, entrez les paramètres que vous avez utilisés pour vous connecter à l'interface de configuration du matériel du fabricant :




Nom	Description
<b>Nom</b>	Affiche le nom du matériel, ainsi que son adresse IP détectée (entre parenthèses).
<b>URL du matériel</b>	L'adresse Web de l'interface de configuration du matériel du fabricant, contient en général l'adresse IP du matériel.
<b>Nom d'utilisateur</b>	Le nom d'utilisateur utilisé pour se connecter au matériel.






Nom	Description
	<div style="background-color: #f9e79f; padding: 10px; border-left: 3px solid #c07040;">  <p>Le nom d'utilisateur saisi ici ne modifie pas le nom d'utilisateur sur le périphérique matériel actuel. Sélectionnez le bouton radio <b>Modifier les paramètres de Management Client et du matériel</b> pour modifier les paramètres des périphériques pris en charge.</p> </div>
<p><b>Mot de passe</b></p>	<p>Le mot de passe utilisé pour se connecter au matériel.</p> <div style="background-color: #f9e79f; padding: 10px; border-left: 3px solid #c07040;">  <p>Le mot de passe saisi ici ne modifie pas le mot de passe sur le périphérique matériel actuel. Sélectionnez le bouton radio <b>Modifier les paramètres de Management Client et du matériel pour modifier les paramètres des périphériques pris en charge.</b></p> </div> <div style="background-color: #d9ead3; padding: 10px; border-left: 3px solid #558b2f; margin-top: 10px;">  <p>Pour plus d'informations sur comment modifier les mots de passe sur plusieurs périphériques matériels, voir Modifier les mots de passe sur les périphériques matériels sur la page 211.</p> </div> <p>En tant qu'administrateur du système, vous devez donner aux autres utilisateurs la permission de voir le mot de passe dans le Management Client. Pour plus d'informations, voir Paramètres des rôles sur la page 374 sous Matériel.</p>


Si le bouton radio **Modifier les paramètres du Management Client et du matériel** est sélectionné (pour le matériel pris en charge), la boîte de dialogue **Modifier le matériel** affiche les paramètres, qui sont également appliqués directement au matériel :



L'application des paramètres avec ce bouton radio sélectionné remplacera les paramètres actuels sur le matériel. Le matériel perdra momentanément sa connexion au serveur d'enregistrement lors de l'application des paramètres.

Nom	Description
Nom	Affiche le nom du matériel, ainsi que son adresse IP détectée (entre parenthèses).
Configuration du réseau	Les paramètres du réseau sur le matériel. Pour ajuster les paramètres du réseau, sélectionnez Configurer sur la page 204.
Configurer	<p>Spécifiez le Protocole Internet (pour les matériels pris en charge) à l'aide de la liste déroulante <b>Version IP</b>.</p> <ul style="list-style-type: none"> <li>Pour IPv4, les valeurs doivent être au format : <b>(0-999).(0-999).(0-999).(0-999)</b></li> <li>Pour IPv6, les valeurs doivent être au format de huit groupes de chiffres hexadécimaux, chacun séparé d'une virgule. Le masque de sous-réseau doit être un numéro entre <b>0-128</b>.</li> </ul> <p>Le bouton <b>Vérifier</b> teste s'il existe actuellement un autre matériel dans le système qui utilise l'adresse IP saisie.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;">  <p>La fonction <b>Vérifier</b> ne détecte pas les conflits avec des matériels éteints, en dehors du système VMS XProtect ou qui ne répondent pas momentanément.</p> </div>
Nom d'utilisateur	<p>Le nom d'utilisateur et le niveau utilisés pour se connecter au matériel. Sélectionnez un autre utilisateur depuis la liste déroulante et ajoutez un nouveau mot de passe à l'aide du champ <b>Mot de passe</b>, tel que décrit ci-dessous.</p> <p>Ajoutez ou supprimez des utilisateurs à l'aide d'actions soulignées en bas de la rubrique <b>Authentification</b> (voir <b>Ajouter un utilisateur sur la page 205</b> ou <b>Supprimer des utilisateurs sur la page 205</b>).</p> <div style="background-color: #ffe4c4; padding: 10px; border: 1px solid #a52a2a;">  <p>La sélection d'un utilisateur n'ayant pas le niveau d'utilisateur le plus élevé spécifié par le fabricant pourrait rendre certaines fonctionnalités indisponibles.</p> </div>
Mot de passe	<p>Le mot de passe utilisé pour se connecter au matériel. Afficher le texte actuellement saisi à l'aide de l'icône  <b>Révéler</b>.</p> <p>Lorsque vous changez le mot de passe, consultez la documentation fournie par le fabricant concernant les règles du mot de passe du matériel en question ou utilisez l'icône</p>

Nom	Description
	<p data-bbox="376 327 1318 432">  <b>Générer un mot de passe</b> pour générer automatiquement un mot de passe qui répond aux exigences du fabricant.                 </p> <div data-bbox="376 454 1385 620" style="background-color: #e1f5fe; padding: 10px; border: 1px solid #cfcfcf;"> <p data-bbox="416 510 1238 591">  Pour plus d'informations sur comment modifier les mots de passe sur plusieurs périphériques matériels, voir <a href="#">Modifier les mots de passe sur les périphériques matériels</a> sur la page 211.                     </p> </div> <p data-bbox="376 674 1355 779">                     En tant qu'administrateur du système, vous devez donner aux autres utilisateurs la permission de voir le mot de passe dans le Management Client. Pour plus d'informations, voir <a href="#">Paramètres des rôles</a> sur la page 374 sous <a href="#">Matériel</a>.                 </p>
<p data-bbox="172 1200 296 1263"><b>Ajouter</b> un utilisateur</p>	<p data-bbox="376 826 1372 896">                     Cliquez sur le lien souligné <b>Ajouter</b> pour ouvrir la boîte de dialogue <b>Ajouter un utilisateur</b> et ajouter un utilisateur au matériel.                 </p> <div data-bbox="376 918 1385 1084" style="background-color: #ffe0b2; padding: 10px; border: 1px solid #cfcfcf;"> <p data-bbox="416 974 1198 1055">  L'ajout d'un utilisateur le configurera automatiquement comme utilisateur actif actuel et remplacera les identifiants saisis auparavant.                     </p> </div> <p data-bbox="376 1137 1390 1319">                     Lorsque vous créez le mot de passe, consultez la documentation fournie par le fabricant concernant les règles du mot de passe du matériel en question ou utilisez l'icône  <b>Générer un mot de passe</b> pour générer automatiquement un mot de passe qui répond aux exigences du fabricant.                 </p> <p data-bbox="376 1346 1278 1451">                     Le niveau d'utilisateur le plus élevé détecté sur le matériel sera automatiquement présélectionné. Il n'est pas conseillé de modifier la valeur par défaut du <b>Niveau d'utilisateur</b>.                 </p> <div data-bbox="376 1473 1385 1639" style="background-color: #ffe0b2; padding: 10px; border: 1px solid #cfcfcf;"> <p data-bbox="416 1529 1222 1610">  La sélection d'un <b>Niveau d'utilisateur</b> autre que le niveau d'utilisateur le plus élevé spécifié par le fabricant pourrait rendre certaines fonctionnalités indisponibles.                     </p> </div>
<p data-bbox="172 1686 296 1789"><b>Supprimer</b> des utilisateurs</p>	<p data-bbox="376 1704 1321 1774">                     Cliquez sur le lien souligné <b>Supprimer</b> pour ouvrir la boîte de dialogue <b>Supprimer des utilisateurs</b> et supprimer des utilisateurs du matériel.                 </p>

Nom	Description
	<div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #add8e6;">  <p data-bbox="507 353 1257 499">Vous ne pouvez pas supprimer l'utilisateur actuellement actif. Pour configurer un nouvel utilisateur, utilisez la boîte de dialogue <b>Ajouter un utilisateur</b> décrite ci-dessus, puis supprimez l'ancien utilisateur à l'aide de l'interface.</p> </div>

Voir également [Gérer le matériel](#).

## Activer/désactiver des périphériques individuels

Les caméras sont **activées** par défaut.

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

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

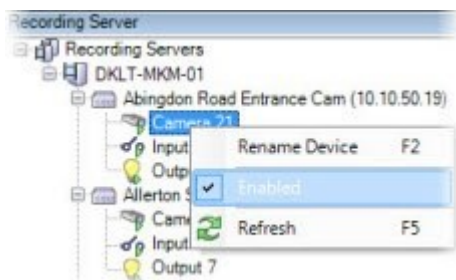
Vous pouvez voir si les périphériques sont activés ou désactivés (les exemples montrent une sortie) :

 Désactivé

 activé

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

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



## Configurer une connexion sécurisée avec le matériel

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

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

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



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

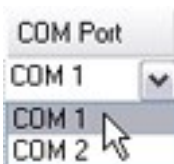
## Activer PTZ sur un encodeur vidéo

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

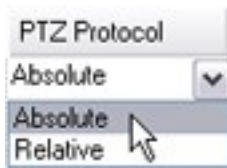
1. Dans la liste des périphériques connectés à l'encodeur vidéo, cochez la case **Activer PTZ** pour les caméras concernées :



2. Dans la colonne **ID du périphérique PTZ**, vérifiez l'ID de chaque caméra.
3. Dans la colonne **Port COM**, sélectionnez quels ports COM (communication série) de l'encodeur vidéo utiliser pour contrôler la fonctionnalité PTZ :



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



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

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

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

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

- Ajouter une position prédéfinie (type 1) sur la page 255
- Ajouter un profil de patrouille sur la page 265

## Gérer le matériel


### Onglet Info (matériel)

Pour des informations sur l'onglet **Info** pour les serveurs distants, consultez l' Onglet Info (serveur distant) sur la page 214.

### Onglet Info (matériel)

Nom	Description
<b>Nom</b>	Saisissez un nom. Le système utilise le nom partout où le matériel est répertorié dans le système et les clients. Le nom ne doit pas nécessairement être unique.  Lorsque vous renommez un matériel, son nom est modifié de manière globale dans le Management Client.
<b>Description</b>	Saisissez une description du matériel (facultatif). La description apparaît dans plusieurs listes au sein du système. Par exemple, lorsque vous arrêtez le curseur de la souris sur le



Nom	Description
	<p>nom du matériel dans le volet <b>Vue d'ensemble</b> :</p> 
<b>Modèle</b>	Identifie le modèle du périphérique.
<b>Numéro de série</b>	Numéro de série du matériel tel que spécifié par le fabricant. Le numéro de série est souvent, mais pas toujours, identique à l'adresse MAC.
<b>Pilote</b>	Identifie le pilote prenant en charge la connexion au matériel.
<b>IE</b>	Ouvre la page d'accueil par défaut du fournisseur du matériel. Vous pouvez utiliser cette page à des fins d'administration du matériel.
<b>Adresse</b>	L'adresse IP ou le nom d'hôte du matériel.
<b>Adresse MAC</b>	Indique l'adresse de contrôle d'accès aux médias (MAC) du matériel du système. Une adresse MAC est un nombre hexadécimal à 12 caractères qui identifie spécifiquement chacun des périphériques d'un réseau.
<b>Dernière modification du mot de passe</b>	Le champ <b>Dernière modification du mot de passe</b> indique l'horodatage du dernier changement de mot de passe en fonction des paramètres de l'heure locale de l'ordinateur où a été modifié le mot de passe.

### Onglet Paramètres (matériel)

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



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

Pour en savoir plus sur l'onglet **Paramètres** pour les serveurs distants, consultez l'onglet Paramètres (serveur à distance) sur la page 215.

### Onglet PTZ (encodeurs vidéo)

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

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



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



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

### Gestion des mots de passe périphériques (explication)



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

Vous pouvez modifier les mots de passe sur plusieurs périphériques matériels en une seule opération.

Initialement, les périphériques pris en charge sont les modèles des périphériques compatibles de Canon, Axis, Bosch, Hanwa, Panasonic, Sony, Hikvision et ONVIF, mais l'interface utilisateur vous affiche directement si un modèle est pris en charge ou non. Vous pouvez également vous rendre sur notre site Web pour vérifier si un modèle est pris en charge : <https://www.milestonesys.com/community/business-partner-tools/supported-devices/>



Pour les périphériques ne prenant pas en charge la gestion des mots de passe périphériques, vous devez modifier le mot de passe d'un périphérique matériel depuis sa page Web, puis saisir manuellement le nouveau mot de passe dans Management Client. Pour plus d'informations, voir Modifier le matériel sur la page 202.

Vous pouvez choisir de laisser le système générer des mots de passe individuels pour chaque périphérique matériel, ou utiliser un seul mot de passe défini par utilisateur pour tous les périphériques matériels. Dans Mots de passe, seuls les caractères imprimables ASCII sont pris en charge.

Le système génère des mots de passe en fonction des exigences du fabricant des périphériques matériels.

Lorsque vous appliquez les nouveaux mots de passe, les périphériques matériels perdent momentanément leur connexion au serveur d'enregistrement.

Après avoir appliqué les nouveaux mots de passe, le résultat de chaque périphérique matériel s'affiche à l'écran. En cas d'échec des modifications, la raison de l'échec s'affiche si le périphérique matériel prend en charge lesdites informations. Depuis l'assistant, vous pouvez créer un rapport sur la réussite ou l'échec des modifications de mot de passe. Les résultats sont tout de même enregistrés dans **Journaux de serveur**.



Pour les périphériques matériels ayant des pilotes ONVIF et plusieurs comptes utilisateurs, seul un administrateur de XProtect ayant les droits administratifs du périphérique matériel, est en mesure de modifier les mots de passe du VMS.

Pour plus d'informations sur comment modifier les mots de passe en une seule opération, voir Modifier les mots de passe sur les périphériques matériels sur la page 211.

## Modifier les mots de passe sur les périphériques matériels



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

Vous pouvez modifier les mots de passe sur plusieurs périphériques matériels en une seule opération. Pour plus d'informations sur cette fonctionnalité et les modèles pris en charge, voir Gestion des mots de passe périphériques (explication) sur la page 210.

### Exigences :

- Le modèle de périphérique matériel prend en charge la gestion des mots de passe des périphériques par Milestone.

Étapes :

1. Dans le volet **Navigation du site** pane, sélectionnez le nœud **Serveurs d'enregistrement** .
2. Faites un clic droit sur le serveur d'enregistrement ou le matériel concerné dans le panneau Vue d'ensemble.
3. Sélectionnez **Modifier le mot de passe du matériel**. Un assistant apparaît.
4. Suivez les instructions à l'écran pour achever les changements.



Le champ **Dernière modification du mot de passe** indique l'horodatage du dernier changement de mot de passe en fonction des paramètres de l'heure locale de l'ordinateur où a été modifié le mot de passe.

5. Le résultat s'affiche sur la dernière page. Si le système échoue lors de la mise à jour d'un mot de passe, cliquez sur **Échec** à côté du périphérique matériel pour en connaître la raison.
6. Vous pouvez également cliquer sur le bouton **Imprimer un rapport** pour afficher la liste complète des mises à jour réussies et infructueuses.
7. Si vous souhaitez modifier le mot de passe sur les périphériques matériels ayant échoué, cliquez sur **Réessayer** et l'assistant recommence l'opération sur lesdits périphériques matériels.



Si vous cliquez sur **Réessayer**, vous perdez l'accès au rapport correspondant à votre première tentative avec l'assistant.



En raison de restrictions liées à la sécurité, certains périphériques matériels peuvent devenir indisponibles durant une période de temps si vous échouez à modifier le mot de passe plusieurs fois de suite. Les restrictions liées à la sécurité varient en fonctions des fabricants.

## Mise à jour du firmware d'un périphérique (explications)



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

Management Client vous permet de mettre à jour le firmware du matériel ayant été ajouté à votre système VMS. Vous pouvez mettre à jour le firmware de plusieurs périphériques en même temps si ces derniers sont compatibles avec le même fichier du firmware.

L'interface utilisateur vous indique directement si un modèle prend en charge les mises à jour du firmware. Vous pouvez également vous rendre sur le site Web de Milestone pour vérifier si un modèle est pris en charge :

<https://www.milestonesys.com/community/business-partner-tools/supported-devices/>



Pour les périphériques qui ne prennent pas en charge les mises à jour du firmware, vous devez mettre à jour le firmware d'un périphérique depuis sa page Web.

Lorsque vous mettez à jour le firmware, les périphériques perdent momentanément leur connexion au serveur d'enregistrement.

Après avoir mis à jour le firmware, le résultat de chaque périphérique s'affiche à l'écran. En cas d'échec des modifications, la raison de l'échec s'affiche si le périphérique matériel prend en charge lesdites informations. Les résultats se trouvent sous **Journaux du serveur**.



Pour les périphériques ayant des pilotes ONVIF et plusieurs comptes utilisateurs, seul un administrateur de XProtect ayant les droits administratifs du périphérique, est en mesure de mettre à jour le firmware du VMS.

Pour plus d'informations sur comment modifier les mots de passe en une seule opération, voir Mettre à jour le firmware sur les périphériques sur la page 213.

## Mettre à jour le firmware sur les périphériques



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

Vous pouvez mettre à jour le firmware de plusieurs périphériques en une seule opération. Pour plus d'informations sur cette fonctionnalité et les modèles pris en charge, voir Mise à jour du firmware d'un périphérique (explications) sur la page 212.

### Exigences :

- Le modèle du périphérique doit prendre en charge les mises à jour du firmware par Milestone.

Étapes :

1. Dans le volet **Navigation du site** pane, sélectionnez le nœud **Serveurs d'enregistrement** .
2. Faites un clic droit sur le serveur d'enregistrement ou le matériel concerné dans le panneau Vue d'ensemble.
3. Sélectionnez **Mettre à jour le firmware du matériel**. Un assistant apparaît.
4. Suivez les instructions à l'écran pour achever les changements.



Vous pourrez peut-être mettre à jour uniquement plusieurs périphériques étant compatibles avec le même fichier du firmware. Le matériel ajouté par le pilote ONVIF se trouve sous **autre**, et non sous le nom du fabricant.

- Le résultat s'affiche sur la dernière page. Si le système échoue lors de la mise à jour du firmware, cliquez sur **Échec** à côté du périphérique pour en connaître la raison.



Milestone décline toute responsabilité pour un dysfonctionnement du périphérique dû à un fichier du firmware ou d'un périphérique incompatible.

## Navigation sur le site : Serveurs et matériel : Gérer les serveurs distants

### Onglet Info (serveur distant)

Nom	Description
<b>Nom</b>	Le système utilise le nom partout où le serveur distant est répertorié dans le système et les clients. Le nom ne doit pas nécessairement être unique.  Lorsque vous renommez un serveur, son nom est modifié de manière globale dans le Management Client.
<b>Description</b>	Saisissez une description du serveur distant (facultatif).  La description apparaît dans plusieurs listes au sein du système. Par exemple, lorsque vous arrêtez le curseur de la souris sur le nom du matériel dans le volet <b>Vue d'ensemble</b> .
<b>Modèle</b>	Affiche le produit XProtect installé sur le site distant.
<b>Version</b>	Affiche la version du système à distance.
<b>Code de licence du logiciel</b>	Code de licence du logiciel du système à distance.

Nom	Description
<b>Pilote</b>	Identifie le pilote prenant en charge la connexion au serveur distant.
<b>Adresse</b>	L'adresse IP ou le nom d'hôte du matériel.
<b>IE</b>	Ouvre la page d'accueil par défaut du fournisseur du matériel. Vous pouvez utiliser cette page à des fins d'administration des matériels ou du système.
<b>ID du système à distance</b>	L'ID unique du système du site distant utilisée par XProtect pour gérer les licences, par exemple.
<b>Nom d'utilisateur Windows</b>	Saisissez le nom de l'utilisateur Windows pour avoir un accès par le biais du bureau distant.
<b>Mot de passe Windows</b>	Saisissez le mot de passe Windows pour avoir un accès par le biais du bureau distant.
<b>Connecter</b>	Ouvre une connexion à distance avec le site distant (sur approbation des identifiants de connexion Windows).

## Onglet Paramètres (serveur à distance)

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

## Onglet Événements (serveur distant)

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

Si la liste semble incomplète :

1. Faites un clic droit sur le serveur distant concerné dans le volet **Vue d'ensemble** et sélectionnez **Mettre le matériel à jour**.
2. La boîte de dialogue répertorie tous les changements (périphériques supprimés, mis à jour et ajoutés) dans le système à distance depuis que vous avez établi ou actualisé pour la dernière fois la configuration Milestone Interconnect. Cliquez sur **Confirmer** pour mettre votre site central à jour avec ces changements.

## Onglet Rappel à distance

Dans l'onglet **Récupération à distance**, vous pouvez gérer les paramètres de récupération d'enregistrement à distance pour le site distant dans une configuration Milestone Interconnect :

Spécifiez les propriétés suivantes :

Nom	Description
<b>Rappeler les enregistrements au max</b>	Détermine la bande passante maximale (en Kbits/s) à utiliser pour rappeler des enregistrements à partir d'un site distant. Cochez la case pour activer la fonction de limitation des rappels.
<b>Rappeler les enregistrements entre</b>	<p>Détermine que le rappel d'enregistrements à partir d'un site distant doit être limité à un intervalle de temps spécifique.</p> <p>Les travaux non terminés à l'heure de fin se poursuivent jusqu'à leur achèvement, donc si l'heure de fin est critique, vous devez la régler plus tôt pour permettre aux travaux non terminés de s'achever.</p> <p>Si le système reçoit une récupération automatique ou une demande de récupération à partir du XProtect Smart Client en dehors de l'intervalle de temps, elle est acceptée, mais n'est pas commencée avant d'avoir atteint l'intervalle de temps sélectionné.</p> <p>Vous pouvez visualiser les tâches de rappel d'enregistrement à distance en instance déclenchées par les utilisateurs à partir du <b>Tableau de bord système</b> -&gt; <b>Tâches actuelles</b>.</p>
<b>Rappeler sur des périphériques en parallèle</b>	Détermine le nombre maximum de périphériques sur lesquels des enregistrements peuvent être récupérés simultanément. Modifiez la valeur par défaut si vous avez besoin de plus ou moins de capacité en fonction des capacités de votre système.

Lorsque vous modifiez les paramètres, plusieurs minutes peuvent être nécessaires pour que les modifications apparaissent dans le système.



Aucune de ces options ne s'applique à la lecture directe des enregistrements à distance. Toutes les caméras configurées pour être lues directement sont disponibles pour une lecture en direct et utilisent la bande passante selon les besoins.



## Navigation sur le site : Périphériques : Travailler avec des périphériques

Les périphériques apparaissent dans le Management Client lorsque vous ajoutez du matériel à l'aide de l'assistant **Ajouter matériel**.

Vous avez la possibilité de gérer les périphériques par le biais de groupes de périphériques s'ils disposent des mêmes propriétés, voir Navigation sur le site : Périphériques : Travailler avec des groupes de périphériques sur la page 227.

Vous pouvez également gérer les périphériques individuellement :

- Caméras
- Microphones
- Haut-parleurs
- Métadonnées
- Entrées
- Sorties

### Périphériques (explications)

Le matériel a un certain nombre de dispositifs que vous pouvez gérer individuellement, par exemple :

- Une caméra physique dispose de périphériques qui représentent les parties de la caméra (objectifs) ainsi que les microphones, les haut-parleurs, les métadonnées, les entrées et les sorties reliés ou intégrés
- Un encodeur vidéo dispose de plusieurs caméras analogiques connectées qui apparaissent dans une liste de périphériques qui représentent les parties de la caméra (objectifs) ainsi que les microphones, les haut-parleurs, les métadonnées, les entrées et les sorties reliés ou intégrés
- Un module d'entrée/sortie comporte des dispositifs qui représentent les canaux d'entrée et de sortie pour les lumières, par exemple
- Un module dédié à l'audio comporte des dispositifs qui représentent les entrées et les sorties des microphones et des haut-parleurs
- Dans une configuration Milestone Interconnect, le système distant apparaît comme un matériel présentant tous les périphériques du système à distance énumérés dans une liste

Le système ajoute automatiquement les périphériques du matériel lorsque vous ajoutez un matériel.



Pour plus d'informations sur le matériel pris en charge, voir la page du matériel supporté sur le site Internet de Milestone (<https://www.milestonesys.com/supported-devices/>).

Les sections suivantes décrivent chaque type de périphérique avec des liens vers les onglets que vous pouvez utiliser pour les gérer.

## Dispositifs de caméra (explications)

Les périphériques de la caméra sont ajoutés automatiquement lorsque vous ajoutez un matériel sur le système et qu'ils sont activés par défaut.

Les périphériques de caméra offrent un flux vidéo au système que les utilisateurs du client peuvent utiliser pour afficher la vidéo en direct ou que le système peut enregistrer pour une lecture ultérieure par les utilisateurs du client. Les rôles déterminent le droit des utilisateurs à visualiser la vidéo.



Pour plus d'informations sur le matériel pris en charge, voir la page du matériel supporté sur le site Internet de Milestone (<https://www.milestonesys.com/supported-devices/>).

Le système est fourni avec une règle de flux de démarrage par défaut qui garantit que les flux audio de toutes les caméras connectées soient automatiquement transmis au système. Comme les autres règles, la règle par défaut peut être désactivée et/ou modifiée selon les besoins.

Activer/désactiver et renommer les périphériques individuels s'effectue au niveau du matériel du serveur d'enregistrement. Voir Activer/désactiver des périphériques par le biais des groupes de périphériques sur la page 224.

Pour toute autre configuration et gestion des caméras, développez **Périphériques** dans le volet Navigation du site, puis sélectionnez **Caméras**. Dans le volet Vue d'ensemble, vous regroupez vos caméras pour une vue d'ensemble aisée de vos caméras. Le regroupement initial est effectué dans le cadre de l'assistant **Ajout de matériel**.

Suivez cet ordre de configuration pour effectuer les tâches les plus courantes liées à la configuration d'un périphérique de caméra :

1. Configurez les paramètres de la caméra (voir Onglet Paramètres (périphériques) sur la page 233).
2. Configurez le flux (voir Onglet Flux (périphériques) sur la page 234).
3. Configurez le mouvement (voir Onglet Mouvement (périphériques) sur la page 245).
4. Configurez l'enregistrement (voir Onglet Enregistrement (périphériques) sur la page 237).
5. Configurez les autres paramètres selon vos besoins.

## Microphones (explications)

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

Les périphériques de micros sont ajoutés automatiquement lorsque vous ajoutez un matériel sur le système. Ils sont par défaut désactivés, vous devez donc les réactiver avant utilisation, soit avec l'assistant **Ajout matériel** soit par la suite. Les micros ne nécessitent aucune licence distincte. Vous pouvez utiliser autant de microphones que nécessaire sur votre système.

Vous pouvez utiliser des microphones entièrement indépendamment des caméras.

Les périphériques de micros offrent un flux audio au système que les utilisateurs du client peuvent utiliser pour écouter en direct ou que le système peut enregistrer pour une lecture ultérieure par les utilisateurs du client. Vous pouvez configurer le système pour recevoir des événements spécifiques de microphone qui déclenchent des actions pertinentes.



Pour plus d'informations sur le matériel pris en charge, voir la page du matériel supporté sur le site Internet de Milestone (<https://www.milestonesys.com/supported-devices/>).

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

Le système est fourni avec une règle de flux de démarrage audio par défaut qui garantit que les flux audio de tous les micros connectés soient automatiquement transmis au système. Comme les autres règles, la règle par défaut peut être désactivée et/ou modifiée selon les besoins.

Activer/désactiver et renommer les périphériques individuels s'effectue au niveau du matériel du serveur d'enregistrement. Pour plus d'informations, voir Activer/désactiver des périphériques par le biais des groupes de périphériques sur la page 224.

Pour toute autre configuration et gestion des caméras, développez **Périphériques** dans le volet Navigation du site de Management Client, puis sélectionnez **Microphones**. Dans le volet de vue d'ensemble, vous regroupez vos micros pour pouvoir les examiner plus facilement. Le regroupement initial est effectué dans le cadre de l'assistant **Ajout de matériel**.

Vous pouvez configurer les périphériques de microphones sur ces onglets :

- Onglet Infos (voir Onglet Info (périphériques) sur la page 230)
- Onglet Paramètres (voir Onglet Paramètres (périphériques) sur la page 233)
- Onglet Enregistrement (voir Onglet Enregistrement (périphériques) sur la page 237)
- Onglet Événements (voir Onglet Événements (périphériques) sur la page 270)

## Périphériques de haut-parleurs (explications)

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

Les périphériques de haut-parleurs sont ajoutés automatiquement lorsque vous ajoutez un matériel sur le système. Ils sont par défaut désactivés, vous devez donc les réactiver avant utilisation, soit avec l'assistant **Ajout matériel** soit par la suite. Les haut-parleurs ne nécessitent aucune licence distincte. Vous pouvez utiliser autant de haut-parleurs que nécessaire sur votre système.

Vous pouvez utiliser des haut-parleurs entièrement indépendamment des caméras.



Pour plus d'informations sur le matériel pris en charge, voir la page du matériel supporté sur le site Internet de Milestone (<https://www.milestonesys.com/supported-devices/>).

Le système envoie un flux audio vers les haut-parleurs lorsque l'utilisateur appuie sur le bouton de conversation dans XProtect Smart Client. L'audio des haut-parleurs n'est enregistré que lorsqu'un utilisateur parle. Les Rôles déterminent le droit des utilisateurs de parler dans les haut-parleurs. Vous ne pouvez pas parler dans les haut-parleurs depuis le Management Client.

Si deux utilisateurs veulent parler en même temps, les rôles déterminent le droit des utilisateurs à parler dans les haut-parleurs. Dans le cadre de la définition des rôles, vous pouvez spécifier la priorité d'un haut-parleur de très haute à très basse. Si deux utilisateurs veulent parler en même temps, l'utilisateur dont le rôle possède la priorité la plus haute remporte la possibilité de parler. Si deux utilisateurs avec le même rôle souhaitent parler en même temps, la règle du premier arrivé premier servi s'applique.

Le système est livré avec une règle de flux audio de démarrage par défaut qui lance le dispositif afin que l'appareil soit prêt à envoyer l'audio activé par l'utilisateur vers les haut-parleurs. Comme les autres règles, la règle par défaut peut être désactivée et/ou modifiée selon les besoins.

Activer/désactiver et renommer les périphériques individuels s'effectue au niveau du matériel du serveur d'enregistrement. Voir Activer/désactiver des périphériques par le biais des groupes de périphériques sur la page 224.

Pour toute autre configuration et gestion des caméras, développez **Périphériques** dans le volet de navigation du site, puis sélectionnez **Microphones**. Dans le volet de vue d'ensemble, vous regroupez vos haut-parleurs pour pouvoir les examiner plus facilement. Le regroupement initial est effectué dans le cadre de l'assistant **Ajout de matériel**.

Vous pouvez configurer les périphériques de haut-parleurs sur les onglets suivants :

- Onglet Info (périphériques) sur la page 230
- Onglet Paramètres (périphériques) sur la page 233
- Onglet Enregistrement (périphériques) sur la page 237

## Périphériques métadonnées (explications)

Les périphériques de métadonnées fournissent des flux de données au système que les utilisateurs du client peuvent utiliser pour afficher des informations sur les données, par exemple, des données qui décrivent l'image vidéo, le contenu ou les objets de l'image, ou la localisation de l'endroit où l'image a été enregistrée. Les métadonnées peuvent être reliées à des caméras, des microphones, ou à des haut-parleurs.

Les métadonnées peuvent être générées par :

- Le périphérique lui-même en fournissant les données. Par exemple une caméra qui diffuse la vidéo
- Un système tiers ou une intégration via un pilote de métadonnées générique

Les métadonnées générées par un périphérique sont automatiquement liées à un ou plusieurs périphériques sur le même matériel.



Pour plus d'informations sur le matériel pris en charge, voir la page du matériel supporté sur le site Internet de Milestone (<https://www.milestonesys.com/supported-devices/>).

Les rôles déterminent le droit des utilisateurs à visualiser les métadonnées.

Le système est fourni avec une règle de flux de démarrage par défaut qui garantit que les flux de métadonnées de tout matériel connecté qui prend en charge les métadonnées soient automatiquement transmis au système. Comme les autres règles, la règle par défaut peut être désactivée et/ou modifiée selon les besoins.

Activer/désactiver et renommer les périphériques individuels s'effectue au niveau du matériel du serveur d'enregistrement. Pour plus d'informations, voir Activer/désactiver des périphériques par le biais des groupes de périphériques sur la page 224.

Pour toute autre configuration et gestion des périphériques de métadonnées, développez **Périphériques** dans le volet Navigation du site, puis sélectionnez **Métadonnées**. Dans le volet de vue d'ensemble, vous regroupez vos périphériques de métadonnées pour pouvoir les examiner plus facilement. Le regroupement initial est effectué dans le cadre de l'assistant **Ajout de matériel**.

Vous pouvez configurer les périphériques de métadonnées sur les onglets suivants :

- Onglet Infos (voir Onglet Info (périphériques) sur la page 230)
- Onglet Paramètres (voir Onglet Paramètres (périphériques) sur la page 233)
- Onglet Enregistrement (voir Onglet Enregistrement (périphériques) sur la page 237)

## Périphériques d'entrée (explications)

Sur de nombreux périphériques, il est possible de connecter des appareils externes aux ports d'entrée du périphérique. Les unités d'entrée sont généralement des capteurs externes. Vous pouvez utiliser ces capteurs externes pour détecter si les portes, les fenêtres ou les portes sont ouvertes, par exemple. Les entrées de ces unités d'entrée externes sont traitées comme des événements par le système.

Vous pouvez utiliser ces événements dans les règles. Vous pourriez par exemple créer une règle spécifiant qu'une caméra devrait commencer à enregistrer lorsqu'une entrée est activée et arrêter d'enregistrer 30 secondes après la désactivation de l'entrée.

Vous pouvez utiliser des périphériques d'entrée de façon entièrement indépendante des caméras.



Avant de définir l'utilisation d'unités externes d'entrée sur un périphérique, vérifiez que le fonctionnement du détecteur est reconnu par le périphérique. La plupart des périphériques peuvent indiquer ceci dans leur interface de configuration ou via les commandes de script Common Gateway Interface (CGI).

Les périphériques d'entrée sont ajoutés automatiquement lorsque vous ajoutez un matériel sur le système. Ils sont par défaut désactivés, vous devez donc les réactiver avant utilisation, soit avec l'assistant **Ajout matériel** soit par la suite. Les périphériques d'entrée ne nécessitent aucune licence distincte. Vous pouvez utiliser autant de périphériques d'entrée que nécessaire sur votre système.



Pour plus d'informations sur le matériel pris en charge, voir la page du matériel supporté sur le site Internet de Milestone (<https://www.milestonesys.com/supported-devices/>).

Activer/désactiver et renommer les périphériques individuels s'effectue au niveau du matériel du serveur d'enregistrement. Voir Activer/désactiver des périphériques par le biais des groupes de périphériques sur la page 224.

Pour toute autre configuration et gestion des caméras, développez **Périphériques** dans le volet Navigation du site, puis sélectionnez **Entrée**. Dans le volet de vue d'ensemble, vous regroupez vos périphériques d'entrée pour pouvoir les examiner plus facilement. Le regroupement initial est effectué dans le cadre de l'assistant **Ajout de matériel**.

Vous pouvez configurer les périphériques d'entrée sur les onglets suivants :

- Onglet Infos (voir Onglet Info (périphériques) sur la page 230)
- Onglet Paramètres (voir Onglet Paramètres (périphériques) sur la page 233)
- Onglet Événements (voir Onglet Événements (périphériques) sur la page 270)

### Activer une entrée manuellement pour la tester

Avec la fonction de règles, vous définissez les règles permettant d'activer ou de désactiver automatiquement une entrée. Vous pouvez également les activer manuellement et vérifier le résultat dans le Management Client :

1. Dans le volet **Vue d'ensemble**, sélectionnez le périphérique d'entrée concerné.
2. Activez l'entrée sur le périphérique physique.
3. Dans le volet **Aperçu**, vérifiez si les témoins d'indication s'allument en vert. Cela signifie que le périphérique d'entrée fonctionne.



```
14:41:05 Activated  
14:41:02 Deactivated  
14:41:01 Activated  
14:41:00 Deactivated  
14:41:00 Activated  
14:40:59 Deactivated  
14:40:59 Activated  
14:40:59 Deactivated
```

## Périphériques de sortie (explications)

Sur de nombreux périphériques, il est possible de connecter des appareils externes aux ports de sortie du périphérique. Cela vous permet d'activer/désactiver les voyants lumineux, les sirènes, etc. par le biais du système.

Vous pouvez utiliser les sorties au moment de créer des règles. Vous pouvez créer des règles qui activent ou désactivent automatiquement les sorties, et des règles qui déclenchent des actions lorsque l'état d'une sortie est modifié.

Les sorties peuvent également être déclenchées manuellement à partir du Management Client et de XProtect Smart Client.



Avant de définir l'utilisation d'unités externes de sortie sur un périphérique, vérifiez que le dispositif peut lui-même contrôler le périphérique connecté à la sortie. La plupart des périphériques peuvent indiquer ceci dans leur interface de configuration ou via les commandes de script Common Gateway Interface (CGI).

Les périphériques de sortie sont ajoutés automatiquement lorsque vous ajoutez un matériel sur le système. Ils sont par défaut désactivés, vous devez donc les réactiver avant utilisation, soit avec l'assistant **Ajout matériel** soit par la suite. Les périphériques de sortie ne nécessitent aucune licence distincte. Vous pouvez utiliser autant de périphériques de sortie que nécessaire sur votre système.



Pour plus d'informations sur le matériel pris en charge, voir la page du matériel supporté sur le site Internet de Milestone (<https://www.milestonesys.com/supported-devices/>).

Activer/désactiver et renommer les périphériques individuels s'effectue au niveau du matériel du serveur d'enregistrement. Voir Activer/désactiver des périphériques par le biais des groupes de périphériques sur la page 224.

Pour toute autre configuration et gestion des caméras, développez **Périphériques** dans le volet Navigation du site, puis sélectionnez **Sortie**. Dans le volet de vue d'ensemble, vous regroupez vos périphériques d'entrée pour pouvoir les examiner plus facilement. Le regroupement initial est effectué dans le cadre de l'assistant **Ajout de matériel**.

Vous pouvez configurer les périphériques de sortie sur les onglets suivants :

- Onglet Info (périphériques) sur la page 230
- Onglet Paramètres (périphériques) sur la page 233


### Activer une sortie manuellement pour la tester

Avec la fonction de règles, vous définissez les règles permettant d'activer ou de désactiver automatiquement une sortie. Vous pouvez également les activer manuellement depuis un client.


Vous pouvez activer une sortie manuellement depuis le Management Client afin de tester la fonctionnalité :

1. Dans le volet **Vue d'ensemble**, sélectionnez le périphérique de sortie concerné.
2. Les éléments suivants sont généralement représentés pour chaque sortie dans le volet **Aperçu** :



3. Sélectionnez ou désélectionnez la case à cocher   pour activer/désactiver la sortie sélectionnée. Lorsqu'une sortie est activée, l'indicateur devient vert :



4. Vous pouvez aussi cliquer sur le bouton rectangulaire  pour activer la sortie pendant la durée définie dans le paramètre **Durée de déclenchement de la sortie** de l'onglet **Paramètres** (il se peut que cette fonction/ce paramètre ne soit pas disponible pour toutes les sorties). Après la durée définie, la sortie est automatiquement désactivée.

## Activer/désactiver des périphériques par le biais des groupes de périphériques

Vous pouvez activer/désactiver des périphériques uniquement par le biais du matériel configuré. Les périphériques de caméra sont par défaut activés et tous les autres appareils sont par défaut désactivés, sauf s'ils sont activés/désactivés manuellement dans l'assistant d'ajout de matériel.

Pour trouver un périphérique à activer ou désactiver par le biais des groupes de périphériques :

1. Dans le volet **Navigation sur le site**, sélectionnez le périphérique.
2. Dans le volet **Vue d'ensemble**, développez le groupe correspondant et cherchez le périphérique.
3. Faites un clic droit sur le périphérique, puis sélectionnez **Accéder au matériel**.
4. Cliquez sur le nœud plus pour voir tous les appareils sur le matériel.
5. Faites un clic droit sur le périphérique que vous souhaitez activer ou désactiver, puis sélectionnez **Activé**.






















## Icônes de statut des périphériques

Lorsque vous sélectionnez un périphérique, les informations relatives à son statut actuel apparaissent dans le volet **Aperçu**.

Les icônes suivantes indiquent le statut des périphériques :

Caméra	Microphone	Haut-parleurs	Métadonnées	Entrées	Sortie	Description
						<b>Périphérique activé et récupération de données :</b> Le périphérique est activé et vous récupérez un flux en direct.
						<b>Périphérique en cours d'enregistrement :</b> Le périphérique enregistre des données sur le système.
						<b>Périphérique temporairement arrêté ou sans alimentation :</b> Une fois arrêté, aucune information n'est transférée au système. S'il s'agit d'une caméra, vous ne pouvez pas afficher la vidéo en direct. Un périphérique arrêté peut toujours communiquer avec le serveur d'enregistrement pour récupérer des événements, configurer des paramètres, etc., contrairement à un périphérique désactivé.
						<b>Périphériques désactivés :</b> Ne peut pas être activé

Caméra	Microphone	Haut-parleurs	Métadonnées	Entrées	Sortie	Description
						automatiquement au moyen d'une règle et ne peut pas communiquer avec le serveur d'enregistrement. Si une caméra est désactivée, vous ne pouvez pas afficher le direct ou la vidéo enregistrée.
						<b>Base de données du périphérique en cours de réparation.</b>
						<b>Périphériques nécessitant de l'attention</b> : Le périphérique ne fonctionne pas correctement. Survolez l'icône du périphérique avec le curseur de la souris pour obtenir une description du problème dans l'infobulle.
						<b>État inconnu</b> : Le statut du périphérique n'est pas connu, par exemple si le serveur d'enregistrement est hors ligne.
						Certaines icônes peuvent être associées comme dans cet exemple dans lequel <b>Périphérique activé et récupération de données</b> est associé avec <b>Périphérique en cours d'enregistrement</b> .

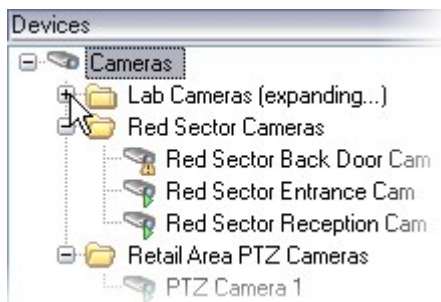
## Navigation sur le site : Périphériques : Travailler avec des groupes de périphériques

Le regroupement de périphériques en groupes de périphériques est contenu dans l'assistant **Ajouter du matériel**, mais vous avez toujours la possibilité de modifier les groupes et d'en ajouter d'autres le cas échéant.

Le regroupement de différents types de périphériques (caméras, microphones, haut-parleurs, métadonnées, entrées et sorties) de votre système constitue un avantage :

- Les groupes de périphériques vous aident à maintenir une vue d'ensemble intuitive des périphériques de votre système
- Les périphériques peuvent être présents dans plusieurs groupes
- Vous pouvez créer des sous-groupes et d'autres sous-groupes dans ces sous-groupes
- Vous pouvez spécifier des propriétés communes pour tous les périphériques d'un groupe de périphériques en une seule fois
- Les propriétés de périphériques définies par le biais du groupe ne sont pas enregistrées pour le groupe, mais pour chaque périphérique individuel
- Lorsque vous traitez de rôles, vous pouvez spécifier des paramètres de sécurité communs pour tous les périphériques d'un groupe de périphériques en une seule fois
- Lorsque vous traitez de règles, vous pouvez appliquer une règle pour tous les périphériques d'un groupe de périphériques en une seule fois

Vous pouvez ajouter autant de groupes de périphériques que nécessaire. En revanche, vous ne pouvez pas mélanger différents types de périphériques (par exemple des caméras et des haut-parleurs) dans un groupe de périphériques.



Créez des groupes de périphériques avec **moins** de 400 périphériques afin de pouvoir afficher et modifier toutes les propriétés.

Si vous supprimez un groupe de périphériques, vous supprimez uniquement le groupe de périphériques à proprement parler. Si vous souhaitez supprimer un périphérique, par exemple une caméra, de votre système, faites-le au niveau du serveur d'enregistrement.

**Les exemples suivants sont basés sur le regroupement de caméras dans des groupes de périphériques, mais le principe s'applique également à tous les périphériques :**

Ajouter un groupe de périphériques sur la page 228

Spécifier les périphériques à inclure dans un groupe de périphériques sur la page 228

Spécifier les propriétés communes pour tous les périphériques d'un groupe de périphériques sur la page 229

## Ajouter un groupe de périphériques

1. Dans le volet **Vue d'ensemble**, faites un clic droit sur le type de périphérique sous lequel vous souhaitez créer un groupe de périphériques.
2. Sélectionnez **Ajouter un groupe de périphériques**.
3. Dans la boîte de dialogue **Ajouter un groupe de périphériques**, spécifiez un nom et une description pour le nouveau groupe de périphériques :



La description s'affiche lorsque vous survolez le groupe de périphériques dans la liste des périphériques avec le curseur de la souris.

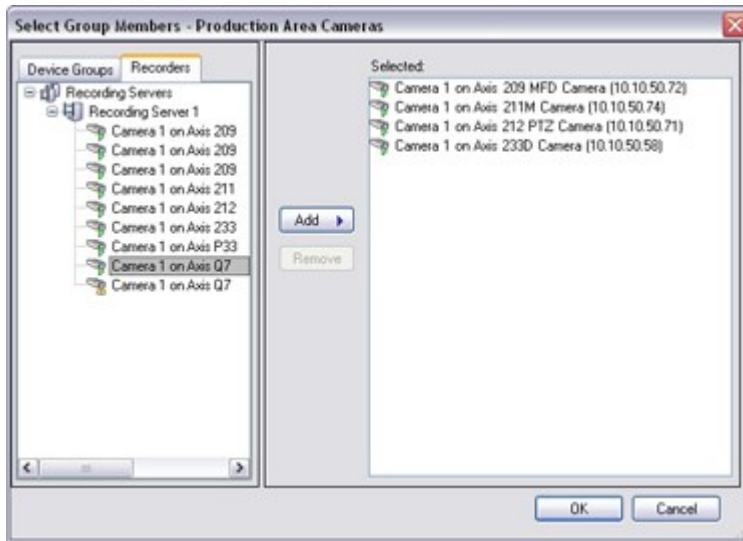
4. Cliquez sur **OK**. Un dossier représentant le nouveau groupe de périphériques apparaît dans la liste.
5. Continuez avec Spécifier les périphériques à inclure dans un groupe de périphériques (voir Spécifier les périphériques à inclure dans un groupe de périphériques sur la page 228).

## Spécifier les périphériques à inclure dans un groupe de périphériques

1. Dans le volet **Vue d'ensemble**, faites un clic droit sur le dossier du groupe de périphériques concerné.
2. Sélectionnez **Modifier les membres du groupe de périphériques**.
3. Dans la fenêtre **Sélectionner les membres du groupe**, sélectionnez l'un des onglets pour trouver le périphérique.

Un périphérique peut être membre de plusieurs groupes de périphériques.

- Sélectionnez les périphériques que vous souhaitez inclure et cliquez sur **Ajouter** ou double-cliquez sur le périphérique :



- Cliquez sur **OK**.
- Si la limite de 400 périphériques est dépassée dans un groupe, vous pouvez ajouter les groupes de périphériques sous formes de sous-groupes dans d'autres groupes de périphériques :



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

Pour les groupes de périphériques, vous pouvez spécifier les propriétés communes pour tous les périphériques d'un groupe de périphériques donné :

- Dans le volet **Vue d'ensemble**, cliquez sur le groupe de périphériques.  
 Dans le volet **Propriétés**, toutes les propriétés **qui sont disponibles sur tous les périphériques du groupe de périphériques** sont répertoriées et groupées dans des onglets.
- Indiquez les propriétés communes pertinentes.  
 Dans l'onglet **Paramètres**, vous pouvez basculer entre les paramètres pour **tous** les périphériques et ceux de périphériques individuels.
- Dans la boîte à outils, cliquez sur **Enregistrer**. Ces paramètres sont enregistrés sur les périphériques individuels, pas dans le groupe de périphériques.

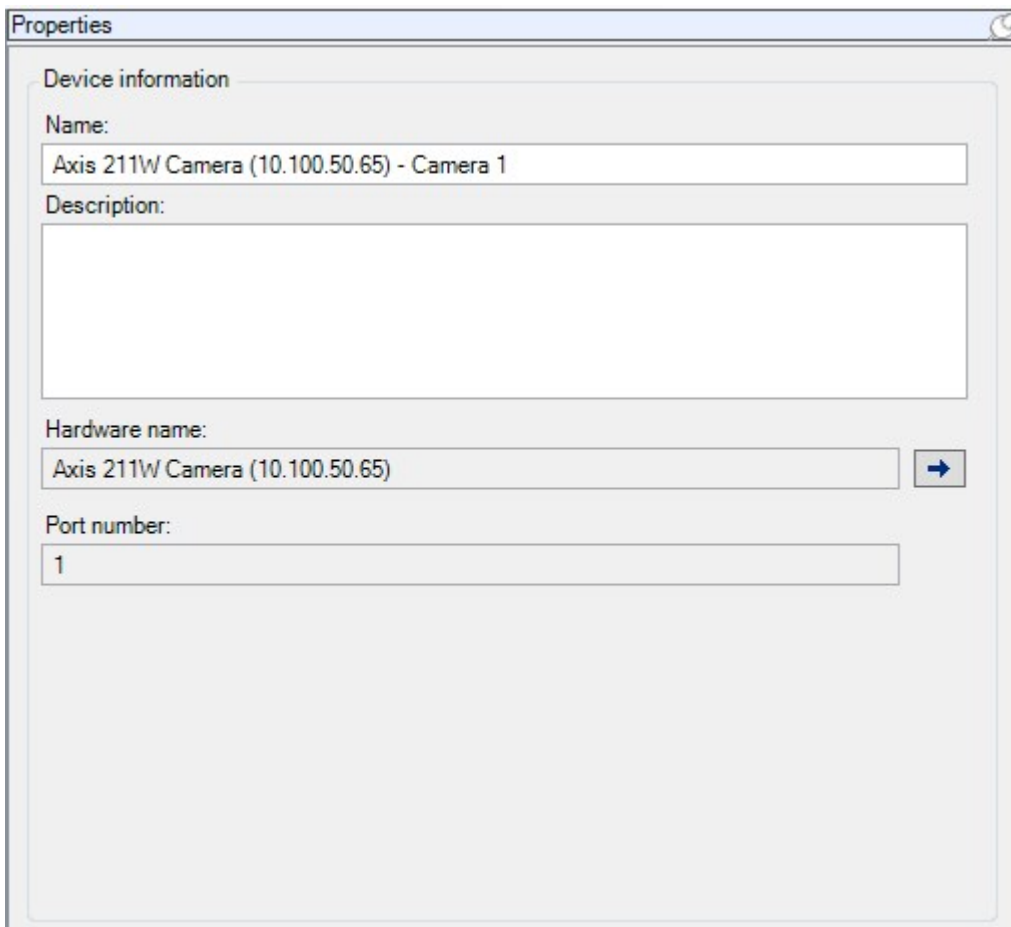
## Navigation sur le site : Onglet Périphériques

### Onglet Info (périphériques)

#### Onglet Infos (explications)

L'onglet **Infos** vous permet d'afficher et de modifier les informations de base concernant un périphérique dans un certain nombre de champs.

Tous les périphériques possèdent un onglet **Infos**.







The screenshot shows a 'Properties' dialog box with a 'Device information' tab. The fields are as follows:

Field	Value
Name:	Axis 211W Camera (10.100.50.65) - Camera 1
Description:	
Hardware name:	Axis 211W Camera (10.100.50.65)
Port number:	1

## Propriétés de l'onglet Info

Nom	Description
<b>Nom</b>	<p>Le nom est utilisé partout où le périphérique apparaît dans une liste sur le système et les clients.</p> <p>Si vous renommez un périphérique, son nom est modifié de manière globale dans le Management Client.</p>
<b>Description</b>	<p>Saisissez une description du périphérique (facultatif).</p> <p>La description apparaît dans plusieurs listes au sein du système. Par exemple, lorsque vous survolez le nom de l'élément dans le volet <b>Vue d'ensemble</b> avec le curseur de la souris.</p>
<b>Nom du matériel</b>	<p>Affiche le nom du matériel avec lequel le périphérique est connecté. Le champ n'est pas modifiable à partir d'ici, mais peut être modifié en cliquant sur le bouton <b>Atteindre</b> situé à côté de lui. Vous serez dirigé vers les informations relatives au matériel, où le nom est modifiable.</p>
<b>Numéro de port</b>	<p>Affiche le port sur lequel le périphérique est raccordé au matériel.</p> <p>Pour du matériel à un seul périphérique, le numéro de port sera généralement de <b>1</b>. Pour du matériel à plusieurs périphériques, tel que les serveurs vidéo comptant plusieurs chaînes, le nombre de port indique généralement le canal sur lequel le périphérique est connecté, par exemple <b>3</b>.</p>
<b>Abréviation</b>	<p>Pour appliquer une abréviation pour la caméra, saisissez-la ici. La longueur maximale de caractères est de 128.</p> <p>Si vous utilisez une smart map, l'abréviation s'affiche automatiquement avec la caméra sur la smart map. Sinon, le nom complet s'affiche.</p>
<b>Coordonnées géographiques</b>	<p>Saisissez l'emplacement géographique de la caméra au format <b>latitude, longitude</b>. La valeur que vous saisissez détermine la position de l'icône de caméra sur la smart map dans XProtect Smart Client.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;">  <p>Le champ sert essentiellement à la smart map et aux intégrations de tiers.</p> </div>

Nom	Description
<p><b>Direction</b></p>	<p>Saisissez le sens de visualisation de la caméra mesuré par rapport à un point en direction du nord sur un axe vertical. La valeur que vous saisissez détermine la direction de l'icône de caméra sur la smart map dans XProtect Smart Client.</p> <p>La valeur par défaut est 0,0.</p> <div data-bbox="389 510 1385 640" style="background-color: #e6f2ff; padding: 5px;">  Le champ sert essentiellement à la smart map et aux intégrations de tiers.                 </div>
<p><b>Champ de vision</b></p>	<p>Saisissez le champ de visualisation en degrés. La valeur que vous saisissez détermine le champ de vision de l'icône de caméra sur la smart map dans XProtect Smart Client.</p> <p>La valeur par défaut est 0,0.</p> <div data-bbox="389 828 1385 958" style="background-color: #e6f2ff; padding: 5px;">  Le champ sert essentiellement à la smart map et aux intégrations de tiers.                 </div>
<p><b>Profondeur</b></p>	<p>Saisissez la profondeur de la caméra en mètres ou en pieds. La valeur que vous saisissez détermine la profondeur de l'icône de caméra sur la smart map dans XProtect Smart Client.</p> <p>La valeur par défaut est 0,0.</p> <div data-bbox="389 1191 1385 1321" style="background-color: #e6f2ff; padding: 5px;">  Le champ sert essentiellement à la smart map et aux intégrations de tiers.                 </div>
<p><b>Aperçu de l'emplacement sur le navigateur</b></p>	<p>Pour vérifier que vous avez saisi les coordonnées géographiques appropriées, cliquez sur le bouton. Google Maps s'ouvre dans votre navigateur Internet standard à la position que vous avez spécifiée.</p> <div data-bbox="389 1491 1385 1621" style="background-color: #e6f2ff; padding: 5px;">  Le champ sert essentiellement à la smart map et aux intégrations de tiers.                 </div>



## Onglet Paramètres (périphériques)

### Onglet Paramètres (explications)

L'onglet **Paramètres** vous permet d'afficher et de modifier les paramètres d'un périphérique dans un certain nombre de champs.

Tous les périphériques possèdent un onglet **Paramètres**.

Les valeurs dans le tableau sont modifiables ou en lecture seule. Après avoir modifié un paramètre au profit d'une valeur autre que la valeur par défaut, la valeur apparaît en gras.

Le contenu du tableau dépend du pilote de périphérique.

Les plages autorisées sont visibles dans la zone d'informations sous le tableau des paramètres :

The screenshot shows a 'Properties' window for an 'Axis 211W Camera'. It contains a table of parameters grouped into sections: General, JPEG - streamed, JPEG 2 - streamed, JPEG 3 - streamed, and MPEG-4 - streamed. The 'Saturation' parameter is selected and highlighted in blue. Below the table, there is a section titled 'Saturation' with a description: 'A numeric value between 0 and 100.'

Axis 211W Camera	
<b>General</b>	
Brightness	50
Include Date	No
Include Time	No
Rotation	0
Saturation	50
Sharpness	0
<b>JPEG - streamed</b>	
Compression	30
Frames per second	8
Resolution	640x480
<b>JPEG 2 - streamed</b>	
Compression	30
Frames per second	8
Resolution	640x480
<b>JPEG 3 - streamed</b>	
Compression	30
Frames per second	8
Resolution	640x480
<b>MPEG-4 - streamed</b>	
Bit rate control priority	Frame rate
Frames per second	30
Maximum bit rate	3000
Maximum compression	100
Minimum compression	0
Resolution	640x480
Target bit rate	9900

**Saturation**  
A numeric value between 0 and 100.

## Paramètres de la caméra (explications)

Vous pouvez afficher ou modifier des paramètres tels que :

- Fluidité d'image par défaut
- Résolution
- Compression
- Le nombre maximal d'images entre les images-clés
- Affichage sur écran du texte/de l'heure/de la date pour une caméra sélectionnée ou pour toutes les caméras d'un groupe de périphériques

Les pilotes des caméras définissent le contenu de l'onglet **Paramètres**. Les pilotes varient en fonction du type de caméra.

Pour les caméras prenant en charge plus d'un type de flux, par exemple MJPEG et MPEG-4/H.264/H.265, vous pouvez utiliser la multidiffusion, voir Multi-streaming (explications) sur la page 235.

Si vous modifiez un paramètre, vous pouvez rapidement vérifier les effets de votre modification si votre volet **Aperçu** est activé. Vous ne pouvez pas utiliser le volet **Aperçu** pour voir les effets des modifications de fluidité d'image parce que les images miniatures dans le volet **Aperçu** utilisent un nombre d'images par seconde différent, défini dans la boîte de dialogue **Options**.

La modification des paramètres de **Images max. entre les images-clés** et **Images max. entre les modes images-clés** peut réduire la performance de certaines fonctionnalités dans XProtect Smart Client. XProtect Smart Client nécessite par exemple la présence d'une image-clé pour lancer la lecture d'une vidéo. Ainsi, une période plus longue entre les images-clés prolonge le démarrage de XProtect Smart Client.

## Onglet Flux (périphériques)

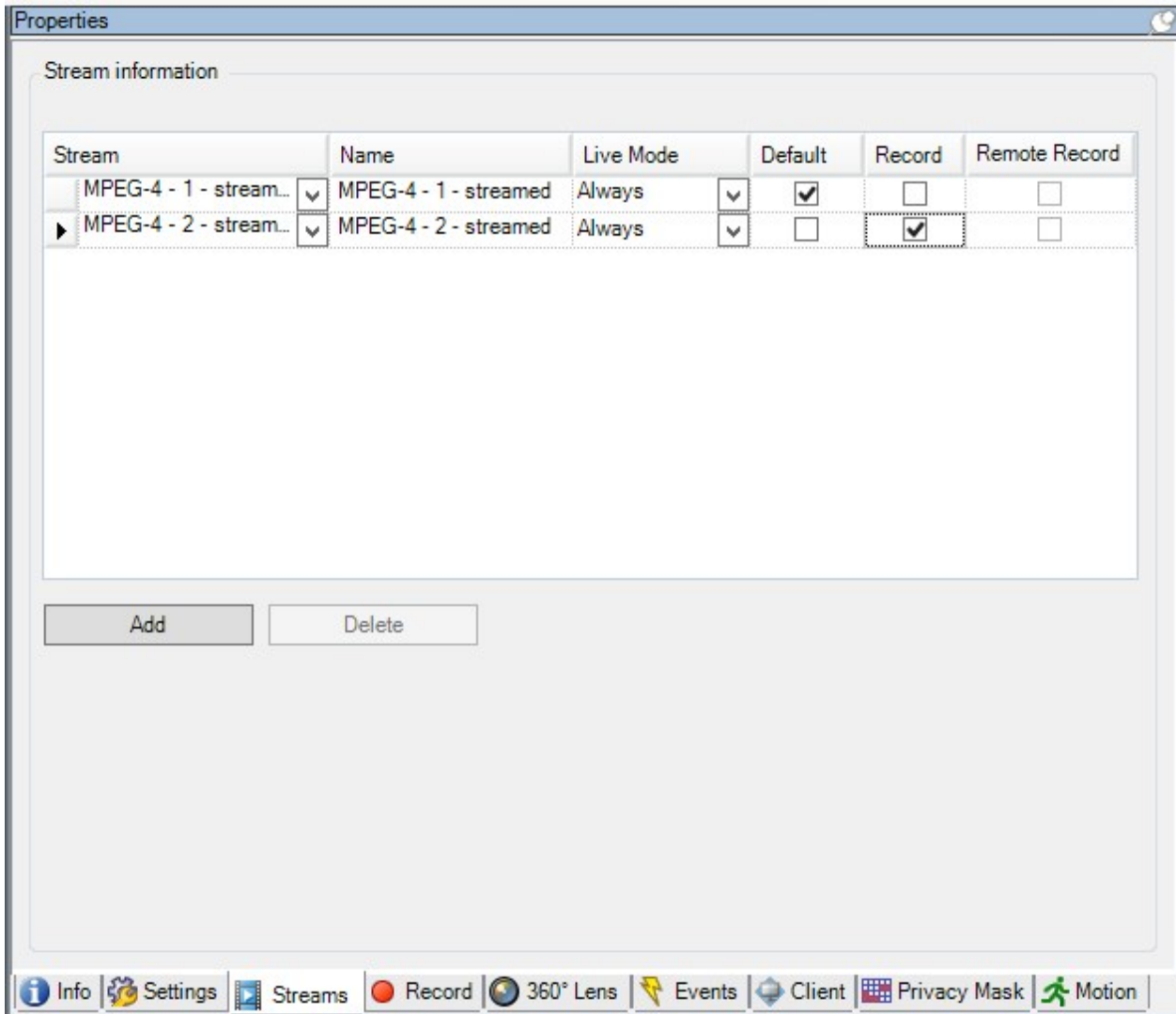
### Onglet Flux (explications)

Les périphériques suivants possèdent un onglet **Flux** :

- Caméras

L'onglet **Flux** répertorie un flux unique par défaut. Il s'agit du flux par défaut de la caméra sélectionnée, utilisée pour le direct et les vidéos enregistrées.

Pour la diffusion en direct, vous pouvez configurer et utiliser autant de flux en direct que le nombre pris en charge par la caméra. En revanche, vous ne pouvez sélectionner qu'un seul flux pour l'enregistrement simultané. Pour modifier le flux à utiliser pour l'enregistrement, cochez la case **Enregistrement** du flux à enregistrer.



### Multi-streaming (explications)

L'affichage de la vidéo en direct ou la lecture d'une vidéo enregistrée ou ne nécessite pas obligatoirement la même qualité vidéo et la même fluidité d'image. Vous pouvez choisir **soit** un flux pour le visionnage en direct et un autre à des fins de lecture **ou** deux flux séparés en direct, mais avec une résolution, un codage et une fluidité d'image différents.

Pour gérer la diffusion et limiter la transmission de données inutiles, la diffusion ne commence pas si :

- Sur l'onglet **Diffusions**, le **Mode En direct** est configuré sur En cas de besoin
- Sur l'onglet **Enregistrer**, l'option **Enregistrement** est désactivée
- Sur l'onglet **Mouvement**, l'option **Détection de mouvement** est désactivée

Si ces conditions sont remplies, la diffusion vidéo s'exécutera uniquement lorsqu'un client la visualisera.

**Exemple 1, vidéo en direct et enregistrée :**

- Pour le visionnage d'une vidéo **en direct**, votre société peut préférer le format H.264 avec une fluidité d'image élevée
- Pour la lecture d'une vidéo **enregistrée**, votre société peut préférer MJPEG à une fluidité d'image inférieure pour préserver de l'espace disque

#### Exemple 2, vidéo en direct locale et à distance :

- Pour le visionnage d'une **vidéo en direct à partir d'un point de fonctionnement local**, votre société peut préférer le format H.264 avec une fluidité d'image élevée afin d'obtenir la meilleure qualité vidéo disponible
- Pour le visionnage d'une **vidéo en direct à partir d'un point de fonctionnement connecté à distance**, votre société peut préférer le format MJPEG avec une fluidité d'image et une qualité inférieures afin de préserver la bande passante du réseau

#### Exemple 3, flux adaptatif :

- Pour le visionnage d'une **vidéo en direct et diminuer la charge sur le CPU et le GPU de l'ordinateur XProtect Smart Client**, votre société peut préférer le format H.264/H.265 avec une fluidité d'image élevée pour correspondre à la résolution requise par XProtect Smart Client lors de l'utilisation du flux adaptatif. Pour plus d'informations, voir Propriétés du profil Smart Client sur la page 300.



Si vous activez le **multicast en direct** sur l'onglet **Client** de la caméra, celle-ci ne fonctionne que sur le flux vidéo par défaut.

Même lorsque les caméras prennent en charge la diffusion mult flux, les capacités individuelles en termes de lecture en direct multiple peuvent varier entre différentes caméras. Consultez la documentation de la caméra pour plus d'informations.

Pour voir si une caméra offre différents types de flux, consultez l'onglet **Paramètres**.

#### Ajouter un flux

1. Dans l'onglet **Flux**, cliquez sur **Ajouter**. Cette action ajoute un second flux à la liste.
2. Dans la colonne **Nom**, modifiez le nom du flux. Le nom s'affiche dans XProtect Smart Client.
3. Dans la colonne **Mode en direct**, sélectionnez quand la diffusion en direct est requise :
  - **Toujours** : le flux s'exécute même si aucun utilisateur XProtect Smart Client ne le demande.
  - **Jamais** : le flux est désactivé. Utilisez cette fonction uniquement pour les flux d'enregistrement, par exemple si vous souhaitez des enregistrements de qualité supérieure et avez besoin de la largeur de bande
  - **Si nécessaire** : le flux est lancé lorsqu'un utilisateur XProtect Smart Client le demande.
4. Dans la colonne **Par défaut**, sélectionnez le flux par défaut.

5. Dans la colonne **Enregistrement**, cochez la case si vous souhaitez enregistrer ce flux ou décochez-la si vous souhaitez uniquement l'utiliser pour des vidéos en direct.
6. Cliquez sur **Enregistrer**.



Si vous réglez un flux sur **Défaut** ou **Enregistrer**, le flux fonctionne toujours indépendamment du paramètre **Mode En direct**. La sélection de **En cas de besoin** et **Toujours** a le même effet dans le système. Si vous sélectionnez **Jamais**, le flux fonctionne mais ne peut pas être visionné en direct.



Si vous ne souhaitez pas que les flux fonctionnent du tout à moins que quelqu'un ne consulte la vidéo en direct, vous pouvez modifier la **Règle de démarrage des flux par défaut** pour les démarrer à la demande avec l'événement prédéfini **Flux client en direct requis**.

## Onglet Enregistrement (périphériques)

### Onglet Enregistrement (explications)

Les périphériques suivants possèdent un onglet **Enregistrer** :

- Caméras
- Microphones
- Haut-parleurs
- Métadonnées

Les enregistrements d'un périphérique sont uniquement sauvegardés dans la base de données une fois que vous avez activé l'enregistrement et que les critères de la règle associée aux enregistrements sont remplis.

Les paramètres qui ne peuvent pas être configurés pour un périphérique apparaissent en grisé.

**Properties**

Recording settings

Recording

- Record on related devices
- Stop manual recording after:  minutes

Pre-buffer

Location:

Time:  seconds

Recording frame rate

JPEG:  FPS

MPEG-4/H.264/H.265:  Record keyframes only

Storage

Local Default

Status:

Status	Database	Location	Used space
OK	Local Default	C:\MediaDatabase	17.7 MB

Total used space:

Remote recordings

Automatically retrieve remote recordings when connection is restored

**Info** | **Settings** | **Streams** | **Record** | **360° Lens** | **Events** | **Client** | **Privacy Mask** | **Motion**

## Activer/désactiver l'enregistrement

Par défaut, l'enregistrement est activé. Pour activer/désactiver l'enregistrement :

1. Dans le panneau **Navigation du site**, sélectionnez **Serveurs d'enregistrement**.
2. Sélectionnez le périphérique requis dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Enregistrer**, cochez ou décochez la case **Enregistrement**.



Vous devez activer l'enregistrement pour le périphérique afin d'enregistrer des données de la caméra. Une règle indiquant les circonstances d'enregistrement d'un périphérique ne fonctionnera pas si vous avez désactivé l'enregistrement pour le périphérique.

## Activer l'enregistrement sur les périphériques connexes

Pour les caméras, vous pouvez activer l'enregistrement pour les périphériques connexes connectés au même serveur d'enregistrement, tels que les microphones, par exemple. Cela signifie que les périphériques connexes enregistrent lorsque la caméra enregistre.

L'enregistrement sur les périphériques connexes est activé par défaut pour les nouvelles caméras, mais vous pouvez désactiver et activer cette fonction selon vos besoins. Pour les caméras existantes du système, la case est décochée par défaut.

1. Dans le panneau **Navigation du site**, sélectionnez **Serveurs d'enregistrement**.
2. Sélectionnez le périphérique caméra requis dans le volet **Vue d'ensemble**.
3. Dans l'onglet **Enregistrer**, cochez ou décochez la case **Enregistrer sur des périphériques associés**.
4. Dans l'onglet **Client**, spécifiez les périphériques associés à cette caméra.

Si vous souhaitez activer l'enregistrement sur des périphériques connexes connectés à un autre serveur d'enregistrement, vous devez créer une règle.

## Pré-enregistrement (explications)

La mise en mémoire-tampon préalable représente la capacité d'enregistrer de l'audio ou de la vidéo avant la survenue de l'événement de déclenchement. Elle s'avère utile lorsque vous souhaitez enregistrer des données audio ou vidéo qui précèdent l'événement de déclenchement de l'enregistrement, par exemple l'ouverture d'une porte.

La mise en mémoire-tampon préalable est possible dans la mesure où le système reçoit continuellement des flux audio et vidéo depuis les périphériques connectés et les enregistre de manière temporaire pendant la période de mise en mémoire-tampon préalable définie.

- Si une règle d'enregistrement est déclenchée, les enregistrements temporaires sont rendus permanents pendant la durée de pré-enregistrement configurée pour cette règle
- Si aucune règle d'enregistrement n'est déclenchée, les enregistrements temporaires dans la mémoire-tampon préalable sont automatiquement supprimés après la durée de mise en mémoire-tampon préalable définie



Pour utiliser la fonction de mémoire-tampon préalable, les périphériques doivent être activés et envoyer un flux au système.

## Périphériques prenant la mise en mémoire-tampon préalable en charge

Les caméras, microphones et haut-parleurs prennent la mise en mémoire-tampon préalable en charge. Concernant les haut-parleurs, les flux sont envoyés uniquement si l'utilisateur XProtect Smart Client se sert de la fonction **Parler au haut-parleur**. En d'autres termes, cela signifie qu'en fonction de la façon dont les flux de votre haut-parleur sont déclenchés, vous disposez d'une petite mise en mémoire-tampon préalable ou d'aucune mise en mémoire-tampon préalable.

Dans la plupart des cas, les haut-parleurs sont configurés de sorte à enregistrer lorsque l'utilisateur XProtect Smart Client se sert de la fonction **Parler au haut-parleur**. Dans ces cas, aucune mémoire-tampon préalable du haut-parleur n'est disponible.

### Stockage des enregistrements temporairement en mémoire-tampon

Vous pouvez choisir l'emplacement de stockage des enregistrements temporairement en mémoire-tampon :

- Dans la mémoire ; la durée de mémoire-tampon est limitée à 15 secondes.
- Sur le disque (dans la base de données multimédia) ; vous pouvez choisir toutes les valeurs.

Le stockage dans la mémoire au lieu du disque améliore les performances du système, mais est uniquement possible pendant des durées de mémoire-tampon plus courtes.

Lorsque des enregistrements sont stockés dans la mémoire et si vous rendez des enregistrements temporaires permanents, les enregistrements temporaires restants sont supprimés et ne peuvent pas être restaurés. Si vous devez pouvoir conserver les enregistrements restants, stockez les enregistrements sur le disque.

### Gérer la mise en mémoire-tampon préalable

#### Activer et désactiver la mise en mémoire-tampon préalable

La mise en mémoire-tampon préalable est activée par défaut avec une durée de trois secondes et un stockage en mémoire.

1. Pour activer/désactiver la mise en mémoire-tampon préalable, cochez/décochez la case **Pré-enregistrement**.

#### Préciser l'emplacement de stockage et la durée de mise en mémoire-tampon

Les enregistrements temporairement en mémoire-tampon sont stockés dans la mémoire ou sur le disque :



1. Pour **Emplacement**, sélectionnez **Mémoire** ou **Disque** et précisez le nombre de secondes.

Le nombre de secondes saisi doit être suffisamment grand pour correspondre à vos exigences dans les différentes règles d'enregistrement définies.

Si vous avez besoin d'une durée de mise en mémoire-tampon supérieure à 15 secondes, sélectionnez **Disque**.

2. Si vous changez l'emplacement par **Mémoire**, le système réduit la durée à 15 secondes automatiquement.

#### Utiliser la mise en mémoire-tampon dans les règles

Lorsque vous créez des règles destinées à déclencher l'enregistrement, vous pouvez choisir de lancer les enregistrements un peu avant l'événement actuel (mémoire-tampon préalable).

**Exemple** : La règle ci-après indique que l'enregistrement doit commencer sur la caméra 5 secondes avant la détection du mouvement sur la caméra.

Perform an action on **Motion Started**  
from **Red Sector Entrance Cam**  
start recording **5 seconds before** on the device on which event occurred



Pour utiliser la fonction d'enregistrement avec mise en mémoire-tampon préalable dans la règle, vous devez activer la mise en mémoire-tampon préalable sur le périphérique en cours d'enregistrement et définir la durée de la mise en mémoire-tampon préalable afin qu'elle soit au minimum égale à celle spécifiée dans la règle.

#### Gérer l'enregistrement manuel

**Arrêter l'enregistrement manuel après** est activé par défaut avec une durée d'enregistrement de cinq minutes. Ceci permet de s'assurer que le système arrête automatiquement tous les enregistrements commencés par les utilisateurs de XProtect Smart Client.

Stop manual recording after:  minutes

1. Pour activer et désactiver l'enregistrement manuel à arrêter automatiquement par le système, cochez/décochez la case **Arrêter l'enregistrement manuel après**.
2. Lorsque vous l'activez, précisez une durée d'enregistrement. Le nombre de minutes que vous spécifiez doit être suffisamment grand pour correspondre aux exigences des divers enregistrements manuels sans surcharger le système.

#### Ajouter des rôles :

Vous devez accorder le droit de démarrer et d'arrêter l'enregistrement manuel aux utilisateurs du client sur chaque caméra dans **Rôles**, dans l'onglet **Périphérique**.

### Utilisation dans les règles :

Les événements que vous pouvez utiliser lorsque vous créez des règles associées à l'enregistrement manuel sont :

- Enregistrement manuel démarré
- Enregistrement manuel arrêté

### Spécifier la fluidité d'image de l'enregistrement

Vous pouvez spécifier la fluidité d'image de l'enregistrement pour le format JPEG.

- Sélectionnez ou saisissez la fluidité d'image de l'enregistrement (en FPS, nombre d'images par seconde) dans la case **Fluidité d'image d'enregistrement : Case (JPEG)**.

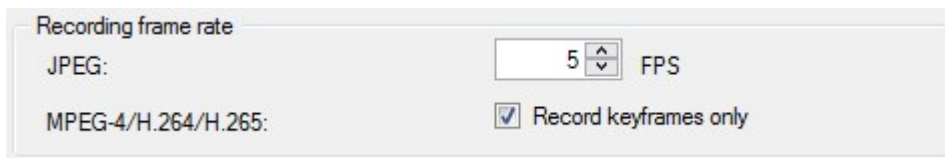


### Activer l'enregistrement des images-clés

Vous pouvez activer l'enregistrement des images-clés pour les flux MPEG-4/H.264/H.265. Cela signifie que le système alterne entre l'enregistrement des images-clés uniquement et l'enregistrement de toutes les images selon les paramètres de vos règles.

Vous pouvez par exemple laisser le système enregistrer des images-clés lorsqu'il n'y a aucun mouvement dans la vue et passer à toutes les images en cas de détection de mouvement pour économiser de l'espace de stockage.

1. Cochez la case **Enregistrer les images-clés uniquement**.

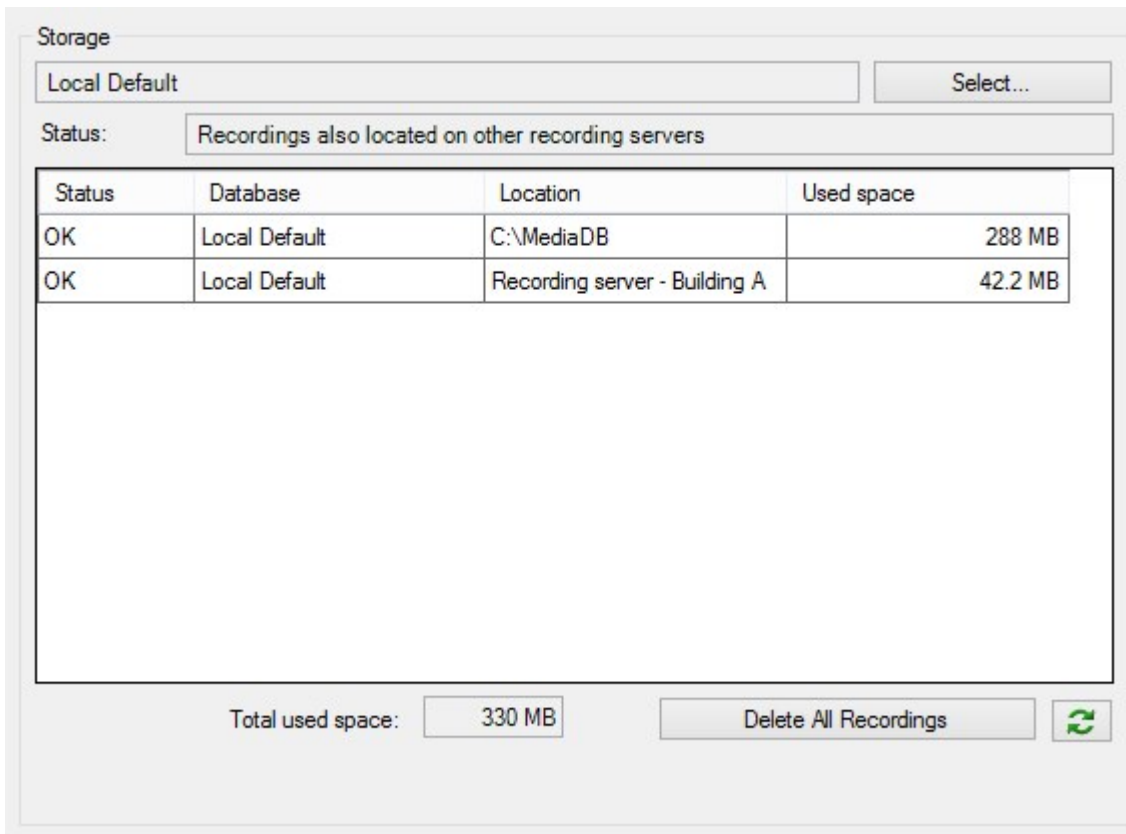


2. Créez une règle qui active la fonction, voir Actions et actions d'arrêt (explications) sur la page 314.

### Stockage (explications)

Dans **Stockage**, vous pouvez surveiller et gérer les bases de données pour un périphérique ou un groupe de périphériques ajoutés au même serveur d'enregistrement.

Au-dessus du tableau, vous voyez la base de données sélectionnée et son statut. Dans cet exemple, la base de données sélectionnée est la base de données par défaut, **Locale par défaut** et son statut est **Des enregistrements sont également situés sur d'autres serveurs d'enregistrement**. L'autre serveur est le serveur d'enregistrement du bâtiment A.



**Possibles statuts pour la base de données sélectionnée**

Nom	Description
<b>Des enregistrements sont également situés sur d'autres serveurs d'enregistrement</b>	La base de données est active et en fonctionnement et contient également des enregistrements dans des espaces de stockage situés sur d'autres serveurs d'enregistrement.
<b>Archives également situées sur l'ancien stockage</b>	La base de données est active et en fonctionnement et possède aussi des archives situées dans d'autres espaces de stockage.
<b>Activé</b>	La base de données est active et en fonctionnement.
<b>Les données de certains des périphériques choisis sont actuellement déplacées vers un autre emplacement</b>	La base de données est active et en fonctionnement et le système déplace des données d'un ou plusieurs périphériques sélectionnés dans un groupe depuis un emplacement vers un autre.

Nom	Description
<b>Les données du périphérique sont actuellement déplacées vers un autre emplacement</b>	La base de données est active et en fonctionnement et le système déplace des données du périphérique sélectionné d'un emplacement vers un autre.
<b>Informations non disponibles en mode redondant</b>	Le système ne peut pas recueillir d'informations d'état au sujet de la base de données lorsque la base de données est en mode de redondance.

Plus bas dans la fenêtre, vous pouvez apercevoir le statut individuel de chaque base de données (**OK, Hors ligne** ou **Ancien stockage**), l'emplacement de chaque base de données et l'espace utilisé par chaque base de données.

Si tous les serveurs sont en ligne, vous pouvez voir l'espace total utilisé pour l'intégralité du stockage dans le champ **Espace total utilisé**.

Avec le bouton **Supprimer tous enregistrements**, vous pouvez supprimer tous les enregistrements pour le périphérique ou le groupe de périphériques si vous avez ajouté tous les périphériques du groupe sur le même serveur. Les données protégées ne sont pas supprimées.

Pour obtenir des informations sur la configuration du stockage, reportez-vous à Onglet Stockage (serveur d'enregistrement) sur la page 158.

### Transfert de périphériques d'un stockage à un autre

Vous pouvez sélectionner un nouvel emplacement de stockage pour vos périphériques en sélectionnant **Choisir....** sous **Stockage**.

Vous pouvez ainsi choisir un autre stockage d'enregistrement dans lequel vos périphériques enregistreront et archiveront leur contenu selon la configuration du stockage.

La sélection d'un nouvel emplacement de stockage des enregistrements n'affecte pas les enregistrements actuels. Ces derniers resteront dans leur emplacement actuel et seront toujours soumis aux conditions définies par la configuration de stockage à laquelle ils appartiennent.

### Enregistrement à distance (explications)



L'option d'enregistrement à distance n'est disponible que si la caméra sélectionnée prend en charge le stockage décentralisé ou s'il s'agit d'une caméra avec une configuration Milestone Interconnect.

Pour garantir la sauvegarde de tous les enregistrements en cas de problèmes réseau, sélectionnez **Récupérer automatiquement les enregistrements à distance lorsque la connexion est rétablie**. Ainsi, les enregistrements sont récupérés automatiquement lorsque la connexion est rétablie.

Le type de matériel sélectionné détermine l'emplacement à partir duquel les enregistrements sont récupérés :

- Pour une caméra dotée d'un espace de stockage local des enregistrements, les enregistrements sont récupérés à partir de l'espace de stockage local des enregistrements
- Pour un système à distance Milestone Interconnect, les enregistrements sont récupérés à partir des serveurs d'enregistrement du système à distance

Vous pouvez utiliser la fonctionnalité ci-après indépendamment de la récupération automatique :

- Enregistrement manuel
- La règle **Récupérer et stocker les enregistrements à distance à partir des <périphériques>**
- La règle **Récupérer et stocker les enregistrements à distance entre <heure de début et de fin> à partir des <périphériques>**

## Onglet Mouvement (périphériques)

### Onglet de mouvement (explications)

Les périphériques suivants possèdent un onglet **Mouvement** :

- Caméras

L'onglet **Mouvement** vous permet d'activer et de configurer la détection du mouvement pour la caméra sélectionnée. La configuration de la détection du mouvement est un élément clé de votre système : Votre configuration de la détection de mouvement définit le moment où le système génère des événements de mouvement et généralement aussi lorsqu'une vidéo est enregistrée.

Le temps passé à chercher la meilleure configuration possible en termes de configuration de détection de mouvement pour chaque caméra vous aide plus tard à éviter les enregistrements inutiles par exemple. En fonction de l'emplacement physique de la caméra, il peut s'avérer utile de tester les paramètres de détection du mouvement dans plusieurs conditions physiques différentes comme par ex. de jour/nuite ou par temps venteux/calme.

Avant de configurer la détection du mouvement pour une caméra, Milestone vous recommande de configurer au préalable les paramètres de qualité d'image de la caméra, tels que la résolution, le codec vidéo et les paramètres de flux sur l'onglet **Paramètres**. Si vous changez plus tard les paramètres de qualité d'image, vous devez toujours tester la configuration de détection du mouvement par la suite.

Si vous avez défini des zones comportant des masques de confidentialité permanents sur l'onglet **Protection de la confidentialité** (voir Onglet Masquage de confidentialité (périphériques) sur la page 275), vous pouvez choisir d'afficher les masques de confidentialité sur l'onglet **Mouvement** en cochant la case **Afficher les masques de confidentialité**.



Aucune détection du mouvement dans les zones couvertes par les masque de confidentialité permanents.


Motion detection

Hardware acceleration:

Automatic

Off

Motion preview



Show privacy masks

---

Manual sensitivity 33

< >

Threshold: 2000

< >

Keyframes only (MPEG-4/H.264/H.265)

Process image every (msec):

Detection resolution:

Generate motion data for smart search

Use exclude regions

Show grid

Show regions

Pen size:

[Info](#) [Settings](#) [Streams](#) [Record](#) [Motion](#) [Fisheye Lens](#) [Events](#)

Vous pouvez configurer tous les paramètres d'un groupe de caméras, mais il est en général préférable de régler les zones à exclure par caméra.

### Activer et désactiver la détection du mouvement

Vous spécifiez le paramètre par défaut de la détection du mouvement dans l'onglet **Outils > Options > Général**.

Pour activer ou désactiver la détection du mouvement par la suite pour une caméra :

- Cochez ou décochez la case **Détection du mouvement** dans l'onglet **Mouvement**



Lorsque la détection du mouvement d'une caméra est désactivée, aucune des règles de la caméra associées à la détection du mouvement ne fonctionne.

### Spécifier les paramètres de détection de mouvement

Vous pouvez spécifier des paramètres relatifs à la quantité de changement requise dans la vidéo d'une caméra afin que le changement soit considéré comme un mouvement. Vous pouvez par exemple spécifier des intervalles entre les analyses de détection du mouvement et des zones d'une image dans lesquelles les mouvements doivent être ignorés. Vous pouvez également ajuster la précision de la détection du mouvement et donc la charge des ressources du système.

### Accélération matérielle (explications)

Pour activer l'accélération matérielle de la détection de mouvement vidéo, sélectionnez **Automatique**. C'est la configuration par défaut lorsque vous ajoutez une caméra. Le système utilise maintenant les ressources du GPU si elles sont disponibles. Ceci réduira la charge du processus sur le serveur d'enregistrement au cours de l'analyse des mouvements sur la vidéo et améliorera la performance générale du serveur d'enregistrement.

L'accélération matérielle de la détection de mouvement vidéo (VMD) utilise des ressources GPU sur :

- Les processeurs Intel prenant en charge Intel Quick Sync
- NVIDIA® affiche les adaptateurs connectés à votre serveur d'enregistrement

La répartition de la charge entre les différentes ressources se fait automatiquement. Dans le nœud **Moniteur système**, vous pouvez vérifier que la charge d'analyse des mouvements actuelle sur les ressources NVIDIA GPU est comprise dans les limites spécifiées dans le nœud **Seuils du moniteur système**. Les témoins de charge NVIDIA GPU sont :

- Décodage NVIDIA
- Mémoire NVIDIA
- Rendu de NVIDIA





Si la charge est trop élevée, vous pouvez ajouter des ressources GPU à votre PC en installant plusieurs adaptateurs graphiques NVIDIA. Milestone ne recommande pas l'utilisation de Scalable Link Interface (SLI) pour la configuration de vos adaptateurs graphiques NVIDIA.

Les produits NVIDIA possèdent différentes capacités de calcul. Pour vérifier que votre produit NVIDIA prend en charge l'accélération matérielle pour les codecs utilisés par votre système Milestone XProtect, cherchez dans le tableau ci-dessous les codecs pris en charge pour la version de capacité de calcul.

Pour trouver la version de capacité de calcul de votre produit NVIDIA, consultez le site Web NVIDIA (<https://developer.nvidia.com/cuda-gpus/>).

Capacité de calcul	Architecture	H.264	H.265
3.x	Kepler	✓	-
5.x	Maxwell	✓	-
6.x	Pascal	✓	✓
7.x	Volta	✓	✓

Pour vérifier si la détection du mouvement vidéo fait l'objet d'une accélération matérielle pour une caméra donnée, activez la connexion du fichier journal du serveur d'enregistrement. Définissez le niveau sur **Débogage** et diagnostics connecté sur DeviceHandling.log. Le journal suit le modèle :  
[heure] [274] DÉBOGAGE – [guide] [nom] Décodage configuré : Automatique : Décodage réel : Intel/NVIDIA

La version du système d'exploitation du serveur d'enregistrement et la génération du CPU peuvent avoir une incidence sur le niveau de performance de l'accélération matérielle de la détection des mouvements vidéo. L'affectation de la mémoire du GPU constitue souvent un goulot d'étranglement avec les versions plus anciennes (la limite typique se situe entre 0,5 Go et 1,7 Go).

Les systèmes basés sur Windows 10 / Server 2016 et les CPU de 6e génération (Skylake) ou plus récents allouent 50 % de la mémoire système au GPU, ce qui permet ainsi de supprimer ou de réduire ce goulot d'étranglement.

Les CPU Intel de 6e génération ne permettent pas le décodage de l'accélération matérielle de H.265, ainsi le niveau de performance est comparable avec le H.264 de ces versions du CPU.

### Activer la sensibilité manuelle

Le paramètre de sensibilité détermine **dans quelle mesure chaque pixel** de l'image doit changer avant que l'on considère qu'il y a mouvement.

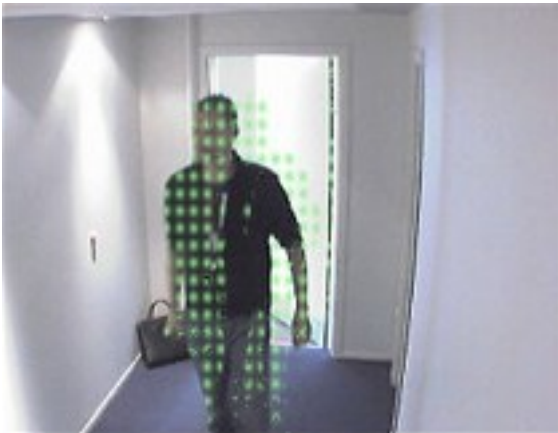
1. Cochez la case **Sensibilité manuelle** dans l'onglet **Mouvement**.
2. Faites glisser le curseur vers la gauche pour un plus grand niveau de sensibilité et vers la droite pour un niveau de sensibilité moindre.

Plus le niveau de sensibilité est **élevé**, et moins les changements requis dans chaque pixel pour constituer un mouvement sont importants.

Plus le niveau de sensibilité est **faible**, et plus les changements requis dans chaque pixel pour constituer un mouvement sont importants.

Les pixels dans lesquels un mouvement est détecté sont surlignés en vert dans l'image de l'aperçu.

3. Sélectionnez une position du curseur dans laquelle seuls les changements détectés que vous considérez comme des mouvements sont mis en surbrillance.



Vous pouvez comparer et définir le paramètre de sensibilité exact entre les caméras à l'aide du numéro à droite du curseur.

### Spécifier le seuil

Le seuil de détection du mouvement détermine **combien de pixels** de l'image doivent changer avant que l'on considère qu'il y a mouvement.

1. Faites glisser le curseur vers la gauche pour un plus grand niveau de mouvement et vers la droite pour un niveau de mouvement moindre.
2. Sélectionnez une position du curseur dans laquelle seuls les changements détectés que vous considérez comme des mouvements sont détectés.

La ligne noire verticale dans la barre d'indication de mouvement indique le seuil de détection du mouvement :  
Quand le mouvement détecté est au-dessus du niveau du seuil de détection sélectionné, la barre passe du vert au rouge, ce qui indique une détection positive.



Barre d'indication de mouvement : passe du vert au rouge lorsque le seuil est dépassé, indiquant la détection positive d'un mouvement.

### Sélectionner les paramètres des images-clés

Détermine si la détection du mouvement est réalisée uniquement sur les images-clés ou sur l'ensemble du flux vidéo. S'applique uniquement à MPEG-4/H.264/H.265.

La détection du mouvement sur les images-clés réduit la quantité de puissance de traitement utilisée pour l'analyse.

Cochez la case **Images-clés uniquement (MPEG-4/H.264/H.265)** pour procéder à la détection du mouvement uniquement sur les images-clés.

### Sélectionner l'intervalle de traitement des images

Vous pouvez sélectionner la fréquence avec laquelle le système procède à une analyse de détection du mouvement.

Dans la liste **Traiter l'image tous les (msec)** :

- Sélectionnez l'intervalle. Par exemple, toutes les 1000 millisecondes correspond à une fois par seconde. La valeur par défaut est de 500 millisecondes.  
L'intervalle est appliqué si la fluidité d'image actuelle est supérieure à l'intervalle défini à cet endroit.

### Spécifier la résolution de la détection

Vous permet d'optimiser la performance de détection du mouvement en analysant uniquement un pourcentage sélectionné de l'image, par exemple 25 %. En analysant 25 % par exemple, seul un quart des pixels de l'image est analysé au lieu de tous les pixels.

L'utilisation de la détection optimisée réduit la quantité de puissance du processeur utilisée pour effectuer l'analyse, mais se traduit également par une détection de mouvement moins précise.

- Dans la liste **Résolution de détection**, sélectionnez la résolution de détection désirée.

### Génération des données de mouvement pour la recherche avancée

Lorsque la fonction **Générer des données de mouvement pour la recherche intelligente** est activée, le système génère des données de mouvement pour les images utilisées pour la détection du mouvement. Par exemple, si vous sélectionnez la détection du mouvement sur les images-clés uniquement, les données de mouvement sont

également produites pour les images-clés uniquement.

Les données de mouvement supplémentaires permettent à l'utilisateur du client, via la fonction de recherche avancée, de rechercher rapidement les enregistrements concernés sur la base du mouvement dans la zone sélectionnée de l'image. Le système ne génère pas de données de mouvement dans les zones couvertes par des masques de confidentialité permanents, mais uniquement dans celles qui sont couvertes par des masques de confidentialité relevables (voir Onglet Masquage de confidentialité (périphériques) sur la page 275).

Le seuil de détection du mouvement et les zones à exclure n'influencent pas les données de mouvement générées.

Vous spécifiez le paramètre par défaut de la génération de données de recherche intelligente dans l'onglet **Outils** > **Options** > **Général**.

### Spécifier l'exclusion de zones

Vous pouvez exclure la détection du mouvement des zones spécifiques de la vision d'une caméra.



Les zones caractérisées par des masques de confidentialité sont exclues de la détection du mouvement. Cochez la case **Afficher les masques de confidentialité** pour les afficher.

Le fait d'exclure la détection du mouvement des zones spécifiques vous aide à éviter la détection de mouvement inutile, par exemple si la caméra couvre une zone où un arbre bouge dans le vent ou un endroit où des voitures passent régulièrement en arrière-plan.

Lorsque vous utilisez l'exclusion de zones avec des caméras PTZ et que cette caméra peut être orientée, inclinée et agrandie, l'exclusion de zone **ne se déplace pas** car est verrouillée en fonction de l'image de la caméra et pas de l'objet.

1. Pour utiliser l'exclusion de zones, cochez la case **Utiliser l'exclusion de zones**.  
Une grille divise l'image de l'aperçu en zones à sélectionner.
2. Pour définir les régions à exclure, faites glisser le curseur de la souris sur les zones requises dans l'image de l'aperçu tout en appuyant sur le bouton gauche de la souris. Le bouton droit de la souris permet d'annuler la zone sélectionnée.

Vous pouvez définir autant de zones à exclure que nécessaire. Les zones exclues apparaissent en bleu :



Les zones à exclure bleues apparaissent uniquement dans l'image d'aperçu de l'onglet **Mouvement**, et non dans les autres images d'aperçu du Management Client ou des clients d'accès.

## Onglet Préréglages (périphériques)


### Onglet Préréglages (explications)

Les périphériques suivants possèdent un onglet **Préréglages** :

- Caméras PTZ prenant en charge les positions prédéfinies.

L'onglet **Préréglages** vous permet de créer ou d'importer des positions prédéfinies, par exemple :

- Dans les règles pour le déplacement d'une caméra PTZ (pan-tilt-zoom) vers une position prédéfinie spécifique lorsqu'un événement survient
- Dans la patrouille, pour le déplacement automatique d'une caméra PTZ entre plusieurs positions prédéfinies
- Pour l'activation manuelle par les utilisateurs XProtect Smart Client

Vous pouvez verrouiller une position prédéfinie si vous souhaitez empêcher les utilisateurs de XProtect Smart Client ou les utilisateurs dotés de droits de sécurité limités de mettre à jour ce préréglage. Les préréglages verrouillés sont indiqués par l'icône .

Les administrateurs dotés de droits de sécurité suffisants pour exécuter une session PTZ réservée (voir Sessions PTZ réservées (explication) sur la page 260) peuvent exécuter la caméra PTZ dans ce mode. Ceci évite que d'autres utilisateurs prennent le contrôle de la caméra. Avec des droits suffisants, vous pouvez libérer les sessions PTZ réservées d'autres utilisateurs (voir Libérer la session PTZ sur la page 260).


Vous attribuez la permission PTZ à des rôles sur l'onglet Sécurité globale (voir Onglet Sécurité globale (rôles) sur la page 377) ou l'onglet PTZ (voir Onglet PTZ (rôles) sur la page 413).

Vous pouvez surveiller le système pour savoir s'il est actuellement en patrouille ou si un utilisateur en a pris le contrôle dans l'espace de la **session PTZ**. (voir Propriétés des sessions PTZ sur la page 261)

Vous pouvez également y modifier les périodes d'expiration des sessions PTZ pour la caméra.

### Properties

**Preview**



**Preset positions**

Use presets from device

- ↕ Dairy products
- ↕ Store entrance
- ↕ Canned foods
- ↕ Soft drinks
- ↕ Fresh products
- ↕ Delicatessen
- ↕ Check-out
- ↕ Frozen products

Add New...

Edit...

Delete

Activate

Default preset ↑ ↓

**PTZ session**

User	Priority	Timeout	Reserved
	0	00:00:00	False

Release
Reserve

Timeout for manual PTZ session: 15 Seconds

Timeout for pause patrolling session: 10 Minutes

Timeout for reserved PTZ session: 1 Hours

Info
Settings
Streams
Record
Motion
Presets
Patrolling
◀ ▶

Ajouter une position prédéfinie (type 1) sur la page 255

Utiliser les positions prédéfinies de la caméra (type 2) sur la page 257

Assigner une position prédéfinie par défaut sur la page 257

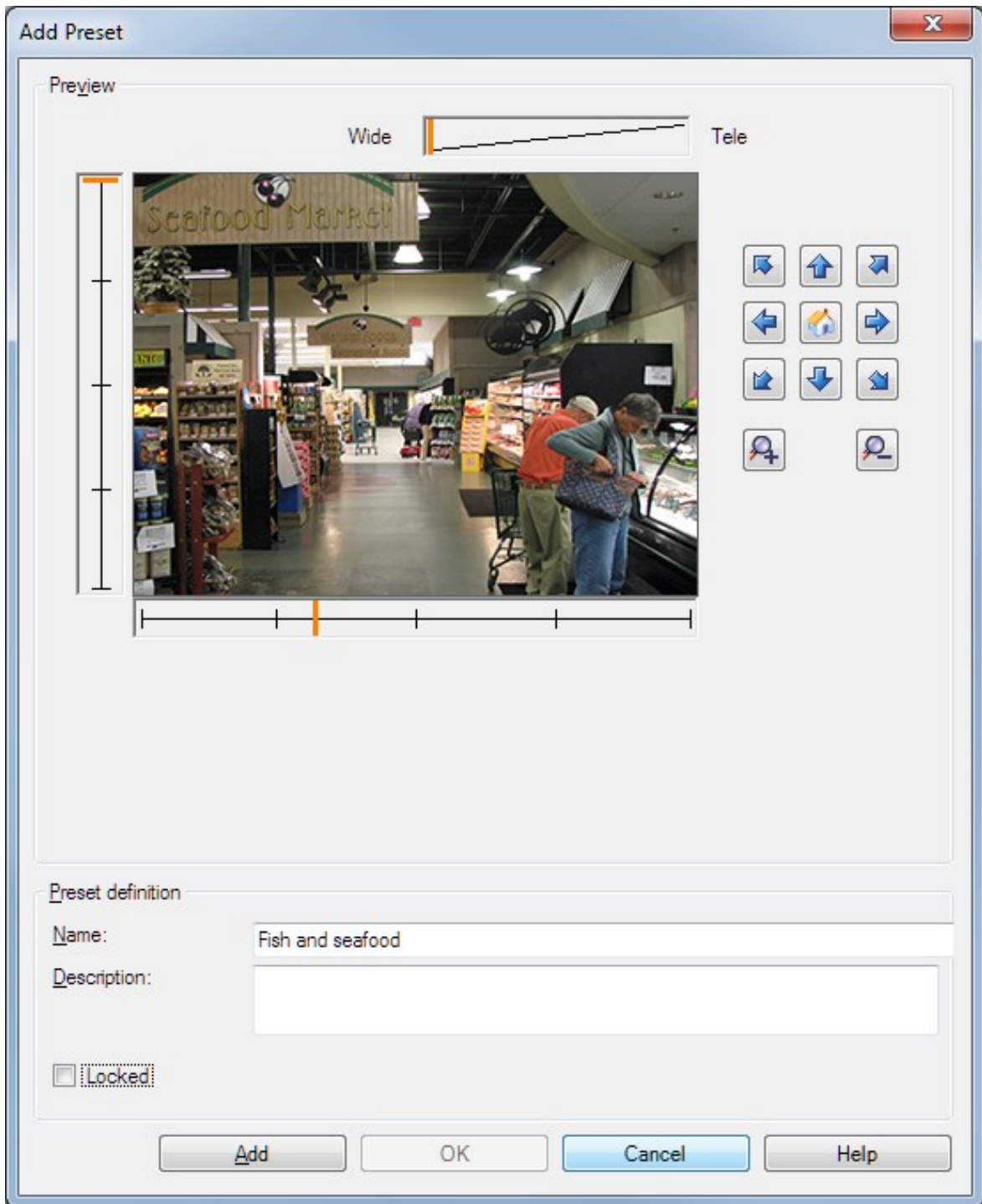
Modifier une position prédéfinie (type 1 seulement) sur la page 257

Tester une position prédéfinie (type 1 seulement) sur la page 260

### [Ajouter une position prédéfinie \(type 1\)](#)

Pour ajouter une position prédéfinie pour la caméra :

1. Cliquez sur **Ajouter nouveau**. La fenêtre **Ajouter un préréglage** s'ouvre :



2. La fenêtre **Ajouter un préréglage** affiche une image d'aperçu en direct depuis la caméra. Utilisez les boutons de navigation et/ou les curseurs pour déplacer la caméra jusqu'à la position souhaitée.
3. Précisez un nom en ce qui concerne la position prédéfinie, dans le champ **Nom**.



4. Facultativement, saisissez une description de la position prédéfinie dans le champ **Description**.
5. Sélectionnez **Verrouillé** si vous souhaitez verrouiller la position prédéfinie. Seuls les utilisateurs dotés des droits suffisants peuvent déverrouiller la position par la suite.
6. Cliquez sur **Ajouter** pour spécifier des préréglages. Continuez à les ajouter jusqu'à ce que vous disposiez de tous les préréglages souhaités.
7. Cliquez sur **OK**. La fenêtre **Ajouter un préréglage** se ferme et ajoute la position à la liste des positions prédéfinies de l'onglet **Préréglages** de la caméra.

### Utiliser les positions prédéfinies de la caméra (type 2)

En alternative à la spécification des positions prédéfinies dans le système, vous pouvez préréglager ces positions pour certaines caméras PTZ directement sur la caméra. Pour ce faire, vous devrez généralement vous connecter à un site Internet de configuration spécifique au produit.

1. Importez les préréglages dans le système en sélectionnant **Utiliser les préréglages à partir du périphérique**.

Tous les préréglages précédemment définis pour la caméra sont supprimés, ce qui a une influence sur les règles et les calendriers de patrouille définis et supprime également les préréglages disponibles pour les utilisateurs XProtect Smart Client.

2. Cliquez sur **Supprimer** pour supprimer les préréglages dont vos utilisateurs n'ont pas besoin.
3. Cliquez sur **Modifier** si vous souhaitez modifier le nom affiché du préréglage (voir Renommer une position prédéfinie (type 2 seulement) sur la page 259).
4. Si vous souhaitez ensuite modifier ces préréglages définis sur le périphérique, modifiez-les sur la caméra, puis réimportez-les.

### Assigner une position prédéfinie par défaut

Si nécessaire, vous pouvez assigner l'une des positions prédéfinies d'une caméra PTZ à la position prédéfinie par défaut de la caméra.

Avoir une position prédéfinie par défaut peut s'avérer utile car cela vous permet de définir les règles indiquant que la caméra PTZ doit être mise en position prédéfinie par défaut dans des circonstances particulières, par exemple après que la caméra PTZ a été utilisée manuellement.

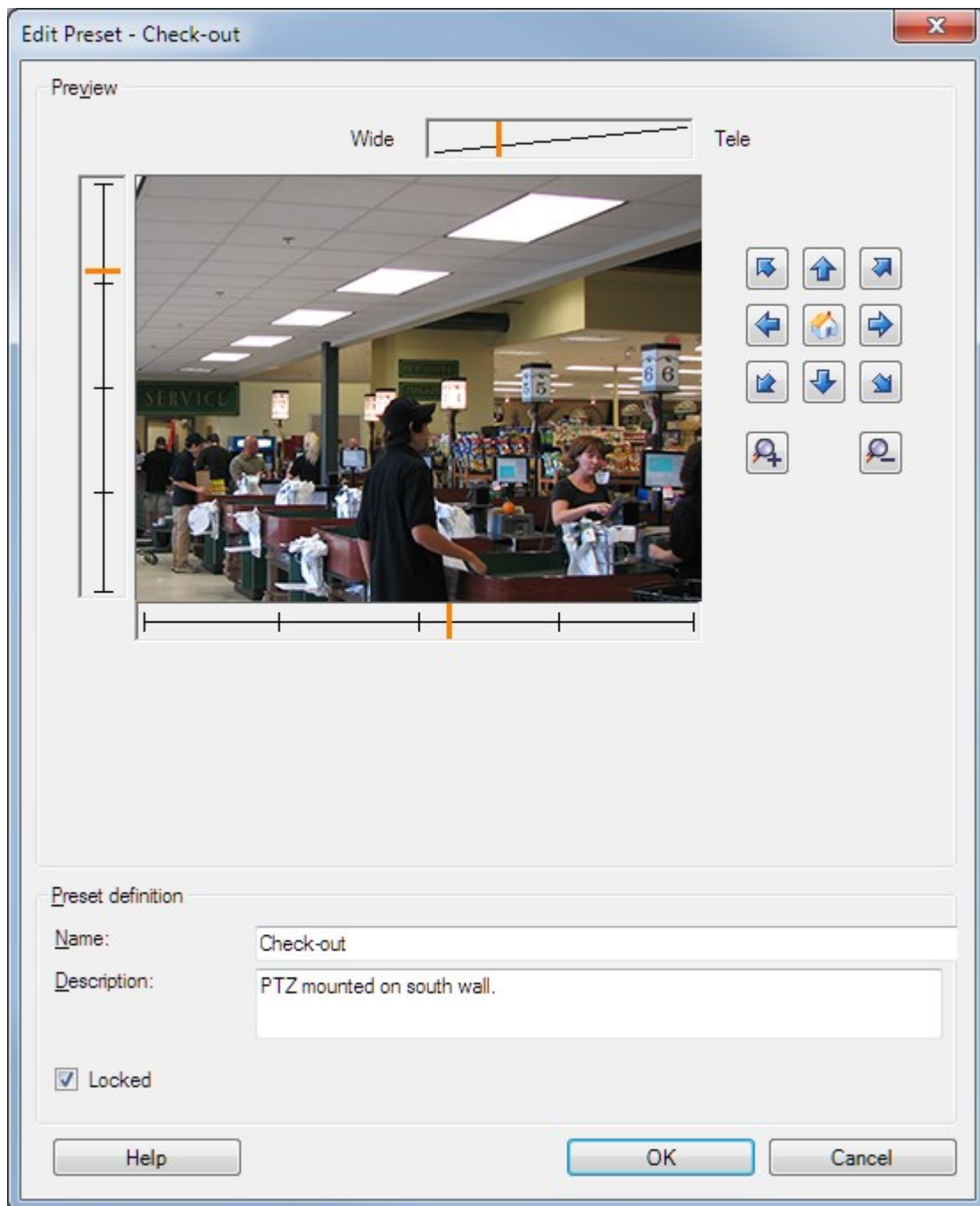
1. Pour assigner une position prédéfinie par défaut, sélectionnez le préréglage concerné dans votre liste de positions prédéfinies.
2. Cochez la case **Préréglage par défaut** sous la liste.

Seule une position prédéfinie peut être définie comme position prédéfinie par défaut.

### Modifier une position prédéfinie (type 1 seulement)

Pour modifier une position prédéfinie existante, définie dans le système :

1. Sélectionnez la position prédéfinie requise dans la liste de l'onglet **Préréglages** des positions prédéfinies à disposition pour la caméra.
2. Cliquez sur **Modifier**. Cela ouvre la fenêtre **Modifier un préréglage** :



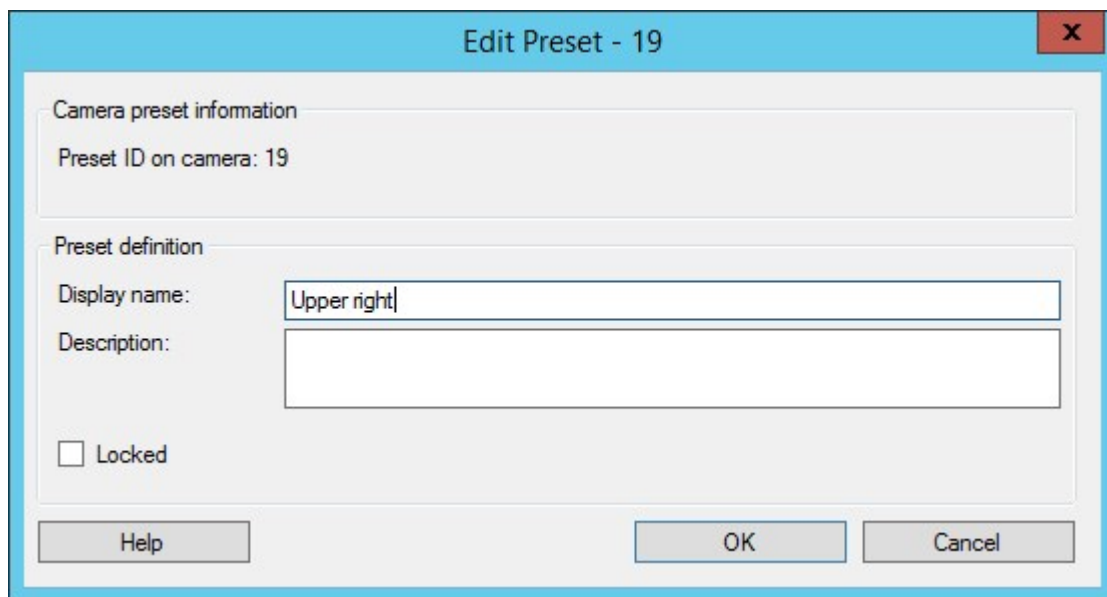
3. La fenêtre **Modifier un préréglage** affiche la vidéo en direct depuis la position prédéfinie. Utilisez les boutons de navigation et/ou les curseurs pour modifier la position prédéfinie en fonction de vos besoins.
4. Changez le nom/le numéro et la description de la position prédéfinie si nécessaire.


5. Sélectionnez **Verrouillé** si vous souhaitez verrouiller la position prédéfinie. Seuls les utilisateurs dotés des droits suffisants peuvent déverrouiller la position par la suite.
6. Cliquez sur **OK**.

### Renommer une position prédéfinie (type 2 seulement)


Pour modifier le nom d'une position prédéfinie dans la caméra :

1. Sélectionnez la position prédéfinie requise dans la liste de l'onglet **Préréglages** des préreglages à disposition pour la caméra.
2. Cliquez sur **Modifier**. Cela ouvre la fenêtre **Modifier un préreglage** :



3. Modifiez le nom et ajoutez une description de la position prédéfinie si nécessaire.
4. Sélectionnez **Verrouillé** si vous souhaitez verrouiller le nom du préreglage. Vous pouvez verrouiller un nom de préreglage si vous souhaitez empêcher les utilisateurs de XProtect Smart Client ou les utilisateurs dotés de droits de sécurité limités de mettre à jour le nom du préreglage ou de le supprimer. Les préreglages verrouillés sont indiqués par l'icône . Seuls les utilisateurs dotés des droits suffisants peuvent déverrouiller le nom du préreglage par la suite.
5. Cliquez sur **OK**.

### Verrouiller une position prédéfinie

Vous pouvez verrouiller une position prédéfinie si vous souhaitez empêcher les utilisateurs de XProtect Smart Client ou les utilisateurs dotés de droits de sécurité limités de mettre à jour ou de supprimer un préreglage. Les préreglages verrouillés sont indiqués par l'icône .

Vous verrouillez les réglages prédéfinis dans le cadre de l'ajout (voir Ajouter une position prédéfinie (type 1) sur la page 255) et de la modification (voir Modifier une position prédéfinie (type 1 seulement) sur la page 257).

### Tester une position prédéfinie (type 1 seulement)

1. Sélectionnez la position prédéfinie requise dans la liste de l'onglet **Préréglages** des positions prédéfinies à disposition pour la caméra.
2. Cliquez sur **Activer**.
3. La caméra se déplace vers la position prédéfinie sélectionnée.

### Sessions PTZ réservées (explication)

En fonction de votre système de surveillance, vous pouvez réserver des sessions PTZ.

Les administrateurs dotés de droits de sécurité suffisants pour exécuter une session PTZ réservée peuvent exécuter la caméra PTZ dans ce mode. Ceci évite que d'autres utilisateurs prennent le contrôle de la caméra. Dans une session PTZ réservée, le système de priorité PTZ standard est ignoré pour éviter que les utilisateurs dotés d'une priorité PTZ plus élevée n'interrompent la session.

Vous pouvez contrôler la caméra dans une session PTZ réservée à partir du XProtect Smart Client et du Management Client.

La réservation d'une session PTZ peut s'avérer utile lorsque vous avez besoin de procéder à des mises à jour ou à des opérations de maintenance urgentes sur une caméra PTZ ou sur ses préréglages sans être interrompu par d'autres utilisateurs.



Vous ne pouvez pas démarrer une session PTZ réservée si un utilisateur ayant une priorité supérieure à la vôtre contrôle la caméra ou si un autre utilisateur a déjà réservé la caméra.

### Libérer la session PTZ

Le bouton **Libère** vous permet de libérer votre session PTZ actuelle de façon à ce qu'un autre utilisateur puisse contrôler la caméra. Lorsque vous cliquez sur **Libérer**, la session PTZ prend immédiatement fin et est mise à la disposition du premier utilisateur qui fera fonctionner la caméra.

Des administrateurs dotés de la permission de sécurité **Libérer la session PTZ** ont le droit de libérer des sessions PTZ réservées par d'autres utilisateurs à tout moment. Ceci peut s'avérer utile lorsque vous avez besoin de procéder à la maintenance de la caméra PTZ ou de ses préréglages par exemple, ou si d'autres utilisateurs ont accidentellement bloqué la caméra dans des situations d'urgence.

### Spécifier les périodes d'expiration des sessions PTZ

Les utilisateurs Management Client et XProtect Smart Client dotés des droits d'utilisateurs nécessaires peuvent interrompre manuellement la patrouille des caméras PTZ.

Vous pouvez indiquer combien de temps doit s'écouler avant que le programme de patrouille habituel reprenne pour toutes les caméras PTZ de votre système :

1. Sélectionnez **Outils > Options**.
2. Dans l'onglet **Général** de la fenêtre **Options**, sélectionnez la durée dans :
  - La liste **Période d'inactivité pour les sessions PTZ manuelles** (la valeur par défaut est de 15 secondes).
  - La liste **Période d'inactivité pour la mise en pause des sessions PTZ** (la valeur par défaut est de 10 minutes).
  - La liste **Période d'inactivité pour les sessions PTZ réservées** (la valeur par défaut est de 1 heure).

Les paramètres s'appliquent à toutes les caméras PTZ de votre système.

Vous pouvez modifier les délais individuellement pour chaque caméra.

1. Dans le volet **Navigation sur le site**, cliquez sur **caméra**.
2. Dans le volet Vue d'ensemble, sélectionnez la caméra.
3. Dans l'onglet **Préréglages**, sélectionnez la durée dans :
  - La liste **Période d'inactivité pour la session PTZ manuelle** (la valeur par défaut est de 15 secondes).
  - La liste **Période d'inactivité pour la mise en pause de la session PTZ** (la valeur par défaut est de 10 minutes).
  - La liste **Période d'inactivité pour la session PTZ réservée** (la valeur par défaut est de 1 heure).

Les paramètres s'appliquent uniquement à cette caméra.

### Propriétés des sessions PTZ

Le tableau **session PTZ** présente l'état actuel de la caméra PTZ.

Nom	Description
<b>Utilisateur</b>	Affiche l'utilisateur qui a appuyé sur le bouton <b>Réservé</b> et contrôle la caméra PTZ à présent. Si une session de patrouille est activée par le système, <b>Patrouille en cours</b> s'affiche.
<b>Priorité</b>	Affiche la priorité PTZ de l'utilisateur. Vous ne pouvez prendre le contrôle que de sessions PTZ d'utilisateurs ayant une priorité inférieure à la vôtre.
<b>Délai</b>	Affiche le temps restant de la session PTZ actuelle.

Nom	Description
d'expiration	
Réservé	Indique si la session actuelle est une session PTZ réservée ou non : <ul style="list-style-type: none"> <li>• <b>Vrai</b> : Réserve</li> <li>• <b>Faux</b> : Non réservée</li> </ul>

Vous pouvez modifier les délais suivants pour chaque caméra PTZ.

Nom	Description
Période d'inactivité pour la session PTZ manuelle	Spécifiez la période d'inactivité pour les sessions PTZ manuelles sur cette caméra si vous souhaitez que le délai soit différent de la période par défaut. Vous pouvez spécifier la période par défaut dans le menu <b>Outils</b> sous <b>Options</b> .
Délai de mise en pause d'un session PTZ en patrouille	Spécifiez le délai de mise en pause des sessions PTZ en patrouille sur cette caméra si vous souhaitez que le délai soit différent de la période par défaut. Vous pouvez spécifier la période par défaut dans le menu <b>Outils</b> sous <b>Options</b> .
Période d'inactivité pour les sessions PTZ réservées	Spécifiez la période d'inactivité pour les sessions PTZ réservées sur cette caméra si vous souhaitez que le délai soit différent de la période par défaut. Vous pouvez spécifier la période par défaut dans le menu <b>Outils</b> sous <b>Options</b> .

## Onglet Patrouilles (périphériques)

### Onglet Patrouille (explications)

Les périphériques suivants possèdent un onglet **Patrouille** :

- Caméras PTZ

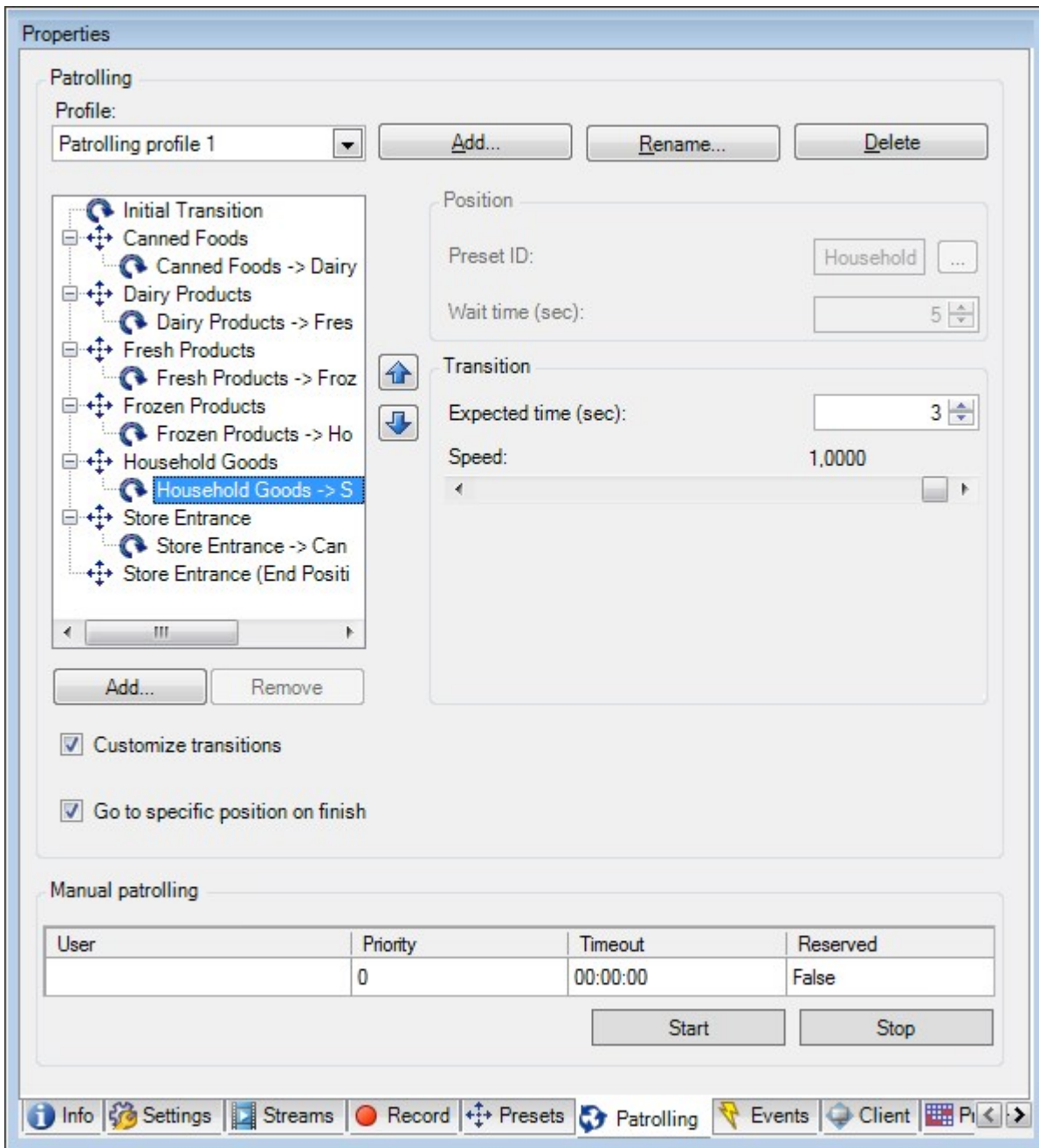
L'onglet **Patrouille** vous permet de créer des profils de patrouille, c'est-à-dire le mouvement automatique d'une caméra PTZ (pan-tilt-zoom) entre plusieurs positions prédéfinies.

Avant de pouvoir vous servir de la fonction Patrouille, vous devez saisir au moins deux positions prédéfinies pour la caméra dans l'onglet **Préréglages**.

Les profils de patrouille définissent la façon dont une patrouille doit avoir lieu. En font notamment partie l'ordre dans lequel la caméra doit se déplacer entre les positions prédéfinies et la durée pendant laquelle elle doit rester à chaque position. Vous pouvez créer un nombre illimité de profils de patrouille et les utiliser dans vos règles. Par exemple, vous pouvez créer une règle spécifiant qu'un profil de patrouille doit être utilisé pendant les heures d'ouverture de jour et un autre pendant la nuit.

Avant d'appliquer un profil de patrouille dans une règle, par exemple, vous pouvez tester le profil de patrouille à l'aide de la patrouille manuelle. Vous pouvez également utiliser la patrouille manuelle pour prendre le contrôle de la patrouille d'un autre utilisateur ou d'une patrouille activée par des règles, dans la mesure où vous disposez d'une priorité PTZ plus élevée.

Vous pouvez surveiller le système pour savoir s'il est actuellement en patrouille ou si un utilisateur en a pris le contrôle dans l'espace de la **Patrouille manuelle**.



L'onglet **Patrouille**, affichant un profil de patrouille avec des transitions personnalisées.

Ajouter un profil de patrouille sur la page 265

Spécifier des positions prédéfinies dans un profil de patrouille sur la page 265

Spécifier la durée à chaque position prédéfinie sur la page 266

Personnaliser les transitions (PTZ) sur la page 266

Spécifier une position de fin sur la page 267

Spécifiez la durée de session PTZ manuelle (voir Onglet Préréglages (périphériques) sur la page 253)



## Ajouter un profil de patrouille

Ajoutez le profil souhaité, à utiliser dans une règle :

1. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter profil** s'ouvre.
2. Dans la boîte de dialogue **Ajouter profil**, donnez un nom au profil de patrouille.
3. Cliquez sur **OK**. Le bouton est désactivé si le nom n'est pas unique.

Le nouveau profil de patrouille est ajouté à la liste **Profil**. Vous pouvez désormais préciser les positions prédéfinies et autres paramètres pour le profil de patrouille.

## Spécifier des positions prédéfinies dans un profil de patrouille

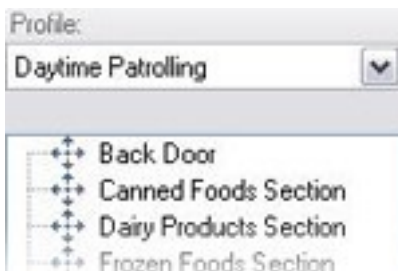
1. Sélectionnez le profil de patrouille dans la liste **Profil** :



2. Cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Sélectionner prédéfinition**, sélectionnez les positions prédéfinies de votre profil de patrouille :



4. Cliquez sur **OK**. Les positions prédéfinies sélectionnées sont ajoutées à la liste de positions prédéfinies du profil de patrouille :



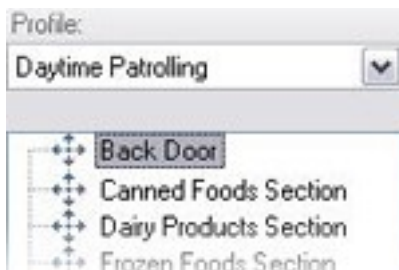
5. La caméra utilise la position prédéfinie la plus haute dans la liste comme premier arrêt lorsqu'elle patrouille en suivant le profil de patrouille. La position prédéfinie suivante depuis le haut constitue le second arrêt, et ainsi de suite.

### Spécifier la durée à chaque position prédéfinie

Lors d'une patrouille, la caméra PTZ reste par défaut pendant 5 secondes sur chaque position prédéfinie indiquée dans le profil de patrouille.

Pour modifier le nombre de secondes :

1. Sélectionnez le profil de patrouille dans la liste **Profil**.
2. Sélectionnez la position prédéfinie pour laquelle vous souhaitez modifier la durée :



3. Indiquez la durée dans le champ **Durée en position (sec)** :
4. Si nécessaire, recommencez pour d'autres positions prédéfinies.

### Personnaliser les transitions (PTZ)

Par défaut, la durée nécessaire au déplacement de la caméra d'une position prédéfinie à une autre, appelée **transition**, est estimée à trois secondes. Durant cette durée, par défaut, la détection du mouvement est désactivée sur la caméra, car un mouvement non pertinent est sinon susceptible d'être détecté alors que la caméra se déplace entre les positions prédéfinies.

La personnalisation des vitesses lors des transitions est uniquement prise en charge si votre caméra accepte le balayage PTZ et si elle est du type où les positions prédéfinies sont configurées et stockées sur le serveur de votre système (caméra PTZ type 1). Sinon, le curseur **vitesse** est grisé.

Vous pouvez personnaliser les éléments suivants :

- La durée de transition estimée
- La vitesse à laquelle la caméra se déplace lors d'une transition

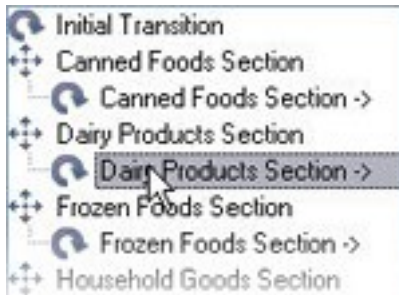
Pour personnaliser les transitions entre les différentes positions prédéfinies :

1. Sélectionnez le profil de patrouille dans la liste **Profil**.
2. Cochez la case **Personnaliser transitions**.



Les indications relatives à la transition sont ajoutées dans la liste des positions prédéfinies.

3. Dans la liste, sélectionnez la transition.



4. Indiquez la durée de transition estimée (en secondes) dans le champ **Temps escompté (sec.)**.

Expected time (secs.)

5. Utilisez le curseur **Vitesse** afin de préciser la vitesse de transition. Lorsque le curseur est complètement à droite, la caméra se déplace à sa vitesse par défaut. Plus vous déplacez le curseur sur la gauche, plus la caméra se déplacera lentement durant la transition choisie.
6. Répétez la procédure le cas échéant pour les autres transitions.

### Spécifier une position de fin

Vous pouvez indiquer que la caméra doit se déplacer vers une position prédéfinie particulière lors d'une patrouille, conformément aux fins sélectionnées du profil de patrouille.

1. Sélectionnez le profil de patrouille dans la liste **Profil**.
2. Cochez la case **Atteindre une position spécifique à la fin**. Cela ouvre la boîte de dialogue **Sélectionner le pré réglage**.
3. Sélectionnez la position de fin, puis cliquez sur **OK**.



Vous pouvez sélectionner n'importe quelle position prédéfinie de la caméra comme position finale, vous n'avez pas à vous limiter aux positions prédéfinies utilisées dans le profil de patrouille.

4. La nouvelle position finale est ajoutée à la liste des profils.

Lors d'une patrouille conformément aux fins sélectionnées du profil de patrouille, la caméra se déplace en position finale indiquée.

### Patrouille manuelle (explications)

Lorsque vous avez conçu un profil de patrouille, vous pouvez le tester avec une patrouille manuelle avant de l'appliquer au système. Utilisez les boutons **Démarrer** et **Arrêter** pour lancer et arrêter la patrouille manuelle.

Si la caméra est déjà en patrouille ou contrôlée par un autre utilisateur, vous ne pouvez démarrer la patrouille manuelle que si vous disposez d'une priorité supérieure.

Si vous démarrez une patrouille manuelle alors que la caméra exécute une patrouille du système activée par des règles, le système reprend cette patrouille lorsque vous arrêtez votre patrouille manuelle. Si un autre utilisateur exécute une patrouille manuelle mais que vous disposez d'une priorité plus élevée et que vous démarrez votre patrouille manuelle, la patrouille manuelle de l'autre utilisateur ne reprendra pas.

Si vous n'arrêtez pas votre patrouille manuelle de vous-même, celle-ci se poursuivra jusqu'à ce qu'une patrouille basée sur des règles ou un utilisateur doté d'une priorité supérieure prenne le contrôle. Lorsque la patrouille du système basée sur des règles s'arrête, le système reprend votre patrouille manuelle. Si un autre utilisateur démarre une patrouille manuelle, votre patrouille manuelle s'arrête et ne reprendra pas.

Lorsque vous arrêtez votre patrouille manuelle et que vous avez défini une position finale pour votre profil de patrouille à l'aide de **Atteindre une position spécifique à la fin**, la caméra revient à cette position.

### Propriétés des patrouilles manuelles

Le tableau **Patrouille manuelle** présente l'état actuel de la caméra PTZ.

Nom	Description
<b>Utilisateur</b>	Affiche l'utilisateur qui a réservé la session PTZ ou démarré une patrouille manuelle et contrôle actuellement la caméra.  Si une session de patrouille est activée par le système, <b>Patrouille en cours</b> s'affiche.
<b>Priorité</b>	Affiche la priorité PTZ de l'utilisateur. Vous ne pouvez prendre le contrôle que de sessions PTZ d'utilisateurs ou de profils de patrouille ayant une priorité inférieure à la vôtre.
<b>Délai d'expiration</b>	Affiche le temps restant des sessions PTZ manuelles ou réservées actuelles.
<b>Réservé</b>	Indique si la session actuelle est une session PTZ réservée ou non. <ul style="list-style-type: none"> <li>• <b>Vrai</b> : Réservé</li> <li>• <b>Faux</b> : Non réservé</li> </ul>

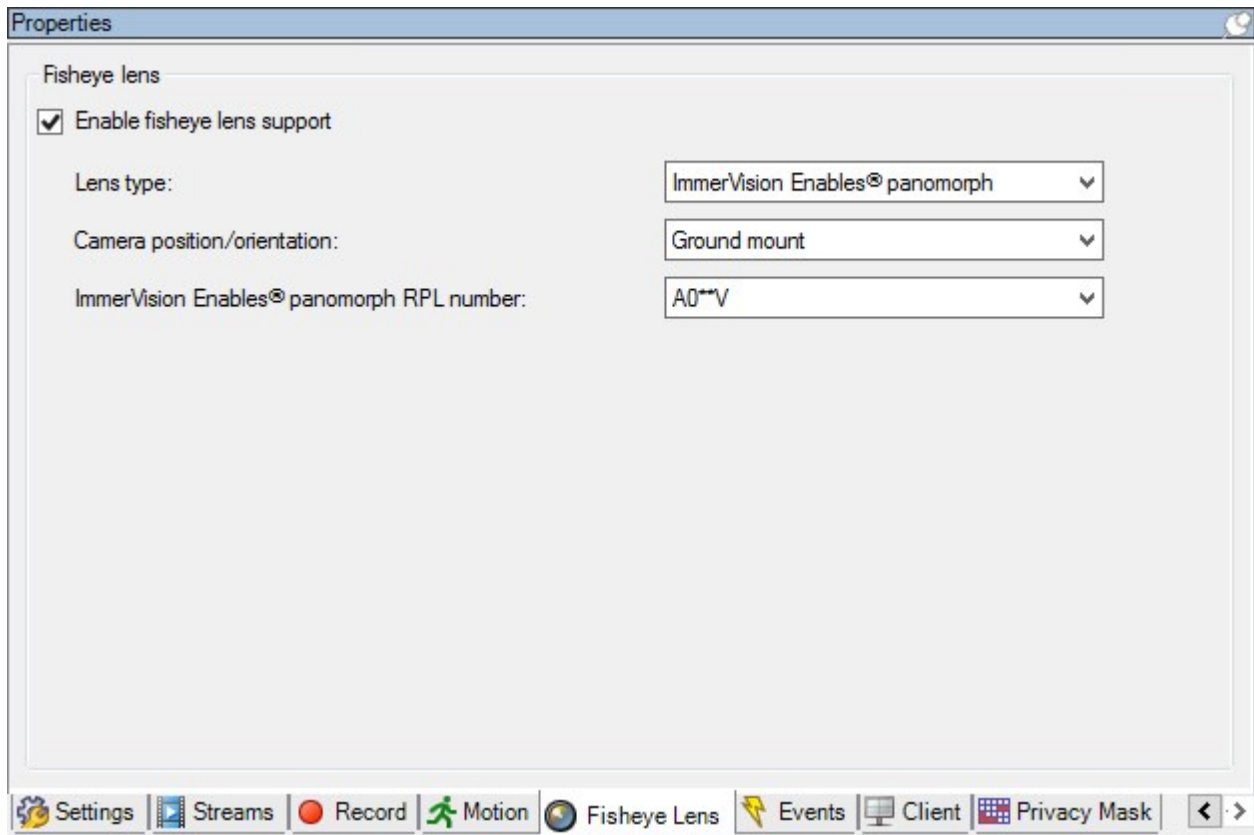
## Onglet Lentille fisheye (périphériques)

### Onglet Lentille Fisheye (explications)

Les périphériques suivants possèdent un onglet **Lentille fisheye** :

- Caméras fixes avec une lentille fisheye

L'onglet **Lentille fisheye** vous permet d'activer et de configurer la prise en charge fisheye de la caméra sélectionnée.



### Activer et désactiver la prise en charge fisheye

La prise en charge fisheye est désactivée par défaut.

Pour l'activer ou la désactiver, cochez ou décochez la case **Activer le support fisheye** de l'onglet **Lentille fisheye**.

### Spécifier les paramètres de la lentille fisheye

Pour activer la prise en charge de la lentille fisheye :

1. Sélectionnez le type de lentille.
2. Indiquez la position physique / l'orientation de la caméra dans la liste **Position/orientation de la caméra**.
3. Sélectionnez le nombre de Lentilles Panomorph Enregistrées (RPL) depuis la liste du numéros de RPL panomorph **ImmerVision Enables®**.

Ceci permet d'identifier et de corriger la configuration de la lentille utilisée avec la caméra. Vous trouverez généralement le numéro RPL sur la lentille elle-même ou sur sa boîte d'origine. Pour en savoir plus sur ImmerVision, les lentilles panomorphes et les RPL, voir le site Internet d'ImmerVision (<https://www.immervisionenables.com/>).

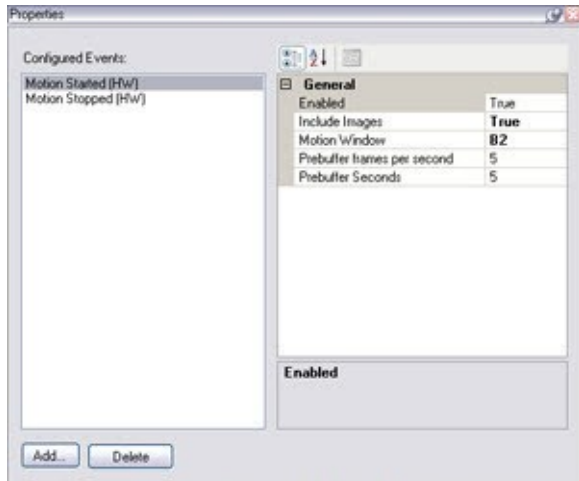
## Onglet Événements (périphériques)

### Onglet Événements (explications)

Les périphériques suivants possèdent un onglet **Événements** :

- Caméras
- Microphones
- Entrées

Outre les événements du système, certains périphériques peuvent être configurés pour déclencher des événements. Vous pouvez utiliser ces événements lors de la création de règles basées sur des événements dans le système. Ils se produisent techniquement sur le matériel/périphérique et non sur le système de surveillance.



Onglet **Événement**, exemple de la **caméra**.

Lorsque vous supprimez un événement, cela affecte toutes les règles qui utilisent l'événement.

- Ajout d'un événement sur la page 271
- Spécifier les propriétés des événements sur la page 271
- Utiliser plusieurs instances d'un événement sur la page 271

## Ajout d'un événement

1. Dans le volet **Vue d'ensemble**, sélectionnez un périphérique.
2. Sélectionnez l'onglet **Événements** et cliquez sur **Ajouter**. La fenêtre **Sélectionner un événement pilote** s'ouvre.
3. Sélectionner un événement. Vous pouvez uniquement sélectionner un événement à la fois.
4. Si vous souhaitez consulter la liste complète de tous les événements, ce qui vous permet d'ajouter des événements qui ont déjà été ajoutés, sélectionnez **Afficher les événements déjà ajoutés**.
5. Cliquez sur **OK**.
6. Dans la boîte à outils, cliquez sur **Enregistrer**.

## Spécifier les propriétés des événements

Vous pouvez spécifier les propriétés pour chaque événement que vous avez ajouté. Le nombre de propriétés dépend du périphérique et de l'élément. Afin que l'événement fonctionne comme prévu, vous devez spécifier une partie ou la totalité des propriétés de la même façon sur le périphérique ainsi que sur cet onglet.

## Utiliser plusieurs instances d'un événement

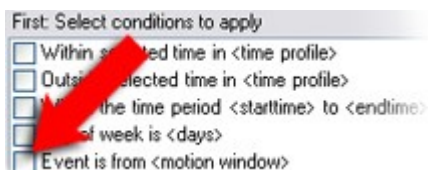
Pour pouvoir spécifier différentes propriétés pour différentes instances d'un événement, vous pouvez ajouter un événement plus d'une fois.



L'exemple suivant est spécifique aux caméras.

**Exemple :** Vous avez configuré la caméra avec deux fenêtres de mouvement appelées A1 et A2. Vous avez ajouté deux instances de l'événement Mouvement démarré (HW). Dans les propriétés de l'une des instances, vous avez précisé l'utilisation de la fenêtre de mouvement A1. Dans les propriétés de l'autre instance, vous avez précisé l'utilisation de la fenêtre de mouvement A2.

Lorsque vous utilisez l'événement dans une règle, vous pouvez spécifier que l'événement doit être basé sur le mouvement détecté dans une fenêtre de mouvement spécifique afin que la règle soit déclenchée :



## Onglet événement (propriétés)

Nom	Description
<b>Événements configurés</b>	Les événements que vous sélectionnez et ajoutez dans la liste d' <b>Événements configurés</b> sont entièrement déterminés par le périphérique et sa configuration. Pour certains types de périphériques, la liste est vide.
<b>Généralités</b>	La liste de propriétés dépend du périphérique et de l'élément. Afin que l'événement fonctionne comme prévu, vous devez spécifier une partie ou la totalité des propriétés de la même façon sur le périphérique ainsi que sur cet onglet.

## Onglet Client (périphériques)

### Onglet Client (explications)

Les périphériques suivants possèdent un onglet **Client** :

- Caméras

Dans l'onglet **Client**, vous pouvez préciser quels autres périphériques sont vus et entendus lorsque vous utilisez la caméra dans XProtect Smart Client.

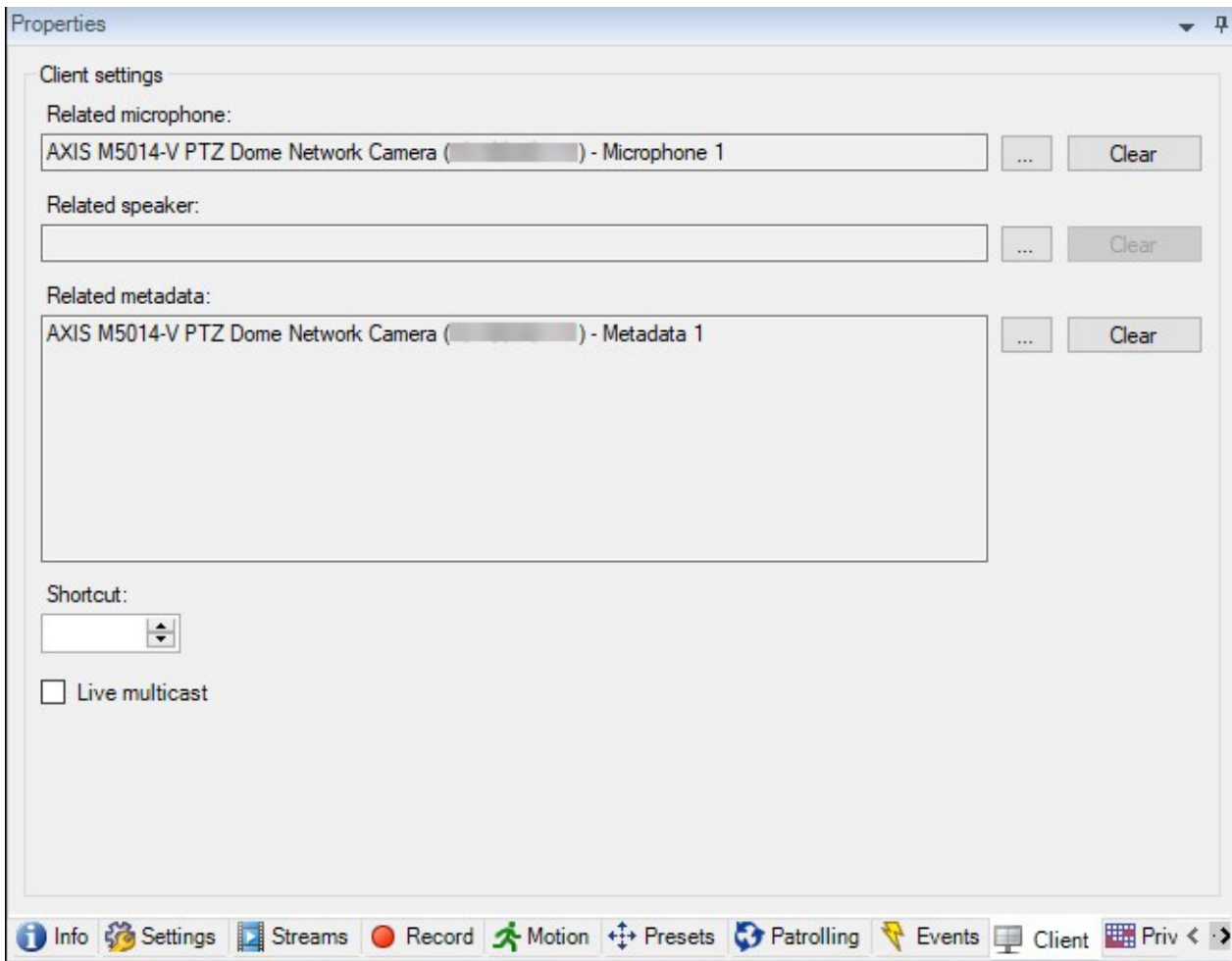
Les périphériques connexes enregistrent aussi lorsque la caméra enregistre, voir Activer l'enregistrement sur les périphériques connexes sur la page 239.

Vous pouvez également activer la **Multidiffusion en direct** sur la caméra. Cela signifie que la caméra effectue une multidiffusion en direct aux clients par le biais du serveur d'enregistrement.



Les flux de multidiffusion ne sont pas cryptés, même si le serveur d'enregistrement utilise le cryptage.







Voir également :

- Activez le multicast pour le serveur d'enregistrement sur la page 182
- Multicast (explications) sur la page 181


### Propriétés de l'onglet Client

Nom	Description
<b>Microphone connexe</b>	Spécifiez depuis quel microphone de la caméra les utilisateurs XProtect Smart Client écoutent la radio par défaut. L'utilisateur XProtect Smart Client peut choisir l'écoute par un autre microphone

Nom	Description
	<p>manuellement le cas échéant .</p> <p>Spécifiez le microphone lié à la caméra de la vidéo push pour diffuser une vidéo avec l'audio.</p> <p>Les microphones connexes enregistrent lorsque la caméra enregistre.</p>
<b>Haut-parleur connexe</b>	<p>Spécifiez depuis quels haut-parleurs de la caméra les utilisateurs XProtect Smart Client parlent par défaut. L'utilisateur XProtect Smart Client peut sélectionner un autre haut-parleur manuellement le cas échéant.</p> <p>Les haut-parleurs connexes enregistrent lorsque la caméra enregistre.</p>
<b>Métadonnées connexes</b>	<p>Indiquez un ou plusieurs périphériques métadonnées sur la caméra à partir desquels les utilisateurs XProtect Smart Client reçoivent des données.</p> <p>Les dispositifs de métadonnées connexes lorsque la caméra enregistre.</p>
<b>Raccourci</b>	<p>Pour faciliter la sélection des caméras pour les utilisateurs XProtect Smart Client, définissez des raccourcis clavier pour la caméra.</p> <ul style="list-style-type: none"> <li>• Créez chaque raccourci de sorte qu'il identifie de manière unique la caméra</li> <li>• Le numéro de raccourci d'une caméra ne peut pas avoir plus de quatre chiffres</li> </ul>
<b>Multicast en direct</b>	<p>Le système prend en charge le multicast de flux en direct depuis le serveur d'enregistrement vers XProtect Smart Client. Pour permettre la multidiffusion des flux en direct depuis la caméra, sélectionnez la boîte à cocher.</p>

Nom	Description
	<div data-bbox="379 322 954 607" style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;">  <p>La multidiffusion en direct ne fonctionne que sur le flux que vous avez spécifié comme étant le flux de la caméra par défaut dans l'onglet <b>Flux</b>.</p> </div> <p data-bbox="379 663 954 801">Vous devez également configurer le mode multicast pour le serveur d'enregistrement. Voir Onglet Multicast (serveur d'enregistrement) sur la page 179.</p> <div data-bbox="379 824 954 1032" style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;">  <p>Les flux de multidiffusion ne sont pas cryptés, même si le serveur d'enregistrement utilise le cryptage.</p> </div>

## Onglet Masquage de confidentialité (périphériques)



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

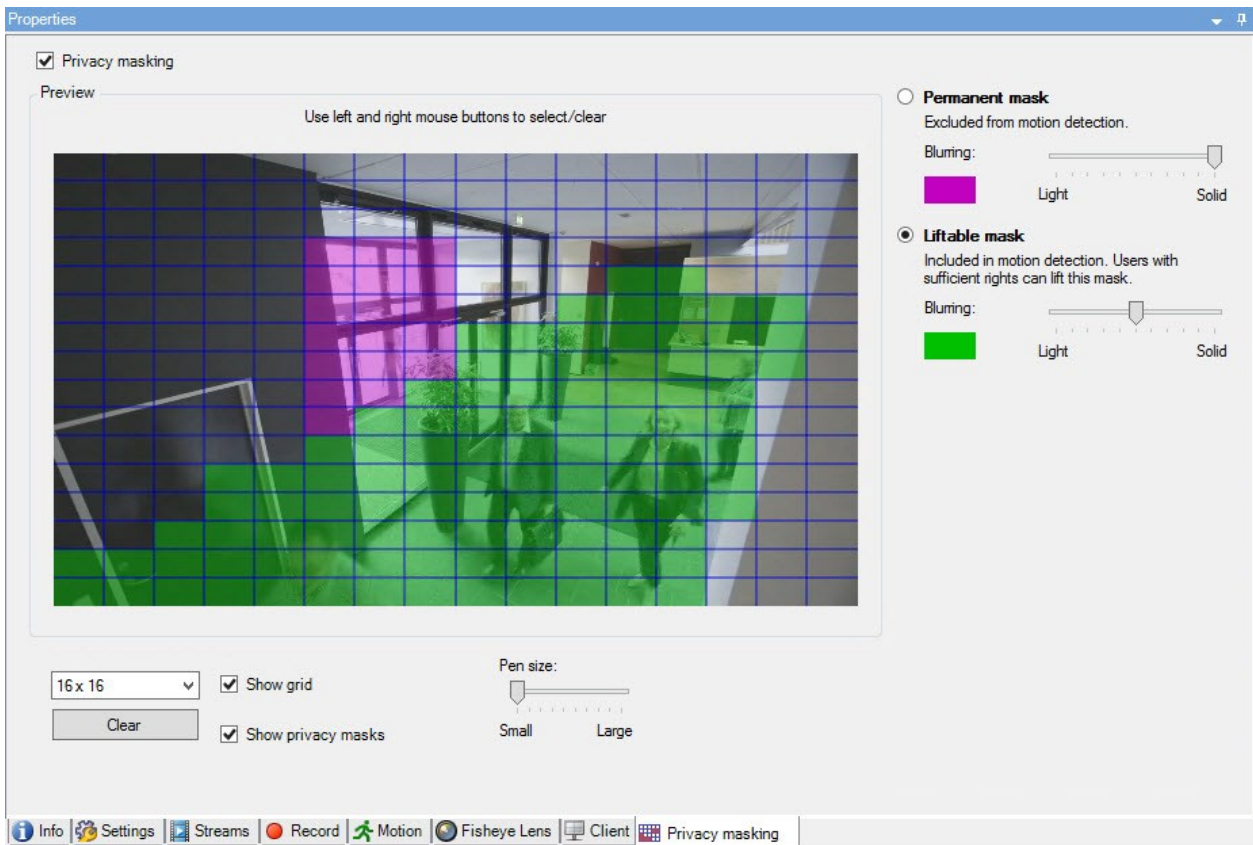
XProtect Essential+ 2018 R1 et suivantes ne prennent pas en charge le masquage de confidentialité ; de ce fait, si vous effectuez une mise à niveau à partir d'un système où les masques de confidentialité sont appliqués, les masques seront supprimés.

### Onglet masquage de confidentialité (explications)

Les périphériques suivants possèdent un onglet **Masque de confidentialité** :

- Caméras

L'onglet **Masquage de confidentialité** vous permet d'activer et de configurer le masque de confidentialité de la caméra sélectionnée.



Les masques de confidentialité sont utilisés et verrouillés sur une zone de l'image de la caméra afin que la zone couverte ne suive pas les mouvements (Panoramique/Inclinaison/Zoom), mais couvre constamment la même zone de l'image de la caméra. Sur certaines caméras PTZ, vous pouvez activer une position en fonction du masquage de confidentialité sur la caméra elle-même.

Dans une configuration Milestone Interconnect, le site central ignore les masques de confidentialité défini dans un site distant. Si vous souhaitez utiliser les mêmes masques de confidentialité, vous devez les redéfinir sur le site central.

- Masquage de confidentialité (explications) sur la page 277
- Activer/désactiver le masquage de confidentialité sur la page 279
- Définir les masques de confidentialité sur la page 279
- Changez le délai d'expiration des masques de confidentialité sur la page 281
- Donner aux utilisateurs l'autorisation d'enlever les masques de confidentialité sur la page 280
- Créez un rapport de configuration de votre configuration du masquage de confidentialité sur la page 282

## Masquage de confidentialité (explications)

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

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

Il existe deux types de masques de confidentialité :

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



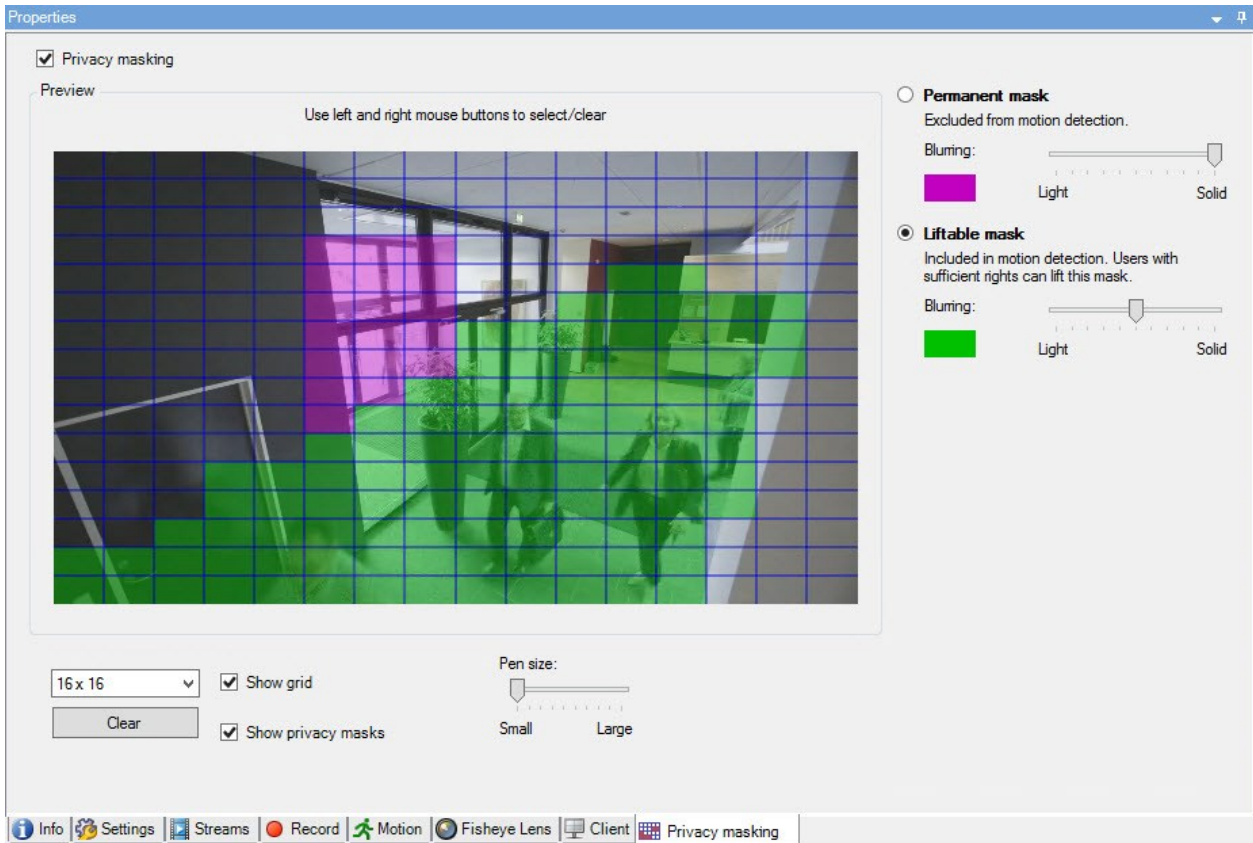
Si vous effectuez une mise à niveau à partir d'un système 2017 R3 ou plus ancien où des masques de confidentialité sont utilisés, les masques seront convertis en masques relevables.

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

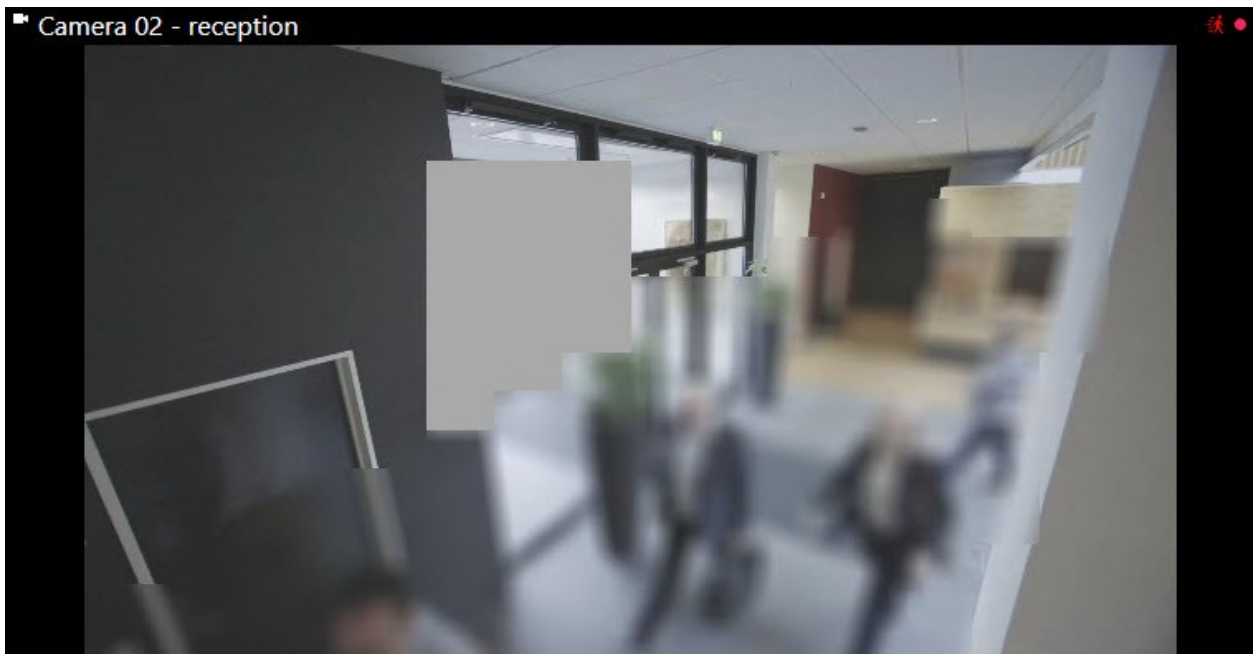


Si vous modifiez les paramètres de masquage de confidentialité très souvent, par exemple, une fois par semaine, votre système peut éventuellement être surchargé.

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



Et voici comment ils s'affichent dans les clients :





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

### Activer/désactiver le masquage de confidentialité

La fonction de masquage de confidentialité est désactivée par défaut.

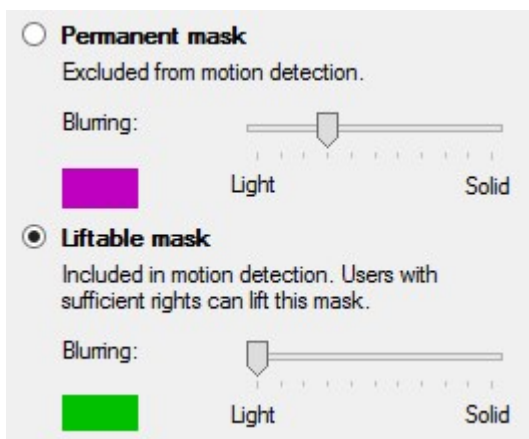
Pour activer/désactiver la fonction de masquage de confidentialité pour une caméra :

- Cochez ou décochez la case **Masquage de confidentialité** dans l'onglet **Masque de confidentialité**

### Définir les masques de confidentialité

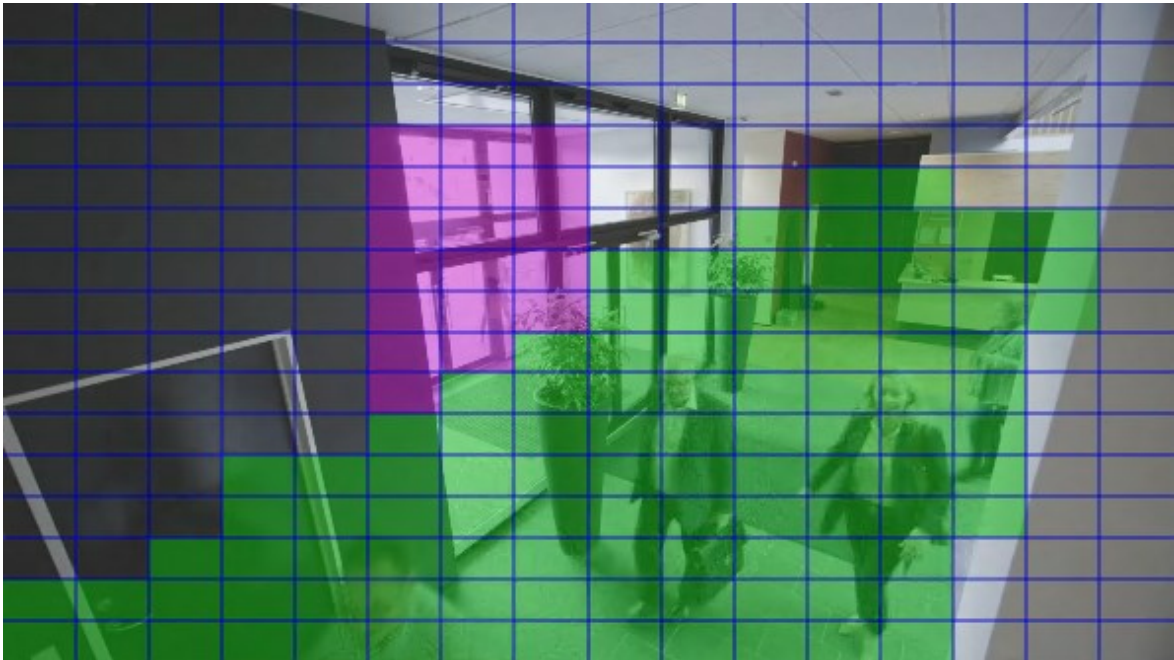
Lorsque vous activez la fonction de masquage de confidentialité sur l'onglet **masquage de confidentialité**, une grille s'applique à l'aperçu de la caméra.

1. Pour couvrir une zone avec un masque de confidentialité, indiquez d'abord si vous souhaitez un masque de confidentialité permanent ou relevable.



2. Faites glisser le pointeur de souris sur l'aperçu. Appuyez sur le bouton gauche de la souris pour sélectionner une cellule de la grille. Appuyez sur le bouton droit de la souris pour décocher une grille de la cellule.

3. Vous pouvez définir autant de zones de masque de confidentialité que nécessaire. Les zones caractérisées par des masques de confidentialité s'affichent en violet et les zones se distinguant par des masques de confidentialité relevables sont en vert.



4. Définissez le mode de couverture des zones doit apparaître dans la vidéo lorsqu'elles s'affichent dans les clients. Utilisez des curseurs pour passer d'un masque de flou lumineux à un masque complètement opaque.



Les masques de confidentialité permanents se trouvent également sur l'onglet **Mouvement**.

5. Dans XProtect Smart Client, vérifiez que le masque de confidentialité apparaît tel que vous l'avez défini.

### Donner aux utilisateurs l'autorisation d'enlever les masques de confidentialité

Par défaut, aucun utilisateur n'a l'autorisation de lever les masques de confidentialité dans XProtect Smart Client.

Pour activer/désactiver l'autorisation :

1. Dans **Rôles**, sélectionnez le rôle pour lequel vous souhaitez donner l'autorisation de lever les masques de confidentialité.
2. Sélectionnez **Caméras**, sélectionnez l'onglet **Sécurité globale**.
3. Cochez la case **Autoriser** de l'autorisation **Lever les masques de confidentialité**.

Les utilisateurs que vous affectez à ce rôle peuvent lever les masques de confidentialité configurés en tant que masques relevables pour lui-même et autoriser le levage pour les autres utilisateur de XProtect Smart Client.



## Changez le délai d'expiration des masques de confidentialité

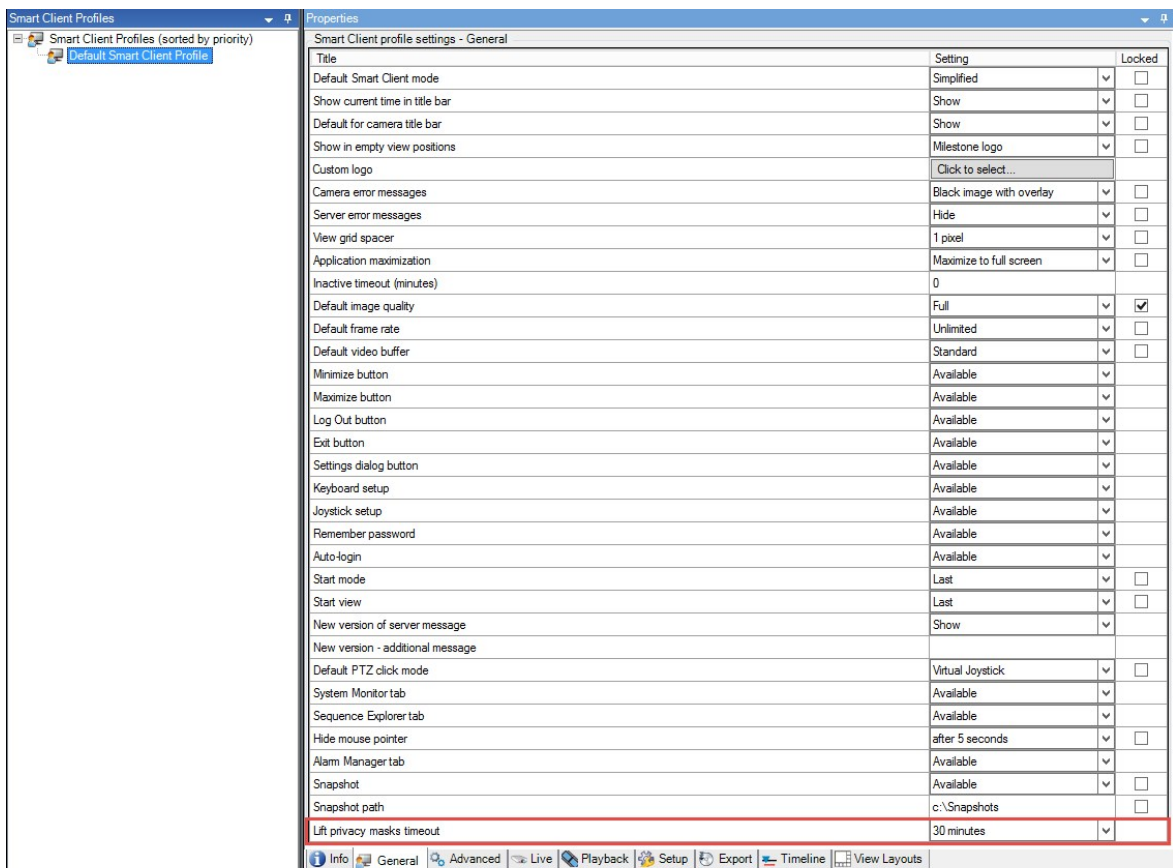
Par défaut, les masques de confidentialité sont levés pendant 30 minutes dans XProtect Smart Client et utilisés par la suite automatiquement, mais vous pouvez modifier tout cela.



Lorsque vous changez le délai d'expiration, n'oubliez pas de le faire pour le profil Smart Client associé au rôle qui a l'autorisation de lever les masques de confidentialité.

Pour changer le délai d'expiration :

1. Dans **Profils Smart Client**, sélectionnez le profil Smart Client concerné.
2. Sur l'onglet **Général**, repérez l'option **Délai d'expiration des masques de confidentialité**.



3. Sélectionnez parmi les valeurs :
  - **2 minutes**
  - **10 minutes**
  - **30 minutes**
  - **1 heure**
  - **2 heures**
  - **Jusqu'à la déconnexion**

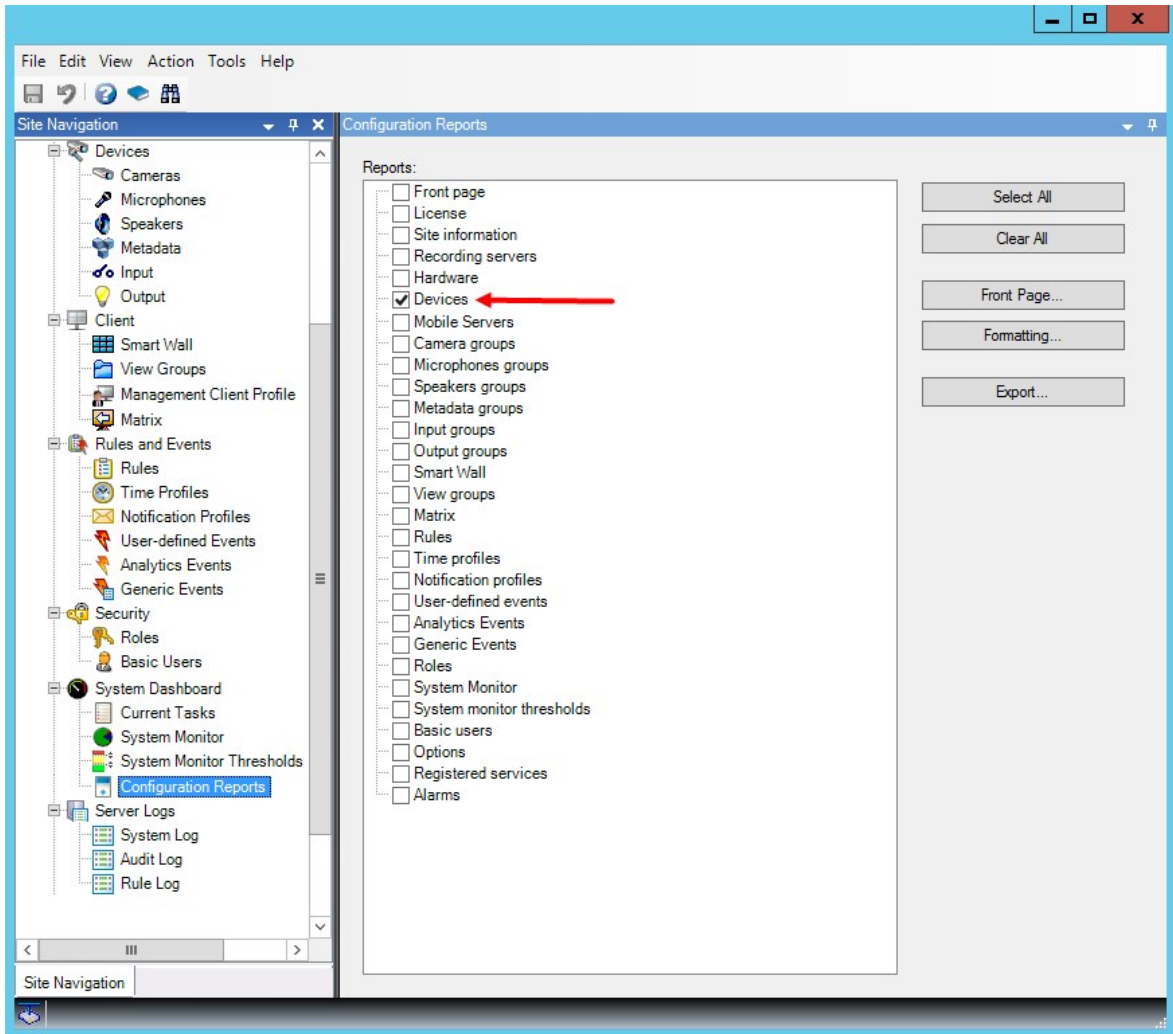
4. Cliquez sur **Enregistrer**.

#### [Créez un rapport de configuration de votre configuration du masquage de confidentialité](#)

Le rapport sur les périphériques comporte des informations relatives aux paramètres actuels de masquage de confidentialité de vos caméras.

Pour configurer un rapport :

1. Dans **Rapports de configuration**, sélectionnez le rapport **Périphériques**.



2. Si vous souhaitez modifier le rapport, vous pouvez modifier la page de couverture et la mise en forme.

3. Cliquez sur l'option **Exportation**, et le système crée le rapport au format de fichier PDF.

Pour obtenir de plus amples informations sur les rapports, voir Rapports de configuration(explications) sur la page 431.

**Onglet Masquage de confidentialité (propriétés)**

Nom	Description
Taille de la	La taille de grille sélectionnée détermine la densité de la grille, peut importe si cette

Nom	Description
<b>grille</b>	<p>dernière est visible ou non dans l'aperçu.</p> <p>Les valeurs disponibles sont 8×8, 16×16, 32×32 ou 64×64.</p>
<b>Effacer</b>	Supprime <b>tous</b> les masques de confidentialité que vous avez spécifiés.
<b>Afficher la grille</b>	Cochez la case <b>Afficher la grille</b> pour afficher le quadrillage.
<b>Afficher les masques de confidentialité</b>	<p>Lorsque vous cochez la case <b>Afficher les masques de confidentialité</b> (option par défaut), les masques de confidentialité permanents apparaissent en violet et les masques relevables en vert.</p> <p>Milestone vous recommande de laisser la case <b>Afficher les masques de confidentialité</b> sélectionnée afin que vos collègues et vous-même puissiez voir la configuration actuelle de la protection de confidentialité.</p>
<b>Taille du pinceau</b>	Utilisez le curseur de <b>taille du pinceau</b> afin d'indiquer la taille des sélections que vous souhaitez effectuer lorsque vous cliquez et déplacez la grille sur les zones sélectionnées. Par défaut, la taille est définie sur petite, ce qui équivaut à un carré de la grille.
<b>Masque permanent</b>	<p>Apparaît en violet dans l'aperçu sur cet onglet et sur l'onglet <b>Mouvement</b>.</p> <p>Les masques de confidentialité permanents sont toujours visibles dans XProtect Smart Client et ne peuvent pas être levés. Peuvent servir à couvrir les zones de la vidéo qui ne requièrent jamais de surveillance, comme les zones publiques où la surveillance n'est pas autorisée. La détection du mouvement est exclue des masques de confidentialité permanents.</p> <p>Vous indiquez la couverture des masques de confidentialité comme étant pleins ou comme ayant un certain niveau de flou. Les paramètres de couverture s'appliquent aussi bien à la vidéo en direct qu'à la vidéo enregistrée.</p>
<b>Masque amovible</b>	<p>Apparaît en ver dans l'aperçu sur cet onglet.</p> <p>Les masques de confidentialité peuvent être relevés dans XProtect Smart Client par des utilisateurs ayant des droits d'utilisateur suffisant. Par défaut, les masques de confidentialité sont levés pendant 30 minutes ou jusqu'à ce que l'utilisateur les applique à nouveau. N'oubliez pas que les masques de confidentialité sont relevés de toutes les caméras auxquelles l'utilisateur a accès.</p> <p>Si l'utilisateur de XProtect Smart Client n'a pas le droit de lever les masques de</p>

Nom	Description
	<p>confidentialité, le système demandera un utilisateur ayant le droit d'autoriser le levage.</p> <p>Vous indiquez la couverture des masques de confidentialité comme étant pleins ou comme ayant un niveau de flou. Les paramètres de couverture s'appliquent aussi bien à la vidéo en direct qu'à la vidéo enregistrée.</p>
<b>Flou</b>	<p>Sélectionnez le niveau de flou des masques de confidentialité dans les clients ou la couverture sur plein à l'aide du curseur.</p> <p>Par défaut, la couverture des zones ayant des masques de confidentialité permanents sont pleins (opaque). Par défaut, les masque de confidentialité relevables sont moyennement flous.</p> <p>Vous pouvez informer les utilisateurs du client au sujet de l'apparence des masques de confidentialité relevables et permanents afin qu'ils soient à mesure de les distinguer.</p>

## Navigation sur le site : Clients

Cet article décrit comment personnaliser l'interface utilisateur pour les opérateurs dans XProtect Smart Client et pour les administrateurs du système dans le Management Client.

### Clients (explications)

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

La section Client du Management Client est composée des éléments suivants :

Nom	Description
<b>XProtect Smart Wall</b>	<p>XProtect Smart Wall est un produit complémentaire qui vous permet de visualiser du contenu venant de XProtect Smart Client sur un mur vidéo dédié.</p> <p>Pour plus d'informations sur XProtect Smart Wall, voir XProtect Smart Wall (explications) sur la page 31.</p>
<b>Groupes de vues</b>	<p>La façon dont la vidéo des caméras s'affiche s'appelle une vue. Pour contrôler qui peut voir</p>

Nom	Description
	<p>quoi dans XProtect Smart Client, vous pouvez créer des groupes de vues pour grouper les vues en entités logiques. Vous pouvez assigner un accès à ces groupes de vues par le biais de rôles et ainsi limiter l'accès à certains groupes de vues à des rôles spécifiques. Sélectionnez <b>Groupes de vues</b> pour créer et travailler avec des groupes de vues pour répondre à vos besoins en matière de surveillance.</p>
<b>Profils Smart Client</b>	<p>Pour pouvoir différencier les utilisateurs XProtect Smart Client, vous pouvez créer des profils Smart Client, les rendre prioritaires et les personnaliser en fonction de vos besoins pour les différentes tâches à effectuer.</p>
<b>Profils Management Client</b>	<p>Pour pouvoir différencier les utilisateurs administrateurs Management Client, vous pouvez créer des profils Management Client, les rendre prioritaires et les personnaliser en fonction de vos besoins pour les différentes tâches à effectuer.</p>
<b>Matrix</b>	<p>Matrix est une fonctionnalité qui permet d'envoyer les vidéos à distance. Lorsque vous utilisez Matrix, vous pouvez déplacer la vidéo d'une caméra au choix sur le réseau de votre système vers un XProtect Smart Client en marche.</p>

## Navigation sur le site : Clients : En cours de configuration de Smart Wall

Cet article décrit comment configurer XProtect Smart Wall.

### Licences XProtect Smart Wall

XProtect Smart Wall nécessite les licences de mur vidéo suivantes :

- Une **licence de base** pour XProtect Smart Wall qui couvre un nombre infini de moniteurs affichant des vidéos sur un mur vidéo

Une licence de base pour XProtect Smart Wall est comprise dans la licence de base pour XProtect Corporate. Si vous avez XProtect Expert, vous pouvez acheter séparément une licence de base pour XProtect Smart Wall.

### Configurer les Smart Wall

Une configuration de Smart Wall consiste à définir le Smart Wall, en ajoutant des moniteurs et en définissant la disposition de l'écran et le cas échéant des préréglages Smart Wall et en spécifiant la disposition et le contenu des différents moniteurs.

Vous n'avez pas besoin de définir des préréglages Smart Wall, si vous voulez uniquement afficher les caméras et les vues XProtect Smart Client que vos utilisateurs XProtect Smart Client peuvent manuellement activer sur le mur vidéo.

Si vous souhaitez utiliser des règles pour changer automatiquement ce qui est affiché sur le mur vidéo, ou si vous avez des scénarios de surveillance typiques pour lesquels vous souhaitez afficher le même contenu sur le mur vidéo chaque fois que le scénario se produit, vous devez définir les préréglages Smart Wall.

La configuration de Smart Wall est très flexible. Vous pouvez inclure tous les moniteurs sur le mur vidéo dans un Smart Wall ou regrouper les moniteurs et configurer un Smart Wall pour chaque groupe. Les préréglages Smart Wall peuvent changer la disposition et le contenu de tous les moniteurs dans un Smart Wall ou seulement quelques-uns des moniteurs. Les moniteurs peuvent faire partie de plusieurs préréglages Smart Wall et Smart Walls. Créez autant de préréglages Smart Wall et Smart Walls que vous avez besoin pour optimiser la couverture de vos scénarios de surveillance classiques.

#### a. Définir le Smart Wall :

1. Développez **Client**, et sélectionnez **Smart Wall**.
2. Dans le panneau **Vue d'ensemble**, faites un clic droit sur **Smart Wall** et sélectionnez **Ajouter Smart Wall**.
3. Indiquez les paramètres relatifs au Smart Wall.
4. Dans les paramètres **Propriétés générales de l'élément de vue**, définissez si vous souhaitez que les informations d'état du système et les barres de titre apparaissent au-dessus des éléments de disposition des caméras.
5. Cliquez sur **OK**.

#### b. Ajouter des moniteurs et définir la disposition du moniteur :

1. Cliquez avec le bouton droit de la souris sur le Smart Wall et sélectionnez **Ajouter un moniteur**.
2. Configurez les dimensions du moniteur de sorte qu'il ressemble à l'un des moniteurs physiques sur le mur vidéo.
3. Utilisez les paramètres de comportement prédéfinis **Préréglage vide** et **Élément de préréglage vide** pour définir ce qui est affiché sur un moniteur avec une disposition de préréglage vide ou dans les éléments de préréglage vides d'un préréglage lorsqu'un nouveau préréglage de Smart Wall est déclenché automatiquement ou sélectionné manuellement dans XProtect Smart Client. Vous pouvez utiliser les préréglages vides et les éléments prédéfinis vides pour le contenu qui n'est pas contrôlé par le préréglage de Smart Wall.
4. Utilisez le paramètre de comportement prédéfini **Insertion d'éléments** pour définir ce qui doit se passer lorsqu'un utilisateur de XProtect Smart Client déplace une caméra sur un élément de disposition dans le préréglage Smart Wall. Sélectionnez **Indépendant** pour remplacer la caméra déjà placée dans l'élément prédéfini avec la nouvelle caméra ou **Lié** pour pousser le contenu des articles de disposition de gauche à droite depuis l'endroit où vous avez inséré la nouvelle caméra.

5. Ajoutez autant de moniteurs que vous pouvez sur le mur vidéo physique.
6. Sélectionnez le Smart Wall et sur l'onglet **Disposition**, cliquez sur **Modifier** pour positionner les différents moniteurs de sorte que leur position ressemble au montage des moniteurs physiques sur le mur vidéo.
7. Cliquez sur **OK**. La même disposition est utilisée dans XProtect Smart Client.

#### c. Ajouter des préréglages Smart Wall (facultatif) :

1. Sélectionnez le Smart Wall et depuis l'onglet **Préréglages** cliquez sur **Ajouter nouveau**.
2. Saisissez un nom et une description, puis cliquez sur **OK**.
3. Cliquez sur **Activer** pour afficher le préréglage Smart Wall sur le mur vidéo.
4. Créez autant de préréglages Smart Wall que vous avez besoin.

#### d. Ajouter une disposition et des caméras aux moniteurs (nécessite un préréglage de Smart Wall) :

1. Sélectionnez un des moniteurs que vous avez créé et à partir de l'onglet **Préréglages**, sélectionnez un préréglage dans la liste pour configurer ce que vous souhaitez que le moniteur sélectionné affiche lorsqu'il est utilisé avec le préréglage Smart Wall sélectionné.
2. Cliquez sur **Modifier**.
3. Cliquez sur le bouton de disposition pour sélectionner la disposition à utiliser avec votre moniteur, puis cliquez sur **OK**.



4. Faites glisser les caméras à partir des onglets **Groupes de périphériques**, **Serveurs d'enregistrement** ou **Hiérarchie des sites fédérés** sur les différents éléments de disposition. Les caméras sur l'onglet **Hiérarchie des sites fédérés** sont accessibles dans une configuration Milestone Federated Architecture. Vous pouvez laisser les éléments de disposition vierges pour qu'ils soient disponibles pour d'autres contenus non contrôlés par le préréglage Smart Wall.
5. Si le moniteur a déjà une disposition pour le préréglage sélectionné, vous pouvez cliquer sur **Effacer** pour définir une nouvelle disposition ou exclure le moniteur du préréglage Smart Wall, de sorte que le moniteur soit disponible pour tout autre contenu qui n'est pas contrôlé par le préréglage Smart Wall.
6. Cliquez sur **OK**.
7. Répétez les étapes, jusqu'à ce que vous ayez ajouté une disposition et des caméras sur les moniteurs que vous souhaitez inclure dans le préréglage Smart Wall.

## Configurer des droits d'utilisateur pour XProtect Smart Wall

Vous pouvez contrôler les tâches que les utilisateurs de XProtect Smart Client peuvent effectuer dans XProtect Smart Wall en spécifiant des droits d'utilisateurs pour les rôles. Les droits d'utilisateurs s'appliquent à tous les utilisateurs assignés à ce rôle. Pour plus d'informations sur les rôles avec les droits Smart Wall, voir Paramètres



des rôles sur la page 374.

Les sélections relatives aux droits d'utilisateurs **Lire**, **Modifier** et **Supprimer** sont toujours appliquées. Pour les droits d'utilisateur **Opérer** et **Lecture**, vous pouvez également accorder les droits d'utilisateur pour une période spécifique en sélectionnant un profil de temps. Par exemple, cette option est utile si vous souhaitez autoriser un utilisateur à modifier le contenu affiché sur un Smart Wall, mais uniquement au cours de ses heures de travail normales.

Afin de configurer des droits d'utilisateur pour un rôle, procédez comme suit :

1. Dans le panneau Navigation du site, développez **Sécurité** et sélectionnez **Rôles**.
2. Dans le volet **Rôles**, sélectionnez un rôle ou créez un nouveau rôle en effectuant un clic droit sur le volet et en sélectionnant **Ajouter le rôle**.
3. Dans la partie supérieure du panneau **Paramètres des rôles**, sélectionnez le Smart Wall.
4. Dans la partie inférieure du panneau Paramètres des rôles, cliquez sur l'onglet **Smart Wall** puis sélectionnez les droits d'utilisateurs à assigner.
  - **Lire** - Voir des Smart Walls dans les applications du client
  - **Modifier** - Modifier des Smart Walls dans les applications du client
  - **Supprimer** - Supprimer des Smart Walls dans les applications du client
  - **Opérer** - Appliquer des dispositions sur le moniteur sélectionné dans les applications du client et activer des préréglages
  - **Lecture** - Passer en revue et gérer des vidéos en direct et enregistrées



Si vous ne sélectionnez pas la permission **Lecture**, les utilisateurs peuvent voir le contenu affiché sur le mur vidéo mais ne peuvent pas le modifier. Si un utilisateur apporte une modification, le système se déconnecte automatiquement de l'état partagé et le contenu du mur vidéo n'est pas affecté. Pour revenir à la vue partagée, cliquez sur **Reconnecter le moniteur Smart Wall**.

5. Facultatif : Afin d'accorder les droits d'utilisateur **Opérer** ou **Lecture** pour une durée spécifique, cochez la case puis sélectionnez le profil de temps.

## Utilisation de règles avec des préréglages Smart Wall (explications)

En combinant les règles et les présélections Smart Wall, vous pouvez contrôler ce qui est affiché sur votre mur vidéo de la même manière que le système utilise des règles pour contrôler le comportement des caméras et autres. Par exemple, une règle peut déclencher votre mur vidéo pour afficher un certain préréglage Smart Wall pendant un certain jour. Vous pouvez même utiliser des règles pour contrôler quels sont les moniteurs individuels dans un écran du mur vidéo. Voir Règles sur la page 338 pour plus d'informations sur la façon de créer des règles.

Exemple d'une règle déclenchant un préréglage Smart Wall :

```
Perform an action in a time interval
day of week is Thursday
Set smart wall London to preset Factory
and Set smart wall London monitor UK Monitor 9 using current layout
to show Camera 1 starting in position 6
```

## Propriétés de Smart Wall

### Onglet Info (propriétés du Smart Wall)

Dans l'onglet **Info** pour un Smart Wall, vous pouvez ajouter et modifier Smart Walls.

Nom	Description
<b>Nom</b>	Le nom du Smart Wall. S'affiche dans XProtect Smart Client sous forme de nom du groupe de vues de Smart Wall.
<b>Description</b>	Une description du Smart Wall. Cette description est utilisée uniquement dans le cadre du Management Client.
<b>Texte d'état</b>	Si ce paramètre est sélectionné, les informations sur l'état de la caméra s'affichent sur les éléments de disposition des caméras sur le mur vidéo.
<b>Pas de barre de titre</b>	Si elle est sélectionnée, tous les éléments de disposition Smart Wall n'ont aucune barre de titre sur le mur vidéo.
<b>Barre de titre</b>	Si elle est sélectionnée, tous les éléments de disposition Smart Wall ont des barres de titre sur le mur vidéo.
<b>Barre de titre avec indicateur En direct</b>	Lorsqu'elle est sélectionnée, les barres de titre de tous les éléments de disposition Smart Wall présentent des indicateurs de mouvement et en direct sur le mur vidéo.

### Onglet Préréglages (propriétés du Smart Wall)

Dans l'onglet **Préréglages** pour un Smart Wall, vous pouvez ajouter et modifier les préréglages Smart Wall.

Nom	Description
<b>Ajouter nouveau</b>	Cliquez pour ajouter un préréglage à votre installation XProtect Smart Wall. Définissez un nom et une description pour le nouveau préréglage Smart Wall.
<b>Modifier</b>	Modifiez le nom et/ou la description d'un préréglage Smart Wall.
<b>Supprimer</b>	Supprimer un préréglage Smart Wall.
<b>Activer</b>	Cliquez pour afficher le préréglage Smart Wall sur le mur vidéo. Vous devez créer des règles avec le préréglage Smart Wall avant que le système ne puisse automatiquement déclencher l'affichage du préréglage Smart Wall. Voir aussi Utilisation de règles avec des préréglages Smart Wall (explications) sur la page 289.

### Onglet Disposition (propriétés du Smart Wall)

Dans l'onglet **Disposition** pour un Smart Wall, vous placez les moniteurs dans votre Smart Wall de sorte que leurs positions ressemblent au montage des moniteurs physiques sur le mur vidéo. La disposition est également utilisée dans le XProtect Smart Client.

Nom	Description
<b>Modifier</b>	Cliquez pour ajuster le positionnement des moniteurs.
<b>Déplacement</b>	Pour déplacer un moniteur vers une nouvelle position, sélectionnez le moniteur pertinent, puis faites-le glisser à la position désirée, ou cliquez sur les boutons flèches pour déplacer le moniteur dans la direction sélectionnée.
<b>Boutons de zoom</b>	Cliquez sur les boutons de zoom avant/arrière de l'aperçu de disposition Smart Wall pour vous assurer de positionner les moniteurs correctement.
<b>Nom</b>	Le nom du moniteur. Le nom s'affiche dans XProtect Smart Client.
<b>Taille</b>	La taille de l'écran physique sur le mur vidéo.
<b>Proportions</b>	Le rapport hauteur/largeur de l'écran physique sur le mur vidéo.

## Propriétés du moniteur

### Onglet Info (propriétés du moniteur)


Dans l'onglet **Infos** pour un moniteur dans un préréglage Smart Wall, vous pouvez ajouter des moniteurs et modifier les paramètres des moniteurs.

Nom	Description
<b>Nom</b>	Le nom du moniteur. Le nom s'affiche dans XProtect Smart Client.
<b>Description</b>	Une description de chaque moniteur. Cette description est utilisée uniquement dans le cadre du Management Client.
<b>Taille</b>	La taille de l'écran physique sur le mur vidéo.
<b>Proportions</b>	Le rapport hauteur/largeur de l'écran physique sur le mur vidéo.
<b>Préréglage vide</b>	Définit ce qui doit être affiché sur un moniteur avec une disposition de préréglage vide quand un nouveau préréglage Smart Wall est déclenché ou sélectionné dans XProtect Smart Client. Sélectionnez <b>Conserver</b> pour garder le contenu actuel de l'écran. Sélectionnez <b>Effacer</b> pour effacer tout le contenu si rien ne s'affiche sur le moniteur.
<b>Élément de préréglage vide</b>	Définit ce qui doit être affiché dans un élément de disposition de préréglage vide quand un nouveau préréglage Smart Wall est déclenché ou sélectionné dans XProtect Smart Client. Sélectionnez <b>Conserver</b> pour garder le contenu actuel dans l'élément de disposition. Sélectionnez <b>Effacer</b> pour effacer le contenu afin que rien ne s'affiche dans l'élément de disposition.
<b>Insertion d'éléments</b>	Définit la façon dont les caméras sont insérées dans la disposition du moniteur lorsqu'il est affiché dans XProtect Smart Client. En sélectionnant <b>Indépendant</b> , seul le contenu de la disposition des éléments concernés change, le reste du contenu de la disposition reste le même. En sélectionnant <b>Lié</b> , les contenus des éléments de disposition sont poussés de gauche à droite. Si, par exemple, une caméra est insérée en position 1, la caméra précédente de la position 1 est poussée à la position 2, la caméra précédente de la position 2 est poussée à la position 3, et ainsi de suite comme illustré dans cet exemple.

Nom	Description

### Onglet Positions prédéfinies (propriétés du moniteur)

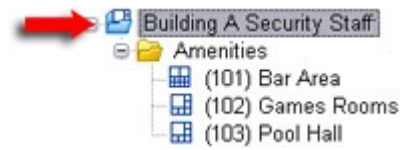
Dans l'onglet **Préréglages** pour un moniteur dans un préréglage Smart Wall, vous pouvez modifier la disposition et le contenu du moniteur dans le préréglage Smart Wall sélectionné.

Nom	Description
<b>Préposition</b>	Une liste de préréglages Smart Wall pour la Smart Wall sélection.
<b>Modifier</b>	<p>Cliquez sur <b>Modifier</b> pour modifier la disposition et le contenu de l'écran sélectionné.</p> <p>Double-cliquez sur une caméra pour supprimer une seule caméra.</p> <p>Cliquez sur <b>Effacer</b> pour définir une nouvelle disposition ou exclure le moniteur dans le préréglage Smart Wall afin que le moniteur soit disponible pour tout autre contenu qui n'est pas contrôlé par le préréglage Smart Wall.</p> <p>Cliquez sur  pour sélectionner la disposition que vous souhaitez utiliser avec votre moniteur dans le préréglage sélectionné, puis cliquez sur <b>OK</b>.</p> <p>Faites glisser les caméras à partir des <b>Groupes de périphériques, Serveurs d'enregistrement</b> ou <b>Sites fédérés</b> sur les différents éléments de disposition. Vous pouvez laisser les éléments de disposition vides, afin qu'ils soient disponibles pour d'autres contenus non contrôlés par le préréglage Smart Wall.</p>

## Navigation sur le site : Clients : Groupes de vues

La façon dont le système présente les vidéos d'une ou plusieurs caméras dans les clients est appelée « vue ». Un groupe de vues est un conteneur d'un ou de plusieurs groupes logiques de telles vues. Dans les clients, un groupe de vues se présente comme un fichier extensible à partir duquel les utilisateurs peuvent sélectionner le groupe

et la vue qu'ils souhaitent afficher :



Exemple de XProtect Smart Client : La flèche indique un groupe de vues, qui contient un groupe logique (appelé Amenities), qui à son tour contient 3 vues.

## Groupes de vues et rôles (explications)

Par défaut, chaque rôle que vous définissez dans le Management Client est également créé comme un groupe de vues. Lorsque vous ajoutez un rôle dans le Management Client, le rôle s'affiche par défaut comme un groupe de vues dans les clients.

- Vous pouvez assigner un groupe de vues en fonction d'un rôle à des utilisateurs/groupes possédant le rôle en question. Vous pouvez changer les droits du groupe de vues en configurant le rôle ultérieurement
- Un groupe de vues basé sur un rôle prend le nom de ce rôle.

**Exemple :** Si vous créez un rôle avec le nom **Personnel de sécurité Immeuble A**, par défaut, il apparaît dans XProtect Smart Client tant que groupe de vues intitulé **Personnel de sécurité Immeuble A**.

En complément des groupes de vues obtenus lorsque vous ajoutez des rôles, vous pouvez en créer autant que vous le souhaitez. Vous pouvez également supprimer des groupes de vues, y compris ceux qui sont automatiquement créés lorsque des rôles sont ajoutés

- Même si un groupe de vues est créé à chaque fois que vous ajoutez un rôle, les groupes de vues ne doivent pas nécessairement correspondre aux rôles. Vous pouvez ajouter, renommer ou supprimer chacun de vos groupes de vues si nécessaire



Si vous renommez un groupe de vues, les utilisateurs des clients déjà connectés doivent se déconnecter et se reconnecter avant que le changement de nom soit visible.

## Ajouter un groupe de vues

1. Faites un clic droit dans **Groupes de vues**, puis sélectionnez **Ajouter groupe de vues**. La boîte de dialogue **Ajouter groupe de vues** s'ouvre.
2. Saisissez le nom et une description facultative du nouveau groupe de vues, puis cliquez sur **OK**.



Aucun rôle n'a le droit d'utiliser le groupe de vues nouvellement ajouté tant que ces droits n'ont pas été précisés. Si vous avez précisé les rôles qui doivent être capables d'utiliser le groupe de vues nouvellement ajouté, les utilisateurs clients déjà connectés avec les rôles pertinents doivent se déconnecter et se reconnecter avant de pouvoir voir le groupe de vues.

## Navigation sur le site : Clients : Profils Smart Client



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

Les profils Smart Client permettent aux administrateurs système de contrôler l'apparence et le comportement de XProtect Smart Client, ainsi que les fonctionnalités et panneaux auxquels les utilisateurs XProtect Smart Client ont accès. Vous pouvez configurer les droits de l'utilisateur pour : les volets et les options, les options de réduction/agrandissement, le contrôle de la durée d'inactivité, le rappel d'un mot de passe ou non, la vue affichée après la connexion, la mise en page de rapports d'impression, le chemin d'exportation, et beaucoup d'autres choses encore.

Pour gérer les profils Smart Client dans le système, développez **Client**, puis sélectionnez **Profils Smart Client**. Vous pouvez également en savoir plus sur la relation entre les profils Smart Client, les rôles et les profils de temps, ainsi que sur la manière de les utiliser ensemble (voir Créer et configurer des profils Smart Client, rôles et profils de temps sur la page 296).

### Ajouter et configurer un profil Smart Client

Vous devez créer un profil Smart Client avant de pouvoir le configurer.

1. Faites un clic droit sur **Profils Smart Client**.
2. Sélectionnez **Ajouter profil Smart Client**.
3. Dans la fenêtre de dialogue **Ajouter profil Smart Client**, saisissez le nom et la description du nouveau profil, puis cliquez sur **OK**.
4. Dans le volet **Vue d'ensemble**, cliquez sur le profil que vous venez tout juste de créer pour le configurer.
5. Ajustez les paramètres sur l'un ou plusieurs, voire tous les onglets disponibles, et cliquez sur **OK**.

### Copier un profil Smart Client

Si vous possédez un profil Smart Client avec des paramètres ou des droits compliqués et avez besoin d'un profil semblable, il peut s'avérer plus simple de copier un profil déjà existant et d'apporter des petits ajustements à la copie plutôt que de créer un tout nouveau profil.

1. Cliquez sur **Profils Smart Client**, faites un clic droit sur le profil dans le panneau **Vue d'ensemble**, sélectionnez **Copier profil Smart Client**.
2. Dans la boîte de dialogue qui s'ouvre, donnez au profil copié un nouveau nom et une description uniques. Cliquez sur **OK**.
3. Dans le volet **Vue d'ensemble**, cliquez sur le profil que vous venez tout juste de créer pour le configurer. Cela est effectué en ajustant les paramètres sur l'un, plusieurs voire tous les onglets disponibles. Cliquez sur **OK**.

## Créer et configurer des profils Smart Client, rôles et profils de temps

Lors de l'utilisation de profils Smart Client, il est important de comprendre l'interaction entre profils Smart Client, rôles et profils de temps :

- Smart Client Les profils concernent les paramètres des droits d'utilisateur dans XProtect Smart Client
- Les rôles concernent les paramètres de sécurité dans les clients, MIP SDK et bien plus encore
- Les profils de temps gèrent les aspects temporels des deux types-profils.

Ces trois fonctionnalité ensemble, assurent un contrôle et des possibilité de personnalisation uniques par rapport aux droits de l'utilisateur XProtect Smart Client.

**Exemple** : Vous avez besoin d'un utilisateur dans votre configuration XProtect Smart Client qui doit uniquement être autorisé à voir la vidéo en direct (pas de lecture) de caméras choisies, et seulement durant les heures ouvrées normales (8 h à 16 h). Une manière de configurer pourrait être comme suit :

1. Créez un profil Smart Client et donnez-lui un nom, par exemple **En direct uniquement**.
2. Précisez les paramètres de lecture/direct nécessaires sur **Direct uniquement**.
3. Créez un profil de temps et donnez-lui un nom, par exemple **Journée uniquement**.
4. Indiquez la période de temps nécessaire sur **Journée uniquement**.
5. Créez un nouveau rôle et donnez-lui un nom, par exemple **Gardien (caméras sélectionnées)**.
6. Précisez les caméras utilisées par le **Gardien (caméras sélectionnées)**.
7. Attribuez le profil **En direct uniquement** Smart Client et le profil de temps **Journée uniquement** au rôle **Gardien (caméras sélectionnées)** pour connecter les trois éléments.

Vous disposez désormais d'une combinaison de trois fonctions créant le résultat souhaité et vous donnant la possibilité d'apporter des ajustements et de procéder à des réglages de précision. Vous pouvez effectuer la configuration dans un ordre différent, par exemple, en créant d'abord le rôle, puis le profil Smart Client et ensuite le profil de temps, ou dans un ordre différent.



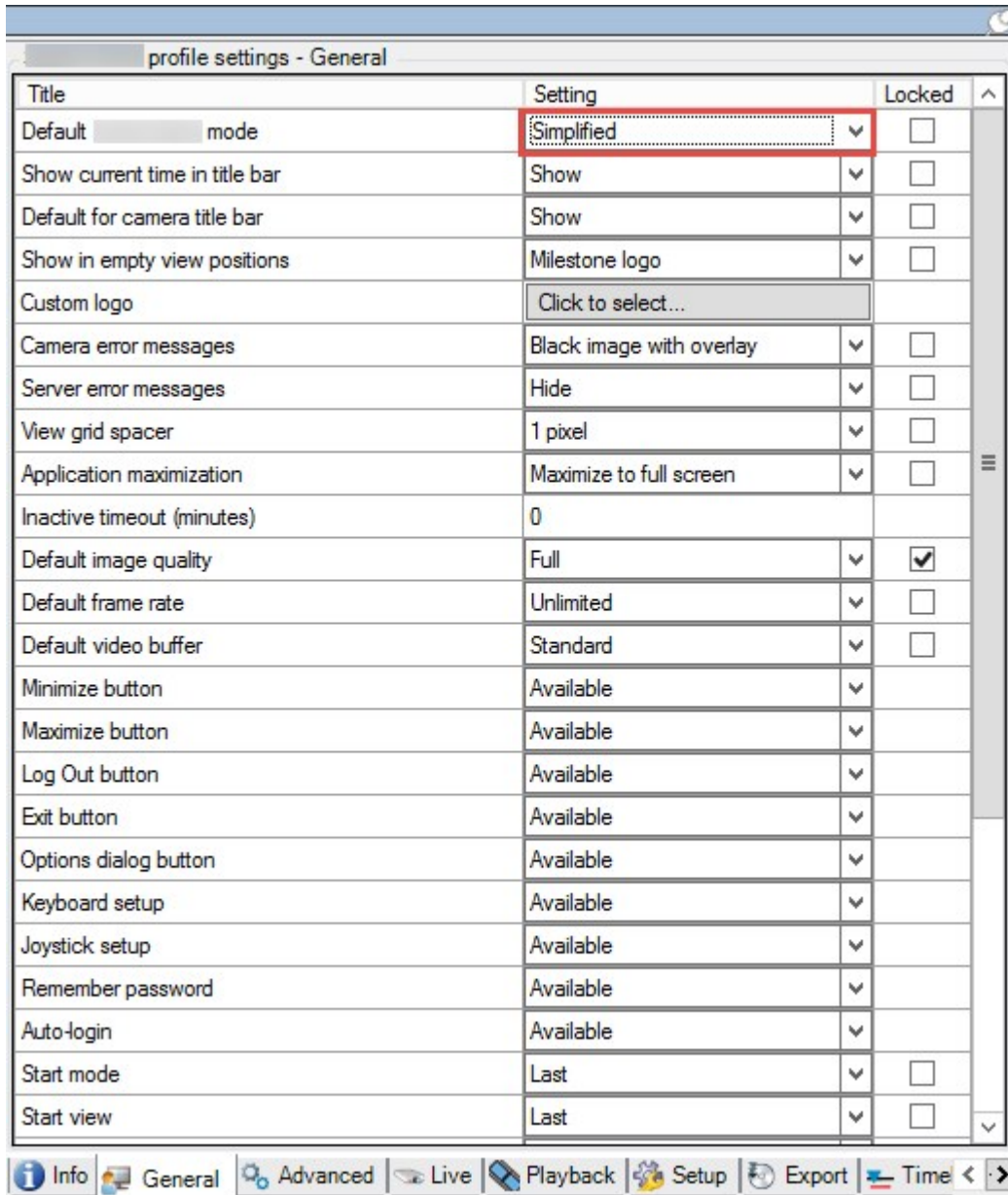
## Définir le mode simplifié comme le mode par défaut

Par l'intermédiaire des profils Smart Client, vous pouvez configurer votre système pour qu'il ouvre automatiquement XProtect Smart Client en mode simplifié avec un ensemble limitée de fonctionnalités et d'onglets. Par défaut, XProtect Smart Client s'ouvre en mode avancé avec l'ensemble complet de fonctionnalités et d'onglets.



Si l'opérateur XProtect Smart Client décide de passer à un mode différent que le mode par défaut, XProtect Smart Client se souviendra de ce paramètre la prochaine fois que l'opérateur ouvrira le programme.

1. Dans Management Client, développez le nœud **Client**.
2. Sélectionnez le profil Smart Client pertinent.
3. Cliquez sur l'onglet **Général**.

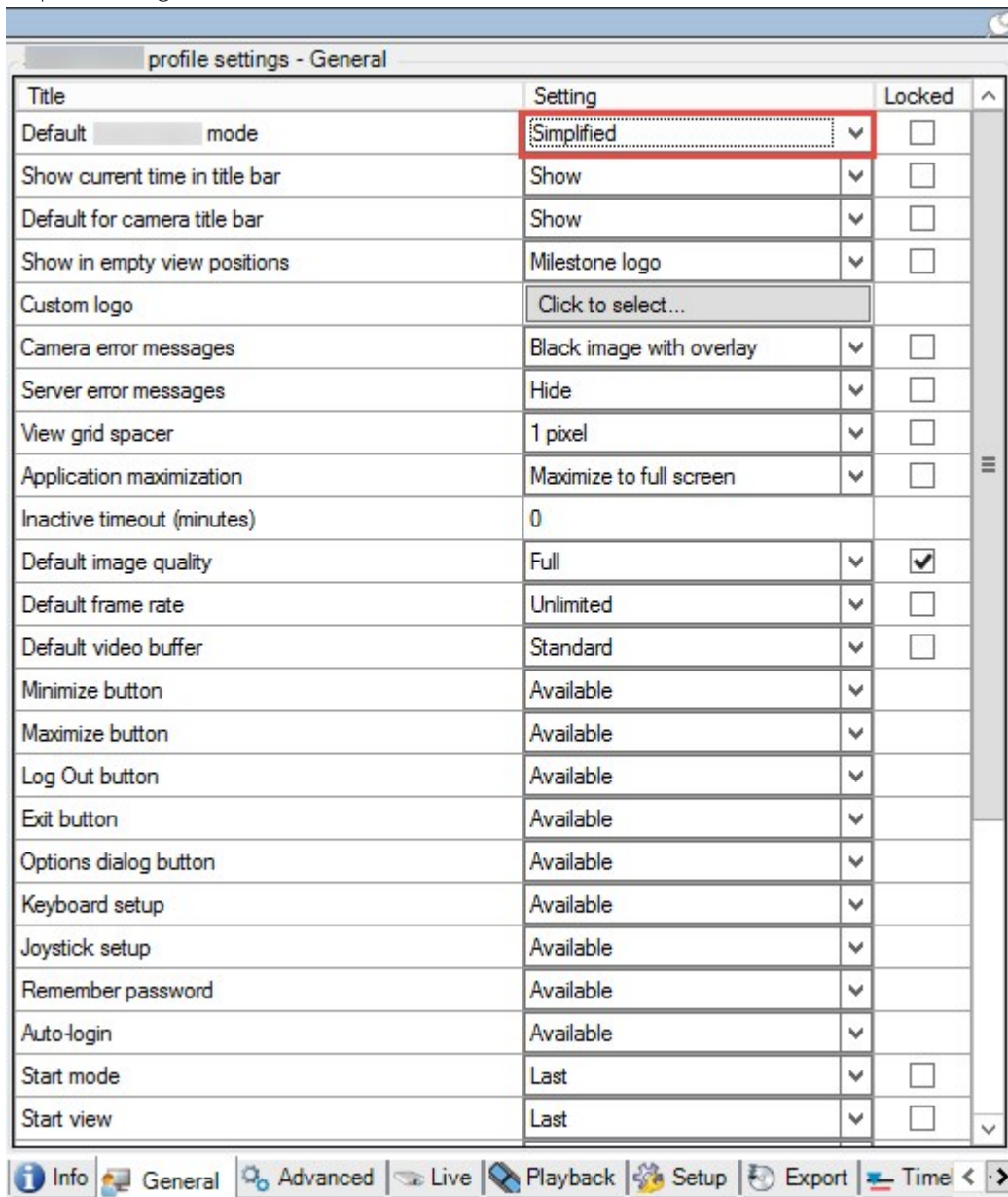


4. Dans la liste **Mode Smart Client par défaut**, sélectionnez **Simplifié**. XProtect Smart Client s'ouvre à présent en mode simplifié pour les utilisateurs associés au profil Smart Client actuel.

## Empêcher des opérateurs de permuter entre mode simple et avancé

Dans XProtect Smart Client, les opérateurs peuvent permuter entre le mode simple et le mode avancé. Toutefois, vous pouvez empêcher les opérateurs XProtect Smart Client de permuter entre les deux modes. Techniquement, vous devez verrouiller les paramètres déterminant si XProtect Smart Client s'ouvre en mode simple ou avancé.

1. Dans Management Client, développez le nœud **Client**.
2. Sélectionnez le profil Smart Client pertinent.
3. Cliquez sur l'onglet **Général**.



4. Vérifiez que la liste Mode **par défaut Smart Client** a la valeur appropriée. Si **Activé**, XProtect Smart Client s'ouvre en mode simple.
5. Cochez la case **Verrouillé**. Le bouton Changer de mode dans XProtect Smart Client est masqué.



Voir également Définir le mode simplifié comme le mode par défaut sur la page 297.

## Propriétés du profil Smart Client

Les onglets suivants vous permettent de spécifier les propriétés de chaque profil Smart Client. Vous pouvez verrouiller les paramètres dans le Management Client le cas échéant, de façon à ce que les utilisateurs de XProtect Smart Client ne puissent pas les modifier.

### Onglet Info (profils Smart Client)


Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
<b>Info</b>	<p>Le nom et la description, la priorité de modification des profils existants et un aperçu des rôles utilisés avec quel profil.</p> <p>Si un utilisateur est membre de plus d'un rôle, chacun avec leur profil Smart Client individuel, l'utilisateur a le profil Smart Client au niveau de priorité le plus élevé.</p>

### Onglet Général (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
<b>Généralités</b>	<p>Paramètres tels que afficher/masquer et minimiser et maximiser les paramètres des menus, connecter/déconnecter, démarrer, période d'inactivité, infos et options de messagerie et activer ou désactiver certains onglets dans XProtect Smart Client.</p>

Onglet	Description
	<div style="background-color: #f9e79f; padding: 10px; border: 1px solid #ccc;">  <p>Si vous <b>masquez</b> les messages d'erreur de la caméra, l'opérateur risque de ne pas voir que la connexion à une caméra a été perdue.</p> </div> <p>Le paramètre de l'<b>Aide en ligne</b> vous permet de désactiver le système d'aide dans XProtect Smart Client.</p> <p>Le paramètre des <b>Tutoriels vidéo</b> vous permettent de désactiver le bouton <b>Tutoriels vidéo</b> dans XProtect Smart Client. Le bouton redirige les opérateurs vers la page des tutoriels vidéo : <a href="https://www.milestonesys.com/support/help-yourself/video-tutorials/">https://www.milestonesys.com/support/help-yourself/video-tutorials/</a></p>

### Onglet Avancé (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
<b>Avancés</b>	<p>Paramètres avancés tels que ceux des fils de décodage maximum, du désentrelacement et des fuseaux horaires.</p> <p><b>Fils de décodage maximum</b> détermine combien de fils de décodage sont utilisés pour décoder les flux vidéo. Cela peut participer à améliorer la performance sur des ordinateurs multicœurs aussi bien en mode direct qu'en mode de lecture. L'amélioration exacte de la performance dépend du flux vidéo. Cela est surtout pertinent lors de l'emploi de flux vidéo haute résolution lourdement codés tels que H.264/H.265, pour lesquels le potentiel d'amélioration de la performance peut être significatif et moins pertinent lors de l'utilisation, par exemple, de JPEG ou MPEG-4.</p> <p>Avec le <b>désentrelacement</b>, vous convertissez la vidéo en format non entrelacé. L'entrelacement détermine la manière dont une image est rafraîchie à l'écran. L'image est rafraîchie tout d'abord en analysant les lignes irrégulières de l'image puis les lignes régulières. Cela permet de disposer d'un taux de rafraîchissement plus rapide, car il y a moins d'informations à traiter à chaque analyse. Toutefois, l'entrelacement peut causer des fluctuations ou les changements dans la moitié des lignes de l'image peuvent être remarqués.</p>

Onglet	Description
	Le <b>flux adaptatif</b> permet à XProtect Smart Client de sélectionner automatiquement les flux vidéo en direct avec la meilleure correspondance de résolution pour les flux requis par l'élément de vue. Cela diminue la charge sur le CPU et le GPU et améliore donc la capacité et la performance de décodage de l'ordinateur. Cela requiert la multidiffusion des flux vidéo en direct avec différentes résolutions à configurer, voir Onglet Flux (périphériques) sur la page 234.

### Onglet En direct (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
<b>En direct</b>	Disponibilité des panneaux/onglets en direct, des boutons de recouvrement et de lecture de la caméra, des cadres de sélection et des modules d'extension MIP associés au direct.

### Onglet Relecture (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
<b>Lecture</b>	Disponibilité des onglets/volets de relecture, de l'agencement des rapports d'impression, de la relecture indépendante, des signets, des cadres de sélection et des modules d'extension MIP associés à la lecture.

### Onglet Configuration (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
<b>Configuration</b>	Disponibilité de la configuration générale/des volets/boutons, du module d'extension MIP associé à la configuration et des droits de modification d'une carte et de la modification de la zone tampon de vidéo en direct.

### Onglet Exportations (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
<b>Exports</b>	Les chemins d'accès, les masques de confidentialité, les formats d'images fixes et de vidéos et ce qu'il faut inclure lors de leur exportation, les formats d'exportation pour XProtect Smart Client – Player et bien plus encore.

### Onglet Chronologie (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
<b>Chronologie</b>	S'il faut inclure l'audio ou non, la visibilité de l'indication de l'heure et du mouvement et enfin, comment traiter les écarts de lecture.  Vous pouvez également indiquer s'il faut afficher des données ou marqueurs supplémentaires à partir d'autres sources.


### Onglet Contrôle d'accès (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
<b>Contrôle d'accès</b>	Sélectionnez si les notifications de demande d'accès doivent apparaître sur l'écran XProtect Smart Client quand elles sont déclenchées par des événements.

### Onglet Gestionnaire d'alarme (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
<b>Gestionnaire d'alarme</b>	<p>Spécifiez si les notifications sur le bureau liées aux alarmes doivent s'afficher sur les ordinateurs où XProtect Smart Client est installé. Les notifications apparaîtront uniquement si XProtect Smart Client est en cours d'exécution, même s'il est minimisé.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;"> <p> Les notifications sur le bureau liées aux alarmes n'apparaissent que lorsque les alarmes ont une certaine priorité, <b>Moyenne</b> ou <b>Haute</b>, par exemple. Pour configurer quelles priorités d'alarme déclenchent les notifications, rendez-vous dans <b>Alarmes &gt; Paramètres des données de l'alarme &gt; Niveaux des données de l'alarme</b>. Pour chaque priorité d'alarme requise, cochez la case <b>Activer les notifications sur le bureau</b>. Voir Paramètres des données de l'alarme sur la page 445.</p> </div>

### Onglet Smart Map (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

Onglet	Description
<b>Smart Map</b>	Spécifier des paramètres pour la fonctionnalité smart map.



Onglet	Description
	<p>Vous pouvez indiquer si OpenStreetMaps peut être disponible en tant qu'arrière-plan géographique, et si XProtect Smart Client crée automatiquement des localisations lorsqu'un utilisateur ajoute une superposition personnalisée sur la smart map.</p> <p>Vous pouvez également préciser à quelle fréquence vous voulez que le système supprime les données relatives aux smart maps sur votre ordinateur. Pour aider XProtect Smart Client à afficher smart map plus rapidement, le client enregistre les données du plan dans le cache de votre ordinateur. Avec le temps ceci pourrait ralentir votre ordinateur.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #add8e6;">  Le cache ne s'applique pas pour Google Maps. </div> <p>Si vous souhaitez utiliser Bing Maps ou Google Maps en tant qu'arrière-plan géographique, saisissez une clé Bing Maps API key ou une clé Maps Static API de Google.</p>

#### Onglet Disposition des vues (profils Smart Client)

Cet onglet vous permet d'indiquer les propriétés suivantes :

## Navigation sur le site : Clients : Profils Management Client



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

Les profils Management Client permettent aux administrateurs de systèmes de modifier l'interface utilisateur Management Client pour d'autres utilisateurs. Associez des profils Management Client à des rôles pour limiter l'interface utilisateur afin de représenter les fonctions disponibles pour chaque rôle d'administrateur.

Pour associer un rôle à un profil Management Client, consultez l'onglet **Info** dans les **Paramètres de rôles**. Voir également Onglet Info (rôles) sur la page 374. Les profils Management Client ne traitent que la représentation visuelle des fonctions du système, et non l'accès à celles-ci. Pour limiter l'accès global d'un rôle aux fonctions du système, consultez l'onglet **Sécurité globale**. Voir également Onglet Sécurité globale (rôles) sur la page 377.



Management Server Il est important que tous les rôles activent le niveau de sécurité **Se connecter** situé dans **Paramètres des rôles > Management Server > Paramètres des rôles** sur la page 374.

Vous pouvez modifier les paramètres relatifs à la visibilité de tous les éléments Management Client. Par défaut, le profil Management Client peut voir toutes les fonctions du Management Client.

- Pour limiter la visibilité d'une fonction, décochez les cases correspondant à la fonction pertinente afin de supprimer la représentation visuelle de la fonction dans le Management Client pour tout utilisateur de Management Client ayant un rôle associé à ce profil Management Client



Outre le rôle intégré d'administrateur, seuls les utilisateurs associés à un rôle bénéficiant des permissions **Gérer la sécurité** pour le serveur de gestion dans l'onglet **Sécurité globale**, peuvent ajouter, modifier et supprimer des profils Management Client.

## Ajouter et configurer un profil Management Client

Si vous ne souhaitez pas utiliser le profil par défaut, vous pouvez créer un profil Management Client avant de pouvoir le configurer.

1. Faites un clic droit sur **Profils Management Client**.
2. Sélectionnez **Ajouter profil Management Client**.
3. Dans la fenêtre de dialogue **Ajouter profil Management Client**, saisissez le nom et la description du nouveau profil, puis cliquez sur **OK**.
4. Dans le volet **Vue d'ensemble**, cliquez sur le profil que vous venez tout juste de créer pour le configurer.
5. Dans l'onglet **Profil**, sélectionnez ou effacez la fonction du profil Management Client.

## Copier un profil Management Client

Si vous possédez un profil Management Client avec des paramètres ou des droits compliqués et avez besoin d'un profil semblable, il peut s'avérer plus simple de copier un profil déjà existant et d'apporter des petits ajustements à la copie plutôt que de créer un tout nouveau profil.

1. Cliquez sur **Profil Management Client**, faites un clic droit sur le profil dans le panneau **Vue d'ensemble**, sélectionnez **Copier profil Management Client**.
2. Dans la boîte de dialogue qui s'ouvre, donnez au profil copié un nouveau nom et une description uniques. Cliquez sur **OK**.
3. Dans le volet **Vue d'ensemble**, cliquez sur le profil et allez dans l'onglet **Info** ou dans l'onglet **Profil** pour configurer le profil.

## Propriétés du profil Management Client

### Info tab (Onglet Info (Profils Management Client))

Dans l'onglet **Info**, vous pouvez configurer les éléments suivants pour les profils Management Client :

Composant	Exigences
<b>Nom</b>	Saisissez un nom pour le profil Management Client.
<b>Priorité</b>	Utilisez les flèches haut et bas pour accorder une priorité au profil Management Client.
<b>Description</b>	Saisissez une description pour le profil. Cette option est facultative.
<b>Rôles utilisant le profil Management Client</b>	Ce champ affiche les rôles que vous avez associés au profil Management Client. Vous ne pouvez pas modifier ce champ.

### Onglet Profil (Profils Management Client)



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

Dans l'onglet **Profil**, vous pouvez activer ou désactiver la visibilité des éléments suivants à partir de l'interface utilisateur Management Client :

#### Navigation

Dans cette rubrique, décidez si un utilisateur administrateur associé au profil Management Client est autorisé à voir les diverses fonctions et fonctionnalités situées dans le panneau **Navigation**.

Élément de navigation	Description
<b>Bases</b>	Permet à l'utilisateur administrateur associé au profil Management Client de voir les <b>Informations sur les licences</b> et les <b>Informations sur le site</b> .
<b>Services de connexion à</b>	Permet à l'utilisateur administrateur associé au profil Management Client de voir la <b>Connexion à la Caméra Axis One-click</b> .

Élément de navigation	Description
distance	
Serveurs	Permet à l'utilisateur administrateur associé au profil Management Client de voir les <b>Serveurs d'enregistrement</b> et les <b>Serveurs de basculement</b> .
Périphériques	Permet à l'utilisateur administrateur associé au profil Management Client de voir les <b>Caméras, Microphones, Haut-parleurs, Métadonnées, Entrée</b> et <b>Sortie</b> .
Client	Permet à l'utilisateur administrateur associé au profil Management Client de voir les <b>Smart Wall, Groupes de vues, Profils Smart Client, Profils Management Client</b> et <b>Matrix</b> .
Règles et événements	Permet à l'utilisateur administrateur associé au profil Management Client de voir les <b>Règles, Profils de temps, Profils de notification, Événements définis par les utilisateurs, Événements analytiques</b> et <b>Événements génériques</b> .
Sécurité	Permet à l'utilisateur administrateur associé au profil Management Client de voir les <b>Rôles</b> et les <b>Utilisateurs basiques</b> .
Tableau de bord système	Permet à l'utilisateur administrateur associé au profil Management Client de voir le <b>Moniteur système</b> , les <b>Seuils du moniteur système</b> , la <b>Protection des preuves</b> , les <b>Tâches en cours</b> et les <b>Rapports de configuration</b> .
Journaux des serveurs	Permet à l'utilisateur administrateur associé au profil Management Client de voir le Journal système, le Journal d'audit, ainsi que le Journal déclenché par les règles.
Contrôle d'accès	Permet à l'utilisateur administrateur associé au profil Management Client de voir les fonctionnalités de <b>Contrôle d'accès</b> , si vous avez ajouté des modules d'intégration ou d'extension au système de contrôle d'accès dans votre système.

## Détails

Dans cette rubrique, décidez si un utilisateur administrateur associé au profil Management Client est autorisé à voir les divers onglets correspondant à un canal des périphériques spécifique, comme par exemple l'onglet **Paramètres** ou l'onglet **Enregistrement** pour les caméras.

Canal du périphérique	Description
<b>Caméras</b>	Permet à l'utilisateur administrateur associé au profil Management Client de voir une partie ou l'intégralité des paramètres et onglets associés aux caméras.
<b>Microphones</b>	Permet à l'utilisateur administrateur associé au profil Management Client de voir une partie ou l'intégralité des paramètres et onglets associés aux microphones.
<b>Haut-parleurs</b>	Permet à l'utilisateur administrateur associé au profil Management Client de voir une partie ou l'intégralité des paramètres et onglets associés aux haut-parleurs.
<b>Métadonnées</b>	Permet à l'utilisateur administrateur associé au profil Management Client de voir une partie ou l'intégralité des paramètres et onglets associés aux métadonnées.
<b>Entrées</b>	Permet à l'utilisateur administrateur associé au profil Management Client de voir une partie ou l'intégralité des paramètres et onglets associés aux entrées.
<b>Sortie</b>	Permet à l'utilisateur administrateur associé au profil Management Client de voir une partie ou l'intégralité des paramètres et onglets associés aux sorties.

### Menu Outils

Dans cette rubrique, décidez si un utilisateur administrateur associé au profil Management Client est autorisé à voir les éléments faisant partie du menu **Outils**.

Option de menu Outil	Description
<b>Services enregistrés</b>	Permet à l'utilisateur administrateur associé au profil Management Client de voir les <b>Services enregistrés</b> .
<b>Rôles effectifs</b>	Permet à l'utilisateur administrateur associé au profil Management Client de voir les <b>Rôles effectifs</b> .
<b>Options</b>	Permet à l'utilisateur administrateur associé au profil Management Client de voir les <b>Options</b> .

## Sites fédérés

Dans cette rubrique, décidez si un utilisateur administrateur associé au profil Management Client est autorisé à voir le panneau de **Hiérarchie des sites fédérés**.

## Navigation sur le site : Clients : En cours de configuration de Matrix

Avec Matrix, vous pouvez envoyer une vidéo d'une caméra au choix sur un réseau opérant votre système aux destinataires Matrix. Un destinataire Matrix est un ordinateur capable d'afficher une vidéo déclenchée par Matrix. Il existe deux types de destinataires Matrix :

- ordinateurs exécutant une application Matrix dédiée
- ordinateurs exécutant XProtect Smart Client

Afin de consulter la liste des destinataires Matrix configurés dans le Management Client, développez **Client** dans le volet **Navigation sur le site**, puis sélectionnez **Matrix**. Une liste des configurations Matrix est affichée dans le volet **Propriétés**.



Chaque destinataire Matrix, qu'il s'agisse d'un ordinateur avec Matrix Monitor ou XProtect Smart Client, doit être configuré en vue de recevoir la vidéo déclenchée Matrix. Pour plus d'informations, voir XProtect Smart Wall (explications) sur la page 31 et XProtect Smart Client (explications) sur la page 26.

## Ajouter des destinataires Matrix

Pour ajouter un destinataire Matrix existant, par exemple une installation Matrix Monitor ou XProtect Smart Client existante, par le biais de Management Client :

1. Agrandissez **Clients**, puis sélectionnez **Matrix**.
2. Faites un clic droit sur **Matrix Configurations** et sélectionnez **Ajouter Matrix**.
3. Remplissez les champs de la boîte de dialogue **Ajouter Matrix**.
  1. Dans le champ **Adresse**, saisissez l'adresse IP ou le nom d'hôte du destinataire Matrix souhaité.
  2. Dans le champ **Port**, saisissez le numéro du port employé par l'installation du destinataire Matrix. Vous trouverez le numéro du port et le mot de passe de la façon suivante : Dans le cas d'une application Matrix Monitor, allez dans la boîte de dialogue Matrix Monitor **Configuration**. Pour XProtect Smart Client, le [manuel de l'utilisateur pour XProtect Smart Client](#).
4. Cliquez sur **OK**.

Vous pouvez maintenant utiliser le destinataire Matrix dans les règles.



Votre système ne vérifie pas si le numéro de port ou le mot de passe fourni est correct ou si le numéro de port, mot de passe ou type précisé correspond au destinataire Matrix réel. Veuillez à saisir les informations correctes.

## Définir les règles d'envoi de vidéos aux destinataires Matrix

Pour envoyer une vidéo aux destinataires Matrix vous devez inclure le destinataire Matrix dans une règle qui déclenche la transmission vidéo au destinataire Matrix associé. Pour cela :

1. Dans le volet **Navigation du site**, agrandissez **Règles et événements** > **Règles**. Faites un clic droit sur **Règles** pour ouvrir l'assistant **Gérer la règle**. Dans la première étape, sélectionnez un type de règle et dans la deuxième étape, une condition.
2. Dans l'étape 3 de **Gérer la règle (Étape 3 : Actions)**, sélectionnez **Configurer Matrix pour consulter l'action <périphériques>**.
3. Cliquez sur le lien Matrix dans la description initiale de règle.
4. Dans la boîte de dialogue **Sélectionner Matrix configuration**, sélectionnez le destinataire Matrix pertinent et cliquez sur **OK**.
5. Cliquez sur le lien des **périphériques** dans la description de règle initiale et définissez à partir de quelle caméra vous souhaitez envoyer une vidéo au destinataire Matrix, puis cliquez sur **OK** pour confirmer votre sélection.
6. Cliquez sur **Finir** si la règle est complète ou définissez, le cas échéant, des actions supplémentaires et/ou une action d'arrêt.



Si vous supprimez un destinataire Matrix, toute règle qui inclut le destinataire Matrix arrêtera de fonctionner.

## Envoyer la même vidéo à plusieurs vues XProtect Smart Client

Si le destinataire Matrix est XProtect Smart Client, vous pouvez envoyer la même vidéo aux positions Matrix dans plusieurs vues de XProtect Smart Client, à condition que les positions de vues de Matrix partagent les mêmes numéro de port et mot de passe :

1. Dans XProtect Smart Client, créez les vues pertinentes et les positions Matrix qui partagent les mêmes numéro de port et mot de passe.
2. Dans le Management Client, ajoutez le XProtect Smart Client pertinent comme destinataire Matrix.
3. Vous pouvez inclure le destinataire Matrix dans une règle.

## Navigation sur le site : Règles et événements

Cet article décrit comment configurer des événements et des règles pour vous aider à déclencher des actions et des alarmes dans le système. Elle explique également comment configurer les notifications par email et les délais des règles.

### Règles et événements (explications)

Les **règles** sont un élément central dans votre système. Les règles déterminent des paramètres très importants tels que le moment où une caméra doit enregistrer, où les caméras PTZ doivent patrouiller, quand les notifications doivent être envoyées, etc.

Exemple - une règle qui précise qu'une caméra particulière doit commencer à enregistrer lorsqu'elle détecte un mouvement :

```
Perform an action on Motion Start
  from Camera 2
start recording 3 seconds before on the device on which event occurred


Perform stop action on Motion End
  from Camera 2
stop recording immediately
```

Les **événements** sont des éléments centraux lorsque vous utilisez l'assistant **Gérer la règle**. Dans l'assistant, les événements sont principalement utilisés pour déclencher des actions. Vous créez par exemple une règle qui précise que si l'**événement** mouvement est détecté, le système de surveillance lance l'**action** qui consiste à enregistrer une vidéo à partir d'une caméra spécifique.

Ces types de conditions peuvent déclencher des règles :

Nom	Description
<b>Événements</b>	Lorsque des événements se produisent sur le système de surveillance, par exemple lorsque le mouvement est détecté ou que le système reçoit une entrée de détecteurs externes.
<b>Intervalle de temps</b>	Lorsque vous entrez des durées spécifiques, par exemple : Jeudi 16 août 2007, de 7 h à 7 h 59 OU chaque samedi et dimanche
<b>Temps récurrent</b>	Lorsque vous configurez une action pour qu'elle soit exécutée sur un calendrier détaillé et périodique.



Nom	Description
	<p>Par exemple :</p> <ul style="list-style-type: none"> <li>• Chaque semaine, le mardi, à chaque heure entre 15h00 et 15h30</li> <li>• Le 15 du mois tous les 3 mois à 11h45</li> <li>• Chaque jour, chaque heure entre 15h00 et 19h00</li> </ul> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0; margin: 10px 0;">  <span style="margin-left: 10px;">L'heure est configurée en fonction des paramètres de l'heure locale du serveur sur lequel Management Client est installé.</span> </div> <p>Pour plus d'informations, voir Temps récurrent sur la page 347.</p>

Vous pouvez travailler avec les éléments suivants sous **Règles et événements** :

- **Règles** : Les règles sont un élément central dans le système. Le comportement de votre système de surveillance est déterminé en grande partie par des règles. Lorsque vous créez une règle, vous pouvez travailler avec tous types d'événements
- **Profils de temps** : Les profils de temps sont des périodes de temps définies dans le Management Client. Ils peuvent être utilisés lors de la création de règles dans le Management Client, par exemple lors de la création d'une règle spécifiant qu'une certaine action doit se dérouler dans un certain profil de temps
- **Profils de notification** : Vous pouvez utiliser les profils de notification pour configurer des notifications par e-mail prêtes à l'emploi, qui peuvent être automatiquement déclenchées par une règle, par exemple lorsqu'un événement particulier se produit.
- **Événements définis par l'utilisateur** : Les événements définis par l'utilisateur sont des événements personnalisés qui font qu'il est possible pour les utilisateurs de déclencher manuellement des événements dans le système ou bien de réagir aux entrées du système
- **Événements analytiques** : Les événements analytiques sont des données reçues de la part de fournisseurs d'analyse de contenu vidéo (VCA) tiers externes. Vous pouvez utiliser les événements analytiques comme base pour les alarmes
- **Événements génériques** : Les événements génériques vous permettent de déclencher des actions sur le serveur d'événements XProtect en envoyant des chaînes simples via le réseau IP à votre système.

Voir Vue d'ensemble des événements sur la page 326 pour obtenir une liste des événements.

## Actions et actions d'arrêt (explications)

Lorsque vous ajoutez des règles (voir Ajouter une règle sur la page 345) dans l'assistant **Gérer la règle**, vous pouvez choisir parmi différentes actions :

First: Select actions to perform

- Start recording
- Set live frame rate on <devices>
- Set recording frame rate on <devices>

Certaines actions exigent une action d'arrêt. **Exemple** : Si vous sélectionnez l'action de **démarrage d'un enregistrement**, il commence et potentiellement continue indéfiniment. En conséquence, l'action de **démarrage d'un enregistrement** a une action d'arrêt obligatoire appelée **Arrêter d'enregistrer**.

L'assistant **Gérer la règle** s'assure que vous spécifiez des actions d'arrêt si nécessaire :


Select stop action to perform

- Stop recording
- Stop feed
- Restore default live frame rate
- Restore default recording frame rate
- Restore default recording frame rate of keyframes for H.264/MPEG4
- Resume patrolling
- Stop patrolling

Sélection des actions d'arrêt. Dans l'exemple, remarquez l'action d'arrêt obligatoire (sélectionnée, grisée), les actions non pertinentes d'arrêt (grisées) et les actions d'arrêt en option (sélectionnables).



Chaque type d'action de votre système XProtect est décrit. Vous pouvez disposer de davantage d'actions si votre installation utilise des produits d'extension ou des plug-ins spécifiques au fournisseur. Pour chaque type d'action, les informations d'action d'arrêt sont également indiquées le cas échéant :

Action	Description
<b>Démarrer l'enregistrement sur &lt;périphériques&gt;</b>	<p>Commencez l'enregistrement et la sauvegarde des données dans la base de données des périphériques choisis.</p> <p>En sélectionnant ce type d'action, l'assistant <b>Gérer la règle</b> vous invite à indiquer :</p> <p>À quel moment l'enregistrement doit commencer. Cela se produit immédiatement ou un certain nombre de secondes avant l'événement déclencheur/début de l'intervalle de temps de déclenchement et sur quels appareils l'action doit avoir lieu.</p> <p>Ce type d'action exige que vous ayez activé l'enregistrement sur les périphériques auxquels l'action est liée. Vous pouvez uniquement enregistrer les données précédant</p>

Action	Description
	<p>un intervalle de temps ou un événement si vous avez activé le pré-tampon pour les dispositifs concernés. L'enregistrement et la définition des paramètres de la mise en mémoire-tampon préalable d'un périphérique sont activés sur l'onglet <b>Enregistrement</b>.</p> <p><b>Action d'arrêt requise</b> : Ce type d'action nécessite une ou plusieurs actions d'arrêt. Dans l'une des étapes suivantes, l'assistant vous invite automatiquement à spécifier l'action d'arrêt : <b>Arrêter l'enregistrement</b>.</p> <p>Sans cette action d'arrêt, un enregistrement pourrait potentiellement continuer indéfiniment. Vous pouvez aussi préciser d'autres actions d'arrêt.</p>
<p><b>Démarrer le flux sur &lt;périphériques&gt;</b></p>	<p>Lancez le flux de données des périphériques vers le système. Lorsque le flux à partir d'un périphérique a commencé, les données sont transférées depuis le périphérique jusqu'au système, auquel cas la visualisation et l'enregistrement sont possible selon le type de données.</p> <p>Lorsque vous sélectionnez ce type d'action, l'assistant <b>Gérer la règle</b> vous invite à indiquer sur quels périphériques les flux doivent être démarrés. Votre système dispose d'une règle par défaut qui assure que les flux soient toujours démarrés sur toutes les caméras.</p> <p><b>Action d'arrêt requise</b> : Ce type d'action nécessite une ou plusieurs actions d'arrêt. Dans l'une des étapes suivantes, l'assistant vous invite automatiquement à spécifier l'action d'arrêt : <b>Arrêter un flux</b>.</p> <p>Vous pouvez également indiquer d'autres actions d'arrêt.</p> <p>Utiliser l'action d'arrêt obligatoire <b>Arrêter un flux</b> pour arrêter un flux provenant d'un périphérique signifie que les données ne sont plus transférées depuis le périphérique jusqu'au système, auquel cas la visualisation et l'enregistrement de la vidéo, par exemple, ne sont plus possibles. Cependant, un périphérique sur lequel vous avez arrêté l'alimentation peut toujours communiquer avec le serveur d'enregistrement, et vous pouvez relancer l'alimentation automatiquement par le biais d'une règle, contrairement au moment où vous avez désactivé manuellement l'appareil.</p> <div style="background-color: #f9e79f; padding: 10px; margin-top: 10px;">  <p>Bien que ce type d'action donne accès aux flux de données de périphériques sélectionnés, il ne garantit pas que la vidéo soit enregistrée, car vous devez spécifier les paramètres d'enregistrement séparément.</p> </div>

Action	Description
Régler <Smart Wall> sur <préréglages>	Définit le XProtect Smart Wall sur un préréglage sélectionné. Spécifiez le préréglage sur l'onglet <b>Préréglages Smart Wall</b> .  <b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Régler le <moniteur> du <Smart Wall> pour afficher des <caméras >	Règle un moniteur XProtect Smart Wall spécifique de façon à ce qu'il affiche la vidéo de caméras sélectionnées en direct sur ce site ou sur tout site enfant configuré dans Milestone Federated Architecture.  <b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Régler le <moniteur> du <Smart Wall> pour afficher le texte <messages>	Réglez un moniteur XProtect Smart Wall spécifique de sorte qu'il affiche un message défini par l'utilisateur d'une longueur maximale de 200 caractères.  <b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Supprimer <caméras> du moniteur <moniteur> <Smart Wall>	Arrêtez d'afficher la vidéo d'une caméra spécifique.  <b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
Définir la fluidité d'image en direct sur <périphériques>	Définit une fluidité d'image précise à utiliser lorsque le système affiche la vidéo en direct provenant de caméras choisies, qui remplace la fluidité d'image par défaut. Indiquez cela sur l'onglet <b>Paramètres</b> .  Lors de la sélection de ce type d'action, l'assistant <b>Gérer la règle</b> vous invite à indiquer sur quelle fluidité d'image définir et sur quels périphériques. Vérifiez toujours que la fluidité d'image que vous spécifiez est disponible sur les caméras concernées.  <b>Action d'arrêt requise</b> : Ce type d'action nécessite une ou plusieurs actions d'arrêt. Dans l'une des étapes suivantes, l'assistant vous invite automatiquement à spécifier l'action d'arrêt : <b>Rétablir la fluidité d'images en direct par défaut</b> .  Sans cette action d'arrêt, il est possible que la fluidité d'image par défaut ne soit jamais

Action	Description
	restaurée. Vous pouvez aussi préciser d'autres actions d'arrêt.
<p><b>Définir la fluidité d'image à l'enregistrement sur &lt;périphériques&gt;</b></p>	<p>Définit une fluidité d'image précise à utiliser lorsque le système sauvegarde la vidéo enregistrée provenant de caméras choisies dans la base de données, au lieu de la fluidité d'image d'enregistrement par défaut.</p> <p>Lors de la sélection de ce type d'action, l'assistant <b>Gérer la règle</b> vous invite à indiquer les fluidités d'image d'enregistrement à définir et sur quels caméras.</p> <p>Vous pouvez uniquement spécifier une fluidité d'image d'enregistrement pour JPEG, un codec vidéo avec lequel chaque image est compressée séparément dans une image JPEG. Ce type d'action exige également que l'enregistrement ait été activé sur les caméras auxquelles l'action est liée. Vous activez l'enregistrement d'une caméra sur l'onglet <b>Enregistrer</b>. La fluidité d'image maximum que vous pouvez préciser dépend des types de caméras concernés et de leur résolution d'image sélectionnée.</p> <p><b>Action d'arrêt requise</b> : Ce type d'action nécessite une ou plusieurs actions d'arrêt. Dans l'une des étapes suivantes, l'assistant vous invite automatiquement à spécifier l'action d'arrêt : <b>Rétablir la fluidité d'images enregistrées par défaut</b>.</p> <p>Sans cette action d'arrêt, il est possible que la fluidité d'image d'enregistrement par défaut ne soit jamais restaurée. Vous pouvez aussi préciser d'autres actions d'arrêt.</p>
<p><b>Établir la fluidité d'images enregistrées pour tous les cadres pour MPEG-4/H.264/H.265 sur &lt;périphériques&gt;</b></p>	<p>Définit la fluidité d'images pour enregistrer toutes les images lorsque le système enregistre la vidéo enregistrée par les caméras sélectionnées dans la base de données, au lieu des images clés seulement. Activer les images clés d'enregistrement uniquement sur l'onglet <b>Enregistrement</b>.</p> <p>Lors de la sélection de ce type d'action, l'assistant <b>Gérer la règle</b> vous invite à choisir sur quels périphériques l'action doit être appliquée.</p> <p>Vous pouvez activer l'enregistrement des images-clés pour MPEG-4/H.264/H.265. Ce type d'action exige également que l'enregistrement ait été activé sur les caméras auxquelles l'action est liée. Vous activez l'enregistrement d'une caméra sur l'onglet <b>Enregistrer</b>.</p> <p><b>Action d'arrêt requise</b> : Ce type d'action nécessite une ou plusieurs actions d'arrêt. Dans l'une des étapes suivantes, l'assistant vous invite automatiquement à spécifier l'action d'arrêt : <b>Rétablir la fluidité d'image à l'enregistrement par défaut des images-clés pour MPEG-4/H.264/H.265</b></p> <p>Sans cette action d'arrêt, il est possible que les paramètres par défaut ne soient jamais</p>

Action	Description
<p><b>Début de la patrouille sur &lt;périphérique&gt; à l'aide de &lt;profil&gt; avec priorité PTZ</b> &lt;&gt;</p>	<p>restaurés. Vous pouvez aussi préciser d'autres actions d'arrêt.</p> <p>Démarre la patrouille PTZ selon un profil de patrouille particulier pour une caméra PTZ particulière avec une priorité particulière. Il s'agit de la définition exacte de la manière dont une patrouille doit avoir lieu, y compris la séquence des positions prédéfinies, les paramètres horaires, etc.</p> <p>Si vous avez actualisé votre système à partir d'une version plus ancienne du système, les anciennes valeurs (<b>très bas, bas, moyen, élevé et très élevé</b>) ont été traduites comme suit :</p> <ul style="list-style-type: none"> <li>• Très bas = 1000</li> <li>• Bas = 2000</li> <li>• Moyen = 3000</li> <li>• Élevé = 4000</li> <li>• Très élevé = 5000</li> </ul> <p>Lors de la sélection de ce type d'action, l'assistant <b>Gérer la règle</b> vous invite à sélectionner un profil de patrouille. Vous pouvez uniquement sélectionner un profil de patrouille sur un périphérique et vous ne pouvez pas sélectionner plusieurs profils de patrouille.</p> <div style="background-color: #e6f2ff; padding: 10px; margin-bottom: 10px;">  Ce type d'action exige que les dispositifs auxquels l'action est liée soient des dispositifs PTZ.         </div> <div style="background-color: #e6f2ff; padding: 10px; margin-bottom: 10px;">  Vous devez définir au moins un profil de patrouille pour le périphérique (ou les périphériques). Vous définissez les profils de patrouille pour une caméra PTZ sur l'onglet <b>Patrouille</b>.         </div> <p><b>Action d'arrêt requise</b> : Ce type d'action nécessite une ou plusieurs actions d'arrêt. Dans l'une des étapes suivantes, l'assistant vous invite automatiquement à spécifier l'action d'arrêt :</p> <p><b>Arrêter la patrouille</b></p> <p>Sans cette action d'arrêt, patrouiller pourrait éventuellement ne jamais s'arrêter. Vous pouvez également indiquer d'autres actions d'arrêt.</p>


Action	Description
<p><b>Mettre la patrouille en pause sur &lt;périphériques&gt;</b></p>	<p>Met la patrouille PTZ en pause. Lors de la sélection de ce type d'action, l'assistant <b>Gérer la règle</b> vous invite à indiquer sur quels périphériques la patrouille doit être mise sur pause.</p> <div data-bbox="424 454 1385 584" style="background-color: #e6f2ff; padding: 10px; margin-bottom: 10px;">  Ce type d'action exige que les dispositifs auxquels l'action est liée soient des dispositifs PTZ.         </div> <div data-bbox="424 633 1385 801" style="background-color: #e6f2ff; padding: 10px; margin-bottom: 10px;">  Vous devez définir au moins un profil de patrouille pour le périphérique (ou les périphériques). Vous définissez les profils de patrouille pour une caméra PTZ sur l'onglet <b>Patrouille</b>.         </div> <p><b>Action d'arrêt requise</b> : Ce type d'action nécessite une ou plusieurs actions d'arrêt. Dans l'une des étapes suivantes, l'assistant vous invite automatiquement à spécifier l'action d'arrêt : <b>Réactiver la patrouille</b></p> <p>Sans cette action d'arrêt, patrouiller pourrait éventuellement se mettre sur pause indéfiniment. Vous pouvez aussi préciser d'autres actions d'arrêt.</p>
<p><b>Adopter la position &lt;préréglages&gt; pour &lt;périphérique&gt; avec la priorité PTZ &lt;priorité&gt;</b></p>	<p>Déplace une caméra spécifique dans une position prédéfinie particulière, toutefois toujours conformément à la priorité. Lors de la sélection de ce type d'action, l'assistant <b>Gérer la règle</b> vous invite à sélectionner une position prédéfinie. Une seule position prédéfinie sur une caméra peut être sélectionnée. Il n'est pas possible de sélectionner plusieurs positions prééglées.</p> <div data-bbox="424 1305 1385 1435" style="background-color: #e6f2ff; padding: 10px; margin-bottom: 10px;">  Ce type d'action exige que les dispositifs auxquels l'action est liée soient des dispositifs PTZ.         </div> <div data-bbox="424 1485 1385 1693" style="background-color: #e6f2ff; padding: 10px; margin-bottom: 10px;">  Cette action nécessite que vous ayez défini au moins une position prédéfinie pour ces dispositifs. Vous définissez des positions prédéfinies pour une caméra PTZ sur l'onglet <b>Positions prédéfinies</b>.         </div> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action</p>

Action	Description
	<p>d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<p><b>Adopter le paramètre prédéfini pour &lt;périphériques&gt; avec la priorité PTZ &lt;priorité&gt;</b></p>	<p>Déplace une caméra ou plusieurs caméras spécifiques sur leurs positions prédéfinies par défaut respectives, toutefois, toujours conformément à la priorité. Lors de la sélection de ce type d'action, l'assistant <b>Gérer la règle</b> vous invite à choisir sur quels périphériques l'action doit être appliquée.</p> <div data-bbox="427 607 1385 891" style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;">  <p>Ce type d'action exige que les dispositifs auxquels l'action est liée soient des dispositifs PTZ.                  Cette action nécessite que vous ayez défini au moins une position prédéfinie pour ces dispositifs. Vous définissez des positions prédéfinies pour une caméra PTZ sur l'onglet <b>Positions prédéfinies</b>.</p> </div> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<p><b>Définir la sortie du périphérique sur &lt;état&gt;</b></p>	<p>Définit une sortie sur un périphérique sur un état particulier (activé ou désactivé). Lors de la sélection de ce type d'action, l'assistant <b>Gérer la règle</b> vous invitera à indiquer l'état à définir et sur quels périphériques.</p> <p>Ce type d'action exige que les périphériques auxquels l'action est liée aient chacun au moins une unité de sortie externe connectée à un port de sortie.</p> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<p><b>Créer le signet sur &lt;périphérique&gt;</b></p>	<p>Crée un signet sur le flux en direct ou les enregistrements à partir d'un périphérique choisi. Un signet fait qu'il est aisé de retracer un certain événement ou une certaine période de temps. Les paramètres du signet sont contrôlés à partir de la boîte de dialogue <b>Options</b>. Lors de la sélection de ce type d'action, l'assistant <b>Gérer la règle</b> vous invite à préciser les détails du signet et à sélectionner les périphériques.</p> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>




Action	Description
<p><b>Lire le &lt;message&gt; audio sur les &lt;périphériques&gt; en &lt;priorité&gt;</b></p>	<p>Lit un message audio sur des périphériques sélectionnés qui sont déclenchés par un événement. Les périphériques sont surtout des haut-parleurs ou des caméras.</p> <p>Ce type d'action vous impose de charger le message dans le système sur l'onglet <b>Outils &gt; Options &gt; Messages audio</b>.</p> <p>Vous pouvez créer davantage de règles pour le même événement et envoyer des messages différents à chaque périphérique, mais toujours selon une priorité. Les priorités qui contrôlent la séquence sont celles qui s'appliquent à la règle et au périphérique pour un rôle sur l'onglet <b>Audio</b> :</p> <ul style="list-style-type: none"> <li>• Si un message est lu et qu'un autre message ayant la même priorité est envoyé au même haut-parleur, le premier message se termine, puis le second commence</li> <li>• Si un message est lu et qu'un autre message ayant une priorité plus élevée est envoyé au même haut-parleur, le premier message sera interrompu et le second commence immédiatement</li> </ul>
<p><b>Envoyer la notification à &lt;profil&gt;</b></p>	<p>Envoie une notification par l'intermédiaire d'un profil de notification particulier. Lorsque vous sélectionnez ce type d'action, l'assistant <b>Gérer le règle</b> vous invite à choisir un profil de notification et à partir de quels périphériques inclure les images pré-alarme. Vous pouvez uniquement sélectionner un profil de notification et vous ne pouvez pas sélectionner plusieurs profils de notification. Un seul profil de notification peut contenir plusieurs destinataires.</p> <p>Vous pouvez également créer d'autres règles pour le même événement et envoyer différentes notifications à chacun des profils de notification. Vous pouvez copier et réutiliser le contenu des règles par un clic droit sur une règle dans la liste des <b>Règles</b>.</p> <p>Ce type d'action nécessite que vous ayez défini au moins un profil de notification. Les images de pré-alarme sont uniquement incluses si vous avez activé l'option <b>Inclure les images</b> pour le profil de notification correspondant.</p> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<p><b>Créer une entrée &lt;entrée au journal&gt;</b></p>	<p>Génère une entrée dans le journal des règles. Lors de la sélection de ce type d'action, l'assistant <b>Gérer la règle</b> vous invite à préciser un texte pour une entrée du journal. Lorsque vous indiquez le texte du journal, vous pouvez insérer rapidement des variables telles que <b>\$DeviceName\$, \$EventName\$</b>, dans le message de journalisation.</p>

Action	Description
	<p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<p><b>Démarrer le module d'extension sur &lt;périphériques&gt;</b></p>	<p>Lance un ou plusieurs modules d'extension. Lors de la sélection de ce type d'action, l'assistant <b>Gérer la règle</b> vous invite à sélectionner les modules d'extension nécessaires et sur quels périphériques lancer les modules d'extension.</p> <p>Ce type d'action exige que vous ayez au moins un ou plusieurs modules d'extension installés sur votre système.</p> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<p><b>Arrêter le module d'extension sur &lt;périphériques&gt;</b></p>	<p>Arrête un ou plusieurs modules d'extension. Lors de la sélection de ce type d'action, l'assistant <b>Gérer la règle</b> vous invitera à sélectionner les modules d'extension nécessaires et sur quels périphériques arrêter les modules d'extension.</p> <p>Ce type d'action exige que vous ayez au moins un ou plusieurs modules d'extension installés sur votre système.</p> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<p><b>Appliquer les nouveaux paramètres sur &lt;périphériques&gt;</b></p>	<p>Modifie les paramètres des périphériques sur un ou plusieurs périphériques. Lorsque vous sélectionnez ce type d'action, l'assistant <b>Gérer la règle</b> vous invite à sélectionner les périphériques concernés et vous pouvez définir les paramètres pertinents sur les périphériques que vous avez spécifiés.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;"> <p> Si vous définissez des paramètres pour plus d'un périphérique, vous pouvez uniquement changer les paramètres qui sont disponibles pour tous les périphériques précisés.</p> </div> <p><b>Exemple</b> : Vous spécifiez que l'action doit être liée au Périphérique 1 et au Périphérique 2. Le Périphérique 1 a les paramètres A, B et C et le Périphérique 2 a les paramètres B, C et D. Dans ce cas, vous pouvez uniquement changer les paramètres disponibles pour les deux périphériques, à savoir les paramètres B et C.</p>

Action	Description
	<p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<p><b>Définir Matrix pour afficher &lt;périphériques&gt;</b></p>	<p>Fait apparaître des vidéos à partir des caméras choisies sur un ordinateur en mesure d'afficher une vidéo déclenchée par Matrix tel qu'un ordinateur sur lequel vous avez installé soit XProtect Smart Client, soit l'application Matrix Monitor.</p> <p>Lors de la sélection de ce type d'action, l'assistant <b>Gérer la règle</b> vous invite à sélectionner un destinataire Matrix et un ou plusieurs périphériques à partir desquels afficher une vidéo sur le destinataire Matrix choisi.</p> <p>Ce type d'action vous permet de sélectionner uniquement un seul destinataire Matrix à la fois. Si vous souhaitez que des vidéos provenant de périphériques sélectionnés apparaissent sur plus d'un destinataire Matrix, vous devriez créer une règle pour chaque destinataire Matrix requis ou utiliser la fonction XProtect Smart Wall. Le fait d'effectuer un clic droit sur une règle dans la liste des <b>Règles</b> vous permet de copier et de réutiliser le contenu des règles. De cette manière, vous pouvez éviter d'avoir à créer entièrement des règles presque identiques.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;"> <p>Dans le cadre de la configuration des destinataires Matrix eux-mêmes, les utilisateurs doivent spécifier le numéro de port et le mot de passe requis pour la communication Matrix. Veillez à ce que les utilisateurs aient accès à cette information.</p> <p> Généralement, les utilisateurs doivent aussi définir les adresses IP des hôtes autorisés à partir desquels les commandes relatives à l'affichage de la vidéo déclenchée par Matrix sont acceptées. Dans ce cas, les utilisateurs doivent également connaître l'adresse IP du serveur de gestion (ou tout autre routeur ou pare-feu utilisé).</p> </div>
<p><b>Envoyer un trap SNMP</b></p>	<p>Génère un petit message qui journalise les événements sur les périphériques sélectionnés. Le texte des traps SNMP est généré automatiquement et ne peut pas être personnalisé. Il peut contenir généralement le type et le nom de source du périphérique sur lequel l'événement s'est produit.</p> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>

Action	Description
<b>Rappeler et sauvegarder les enregistrements à distance depuis les &lt;périphériques&gt;</b>	<p>Récupère et stocke les enregistrements à distance provenant des périphériques sélectionnés (prenant en charge les enregistrements locaux) au cours d'une période spécifiée et après l'événement déclencheur.</p> <p>Cette règle est indépendante du paramètre <b>Rappeler les enregistrements à distance automatiquement lorsque la connexion est rétablie</b>.</p> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<b>Récupérer et stocker les enregistrements à distance entre &lt;heure de début / de fin&gt; et &lt;périphériques&gt;</b>	<p>Récupère et stocke les enregistrements à distance de périphériques choisis (qui prennent en charge l'enregistrement local) au cours d'une période spécifiée.</p> <p>Cette règle est indépendante du paramètre <b>Rappeler les enregistrements à distance automatiquement lorsque la connexion est rétablie</b>.</p> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<b>Enregistrer une image jointe</b>	<p>Veille à ce que lorsqu'une image est reçue de l'événement Images reçues (envoyées via e-mail SMTP à partir d'une caméra), elle est sauvegardée pour usage ultérieur. À l'avenir, d'autres événements peuvent éventuellement déclencher cette action.</p> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<b>Activer l'archivage sur &lt;archives&gt;</b>	<p>Lance l'archivage d'une ou de plusieurs archives. Lors de la sélection de ce type d'action, l'assistant <b>Gérer la règle</b> vous invite à sélectionner les archives concernées.</p> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt. Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<b>Déclencher &lt;événement défini par l'utilisateur&gt; sur &lt;site&gt;</b>	<p>Surtout pertinent au sein de Milestone Federated Architecture, mais vous pouvez également l'utiliser dans la configuration d'un site unique. Utilisez la règle pour déclencher un événement défini par utilisateur sur un site, normalement un site à distance au sein d'une hiérarchie fédérée.</p> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action</p>

Action	Description
	d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.
<b>Afficher &lt;notification de demande d'accès&gt;</b>	<p>Vous permet d'accéder aux notifications de demande qui apparaissent sur l'écran XProtect Smart Client lorsque les critères correspondant aux événements déclencheurs sont respectés. Milestone recommande que vous utilisiez des événements de contrôle d'accès en tant qu'événements déclencheurs pour cette action, car les notifications de demande d'accès sont généralement configurées pour une utilisation sur des commandes et caméras de contrôle d'accès connexes.</p> <p>Ce type d'action exige que vous ayez au moins un plug-in de contrôle d'accès installé sur votre système.</p> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<b>Définir la &lt;caméra&gt; sur le &lt;canal DLNA basé sur la règle&gt;</b>	<p>En fonction des événements, les caméras sont associées au canal DLNA basé sur la règle. Ce type d'action nécessite qu'un serveur DLNA soit installé sur votre système.</p> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<b>Supprimer la &lt;caméra&gt; du &lt;canal DLNA basé sur la règle&gt;</b>	<p>En fonction des événements, les caméras sont supprimées du canal DLNA basé sur la règle. Ce type d'action nécessite qu'un serveur DLNA soit installé sur votre système.</p> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<b>Supprimer la caméra actuelle du &lt;canal DLNA basé sur la règle&gt;</b>	<p>La caméra au flux actif est supprimée du canal DLNA basé sur la règle en fonction des événements. Ce type d'action nécessite qu'un serveur DLNA soit installé sur votre système.</p> <p><b>Aucune action d'arrêt obligatoire</b> : Ce type d'action ne nécessite aucune action d'arrêt.Vous pouvez spécifier des actions optionnelles d'arrêt à exécuter pour un événement ou après une période de temps.</p>
<b>Modifier le mot de passe sur les</b>	Change le mot de passe sur les périphériques sélectionnés pour un mot de passe généré aléatoirement en fonction des exigences du mot de passe pour le périphérique

Action	Description
<p><b>périphériques matériel</b></p>	<p>concerné. Pour une liste des périphériques pris en charge, voir <a href="https://www.milestonesys.com/community/business-partner-tools/supported-devices/">https://www.milestonesys.com/community/business-partner-tools/supported-devices/</a>.</p> <div data-bbox="424 416 1385 584" style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;">  <p>Cette action est seulement disponible lorsque vous configurez une règle qui utilise le type de règle <b>Effectuer une action sur un &lt;recurring time&gt;</b>.</p> </div> <p>Les événements suivants sont disponibles pour l'action :</p> <ul style="list-style-type: none"> <li>• Programmation du changement du mot de passe commencée sur la page 338</li> <li>• Programmation du changement du mot de passe exécutée avec succès sur la page 338</li> <li>• Programmation du changement du mot de passe exécutée avec des erreurs sur la page 338</li> </ul> <p>Ce type d'action n'a pas d'action d'arrêt.</p> <p>Vous pouvez consulter la progression de cette action dans le nœud <b>Tâches actuelles</b>. Pour de plus amples informations, voir Tâches actuelles (explications) sur la page 431.</p> <p>Pour consulter les résultats de l'action - allez sur le nœud <b>Journaux du serveur</b>, dans l'onglet <b>Journaux du système</b>. Pour de plus amples informations, voir Onglet Journaux de serveurs (options) sur la page 126.</p> <p>Pour de plus amples informations, voir Journaux système (propriétés) sur la page 435.</p>

## Vue d'ensemble des événements

Lorsque vous créez une règle basée sur l'événement dans l'assistant **Gérer la règle**, vous pouvez effectuer une sélection entre différents types d'événements : Pour que vous puissiez avoir un bon aperçu, les événements que vous pouvez sélectionner apparaissent dans une liste établie par groupes selon s'ils sont :

### Matériel :

Certains matériels peuvent créer eux-mêmes des événements, comme par exemple pour la détection du mouvement. Vous pouvez les utiliser en tant qu'événements mais vous devez les configurer sur le matériel avant de pouvoir les utiliser dans le système. Vous pourrez peut-être utiliser uniquement les événements énumérés sur certains périphériques car tous les types de caméras ne peuvent pas détecter la modification ou les changements de température.

**Matériel - Évènements configurables :**

Les événements configurables sur les périphériques sont automatiquement importés à partir des pilotes de périphériques. Cela signifie qu'ils varient d'un matériel à l'autre et ne sont pas mentionnés ici. Les événements configurables ne sont pas déclenchés tant que vous ne les avez pas ajoutés au système et ne les avez pas configurés sur l'onglet **Évènement** pour le matériel. Certains des événements configurables exigent également que vous configuriez la caméra (matériel).

**Matériel - Évènements prédéfinis :**

Évènement	Description
<b>Erreur de communication (Matériel)</b>	Se produit lors de la perte d'une connexion à un matériel.
<b>Communication démarrée (Matériel)</b>	Se produit lorsqu'une tentative de communication avec un matériel réussit.
<b>Communication arrêtée (Matériel)</b>	Se produit lorsqu'une tentative d'arrêt de la communication avec un matériel réussit.

**Périphériques - Évènements configurables :**

Les événements configurables sur les périphériques sont automatiquement importés à partir des pilotes de périphériques. Cela signifie qu'ils varient d'un périphérique à l'autre et ne sont pas mentionnés ici. Les événements configurables ne sont pas déclenchés tant que vous ne les avez pas ajoutés au système et ne les avez pas configurés sur l'onglet **Évènement** sur un périphérique.

**Périphériques - Évènements prédéfinis :**

Évènement	Description
<b>Référence de signet demandée</b>	Se produit lorsqu'un signet est créé en mode direct ou lecture dans les clients. De plus, une exigence d'utilisation de la règle d'enregistrement sur signet.

Événement	Description
<b>Erreur de communication (Périphérique)</b>	A lieu lorsqu'une connexion à un périphérique est perdue, ou lorsqu'une tentative de communication avec un périphérique échoue.
<b>Communication démarrée (Périphérique)</b>	A lieu lorsqu'une tentative de communication avec un périphérique réussit.
<b>Communication arrêtée (Périphérique)</b>	A lieu lorsqu'une communication avec un périphérique est bien arrêtée.
<b>Verrouillage des preuves modifié</b>	Se produit quand une preuve protégée est modifiée pour les périphériques par un utilisateur client ou via le MIP SDK.
<b>Preuves verrouillées</b>	Se produit quand une protection des preuves est créée pour les périphériques par un utilisateur client ou via le MIP SDK.
<b>Preuves déverrouillées</b>	Se produit quand la protection des preuves est supprimée pour les périphériques par un utilisateur client ou via le MIP SDK.
<b>Dépassement de la capacité d'alimentation démarré</b>	<p>Le dépassement de la capacité d'alimentation (dépassement de capacité multimédia) a lieu lorsqu'un serveur d'enregistrement ne peut pas traiter les données reçues aussi rapidement que l'indique la configuration et qu'il est par conséquent obligé d'ignorer certains enregistrements.</p> <p>Si le serveur est sain, le dépassement de la capacité d'alimentation se produit car le disque lent enregistre. Vous pouvez y remédier soit en réduisant la quantité de données écrites, soit en améliorant la performance de stockage du système. Réduit la quantité de données écrites en réduisant la fluidité d'image, la résolution ou la qualité d'image sur vos caméras, mais cela peut détériorer la qualité de l'enregistrement. Si cela ne vous intéresse pas, améliorez alors la performance de stockage de votre système en installant des pilotes supplémentaires pour partager la charge ou bien en installant des disques ou des contrôleurs plus rapides.</p> <p>Vous pouvez utiliser cet événement pour déclencher des actions qui vous aident à éviter le problème, par exemple, pour réduire la fluidité d'images d'enregistrement.</p>
<b>Dépassement de la capacité</b>	A lieu lorsque le dépassement de capacité (voir Dépassement de la capacité d'alimentation démarré sur la page 328) se termine.



Événement	Description
<b>d'alimentation arrêtée</b>	
<b>Alimentation du Live Client demandée</b>	<p>A lieu lorsque des utilisateurs du client demandent un flux en direct à partir d'un périphérique.</p> <p>L'événement se produit à la demande, même si la demande de l'utilisateur client échoue par la suite, par exemple parce que l'utilisateur client ne possède pas les droits nécessaires pour voir le flux demandé en direct ou parce que le flux est arrêté pour une raison quelconque.</p>
<b>Alimentation du Live Client terminée</b>	<p>A lieu lorsque des utilisateurs du client ne demandent plus un flux en direct à partir d'un périphérique.</p>
<b>Enregistrement manuel démarré</b>	<p>Se produit quand un utilisateur client démarre une session d'enregistrement pour une caméra.</p> <p>L'événement est déclenché même si le périphérique est déjà en cours d'enregistrement via les actions de règles.</p>
<b>Enregistrement manuel arrêté</b>	<p>Se produit quand un utilisateur client arrête une session d'enregistrement pour une caméra.</p> <p>Si le système de règles a aussi commencé une session d'enregistrement, il continue d'enregistrer même après l'arrêt de l'enregistrement manuel.</p>
<b>Référence de données marquées demandée</b>	<p>Se produit quand la protection de la preuve est effectuée en mode lecture dans les clients ou via le MIP SDK.</p> <p>Un événement est créé et vous pouvez l'utiliser dans vos règles.</p>
<b>Mouvement démarré</b>	<p>A lieu lorsque le système détecte un mouvement dans la vidéo reçue des caméras.</p> <p>Ce type d'événement exige que la détection du mouvement du système soit activée en ce qui concerne les caméras auxquelles l'événement est lié.</p> <p>Outre la détection de mouvement du système, certaines caméras peuvent détecter le mouvement elles-mêmes et déclencher l'événement <b>Démarrage de mouvements (HW)</b>, mais cela dépend de la configuration du périphérique de caméra et du système. Voir également Matériel - Événements configurables : sur la page 327.</p>

Événement	Description
<b>Mouvement arrêté</b>	<p>A lieu lorsque le mouvement n'est plus détecté dans la vidéo reçue. Voir également Mouvement démarré sur la page 329.</p> <p>Ce type d'événement exige que la détection du mouvement du système soit activée en ce qui concerne les caméras auxquelles l'événement est lié.</p> <p>Outre la détection de mouvement du système, certaines caméras peuvent détecter le mouvement elles-mêmes et déclencher l'événement Arrêt des mouvements (HW), mais cela dépend de la configuration du périphérique de caméra et du système. Voir également Matériel - Évènements configurables : sur la page 327.</p>
<b>Sortie activée</b>	<p>Se produit quand un port de sortie externe sur un périphérique est activé.</p> <p>Ce type d'événement exige qu'au moins un périphérique sur votre système prenne en charge les ports de sortie.</p>
<b>Sortie modifiée</b>	<p>Se produit quand l'état d'un port de sortie externe sur un périphérique est modifié.</p> <p>Ce type d'événement exige qu'au moins un périphérique sur votre système prenne en charge les ports de sortie.</p>
<b>Sortie désactivée</b>	<p>A lieu lorsqu'une unité de sortie externe connectée à un port de sortie sur un périphérique est désactivé.</p> <p>Ce type d'événement exige qu'au moins un périphérique sur votre système prenne en charge les ports de sortie.</p>
<b>Session manuelle PTZ démarrée</b>	<p>A lieu lorsqu'une session PTZ manuelle (à l'inverse d'une session PTZ basée sur une patrouille programmée ou automatiquement déclenchée par un événement) est déclenchée sur une caméra.</p> <p>Ce type d'action exige que les caméras auxquelles l'événement est lié soient des caméras PTZ.</p>
<b>Session manuelle PTZ arrêtée</b>	<p>A lieu lorsqu'une session PTZ manuelle (à l'inverse d'une session PTZ basée sur une patrouille programmée ou automatiquement déclenchée par un événement) est arrêtée sur une caméra.</p> <p>Ce type d'action exige que les caméras auxquelles l'événement est lié soient des caméras PTZ.</p>
<b>Enregistrement</b>	<p>A lieu dès que l'enregistrement commence. Il existe un événement distinct pour le</p>

Événement	Description
démarré	démarrage de l'enregistrement manuel.
<b>Enregistrement arrêté</b>	A lieu lorsque l'enregistrement est arrêté. Il existe un événement distinct pour l'arrêt de l'enregistrement manuel.
<b>Paramètre modifié</b>	A lieu lorsque des paramètres sur un périphérique sont correctement modifiés.
<b>Erreur : paramètres modifiés</b>	A lieu lorsqu'une tentative de modification des paramètres d'un périphérique échoue.

#### Événements externes - Événements prédéfinis :

Événement	Description
<b>Demander la diffusion d'un message audio</b>	Activé lorsque la lecture de messages audio est requise via le MIP SDK. Au travers du MIP SDK, un vendeur tiers peut développer des modules d'extension personnalisés (par exemple, l'intégration à des systèmes de contrôle de l'accès externes ou semblables) à votre système.
<b>Demander le départ de l'enregistrement</b>	Activé lorsque le démarrage des enregistrements est demandé via MIP SDK. Au travers du MIP SDK, un vendeur tiers peut développer des modules d'extension personnalisés (par exemple, l'intégration à des systèmes de contrôle de l'accès externes ou semblables) à votre système.
<b>Demande Arrêter l'enregistrement</b>	Activé lorsque l'arrêt des enregistrements est demandé via MIP SDK. Au travers du MIP SDK, un vendeur tiers peut développer des modules d'extension personnalisés (par exemple, l'intégration à des systèmes de contrôle de l'accès externes ou semblables) à votre système.

**Événements externes - Événements génériques :**

Les événements génériques vous permettent de déclencher des actions dans le système en envoyant des chaînes simples via le réseau IP au système. L'objectif des événements génériques est d'autoriser autant de sources externes que possible pour interagir avec le système.

**Événements externes - Événements définis par l'utilisateur :**

Plusieurs événements personnalisés pour convenir à votre système peuvent éventuellement également être sélectionnés. Vous pouvez utiliser ces événements définis par l'utilisateur pour :

- Donner la possibilité aux utilisateurs du client de déclencher manuellement des événements tout en visualisant une vidéo en direct dans les clients
- D'innombrables autres objectifs. Par exemple, vous pouvez créer des événements définis par l'utilisateur qui ont lieu si un type particulier de données est reçu d'un périphérique

Voir également Événements définis par l'utilisateur (explications) sur la page 356

**Serveurs d'enregistrement :**

Événement	Description
<b>Archive disponible</b>	A lieu lorsqu'une archive d'un serveur d'enregistrement est disponible après avoir été indisponible. Voir également Archive non disponible sur la page 332.
<b>Archive non disponible</b>	A lieu lorsqu'une archive pour un serveur d'enregistrement devient indisponible, par exemple la connexion avec une archive sur un volume connecté au réseau est perdue. Dans ce cas, vous ne pouvez pas archiver d'enregistrements.  Vous pouvez utiliser l'événement, par exemple, pour déclencher une alarme ou un profil de notification afin qu'un e-mail de notification soit automatiquement envoyé aux personnes appropriées de votre organisation.
<b>Archive non terminée</b>	A lieu lorsqu'une archive d'un serveur d'enregistrement n'est pas terminée et quand le dernier archivage est fait lorsque le prochain est programmé pour commencer.
<b>La base de données supprime les fichiers avant la taille de</b>	Se produit lorsque l'horaire de rétention est atteint avant la taille limite de la base de données.

Événement	Description
<b>rétenion fixée</b>	
<b>La base de données supprime les fichiers avant l'horaire de rétention fixé</b>	Se produit lorsque la taille limite de la base de données est atteinte avant l'horaire de rétention fixé.
<b>Disque de base de données pleine - Archivage automatique</b>	<p>A lieu lorsqu'un disque de base de données n'a plus d'espace libre. Un disque de base de données est considéré comme saturé lorsqu'il contient moins de 5 Go d'espace libre :</p> <p>Les plus anciennes données d'une base de données seront toujours auto-archivées (ou supprimées si aucune archive suivante n'est définie) dès qu'il y a moins de 5 Go d'espace libre.</p>
<b>Disque de base de données plein - Suppression en cours</b>	Se produit lorsqu'un disque de base de données est plein et qu'il reste moins d'1 Go d'espace libre. Les données sont supprimées même si une nouvelle archive est définie. Une base de données a toujours besoin de 250 Mo d'espace libre. Si cette limite est atteinte (si les données ne sont pas supprimées assez rapidement), aucune autre donnée n'est ajoutée à la base de données tant que de l'espace n'a pas été libéré. La taille maximum réelle de votre base de données est la quantité de giga-octets que vous spécifiez, moins 5 Go.
<b>Base de données pleine - Archivage automatique</b>	A lieu lorsqu'une archive pour un serveur d'enregistrement est pleine et qu'elle a besoin d'un archivage automatique dans une archive de stockage.
<b>Réparation de la base de données</b>	A lieu lorsqu'une base de données est corrompue, auquel cas le système applique automatiquement deux méthodes différentes de réparation.
<b>Zone de stockage de base de données disponible</b>	<p>A lieu lorsqu'un stockage d'un serveur d'enregistrement est disponible après avoir été indisponible. Voir également Zone de stockage de base de données non disponible sur la page 333.</p> <p>Par exemple, vous pouvez utiliser l'événement pour lancer l'enregistrement s'il a été arrêté par l'événement <b>Stockage de base de données non disponible</b>.</p>
<b>Zone de stockage de base de données non disponible</b>	A lieu lorsque le stockage pour un serveur d'enregistrement devient indisponible, par exemple si la connexion à un stockage situé sur une unité de réseau est perdue. Dans ce cas, vous ne pouvez pas archiver d'enregistrements.

Événement	Description
	Vous pouvez utiliser l'événement, par exemple, pour arrêter l'enregistrement, déclencher une alarme ou un profil de notification afin qu'un e-mail de notification soit automatiquement envoyé aux personnes appropriées de votre organisation.
<b>Erreur de la communication cryptée de redondance</b>	Survient lorsqu'il y a une erreur de communication SSL entre le serveur de redondance et les serveurs d'enregistrement surveillés.
<b>Redondance commencée</b>	A lieu lorsqu'un serveur d'enregistrement de basculement se substitue à un serveur d'enregistrement. Voir également Serveurs d'enregistrement de redondance (explications) sur la page 185.
<b>Redondance arrêtée</b>	A lieu lorsqu'un serveur d'enregistrement devient à nouveau disponible, et peut se substituer au serveur d'enregistrement de basculement.

### Événements moniteur système

Les événements du moniteur système sont déclenchés par le dépassement des valeurs limites configurées dans le nœud des **Seuils du moniteur système**. Voir également Seuils du Moniteur système (explication) sur la page 425.



Cette fonctionnalité nécessite que le service Data Collector soit en cours d'exécution.

### Moniteur système - Serveur :

Événement	Description
<b>Utilisation du processeur critique</b>	Se produit lorsque l'utilisation du CPU dépasse le seuil critique du CPU.
<b>Usage du processeur normal</b>	Se produit lorsque l'utilisation du CPU retombe sous le seuil d'alerte du CPU.
<b>Avertissement d'usage</b>	Se produit lorsque l'utilisation du CPU dépasse le seuil d'alerte du CPU ou

Événement	Description
<b>du processeur</b>	redevient inférieur au seuil critique du CPU.
<b>Utilisation de la mémoire critique</b>	Se produit lorsque l'utilisation de la mémoire dépasse le seuil critique de la mémoire.
<b>Utilisation de la mémoire normale</b>	Se produit lorsque l'utilisation de la mémoire redevient inférieure au seuil d'alerte de la mémoire.
<b>Avertissement d'utilisation de la mémoire</b>	Se produit lorsque l'utilisation de la mémoire dépasse le seuil d'alerte de la mémoire ou redevient inférieur au seuil d'utilisation critique de la mémoire.
<b>Décodage critique NVIDIA</b>	Se produit lorsque l'utilisation du décodage NVIDIA dépasse le seuil critique de NVIDIA.
<b>Décodage normal NVIDIA</b>	Se produit lorsque l'utilisation du décodage NVIDIA redevient inférieur au seuil d'alerte de NVIDIA.
<b>Avertissement du décodage NVIDIA</b>	Se produit lorsque l'utilisation du décodage NVIDIA dépasse le seuil d'alerte du décodage NVIDIA ou redevient inférieur au seuil critique de NVIDIA.
<b>Mémoire critique NVIDIA</b>	Se produit lorsque l'utilisation de la mémoire NVIDIA dépasse le seuil critique de la mémoire NVIDIA.
<b>Mémoire normale NVIDIA</b>	Se produit lorsque l'utilisation de la mémoire NVIDIA redevient inférieure au seuil d'alerte de NVIDIA.
<b>Avertissement de la mémoire NVIDIA</b>	Se produit lorsque l'utilisation de la mémoire NVIDIA dépasse le seuil d'alerte de la mémoire NVIDIA ou redevient inférieure au seuil critique de NVIDIA.
<b>Rendu critique NVIDIA</b>	Se produit lorsque l'utilisation de NVIDIA dépasse le seuil critique du NVIDIA.
<b>Rendu normal de NVIDIA</b>	Se produit lorsque l'utilisation de NVIDIA redevient inférieure au seuil d'alerte du NVIDIA.
<b>Avertissement du rendu NVIDIA</b>	Se produit lorsque l'utilisation de la mémoire NVIDIA dépasse le seuil d'alerte du rendu NVIDIA ou redevient inférieure au seuil critique de NVIDIA.

Événement	Description
<b>Disponibilité du service critique</b>	Se produit lorsqu'un service de serveur s'arrête de fonctionner. Il n'existe aucune valeur de seuil pour cet événement.
<b>Disponibilité du service normale</b>	Se produit lorsque l'état d'un service de serveur se remet à fonctionner. Il n'existe aucune valeur de seuil pour cet événement.

**Moniteur système - Caméra :**

Événement	Description
<b>FPS en direct critique</b>	Se produit lorsque le FPS en direct devient inférieur au seuil critique de FPS en direct.
<b>FPS en direct normal</b>	Se produit lorsque le FPS en direct dépasse le seuil d'alerte de FPS en direct.
<b>Avertissement FPS en direct</b>	Se produit lorsque le FPS en direct devient inférieur au seuil critique de FPS en direct ou dépasse le seuil critique de celui-ci.
<b>FPS d'enregistrement critique</b>	Se produit lorsque le FPS d'enregistrement devient inférieur au seuil critique du FPS d'enregistrement.
<b>FPS d'enregistrement normal</b>	Se produit lorsque le FPS d'enregistrement dépasse le seuil d'alerte du FPS d'enregistrement.
<b>Avertissement FPS d'enregistrement</b>	Se produit lorsque le FPS en direct devient inférieure au seuil d'alerte FPS d'enregistrement ou dépasse le seuil critique de FPS d'enregistrement.
<b>Espace utilisé critique</b>	Se produit lorsque l'espace utilisé pour les enregistrements par une caméra spécifique dépasse le seuil critique d'espace utilisé.
<b>Espace utilisé normal</b>	Se produit lorsque l'espace utilisé pour les enregistrements par une caméra spécifique redevient inférieur au seuil d'alerte d'espace utilisé.
<b>Avertissement d'espace utilisé</b>	Se produit lorsque l'espace utilisé pour les enregistrements par une caméra spécifique dépasse le seuil d'alerte d'espace utilisé ou devient inférieur au seuil critique d'espace utilisé.



**Moniteur système - Disque :**

Événement	Description
<b>Espace libre critique</b>	Se produit lorsque l'espace de stockage utilisé dépasse le seuil critique d'espace libre.
<b>Espace libre normal</b>	Se produit lorsque l'espace de stockage utilisé devient inférieur au seuil critique d'espace libre.
<b>Avertissement d'espace libre</b>	Se produit lorsque l'espace de stockage utilisé dépasse le seuil d'alerte d'espace utilisé ou redevient inférieur au seuil critique d'espace libre.

**Moniteur système - Stockage :**

Événement	Description
<b>Durée de rétention critique</b>	Se produit lorsque le système prédit que l'espace libre de stockage sera plus vite consommé que la valeur de seuil critique du temps de rétention. Par exemple, lorsque les données des flux vidéo consomment l'espace de stockage plus rapidement que prévu.
<b>Durée de rétention normale</b>	Se produit lorsque le système prédit que l'espace libre de stockage sera plus vite consommé que la valeur de seuil d'alerte du temps de rétention. Par exemple lorsque les données des flux vidéo consomment l'espace de stockage à la vitesse prévue.
<b>Avertissement de durée de rétention</b>	Se produit lorsque le système prédit que l'espace de stockage sera plus vite consommé que la valeur de seuil d'alerte du temps de rétention ou moins rapidement que la valeur de seuil critique du temps de rétention. Par exemple, lorsque les données des flux vidéo consomment l'espace de stockage plus rapidement que prévu en raison d'un nombre de mouvements accrus détectés par les caméras configurées pour passer en mode enregistrement en cas de détection de mouvement.

**Autre :**

Événement	Description
<b>Échec d'activation automatique des licences</b>	Se produit lorsque l'activation automatique des licences a échoué.  Il n'existe aucune valeur de seuil pour cet événement.
<b>Programmation du changement du mot de passe commencée</b>	A lieu lorsque démarre la programmation du changement du mot de passe.
<b>Programmation du changement du mot de passe exécutée avec succès</b>	A lieu lorsqu'une programmation du changement du mot de passe s'achève sans erreur.
<b>Programmation du changement du mot de passe exécutée avec des erreurs</b>	A lieu lorsqu'une programmation du changement du mot de passe s'achève avec des erreurs.

**Événements à partir des intégrations et des produits complémentaires :**

Les événements à partir des intégrations et des produits complémentaires peuvent être utilisés dans le système de règles :

- Les événements analytiques peuvent également être utilisés dans le système de règles

## Règles

### Règles (explications)

Les règles spécifient les actions à réaliser dans des conditions particulières. Exemple : Lorsqu'un mouvement est détecté (condition), une caméra doit commencer à enregistrer (action).

Voici des **exemples** de ce que vous pouvez faire avec les règles :

- Débuter et terminer un enregistrement
- Régler la fluidité d'images en direct (autre que par défaut)
- Régler la fluidité d'images enregistrées (autre que par défaut)
- Débuter et terminer une patrouille PTZ
- Mettre en pause et reprendre une patrouille PTZ
- Déplacer les caméras PTZ dans des positions spécifiques

- Activer/désactiver des sorties
- Envoyer des notifications par e-mail
- Journaliser des entrées
- Générer des événements
- Appliquer de nouveaux paramètres aux périphériques, par exemple une résolution différente sur une caméra
- Faire apparaître la vidéo dans les destinataires Matrix
- Activer et arrêter des modules d'extension
- Activer et arrêter des flux de périphériques

Le fait d'arrêter un périphérique signifie qu'aucune vidéo n'est plus transférée à partir du périphérique vers le système, auquel cas ni le visionnement en direct, ni l'enregistrement ne sont possibles. Au contraire, un périphérique sur lequel vous avez arrêté l'alimentation peut toujours communiquer avec le serveur d'enregistrement, et vous pouvez lancer l'alimentation automatiquement depuis le périphérique par le biais d'une règle, contrairement à l'arrêt manuel de l'appareil dans le Management Client.



Le contenu de certaines règles peut demander à ce que certaines fonctions soient activées pour les périphériques concernés. Par exemple, une règle qui précise qu'une caméra doit enregistrer, ne fonctionne pas comme souhaité si l'enregistrement n'est pas activé pour la caméra concernée. Avant de créer une règle, Milestone vous recommande donc vivement de vérifier que les périphériques impliqués sont capables de fonctionner conformément aux intentions.

### Règles par défaut (explications)

Votre système contient un certain nombre de règles par défaut que vous pouvez utiliser sans autre forme de configuration pour les fonctions élémentaires. Vous pouvez désactiver ou modifier les règles par défaut en fonction de vos besoins. Si vous modifiez ou désactivez les règles par défaut, votre système peut ne pas fonctionner selon vos souhaits, ni garantir que les flux vidéo ou audio arrivent automatiquement au système.

Règle par défaut	Description
<b>Aller au préréglage en fin de PTZ</b>	Veille à ce que les caméras PTZ se déplacent à leurs positions prédéfinies par défaut respectives après qu'elles ont été opérées manuellement. Cette règle n'est pas activée par défaut.

Règle par défaut	Description
	Même lorsque la règle est activée, vous devez avoir des positions prédéfinies par défaut en ce qui concerne les caméras PTZ concernées pour que la règle fonctionne. Pour ce faire, allez dans l'onglet <b>Préréglages</b> .
<b>Lire le message audio sur demande</b>	<p>Veille à ce que la vidéo soit enregistrée automatiquement lorsqu'une requête externe se produit.</p> <p>La demande est toujours déclenchée par un système s'intégrant en externe avec votre système, et la règle est principalement utilisée par les intégrateurs de systèmes externes ou de modules d'extension.</p>
<b>Enregistrer sur signet</b>	<p>S'assure que la vidéo est enregistrée automatiquement lorsqu'un opérateur configure un signet dans XProtect Smart Client. Cette action n'est possible que si vous avez activé l'enregistrement des caméras concernées. Par défaut, l'enregistrement est activé.</p> <p>Pour cette règle, la durée d'enregistrement par défaut est fixée à trois secondes avant le positionnement du signet et 30 secondes après le positionnement du signet. Vous pouvez modifier les temps d'enregistrement par défaut dans la règle. La mise en mémoire-tampon préalable configurable dans l'onglet Enregistrement doit être identique ou supérieure à la durée de pré-enregistrement.</p>
<b>Enregistrer sur mouvement</b>	<p>Veille à ce que tant que le mouvement est détecté par les caméras, la vidéo est enregistrée, à condition que l'enregistrement soit activé pour les caméras en question. Par défaut, l'enregistrement est activé.</p> <p>Bien que la règle par défaut indique un enregistrement basé sur la détection du mouvement, elle ne garantit pas que la vidéo soit enregistrée par le système car vous pouvez avoir désactivé l'enregistrement d'une caméra individuelle pour une ou plusieurs caméras. Même lorsque l'enregistrement est activé, il ne faut pas oublier que la qualité des enregistrements peut être affectée par les paramètres d'enregistrement de chaque caméra.</p>
<b>Enregistrer sur demande</b>	<p>Veille à ce que la vidéo soit enregistrée automatiquement lorsqu'une demande externe survient, à condition que l'enregistrement soit activé pour les caméras en question. Par défaut, l'enregistrement est activé.</p> <p>La demande est toujours déclenchée par un système s'intégrant en externe avec votre système, et la règle est principalement utilisée par les intégrateurs de systèmes externes ou de modules d'extension.</p>

Règle par défaut	Description
<b>Activer le flux audio</b>	<p>Veille à ce que les flux audio de tous les microphones et haut-parleurs connectés soient automatiquement alimentés vers le système.</p> <p>Bien que la règle par défaut donne accès aux flux audio des microphones et haut-parleurs connectés immédiatement après installation du système, elle ne garantit pas que l'audio sera enregistré, car les paramètres d'enregistrement doivent être précisés séparément.</p>
<b>Activer le flux vidéo</b>	<p>Veille à ce que les flux vidéo de toutes les caméras connectées soient automatiquement alimentés vers le système.</p> <p>Bien que la règle par défaut donne accès aux flux vidéo des caméras connectées immédiatement après installation du système, elle ne garantit pas que la vidéo soit enregistrée, car les paramètres d'enregistrement des caméras doivent être précisés séparément.</p>
<b>Activer le flux de métadonnées</b>	<p>Veille à ce que les flux de données de toutes les caméras connectées soient automatiquement alimentés vers le système.</p> <p>Bien que la règle par défaut donne accès aux flux de données des caméras connectées immédiatement après installation du système, elle ne garantit pas que les données soient enregistrées, car les paramètres d'enregistrement des caméras doivent être précisés séparément.</p>
<b>Afficher la notification de demande d'accès</b>	<p>Veille à ce que tous les événements de contrôle d'accès classés comme « Demande d'accès », entraîne l'apparition d'une notification de demande d'accès dans XProtect Smart Client, à moins que la fonction de notification ne soit désactivée dans le profil Smart Client.</p>

### Recréer les règles par défaut

Si vous supprimez une règle par défaut sans le vouloir, vous pouvez la recréer en saisissant le texte ci-après :

Règle par défaut	Texte à saisir
<b>Aller au</b>	Réaliser une action sur session manuelle PTZ arrêtée de toutes les caméras

Règle par défaut	Texte à saisir
<b>préréglage en fin de PTZ</b>	Passer immédiatement à la position prédéfinie par défaut sur le périphérique sur lequel l'événement s'est produit
<b>Lire le message audio sur demande</b>	Exécuter une action sur un message audio sur demande Lire le message audio à partir des métadonnées disponibles sur les périphériques ayant la priorité 1
<b>Enregistrer sur signet</b>	Réaliser une action sur Référence de signet demandée par toutes les caméras, tous les microphones, tous les haut-parleurs lance l'enregistrement trois secondes auparavant sur le périphérique sur lequel l'événement s'est produit. Réaliser une action 30 secondes immédiatement après l'arrêt de l'enregistrement
<b>Enregistrer sur mouvement</b>	Réaliser une action sur Mouvement lancé par toutes les caméras lance l'enregistrement trois secondes avant sur le périphérique sur lequel l'événement s'est produit Réaliser une action d'arrêt sur Mouvement arrêté par les caméras arrête l'enregistrement trois secondes après
<b>Enregistrer sur demande</b>	Réaliser une action sur Demander le départ de l'enregistrement d'une source externe lance l'enregistrement immédiatement sur les périphériques à partir de métadonnées Réaliser une action d'arrêt sur Demander l'arrêt de l'enregistrement d'une source externe arrête l'enregistrement immédiatement
<b>Activer le flux audio</b>	Exécuter une action dans un intervalle de temps lance toujours les flux sur tous les microphones, tous les haut-parleurs Réaliser une action lorsque l'intervalle de temps termine immédiatement le flux
<b>Activer le flux</b>	Exécuter une action dans un intervalle de temps lance toujours les flux sur toutes les caméras Réaliser une action lorsque l'intervalle de temps termine immédiatement le flux
<b>Activer le flux de métadonnées</b>	Exécuter une action dans un intervalle de temps lance toujours les flux sur toutes les métadonnées Réaliser une action lorsque l'intervalle de temps termine immédiatement le flux

Règle par défaut	Texte à saisir
<b>Afficher la notification de demande d'accès</b>	Exécuter une action sur demande d'Accès (Catégories de Contrôle d'accès) à partir des Systèmes [+ unités]  Afficher la notification de demande d'accès intégrée

### Complexité de la règle (explications)

Votre nombre exact d'options dépend du type de règle que vous souhaitez créer et du nombre de périphériques à disposition sur votre système. Les règles offrent un degré élevé de flexibilité : vous pouvez associer un événement et des conditions de temps, spécifier plusieurs actions dans une seule règle et souvent créer des règles qui couvrent plusieurs ou tous les périphériques de votre système.

Vous pouvez rendre vos règles aussi simples ou aussi complexes que nécessaire. Par exemple, vous pouvez créer des règles très simples basées sur une durée :

Exemple	Explication
<b>Règle très simple basée sur une durée</b>	Les lundis entre 08h30 et 11h30 (condition de temps), les caméras 1 et 2 lancent l'enregistrement (action) au début de la période spécifiée et arrêtent l'enregistrement (arrêt d'action) lorsque la période spécifiée expire.
<b>Règle très simple basée sur un événement</b>	Lorsqu'un mouvement est détecté (condition d'événement) sur la Caméra 1, Caméra 1 lance immédiatement l'enregistrement (action) puis arrête l'enregistrement (arrêt d'action) après 10 secondes.  Même si une règle basée sur événement est activée par un événement sur un périphérique, vous pouvez préciser que des actions doivent avoir lieu sur un ou plusieurs périphériques différents.
<b>Règle impliquant plusieurs périphériques</b>	Lorsqu'un mouvement est détecté (condition d'événement) sur la caméra 1, la caméra 2 doit immédiatement lancer l'enregistrement (action) puis la sirène raccordée à la sortie 3 doit sonner (action) immédiatement. Puis, après écoulement de 60 secondes, la caméra 2 doit arrêter l'enregistrement (arrêt

Exemple	Explication
	d'action), et la sirène raccordée à la sortie 3 doit arrêter de sonner (arrêt d'action).
<b>Règle combinant la durée, les événements et les périphériques</b>	Lorsqu'un mouvement est détecté (condition d'événement) sur la caméra 1, que le jour de la semaine est samedi ou dimanche (condition de temps), la caméra 1 et la caméra 2 lancent immédiatement l'enregistrement (action), et une notification est envoyée au responsable de la sécurité (action). Puis, 5 secondes après la fin de détection du mouvement sur la caméra 1 ou 2, les 2 caméras arrêtent l'enregistrement (arrêt d'action).

Selon les besoins de votre entreprise, il convient souvent de créer plusieurs règles simples plutôt que de créer quelques règles complexes. Même si cela signifie que vous avez plus de règles dans votre système, cela offre un moyen simple de conserver un aperçu des actions de vos règles. Le fait de ne pas compliquer les règles veut également dire que vous avez plus de flexibilité lorsqu'il s'agit de désactiver/activer des éléments de règle individuels. Avec des règles simples, vous pouvez désactiver/activer des règles complètes le cas échéant.

### Valider les règles (explications)

Vous pouvez valider le contenu d'une règle individuelle ou de toutes les règles en une seule fois. Lorsque vous créez une règle, l'assistant **Gérer la règle** veille à ce que tous les éléments de la règle aient un sens. Toutefois, lorsqu'une règle a existé pendant quelque temps, il est possible qu'un ou que plusieurs éléments de la règle aient pu être affectés par une autre configuration et il est possible que la règle ne fonctionne plus. Par exemple, si une règle est déclenchée par un profil de temps spécifique, la règle ne fonctionnera plus si le profil de temps en question a été effacé ou si vous ne disposez plus des permissions vous permettant d'y accéder. Il peut être difficile de se faire une vue d'ensemble de tels effets involontaires de configuration.

La validation des règles vous aide à suivre les règles concernées par une modification. La validation a lieu en se basant sur chaque règle et chaque règle est validée de manière isolée. Il n'est pas possible de valider les règles les unes par rapport aux autres (par exemple pour savoir si une règle est en conflit avec une autre), même lors de l'utilisation de la fonction **Valider toutes les règles**.



Il n'est pas possible de valider si la configuration des conditions préalables en-dehors de la règle elle-même empêche la règle de fonctionner. Par exemple, une règle qui indique qu'un enregistrement doit avoir lieu lorsqu'un mouvement est détecté par une caméra précise est validée si les éléments de la règle sont corrects et cela même si la détection du mouvement (qui est activée au niveau de la caméra, et non au travers des règles) n'a pas été activée pour la caméra concernée.



Vous pouvez valider une règle individuelle ou toutes les règles en même temps en faisant un clic droit sur la règle à valider et en sélectionnant **Valider la règle** ou **Valider toutes les règles**. Une boîte de dialogue vous indique si la ou les règles ont été bien validées. Si vous choisissez de valider plus d'une règle et qu'une ou plusieurs règles n'ont pas été exécutées, la boîte de dialogue énumère les noms des règles affectées.



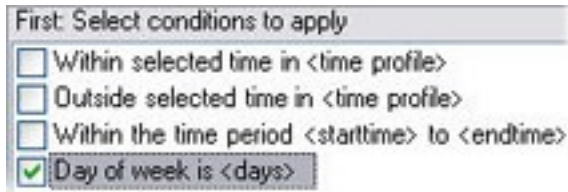
### Ajouter une règle

Lorsque vous créez des règles, vous êtes guidé par l'assistant **Gérer la règle** qui ne contient que les options pertinentes.

Il veille à ce qu'une règle ne contienne pas d'éléments manquants. En fonction du contenu de votre règle, il suggère automatiquement des actions d'arrêt appropriées (à savoir ce qui devrait se passer lorsqu'une règle n'est plus applicable), afin de veiller à ce que vous ne créiez pas accidentellement des règles sans fin.

1. Cliquez avec le bouton droit sur l'article **Règles > Ajouter une règle**. Cela ouvre l'assistant **Gestion des règles**. L'assistant vous guide dans la spécification du contenu de votre règle.
2. Spécification d'un nom et d'une description de la nouvelle règle dans les champs **Nom** et **Description** respectivement.
3. Sélectionnez le type pertinent de condition de la règle : soit une règle qui effectue une ou plusieurs actions lorsqu'un événement particulier a lieu, soit une règle qui exécute plusieurs actions lorsqu'une période de temps précise est saisie.
4. Cliquez sur **Suivant** dans l'assistant pour passer à l'étape seconde de l'assistant. Dans la seconde étape de l'assistant, définissez les autres conditions de la règle.

- Sélectionnez une ou plusieurs conditions, par exemple **Le jour de la semaine est <jour>** :



En fonction de vos sélections, modifiez la description de la règle dans la partie inférieure de la fenêtre de l'assistant :



Cliquez sur les éléments soulignés en **italique gras** pour préciser le contenu exact. Par exemple, le fait de cliquer sur le lien **jours** dans notre exemple, vous permet de sélectionner un ou plusieurs jours de la semaine lors desquels la règle est applicable.

- Après avoir indiqué vos conditions exactes, cliquez sur **Suivant** pour passer à la prochaine étape de l'assistant et sélectionner les actions qui doivent être couvertes par la règle. En fonction du contenu et de la complexité de votre règle, vous devrez peut-être définir d'autres étapes, telles que des événements et des actions d'arrêt. Par exemple, si une règle indique qu'un périphérique doit exécuter une action particulière durant un intervalle de temps (par exemple les jeudis entre 8h00 et 10h30), l'assistant peut vous demander de préciser ce qui doit se passer et quand l'intervalle de temps se termine.
- Votre règle est activée par défaut après sa création si ses conditions sont satisfaites. Si vous ne voulez pas que votre règle soit activée directement, décochez la case **Activé**.
- Cliquez sur **Terminer**.

### Modifier, copier et renommer une règle

- Dans le volet **Vue d'ensemble**, faites un clic droit sur la règle concernée.
- Sélectionnez :  
**Modifier règle** ou **Copier règle** ou **Renommer règle**. L'assistant **Gérer la règle** s'ouvre.
- Dans l'assistant, renommez et/ou modifiez la règle. Si vous avez sélectionné **Copier règle**, l'assistant s'ouvre, affichant une copie de la règle sélectionnée.
- Cliquez sur **Terminer**.

### Désactiver et activer une règle

Votre système applique une règle dès que les conditions de la règle s'appliquent ce qui signifie qu'elle est active. Si vous ne voulez pas qu'une règle soit active, vous pouvez la désactiver. Lorsqu'une règle est désactivée, le système n'applique pas la règle, même si les conditions s'appliquent. Vous pouvez facilement activer/désactiver la

règle ultérieurement.

### Désactiver une règle

1. Dans le volet **Vue d'ensemble**, sélectionnez la règle.
2. Décochez la case **Activé** dans le volet **Propriétés**.
3. Cliquez sur **Sauvegarder** dans la barre d'outils.
4. Une icône avec une croix rouge indique que la règle a été désactivée dans la liste des **règles** :



### Activer une règle

Lorsque vous souhaitez réactiver la règle, sélectionnez la règle, cochez la case **Activer** et sauvegardez la configuration.

## Temps récurrent

Lorsque vous configurez une action pour qu'elle soit exécutée sur un calendrier détaillé et périodique.

Par exemple :

- Chaque semaine, le mardi, à chaque heure entre 15h00 et 15h30
- Le 15 du mois tous les 3 mois à 11h45
- Chaque jour, chaque heure entre 15h00 et 19h00



L'heure est configurée en fonction des paramètres de l'heure locale du serveur sur lequel Management Client est installé.

Vous pouvez éventuellement sélectionner un profil de temps pour assurer que la règle ne s'exécute que dans ou en dehors de l'intervalle du profil de temps.

Pour des instructions générales sur comment configurer une nouvelle règle, voir [Ajouter une règle](#) sur la page 345.

Pour en savoir plus sur les profils de temps, voir [Profils temporels](#) sur la page 347.

## Profils temporels

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

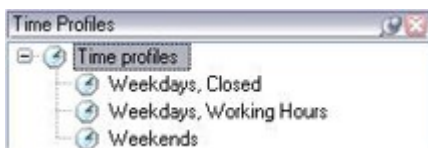
Les profils de temps sont des périodes de temps définies par l'administrateur. Vous pouvez utiliser les profils de temps lors de la création de règles, par exemple une règle spécifiant qu'une certaine action doit se dérouler dans une certaine période de temps.

En outre, les profils de temps sont attribués aux rôles en plus des profils Smart Client. Par défaut, il est attribué par défaut à tous les rôles le profil de temps **Toujours**. Cela signifie que les membres de rôles avec ce profil de temps par défaut n'ont aucune limite de temps sur leurs droits d'utilisateurs dans le système. Vous pouvez également assigner un profil de temps alternatif à un rôle.

Les profils de temps sont très souples : ils peuvent être basés sur une ou plusieurs périodes uniques, une ou plusieurs périodes récurrentes ou une combinaison de périodes uniques et récurrentes. Beaucoup d'utilisateur peuvent maîtriser les concepts des périodes de temps uniques et récurrentes des applications du calendrier, comme celle dans Outlook de Microsoft®.

Les profils de temps s'appliquent toujours à l'heure locale. Cela signifie que si votre système est doté de serveurs d'enregistrement dans différents fuseaux horaires, les actions (par ex. enregistrement des caméras) associées aux profils de temps sont exécutées dans chaque heure locale du serveur d'enregistrement. Exemple : Si vous avez un profil de temps couvrant la période allant de 8h30 à 9h30, toutes les actions associées à un serveur d'enregistrement à New York sont exécutées entre 8h30 et 9h30 heure de New York, tandis que les mêmes actions sur un serveur placé à Los Angeles ont lieu plus tard, lorsqu'il est entre 8h30 et 9h30 à Los Angeles.

Les profils de temps sont créés et gérés en développant **Règles et événements > Profils de temps**. Une liste de **profils de temps** s'ouvre : Exemple seulement :



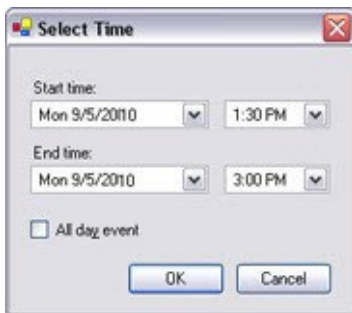
Pour voir une alternative aux profils de temps, reportez-vous aux Profils de temps toute la journée (explications) sur la page 350.

### Spécifier un profil de temps

1. Dans la liste des **profils de temps**, faites un clic droit dans **Profils de temps > Ajouter profil de temps**. Cela ouvre la fenêtre **Profil de temps**.
2. Dans la fenêtre **Profil de temps**, saisissez un nom pour le nouveau profil de temps dans le champ **Nom**. Facultativement, saisissez une description du nouveau profil de temps dans le champ **Description**.
3. Dans le calendrier de la fenêtre **Profil de temps**, sélectionnez **Vue quotidienne**, **Vue hebdomadaire**, ou **Vue mensuelle**, puis faites un clic droit à l'intérieur du calendrier et sélectionnez **Ajouter une période unique** ou **Ajouter une période récurrente**.
4. Une fois que vous avez spécifié les périodes pour votre profil de temps, cliquez sur **OK** dans la fenêtre **Profil de temps**. Votre système ajoute le nouveau profil de temps dans la liste des **profils de temps**. Si à un stade ultérieur vous voulez modifier ou supprimer le profil de temps, vous pouvez également le faire à partir de la liste des **profils de temps**.

## Ajouter une période unique

Lorsque vous sélectionnez **Ajouter une période unique**, la fenêtre **Sélectionner la période** s'affiche :

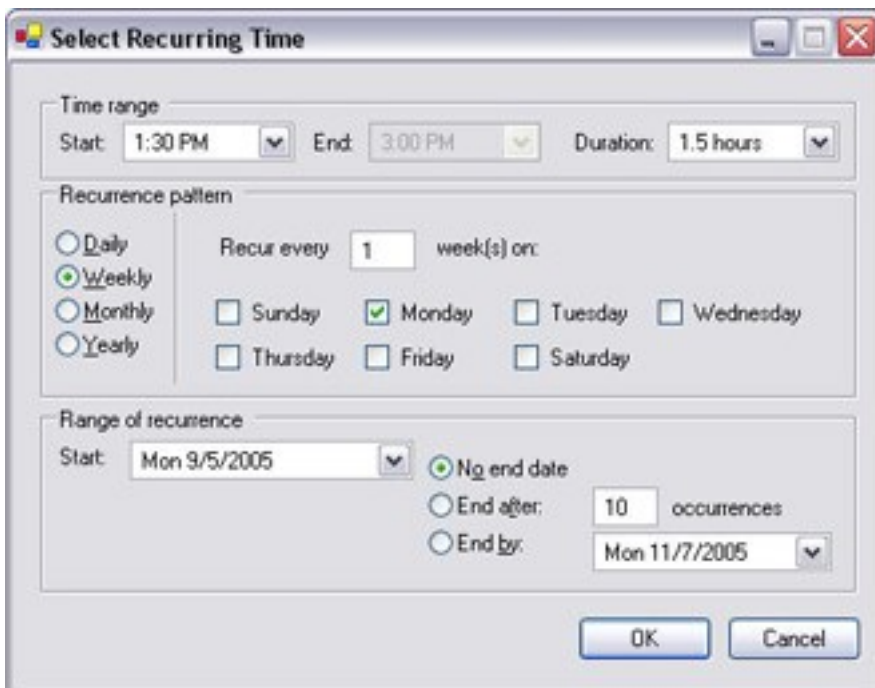


Le format de présentation de la date et de l'heure peut s'afficher différemment sur votre système.

1. Dans la fenêtre **Sélectionner la période**, indiquez une **Heure de début** et une **Heure de fin**. Si la période doit couvrir des journées entières, cochez la case **Événement d'un jour**.
2. Cliquez sur **OK**.

## Spécifier une période récurrente

Lorsque vous sélectionnez **Ajouter une période récurrente**, la fenêtre **Sélectionner la période récurrente** s'affiche :



1. Dans la fenêtre **Sélectionner la période**, indiquez la plage horaire, le modèle de périodicité et la plage de périodicité.
2. Cliquez sur **OK**.



Un profil de temps peut contenir plusieurs périodes. Si vous souhaitez que votre profil de temps contienne d'autres périodes, ajoutez des périodes uniques ou récurrentes.

### Modifier un profil de temps

1. Dans la liste des **profils de temps** du volet **Vue d'ensemble**, faites un clic droit sur le profil de temps concerné, puis sélectionnez **Modifier le profil de temps**. Cela ouvre la fenêtre **Profil de temps**.
2. Modifiez le profil de temps en fonction de vos besoins. Après modification du profil de temps, cliquez sur **OK** dans la fenêtre **Profil de temps**. Vous revenez dans la liste des **profils de temps**.



Dans la fenêtre **Informations profil de temps**, vous pouvez modifier le profil de temps selon vos besoins. N'oubliez pas qu'un profil de temps peut contenir plusieurs périodes et que les périodes peuvent être récurrentes. Le petit aperçu mensuel dans le coin supérieur droit peut vous aider à obtenir un aperçu rapide des périodes couvertes par le profil, car les dates contenant des heures spécifiques sont en gras.



Dans cet exemple, les dates en gras indiquent que les périodes s'étendent sur plusieurs jours et qu'une durée récurrente a été précisée les lundis.

### Profils de temps toute la journée (explications)

Lorsque les caméras sont placées à l'extérieur, il est souvent nécessaire de diminuer la résolution des caméras, d'activer le noir et blanc ou de modifier d'autres paramètres lorsqu'il fait sombre ou lorsqu'il y a beaucoup de soleil. Le plus au nord ou le plus au sud par rapport à l'équateur se trouvent les caméras, plus les heures de lever et de coucher du soleil varient au cours de l'année. Ce qui fait qu'il est impossible d'utiliser des profils de temps fixes pour ajuster les paramètres de la caméra en fonction de la lumière.

Dans une telle situation, vous pouvez créer des profils de temps toute la journée en lieu et place afin de définir le lever et le coucher de soleil dans une zone géographique spécifique. Au travers des coordonnées géographiques, le système calcule les heures de lever et de coucher du soleil et incorpore même l'heure d'été ou l'heure d'hiver. Ainsi, le profil de temps suit automatiquement les changements annuels de lever/coucher du soleil dans la zone choisie, faisant que le profil est actif uniquement lorsque nécessaire. Toutes les heures et toutes les dates se

basent sur les paramètres de date et d'heure des serveurs de gestion. Vous pouvez également définir un décalage négatif ou positif (en minutes) pour l'heure de début (lever du soleil) et l'heure de fin (coucher du soleil). Le décalage pour l'heure de début et de fin peut être identique ou différent.

Vous pouvez utiliser les profils de temps toute la journée quand vous créez des règles, mais également des rôles.

### Créer un profil de temps toute la journée

1. Développez le dossier **Règles et événements** > **Profils de temps**.
2. Dans la liste des **profils de temps**, faites un clic droit dans **Profils de temps** et sélectionnez **Ajouter profil de temps toute la journée**.
3. Dans la fenêtre **Profil de temps toute la journée**, soumettez les informations nécessaires. Pour gérer les périodes de transition entre le jour et la nuit, vous avez la possibilité de décaler l'activation et la désactivation du profil. L'heure et le nom des mois sont affichés dans la langue désignée conformément aux réglages régionaux/de langue de votre ordinateur.
4. Pour voir l'emplacement des coordonnées géographiques saisies sur une carte, cliquez sur **Montrer la position dans le navigateur**. Cette action ouvre un navigateur dans lequel vous pouvez voir l'emplacement.
5. Cliquez sur **OK**.

### Propriétés du profil de temps journalier

Réglez les paramètres suivants pour le profil de temps toute la journée :

Nom	Description
<b>Nom</b>	Le nom du profil.
<b>Description</b>	Une description du profil (facultatif).
<b>Coordonnées géographiques</b>	Coordonnées géographiques qui indiquent l'emplacement physique des caméras attribuées au profil.
<b>Décalage lever du soleil</b>	Nombre de minutes (+/-) en fonction desquelles l'activation du profil est décalée par le lever du soleil.
<b>Décalage coucher du soleil</b>	Nombre de minutes (+/-) en fonction desquelles la désactivation du profil est décalée par le coucher du soleil.
<b>Fuseau horaire</b>	Fuseau horaire qui indique l'emplacement physique des caméras.

## Profils de notification

### Profils de notification (explications)

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

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



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

### Conditions préalables à la création des profils de notification

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

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

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

1. Rendez-vous sur **Outils > Options**. Cela ouvre la fenêtre **Options**.
2. Configurez le serveur de messagerie dans l'onglet **Serveur de messagerie** (Onglet Serveur de messagerie (options) sur la page 127), ainsi que les paramètres de compression dans l'onglet **Génération AVI** Onglet Génération AVI (options) sur la page 128.

### Ajouter des profils de notification

1. Développez **Règles et événements**, faites un clic droit sur **Profils de notification > Ajouter profil de notification**. Cela ouvre l'assistant **Ajouter profil de notification**.
2. Précisez le nom et une description. Cliquez sur **Suivant**.



- Saisissez le destinataire, l'objet, le texte du message et la durée entre les messages :

**Add Notification Profile**

**E-mail**

Recipients:  
aa@aa.aa

Subject:  
\$DeviceName\$ detection at \$TriggerTime\$

Message text:

Add system information (click links to insert variables into text field)

[Recording server name](#)  
[Hardware name](#)  
[Device name](#)  
[Rule name](#)  
[Trigger time](#)

Time btw. e-mails: 0 Seconds **Test E-mail**

**Data**

Include images  Include AVI

Number of images: 5 Time before event (sec): 2

Time btw. images (ms): 500 Time after event (sec): 4

Embed images in e-mail Frame rate: 5

Notifications containing H.265 encoded video require a computer that supports hardware acceleration.

Help < Back Finish Cancel

- Pour envoyer une notification par e-mail test aux destinataires indiqués, cliquez sur **Tester e-mail**.
- Pour inclure des photos de pré-alarme, sélectionnez **Inclure images** et indiquez le nombre de photos, la durée entre les photos et l'intégration des photos dans le message ou non.
- Pour inclure des clips vidéo AVI, sélectionnez **Inclure AVI** et indiquez la durée avant et après l'événement ainsi que la fluidité de l'image.



Les notifications contenant une vidéo H.265 cryptée nécessiteront un ordinateur prenant en charge l'accélération du matériel.

7. Cliquez sur **Terminer**.

### Utiliser des règles pour déclencher des notifications par e-mail

Utilisez l'assistant **Gérer la règle** pour créer des règles. L'assistant vous guide tout au long des étapes pertinentes. Vous spécifiez l'utilisation d'un profil de notification à l'étape où vous indiquez les actions de la règle.

Lorsque vous sélectionnez l'action **Envoyer notification à <profil>**, vous pouvez sélectionner le profil de notification correspondant et les caméras depuis lesquelles les enregistrements à inclure dans les notifications par e-mail du profil de notification doivent être issus :

Send notification to 'profile'  
images from recording device

Dans **Gérer les règles**, vous cliquez sur les liens pour effectuer vos sélections.

N'oubliez pas que les enregistrements ne peuvent être inclus dans les notifications par e-mail du profil de notification à moins que quelque chose ne soit effectivement enregistré. Si vous souhaitez intégrer des photos ou des clips vidéos AVI dans les notifications par e-mail, vérifiez que la règle indique que l'enregistrement doit avoir lieu. L'exemple suivant provient d'une règle incluant à la fois l'action **Commencer l'enregistrement** et l'action **Envoyer la notification à** :

Next: Edit the rule description (click an underlined item)

Perform an action on Input Activated  
from Red Sector Door Sensor  
start recording 5 seconds before on Red Sector Entrance Cam  
and Send notification to 'Security: Red Sector Entrance'  
images from Red Sector Entrance Cam

Perform action 10 seconds after  
stop recording immediately

### Profils de notification (propriétés)

Indiquer les propriétés suivantes pour les profils de notification :

Composant	Exigences
Nom	Entrez un nom descriptif pour le profil de notification. Le nom apparaît ensuite lorsque vous

Composant	Exigences
	sélectionnez le profil de notification au cours du processus de création de règle.
<b>Description (facultatif)</b>	Saisissez une description du profil de notification. La description apparaît lorsque vous pointez votre curseur sur le profil de notification, dans la liste <b>Profils de notification</b> du volet Vue d'ensemble.
<b>Destinataires</b>	Entrez les adresses e-mail auxquelles les notifications par e-mail du profil de notification doivent être envoyées. Pour saisir plusieurs adresses e-mail, séparez les adresses par un point-virgule. Exemple : aa@aaa.aa;bb@bbb.bb;cc@ccc.cc
<b>Objet</b>	Entrez le texte que vous souhaitez faire apparaître dans le champ objet d'une notification par e-mail.  Vous pouvez insérer des variables système, telles que le <b>nom du Périphérique</b> , dans le champ de texte message et objet. Pour insérer des variables, cliquez sur les liens de variables requises dans la case située sous le champ.
<b>Texte du message</b>	Saisissez le texte que vous souhaitez faire apparaître dans le corps des notifications par e-mail. Outre le texte du message, le corps de chaque notification par e-mail contient automatiquement l'information suivante : <ul style="list-style-type: none"> <li>• Ce qui a déclenché la notification par e-mail</li> <li>• La source de toute image fixe ou clip vidéo AVI attaché(e)</li> </ul>
<b>Temps entre les e-mails</b>	Spécifiez le temps minimum requis (en secondes) devant s'écouler entre chaque envoi de notification par e-mail. Exemples : <ul style="list-style-type: none"> <li>• Si vous indiquez une valeur de <b>120</b>, 2 minutes minimum s'écoulent entre chaque envoi de notification par e-mail, même si le profil de notification est de nouveau déclenché par une règle avant la fin des 2 minutes</li> <li>• Si vous indiquez une valeur de <b>0</b>, les notifications par e-mail sont envoyées à chaque déclenchement du profil de notification par une règle. Potentiellement, cela peut entraîner un très grand nombre d'envois de notifications par e-mail. Si vous utilisez la valeur <b>0</b>, vous devez ainsi soigneusement décider si vous souhaitez utiliser le profil de notification avec des règles susceptibles d'être déclenchées régulièrement</li> </ul>
<b>Nombre d'images</b>	Indiquez le nombre maximum d'images fixes que vous souhaitez inclure dans chaque notification par e-mail du profil de notification. Par défaut, ce nombre d'images est de cinq.

Composant	Exigences
<b>Temps entre les images (ms)</b>	Spécifiez le nombre de millisecondes désiré entre les enregistrements présentés sur les images incluses. Exemple : Avec une valeur par défaut de 500 millisecondes, les images incluses afficheront les enregistrements présentés espacés d'une demi-seconde.
<b>Temps avant l'événement (sec.)</b>	Ce paramètre est utilisé pour spécifier le début du fichier AVI. Par défaut, le fichier AVI contient les enregistrements débutés 2 secondes avant le déclenchement du profil de notification. Vous pouvez le remplacer par le nombre de secondes requis.
<b>Temps après l'événement (sec.)</b>	Ce paramètre est utilisé pour spécifier la fin du fichier AVI. Par défaut, le fichier AVI prend fin 4 secondes après le déclenchement du profil de notification. Vous pouvez le remplacer par le nombre de secondes requis.
<b>Nombre d'images par seconde</b>	Spécifiez le nombre d'images par seconde que vous souhaitez que le fichier AVI contienne. Par défaut, les images sont au nombre de cinq. Plus la fluidité d'images est élevée, plus la qualité d'image et la taille du fichier AVI sont importantes.
<b>Insérer les images dans l'e-mail</b>	Si sélectionné (par défaut), les images sont insérées dans le corps des notifications par e-mail. Dans le cas contraire, les images sont intégrées en pièces jointes aux notifications par e-mail.

## Événements définis par l'utilisateur

### Événements définis par l'utilisateur (explications)

Si l'événement nécessaire n'est pas sur la liste **Vue d'ensemble des événements**, vous pouvez créer vos propres événements définis par l'utilisateur. Utilisez de tels événements définis par l'utilisateur pour intégrer d'autres systèmes à votre système de surveillance.

Les événements définis par l'utilisateur vous permettent d'utiliser les données provenant d'un système de contrôle d'accès tiers sous forme d'événements dans le système. Les événements peuvent ensuite déclencher des actions. Ainsi, vous pouvez par exemple, commencer à enregistrer une vidéo à partir des caméras pertinentes lorsqu'une personne entre dans un bâtiment.

Vous pouvez également utiliser les événements définis par l'utilisateur dans le cas d'événements à déclenchement manuel tout en visionnant une vidéo en direct dans XProtect Smart Client ou automatiquement s'ils sont utilisés dans des règles. Par exemple, lorsqu'un événement défini par l'utilisateur 37 a lieu, la caméra PTZ 224 doit arrêter de patrouiller et aller sur la position prédéfinie 18.

Au travers des rôles, vous définissez lequel de vos utilisateurs peut déclencher les événements définis par l'utilisateur. Vous pouvez utiliser les événements définis par l'utilisateur de deux manières et en même temps le cas échéant :

Événements	Description
<p><b>Pour fournir la possibilité de déclencher manuellement des événements dans XProtect Smart Client</b></p>	<p>Dans ce cas, les événements définis par l'utilisateur font qu'il est possible pour les utilisateurs finaux de déclencher manuellement des événements tout en visualisant une vidéo en direct dans XProtect Smart Client. Lorsqu'un événement défini par l'utilisateur survient parce qu'il est déclenché manuellement par un utilisateur XProtect Smart Client, une règle peut déclencher qu'une ou plusieurs action(s) doivent se produire sur le système.</p>
<p><b>Pour fournir la possibilité de déclencher des événements au travers d'API</b></p>	<p>Dans ce cas, vous pouvez déclencher les événements définis par l'utilisateur depuis l'extérieur du système de surveillance. L'utilisation des événements définis par l'utilisateur de la manière décrite nécessite l'usage d'une API (Application Program Interface, Un ensemble de blocs de construction pour la création ou la personnalisation d'applications logicielles) séparée lors du déclenchement de l'événement défini par l'utilisateur. L'authentification au travers d'Active Directory est nécessaire pour utiliser de cette manière les événements définis par l'utilisateur. Cela veille à ce que si les événements définis par l'utilisateur peuvent être déclenchés depuis l'extérieur du système de surveillance, seuls les utilisateurs autorisés peuvent le faire.</p> <p>Par ailleurs, les événements définis par l'utilisateur peuvent être associés, via l'API, à des métadonnées, définissant certains périphériques ou groupes de périphériques. Cette fonction est très utile lors de l'emploi d'événements définis par l'utilisateur pour déclencher des règles : vous évitez d'avoir une règle pour chaque périphérique qui finalement fait la même chose. Exemple : Une société utilise un contrôle de l'accès, avec 35 entrées, chacune dotée d'un périphérique de contrôle de l'accès. Lorsqu'un périphérique de contrôle de l'accès est activé, un événement défini par l'utilisateur est déclenché dans le système. Cet événement défini par l'utilisateur est utilisé dans une règle pour lancer l'enregistrement sur une caméra associée au périphérique activé de contrôle de l'accès. La caméra associée à une règle est définie dans les métadonnées. Ainsi, la société n'a pas besoin d'avoir 35 événements définis par l'utilisateur et 35 règles déclenchées par des événements définis par l'utilisateur. Un seul événement défini par l'utilisateur et une seule règle suffisent.</p> <p>Quand vous utilisez des événements définis par l'utilisateur de cette manière, il est possible que vous ne vouliez pas qu'ils soient toujours disponibles au déclenchement manuel dans XProtect Smart Client. Vous pouvez utiliser les rôles pour définir quels événements définis par l'utilisateur doivent être visibles dans XProtect Smart Client.</p>

Quelle que soit la manière dont vous utilisez les événements définis par l'utilisateur, vous devez ajouter chacun de ces événements par le biais du Management Client.



Si vous renommez un événement défini par l'utilisateur, les utilisateurs XProtect Smart Client déjà connectés doivent se déconnecter et se reconnecter avant que le changement de nom soit visible.



Si vous supprimez un événement défini par l'utilisateur, les règles dans lesquelles l'événement défini par l'utilisateur est utilisé sont affectées. De la même manière, un événement défini par l'utilisateur effacé disparaît de XProtect Smart Client seulement après déconnexion des utilisateurs XProtect Smart Client.

### Ajouter un événement défini par l'utilisateur

1. Développez **Règles et événements** > **Événements définis par l'utilisateur**.
2. Dans le volet **Vue d'ensemble**, faites un clic droit sur **Événements** > **Ajouter un événement défini par l'utilisateur**.
3. Saisissez un nom pour le nouvel événement défini par l'utilisateur et cliquez sur **OK**. L'événement défini par l'utilisateur nouvellement ajouté apparaît désormais dans la liste du volet **Vue d'ensemble**.

L'utilisateur peut désormais déclencher l'événement défini par l'utilisateur manuellement dans XProtect Smart Client s'il possède les droits correspondants.

### Renommer un événement défini par l'utilisateur

1. Développez **Règles et événements** > **Événements définis par l'utilisateur**.
2. Dans le volet **Vue d'ensemble**, sélectionnez l'événement défini par l'utilisateur.
3. Dans le volet **Propriétés**, remplacez le nom existant.
4. Dans la boîte à outils, cliquez sur **Enregistrer**.

## Événements analytiques

### Événements analytiques (explications)

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

L'utilisation d'événements analytiques comme base des alarmes est un processus à trois étapes :

- La première : activation de la fonction événements analytiques et configuration de sa sécurité. Utilisez une liste d'adresses autorisées pour contrôler les expéditeurs de données d'événements au système et le port d'écoute du serveur
- La deuxième : création d'un événement analytique, éventuellement avec une description de l'événement, et test
- La troisième : utilisation de l'événement analytique comme source de définition d'une alarme

Vous pouvez configurer les événements analytiques dans la liste **Règles et événements** du volet **Navigation sur le site**.

Pour utiliser des événements basés VCA, un outil VCA tiers est nécessaire pour fournir les données au système. Le choix de l'outil VCA à utiliser vous revient, tant que les données fournies par l'outil respectent le format. Ce format est expliqué dans la [Documentation de MIP SDK](#) sur des événements analytiques.

Contactez le fournisseur de votre système pour en savoir plus. Les outils VCA tiers sont développés par des partenaires indépendants proposant des solutions basées sur une plate-forme ouverte Milestone. Ces solutions peuvent avoir un impact sur les performances du système.

### Ajouter et modifier un événement analytique

#### Ajouter un événement analytique

1. Développez **Règles et événements**, faites un clic droit sur **Événements analytiques**, puis sélectionnez **Ajouter nouveau**.
2. Dans la fenêtre **Propriétés**, saisissez un nom pour le nouveau profil de temps dans le champ **Nom**.
3. Saisissez un texte de description dans le champ **Description** le cas échéant.
4. Dans la boîte à outils, cliquez sur **Enregistrer**. Vous pouvez tester la validité de l'événement en cliquant sur **Événement test**. Vous pouvez à chaque instant corriger les erreurs signalées dans le test et effectuer le test autant de fois que vous le souhaitez et à n'importe quel moment du processus.

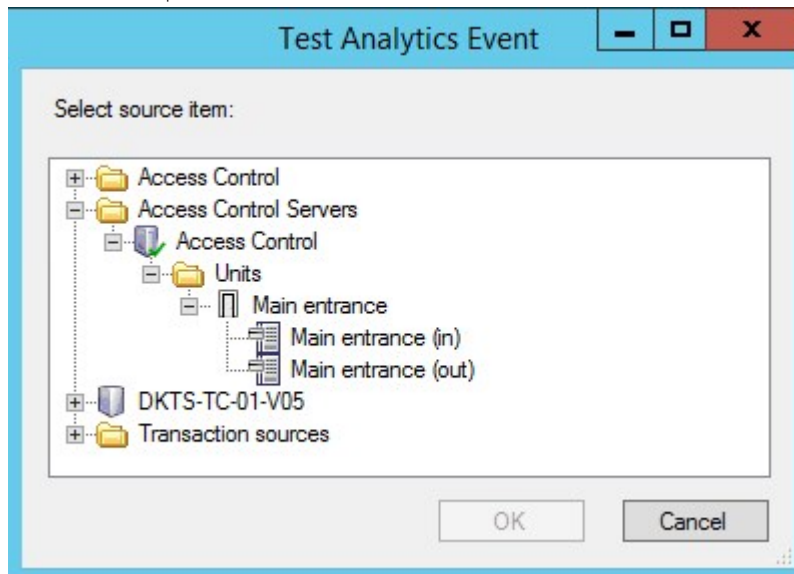
#### Modifier un événement analytique

1. Cliquez sur un événement analytique existant pour afficher la fenêtre **Propriétés** dans laquelle vous pouvez modifier les champs concernés.
2. Vous pouvez tester la validité de l'événement en cliquant sur **Événement test**. Vous pouvez à chaque instant corriger les erreurs signalées dans le test et effectuer le test autant de fois que vous le souhaitez et à n'importe quel moment du processus.

### Tester un événement analytique

Après avoir créé un événement analytique, vous pouvez tester les exigences (voir Événement analytique test (propriétés) sur la page 360), par exemple vérifier si la fonction événements analytiques a été activée dans Management Client.

1. Sélectionnez un événement analytique existant.
2. Dans les propriétés, cliquez sur le bouton **Évènement test**. Une fenêtre s'ouvre affichant toutes les sources d'événements possibles.



3. Sélectionnez la source de votre événement test, par exemple une caméra. La fenêtre se ferme et une nouvelle fenêtre s'ouvre et passe par quatre différents stades qui doivent être respectés pour que l'événement analytique fonctionne.



Comme autre test, vous pouvez dans XProtect Smart Client vérifier si l'événement analytique a été envoyé au serveur d'événement. Pour ce faire, ouvrez XProtect Smart Client et affichez l'événement dans l'onglet **Gestionnaire d'alarme**.

### Voir également

Événements analytiques (explications) sur la page 358

### Événement analytique test (propriétés)

Lorsque vous testez les exigences d'un événement analytique, une fenêtre s'ouvre et vérifie quatre stades et fournit les descriptions des erreurs et les solutions possibles.



Condition	Description	Messages d'erreur et solutions
<b>Changements sauvegardés</b>	Si l'événement est nouveau, est-il sauvegardé ? Ou si le nom de l'événement a été modifié, ces modifications sont-elles enregistrées ?	<b>Sauvegarde des changements avant le test de l'événement analytique.</b> Solution/explication : Enregistrer les modifications.
<b>Événements d'analyse activés</b>	La fonction Évènement d'analyse est-elle activée ?	<b>Les événements analytiques n'ont pas été activés.</b> Solution/explication : Activez la fonction Évènements d'analyse. Pour faire cela, cliquez sur <b>Outils &gt; Options &gt; Événements analytiques</b> et cochez la case <b>Activé</b> .
<b>Adresse permise</b>	L'adresse IP ou le nom d'hôte de la machine qui envoie le ou les événement(s) est-il/elle autorisé(e) (indiqué(e) dans la liste d'adresses des événements d'analyse) ?	<b>Le nom d'hôte local doit être ajouté comme adresse autorisée pour le service d'événements d'analyse.</b> Solution/explication : Ajoutez votre machine à la liste d'adresse des événements analytiques des adresses IP ou noms d'hôtes autorisés.  <b>Erreur lors de la résolution de l'hôte local.</b> Solution/explication : L'adresse IP ou le nom d'hôte de la machine est introuvable ou incorrect.
<b>Envoi d'événement analytique</b>	L'envoi d'un événement test au serveur d'évènements a-t-il réussi ?	Voir le tableau ci-dessous.

Chaque étape porte la mention Échec :  ou réussite : .

Messages d'erreur et solutions pour la condition **Envoi d'événement analytique** :

Message d'erreur	Solution
<b>Serveur d'événements introuvable</b>	Impossible de trouver le serveur d'évènements sur la liste des services inscrits.

Message d'erreur	Solution
<b>Erreur lors de la connexion au serveur d'événements</b>	Impossible de se connecter au serveur d'événement sur le port défini. L'erreur est sûrement le résultat de problèmes de réseau ou de l'interruption du service du Event Server.
<b>Erreur lors de l'envoi de l'événement analytique</b>	La connexion au serveur d'événement a été établie mais il est impossible d'envoyer l'événement. Probablement en raison d'un problème de réseau, un dépassement du délai par exemple.
<b>Erreur lors de la réception de la réponse du serveur d'événements</b>	L'événement a été envoyé au serveur d'événement mais aucune réponse n'a été reçue. L'erreur est sûrement le résultat d'un problème de réseau ou d'un port occupé.  Reportez-vous au journal du serveur d'événements, généralement situé sous <i>ProgramData\Milestone\XProtect Event Server\Logs\</i> .
<b>Événement analytique inconnu du serveur d'événements</b>	Le service Event Server ne connaît pas cet événement. La raison la plus probable à cela est que l'événement ou des modifications apportées à l'événement n'ont pas été enregistrés.
<b>Événement analytique reçu par le serveur d'événements</b>	Le format de l'événement est incorrect.
<b>Expéditeur non autorisé par le serveur d'événements</b>	Le plus probable est que votre machine ne figure pas dans la liste des d'adresses IP ou noms d'hôtes autorisés.
<b>Erreur interne dans le serveur d'événements</b>	Erreur de serveur d'événements.  Reportez-vous au journal du serveur d'événements, généralement situé sous <i>ProgramData\Milestone\XProtect Event Server\Logs\</i> .
<b>Réponse du serveur d'événements invalide</b>	La réponse n'est pas valide. Le port est peut-être occupé ou il y a des problèmes réseau.  Reportez-vous au journal du serveur d'événements, généralement situé sous <i>ProgramData\Milestone\XProtect Event Server\Logs\</i> .
<b>Réponse inconnue du serveur d'événements</b>	La réponse est valide mais incompréhensible. L'erreur est sûrement le résultat d'un problème de réseau ou d'un port occupé.

Message d'erreur	Solution
	Reportez-vous au journal du serveur d'événements, généralement situé sous <i>ProgramData\Milestone\XProtect Event Server\Logs\</i> .
<b>Erreur imprévue</b>	Veuillez contacter l'assistance Milestone pour obtenir de l'aide.

### Modifier les paramètres des événements analytiques

Dans la barre d'outils, allez dans **Outils > Options > Événements analytiques** pour modifier les paramètres pertinents.

## Événements génériques

### Événements génériques (explications)



Cette fonction ne fonctionne pas si vous n'avez pas installé au préalable le serveur d'événements XProtect.

Les événements génériques vous permettent de déclencher des actions sur le serveur d'événements XProtect en envoyant des chaînes simples via le réseau IP à votre système.

Vous pouvez utiliser tout matériel ou logiciel qui peut envoyer des chaînes via TCP ou UDP pour déclencher des événements génériques. Votre système peut analyser des paquets de données TCP ou UDP reçus et déclencher automatiquement des événements génériques si les critères spécifiques sont satisfaits. De cette manière, vous pouvez intégrer votre système avec des sources externes, par exemple des sources de contrôle d'accès et des systèmes d'alarme. Le but est d'autoriser autant de sources externes que possible pour interagir avec le système.

Grâce au concept des sources de données, vous évitez d'avoir à adapter les outils tiers pour répondre aux normes de votre système. Les sources de données vous permettent de communiquer avec un matériel ou un logiciel particulier sur un port IP spécifique et d'affiner la manière dont le nombre d'octets qui arrivent sur ce port sont interprétés. Chaque type d'événement générique s'associe à une source de données et crée un langage utilisé pour la communication avec une partie de matériel ou de logiciel précise.

Le fait de travailler avec des sources de données nécessite une connaissance générale de la mise en réseau IP, outre une connaissance spécifique du logiciel et du matériel à partir duquel vous souhaitez créer l'interface. Il existe plusieurs paramètres que vous pouvez utiliser et aucune solution prête à l'emploi pour savoir comment faire. En fait, votre système fournit les outils et non pas la solution. Au contraire des événements définis par l'utilisateur, les événements génériques n'ont pas d'authentification. Ainsi, ils sont plus faciles à déclencher, mais afin d'éviter de nuire à la sécurité, seuls les événements provenant de l'hôte local sont acceptés. Vous pouvez autoriser d'autres adresses IP clients depuis l'onglet **Événements génériques** du menu **Options**.

## Ajouter un événement générique

Vous pouvez définir des événements génériques pour aider le VMS à reconnaître des chaînes spécifiques dans les paquets TCP ou UDP à partir d'un système externe. En fonction d'un événement générique, vous pouvez configurer Management Client pour déclencher des actions, par exemple démarrer un enregistrement ou des alarmes.

### Configuration

Vous avez des événements génériques activés et avez précisé les destinations sources autorisées. Pour plus d'informations, voir Onglet Événements génériques (options) sur la page 135.

Pour ajouter un événement générique :

1. Déroulez **Règles et événements**.
2. Cliquez avec le bouton droit sur **Événements génériques** et sélectionnez **Ajouter un nouvel**.
3. Remplissez les informations et propriétés nécessaires. Pour plus d'informations, voir Événements génériques (propriétés) sur la page 364.
4. (facultatif) Pour valider que l'expression de la recherche est valide, saisissez une chaîne de recherche dans le champ **Contrôler si l'expression correspond à la chaîne de l'expression** correspondant aux paquets attendus :
  - **Correspondance** - la chaîne peut être validée par rapport à l'expression de la recherche
  - **Aucune correspondance** - l'expression de la recherche est invalide. Modifiez-la et réessayez



Dans XProtect Smart Client, vous pouvez vérifier si vos événements génériques ont été reçus par le serveur d'événement. Vous le faites dans la **Liste des alarmes** dans l'onglet **Gestionnaire des alarmes** en sélectionnant **Événements**.

## Événements génériques (propriétés)

Composant	Exigences
<b>Nom</b>	Nom unique pour l'événement générique. Le nom doit être unique parmi tous les types d'événements, tels que les événements définis par l'utilisateur, les événements analytiques, etc.
<b>Activé</b>	Par défaut, les événements génériques sont activés. Supprimez la coche pour désactiver l'événement.

Composant	Exigences
Expression	<p>Expression que le système doit chercher lors de l'analyse de paquets de données. Vous pouvez vous servir des opérateurs suivants :</p> <ul style="list-style-type: none"> <li>• <b>( )</b>: Utilisés pour garantir le traitement de termes associés en tant qu'unité logique. Ils peuvent être utilisés pour imposer un certain ordre de traitement au cours de l'analyse</li> </ul> <p><b>Exemple</b> : Les critères de recherche « <b>(Utilisateur001 OU Porte053) ET Dimanche</b> » traitent les deux termes entre parenthèses en premier, puis le résultat est combiné à la dernière partie de la chaîne. Ainsi, le système cherche tout d'abord n'importe quel paquet contenant les termes <b>Utilisateur001</b> ou <b>Porte053</b>, puis il analyse les résultats pour voir quels paquets contiennent également le mot <b>Dimanche</b>.</p> <ul style="list-style-type: none"> <li>• <b>ET</b> : Avec un opérateur ET, vous indiquez que les termes des deux côtés de l'opérateur ET doivent être présents</li> </ul> <p><b>Exemple</b> : Les critères de recherche « <b>Utilisateur001 ET Porte053 ET Dimanche</b> » ne renvoient un résultat que si les termes <b>Utilisateur001</b>, <b>Porte053</b> et <b>Dimanche</b> sont inclus dans votre expression. Il ne suffit pas qu'un ou deux des termes soient présents. Plus vous combinez de termes avec ET, moins vous obtenez de résultats.</p> <ul style="list-style-type: none"> <li>• <b>OU</b> : Avec un opérateur OU, vous indiquez que l'un ou l'autre terme doit être présent</li> </ul> <p><b>Exemple</b> : Les critères de recherche « <b>Utilisateur001 OR Porte053 OR Dimanche</b> » renvoient tous les résultats contenant <b>Utilisateur001</b>, <b>Porte053</b> ou <b>Dimanche</b>. Plus vous combinez de termes avec OU, plus vous obtenez de résultats.</p>
Type d'expression	<p>Indique le degré de particularité du système lors de l'analyse des paquets de données reçus. Les options sont les suivantes :</p> <ul style="list-style-type: none"> <li>• <b>Rechercher</b> : Pour que l'événement ait lieu, le paquet de données reçu doit contenir le texte indiqué dans le champ <b>Expression</b>, bien qu'il puisse avoir également plus de contenu</li> </ul> <p><b>Exemple</b> : Si vous avez indiqué que le paquet reçu devait contenir les termes <b>Utilisateur001</b> et <b>Porte053</b>, l'événement est déclenché si le paquet reçu contient les termes <b>Utilisateur001</b> et <b>Porte053</b> et <b>Dimanche</b> car vos deux termes requis sont contenus dans le paquet reçu</p> <ul style="list-style-type: none"> <li>• <b>Correspondance</b> : Pour que l'événement ait lieu, le paquet de données reçu doit contenir exactement le texte indiqué dans le champ <b>Expression</b> et rien d'autre</li> </ul>

Composant	Exigences
	<ul style="list-style-type: none"> <li>• <b>Expression standard</b> : Pour que l'événement ait lieu, le texte indiqué dans le champ <b>Expression</b> doit identifier des modèles particuliers dans les paquets de données reçus</li> </ul> <p>Si vous passez de <b>Rechercher</b> ou <b>Correspondance</b> à <b>Expression standard</b>, le texte dans le champ <b>Expression</b> est automatiquement traduit par une expression standard.</p>
<b>Priorité</b>	<p>La priorité doit être indiquée par un nombre compris entre 0 (priorité la plus faible) et 999999 (priorité la plus élevée).</p> <p>Le même paquet de données peut être analysé pour différents événements. La possibilité d'attribuer une priorité à chaque événement vous permet de gérer l'événement qui doit être déclenché si un paquet reçu correspond aux critères pour plusieurs événements.</p> <p>Lorsque le système reçoit un paquet TCP et/ou UDP, l'analyse du paquet commence par l'analyse de l'événement à la priorité la plus élevée. Ainsi, lorsqu'un paquet correspond aux critères pour plusieurs événements, seul l'événement à la priorité la plus élevée est déclenché. Si un paquet correspond aux critères pour plusieurs événements avec une priorité identique, par ex. deux événements avec une priorité à 999, tous les événements avec cette priorité sont déclenchés.</p>
<b>Vérifier si l'expression correspond à la chaîne d'événement</b>	<p>Une chaîne d'événement à tester par rapport à l'expression saisie dans le champ <b>Expression</b>.</p>

### Source de données d'un événement générique (propriétés)

Composant	Exigences
<b>Source de données</b>	<p>Vous pouvez choisir entre deux sources de données par défaut et définir une source de données personnalisée. Votre choix dépend du type de votre programme tiers et/ou du type de matériel ou logiciel à partir duquel vous souhaitez établir une interface :</p>

Composant	Exigences
	<p><b>Compatible</b> : Les propriétés par défaut sont activées, écho de tous les octets, TCP et UDP, IPv4 uniquement, port 1234, aucun séparateur, hôte local uniquement, encodage de pages de codes actuel (ANSI).</p> <p><b>International</b> : Les propriétés par défaut sont activées, écho des statistiques uniquement, TCP uniquement, IPv4+6, port 1235, &lt;CR&gt;&lt;LF&gt; comme séparateur, hôte local uniquement, encodage UTF-8. (&lt;CR&gt;&lt;LF&gt; = 13,10).</p> <p>[Source de données A]</p> <p>[Source de données B]</p> <p>etc.</p>
<b>Nouveau</b>	Cliquez pour créer une nouvelle source de données.
<b>Nom</b>	Nom de la source de données.
<b>Activé</b>	Par défaut, les sources de données sont activées. Décochez la case pour désactiver la source de données.
<b>Réinitialiser</b>	Cliquez pour réinitialiser tous les paramètres de la source de données sélectionnée. Le nom saisi dans le champ <b>Nom</b> est conservé.
<b>Port</b>	Le numéro de port de la source de données.
<b>Sélecteur type de protocole</b>	<p>Les protocoles que le système doit écouter et analyser en vue de détecter les événements génériques :</p> <p><b>Tout</b> : TCP aussi bien que UDP.</p> <p><b>TCP</b> : TCP uniquement.</p> <p><b>UDP</b> : UDP uniquement.</p> <p>Les paquets TCP et UDP utilisés pour les événements génériques peuvent contenir des caractères spéciaux, tels que @, #, +, ~, etc.</p>
<b>Sélecteur type IP</b>	Types d'adresses IP à sélectionner : IPv4, IPv6 ou les deux.
<b>Octets de séparation</b>	Sélectionnez les octets séparateurs utilisés pour séparer les enregistrements d'événements génériques individuels. Le type de source de données <b>International</b> par défaut (voir Source de données sur la page 366) est <b>13,10</b> . (13,10 = <CR><LF>).

Composant	Exigences
Sélecteur type d'écho	<p>Formats de retour d'écho disponibles :</p> <ul style="list-style-type: none"> <li>• <b>Statistiques d'écho</b> : Renvoie le format suivant : <b>[X],[Y],[Z],[Nom de l'événement générique]</b>  [X] = numéro de demande.  [Y] = nombre de caractères.  [Z] = nombre de concordances avec un événement générique.  <b>[Nom de l'événement générique]</b> = nom saisi dans le champ <b>Nom</b></li> <li>• <b>Écho de tous les octets</b> : Produit un écho de tous les octets</li> <li>• <b>Pas d'écho</b> : Supprime tous les échos</li> </ul>
Sélecteur type d'encodage	Par défaut, la liste affiche uniquement les options les plus pertinentes. Cochez la case <b>Afficher tout</b> pour afficher toutes les options de codage à disposition.
Afficher tout	Cf. le point précédent.
Adresses IPv4 externes autorisées	Spécifiez les adresses IP avec lesquelles le serveur de gestion doit pouvoir communiquer afin de gérer les événements externes. Vous pouvez également utiliser cette fonction pour exclure les adresses IP dont vous ne souhaitez pas recevoir de données.
Adresses IPv6 externes autorisées	Spécifiez les adresses IP avec lesquelles le serveur de gestion doit pouvoir communiquer afin de gérer les événements externes. Vous pouvez également utiliser cette fonction pour exclure les adresses IP dont vous ne souhaitez pas recevoir de données.



Les plages peuvent être précisées dans chacune des quatre positions telles que **100, 105, 110-120**. Par exemple, toutes les adresses sur le réseau 10.10 peuvent être autorisées par **10.10.[0-254].[0-254]** ou par **10.10.255.255**.

## Navigation sur le site : Sécurité

Cet article décrit comment créer des utilisateurs basiques et comment configurer des rôles, spécifier des droits d'utilisateur pour un rôle et assigner des utilisateurs.



## Rôles (explications)

Les rôles déterminent les périphériques auxquels les utilisateurs peuvent accéder. Les rôles déterminent également les droits et assurent la sécurité au sein du système de gestion vidéo. Vous devez tout d'abord ajouter des rôles, puis ajouter des utilisateurs et des groupes et enfin, ajouter un profil Smart Client et un profil Management Client ainsi que d'autres profils par défaut appartenant à chaque rôle. Les rôles que vous pouvez créer dans le système disposent de leurs propres groupes de vues dans XProtect Smart Client, dans lesquels leurs vues sont créées et stockées.



Il est important que tous les rôles activent le niveau de sécurité Management Server **Se connecter situé** dans **Paramètres des rôles > Management Server > Onglet Sécurité globale (rôles)** sur la page 377.

Vous ajoutez des utilisateurs et groupes au rôle **Administrateurs** tout comme vous le feriez pour tout autre rôle. Voir Assigner et supprimer des utilisateurs et groupes aux/des rôles sur la page 373).

Outre le rôle **Administrateurs**, vous pouvez ajouter autant de rôles que nécessaire en fonction de vos besoins. Vous pourriez, par exemple, avoir des rôles différents pour les utilisateurs de XProtect Smart Client en fonction des caméras auxquelles vous souhaitez qu'ils puissent accéder ou d'autres restrictions d'ordre similaire. Pour configurer les rôles dans votre système, développez le menu **Sécurité > Rôles**.

## Droits d'un rôle (explications)

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

Lorsque vous créez un rôle dans votre système, vous pouvez lui donner un nombre de droits vis-à-vis des composants ou fonctions du système auxquels le rôle en question peut accéder ou qu'il peut utiliser. Vous pouvez par exemple créer des rôles qui disposent uniquement des droits relatifs aux fonctions de XProtect Smart Client ou d'autres clients d'affichage Milestone, avec les droits nécessaires pour ne voir que certaines caméras. Si vous créez de tels rôles, ces rôles ne doivent pas avoir de droits d'accès et d'utilisation du Management Client, mais avoir uniquement accès à une partie ou à l'intégralité des fonctions disponibles dans XProtect Smart Client ou dans d'autres clients. Pour adresser ce problème, vous souhaitez peut-être configurer un rôle disposant de certains des droits d'administrateur les plus courants, comme, par exemple, les droits d'ajout et de suppression de caméras, de serveurs et autres fonctions similaires.

Vous pouvez créer des rôles qui disposent d'une partie ou de l'intégralité des droits d'un administrateur système. Par exemple, ceci peut s'avérer pertinent si votre organisation souhaite faire la distinction entre les personnes pouvant gérer un sous-ensemble du système et les personnes qui peuvent gérer l'ensemble du système. Cette fonction vous permet de fournir des permissions différenciées aux administrateurs de façon à ce qu'ils puissent accéder à une large gamme de fonctions système, les modifier ou encore les changer, comme, par exemple, le droit de modifier les paramètres des serveurs ou caméras de votre système. Ces permissions sont spécifiées sur l'onglet Sécurité globale (voir Onglet Sécurité globale (rôles) sur la page 377). Au minimum, pour permettre à l'administrateur du système différencié de lancer le Management Client, vous devez accorder des permissions Lire à ce rôle sur le serveur de gestion.



Il est important que tous les rôles activent le niveau de sécurité Management Server **Se connecter** situé dans **Paramètres des rôles > Management Server > Onglet Sécurité globale (rôles)** sur la page 377.

Vous pouvez également refléter ces restrictions dans l'interface utilisateur du Management Client pour chaque rôle en associant le rôle à un profil Management Client supprimant les fonctions système correspondantes de l'interface utilisateur. Voir Navigation sur le site : Clients : Profils Management Client sur la page 305 pour plus d'informations.

Pour doter un rôle de tels droits d'administrateur différenciés, la personne détentrice du rôle d'administrateur complet par défaut doit installer le rôle dans **Sécurité > Rôles > Onglet info > Ajouter nouveau**. Lorsque vous configurez le nouveau rôle, vous pouvez ensuite associer le rôle à vos propres profils comme vous le feriez pour tout autre rôle dans le système, ou utiliser les profils par défaut du système. Pour de plus amples informations, voir Ajouter et gérer un rôle sur la page 372.

Une fois que vous avez spécifié les profils que vous souhaitez associer au rôle, allez dans l'onglet **Sécurité globale** pour spécifier les droits du rôle.



Les droits que vous pouvez configurer pour un rôle sont différents d'un produit à l'autre. Vous ne pouvez accorder tous les droits disponibles à un rôle que dans XProtect Corporate.

## Utilisateurs (explications)

Le terme **utilisateurs** fait principalement référence aux utilisateurs en mesure de se connecter au système de surveillance par le biais des clients. Vous pouvez configurer ces utilisateurs des deux manières suivantes :

- En tant qu'**utilisateurs basiques**, authentifiés par une combinaison nom d'utilisateur/mot de passe
- En tant qu'**utilisateurs Windows**, authentifiés à partir de leurs identifiants de connexion Windows.

### Utilisateurs Windows

Vous pouvez ajouter des utilisateurs Windows en utilisant Active Directory. Active Directory (AD) est un service d'annuaire mis en œuvre par Microsoft pour les réseaux avec domaine Windows. Il est inclus dans la plupart des systèmes d'exploitation Windows Server. Il identifie les ressources sur un réseau afin que les utilisateurs ou applications puissent y accéder. L'Active Directory utilise les concepts d'utilisateurs et de groupes.

Les utilisateurs sont des objets de l'Active Directory représentant des individus avec un compte utilisateur. Exemple :



Les groupes sont des objets de l'Active Directory contenant plusieurs utilisateurs. Dans cet exemple, le Groupe d'administration compte trois utilisateurs :



Les groupes peuvent contenir un nombre illimité d'utilisateurs. En ajoutant un groupe au système, vous ajoutez tous ses membres en même temps. Une fois que vous avez ajouté le groupe au système, toute modification effectuée ultérieurement sur le groupe dans l'Active Directory, lorsque vous ajoutez de nouveaux membres ou supprimez d'anciens membres ultérieurement par exemple, sera immédiatement reflétée dans le système. Un utilisateur peut être un membre appartenant à plusieurs groupes en même temps.

Vous pouvez utiliser Active Directory pour ajouter au système des informations existantes sur les utilisateurs et groupes et en tirer des avantages :

- Les utilisateurs et groupes sont spécifiés centralement dans Active Directory. Vous n'avez donc pas à créer des comptes utilisateur à partir de rien
- Vous n'avez pas besoin de configurer l'authentification des utilisateurs du système car Active Directory prend l'authentification en charge

Avant que vous puissiez ajouter des utilisateurs et groupes par le biais du service Active Directory, vous devez disposer d'un serveur doté d'Active Directory installé sur votre réseau.

## Utilisateurs

Si votre système ne dispose pas d'un accès à Active Directory, créez un utilisateur basique (voir Utilisateurs (explications) sur la page 370). Pour obtenir des informations sur la configuration des utilisateurs basiques, voir Créer un utilisateur basique (voir Créer des utilisateurs de base sur la page 420).

## Ajouter et gérer un rôle

1. Développez **Sécurité**, et cliquez avec le bouton droit sur **Rôles**.
2. Sélectionnez **Ajouter un rôle**. La boîte de dialogue **Ajouter rôle** s'ouvre.
3. Saisissez un nom et une description du nouveau rôle puis cliquez sur **OK**.
4. Le nouveau rôle est ajouté à la liste **Rôles**. Par défaut, un nouveau rôle n'est associé à aucun utilisateur/groupe, mais est associé à divers profils par défaut.
5. Pour choisir des profils Smart Client et Management Client différents, des profils de verrouillage des preuves ou des profils de temps, cliquez sur les menus déroulants.
6. Vous pouvez maintenant assigner les utilisateurs/groupes au rôle, et spécifier à quelles fonctions du système ils peuvent accéder.

Pour de plus amples informations, veuillez consulter la section Assigner et supprimer des utilisateurs et groupes aux/des rôles sur la page 373 et Paramètres des rôles sur la page 374.

## Copier, renommer ou supprimer un rôle

### Copier un rôle

Si vous avez un rôle avec des paramètres et/ou droits complexes et qu'il vous faut un rôle similaire ou quasi similaire, il peut être plus simple de copier le rôle déjà existant et d'apporter de petites modifications à la copie plutôt que de créer un nouveau rôle à partir de zéro.

1. Développez le menu **Sécurité**, cliquez sur **Rôles**, faites un clic droit sur le rôle pertinent et sélectionnez **Copier Rôle**.
2. Dans la boîte de dialogue qui s'ouvre, donnez au rôle copié un nouveau nom spécifique ainsi qu'une description.
3. Cliquez sur **OK**.

### Renommer un rôle

Si vous renommez un rôle, cela ne modifie pas le nom du groupe de vues basé sur le rôle.

1. Développez **Sécurité**, et cliquez avec le bouton droit sur **Rôles**.
2. Faites un clic droit sur le rôle requis et sélectionnez **Renommer Rôle**.
3. Dans la boîte de dialogue qui s'ouvre, modifiez le nom du rôle.
4. Cliquez sur **OK**.

## Supprimer un rôle

1. Développez **Sécurité**, et cliquez sur **Rôles**.
2. Cliquez avec le bouton droit sur le rôle indésirable, puis sélectionnez **Supprimer**.
3. Cliquez sur **Oui**.



Si vous supprimez un rôle, vous ne supprimez pas automatiquement le groupe de vues basé sur le rôle.

## Assigner et supprimer des utilisateurs et groupes aux/des rôles

Pour assigner ou supprimer des utilisateurs Windows ou groupes ou des utilisateurs de base à/d'un rôle :

1. Développez **Sécurité**, et cliquez avec le bouton droit sur **Rôles**. Ensuite, sélectionnez le rôle requis dans le volet **Vue d'ensemble** :
2. Dans le **panneau Propriétés**, sélectionnez l'onglet **Utilisateurs et Groupes** en bas.
3. Cliquez sur **Ajouter**, sélectionnez **Utilisateur Windows** ou **Utilisateur de base**.

### Assigner des utilisateurs Windows et groupes à un rôle

1. Sélectionner **Utilisateur Windows**. Cela ouvre la boîte de dialogue **Sélectionner des utilisateurs, ordinateurs et groupes** :
2. Vérifiez que le type d'objet requis est spécifié. Si, par exemple, il vous faut ajouter un ordinateur, cliquez sur **Types d'objet** et indiquez **Ordinateur**. Vérifiez également que le domaine requis figure dans le champ **À partir de cet emplacement**. Dans le cas contraire, cliquez sur le bouton **Emplacements** afin de rechercher le domaine requis.
3. Dans la case **Entrer les noms d'objet à sélectionner**, saisissez les noms des utilisateurs, initiales, ou autres types d'identifiant pertinents que l'Active Directory peut reconnaître. Utilisez la fonction **Vérifier les noms** pour vérifier qu'Active Directory reconnaît bien les noms ou initiales que vous avez saisis. Sinon, utilisez la fonction « **Avancée...** » pour rechercher des utilisateurs ou des groupes.
4. Cliquez sur **OK**. Les utilisateurs/ groupes sélectionnés sont maintenant ajoutés à la liste des utilisateurs de l'onglet **Utilisateurs et Groupes** que vous avez assignés au rôle sélectionné. Vous pouvez ajouter plus d'utilisateurs et de groupes en saisissant plusieurs noms séparés par un point-virgule (;).

### Assigner des utilisateurs de base à un rôle

1. Sélectionner un **utilisateur basique**. Cela ouvre la boîte de dialogue **Sélectionner des utilisateurs de base à ajouter au rôle** :
2. Sélectionnez le(s) utilisateur(s) basique(s) que vous souhaitez assigner à ce rôle.

3. Facultatif : Cliquez sur **Nouveau** pour créer une nouvelle source de données.
4. Cliquez sur **OK**. Les utilisateurs basiques sélectionnés sont maintenant ajoutés à la liste des utilisateurs basiques de l'onglet **Utilisateurs et Groupes** qui ont été assignés au rôle sélectionné.

### Supprimer des utilisateurs et groupes d'un rôle

1. Dans l'onglet **Utilisateurs et Groupes**, sélectionnez l'utilisateur ou le groupe que vous souhaitez supprimer et cliquez sur le bouton **Supprimer** en bas de l'onglet. Vous pouvez sélectionner plusieurs utilisateurs ou groupes, ou une combinaison de groupes et d'utilisateurs individuels, le cas échéant.
2. Confirmez que vous souhaitez supprimer le ou les utilisateur(s) et/ou groupe(s). Cliquez sur **Oui**.



Un utilisateur peut également avoir des rôles au travers d'appartenances à des groupes. Auquel cas, vous ne pouvez supprimer l'utilisateur individuel du rôle. Par ailleurs, les membres de groupes peuvent également avoir des rôles en tant qu'individus. Pour voir les rôles que les utilisateurs, groupes, ou membres individuels d'un groupe ont, utilisez la fonction **Afficher les rôles effectifs**.

### Afficher les rôles effectifs

Grâce à la fonction Rôles effectifs, vous pouvez afficher tous les rôles d'un utilisateur ou groupe sélectionné. Ceci peut s'avérer pratique si vous utilisez des groupes et qu'il s'agit de leur moyen de voir à quels rôles un utilisateur spécifique est affilié.



1. Ouvrez la fenêtre **Rôles effectifs** en développant **Sécurité**, puis faites un clic droit sur **Rôles et sélectionnez Rôles effectifs**.
2. Si vous voulez en savoir plus sur un utilisateur basique, saisissez le nom dans le champ **Nom d'utilisateur**. Cliquez sur **Réactualiser** pour afficher les rôles de l'utilisateur.
3. Si vous utilisez des utilisateurs ou des groupes Windows dans Active Directory, cliquez sur le bouton de navigation "...". Sélectionnez le type d'objet, entrez le nom et cliquez sur **OK**. Les rôles d'utilisateur s'affichent automatiquement.

### Paramètres des rôles

#### Onglet Info (rôles)

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

Dans l'onglet **Info** d'un rôle, vous pouvez configurer les éléments suivants :

Nom	Description
<b>Nom</b>	Saisissez un nom pour le rôle.
<b>Description</b>	Saisissez une description pour le rôle.
<b>Profil Management Client</b>	<p>Sélectionnez un profil Management Client pour l'associer au rôle.</p> <p>Vous ne pouvez pas appliquer ceci au rôle d'<b>Administrateurs</b> par défaut.</p> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #0070c0;">  Nécessite une autorisation pour gérer la sécurité du serveur de gestion.                 </div>
<b>Profil Smart Client</b>	<p>Sélectionnez un profil Smart Client pour l'associer au rôle.</p> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #0070c0;">  Nécessite une autorisation pour gérer la sécurité du serveur de gestion.                 </div>
<b>Profil de temps par défaut</b>	<p>Sélectionnez un profil de temps par défaut pour l'associer au rôle.</p> <p>Vous ne pouvez pas appliquer ceci au rôle d'<b>Administrateurs</b> par défaut.</p>
<b>Profil de verrouillage des preuves</b>	Sélectionnez un profil de protection des preuves pour l'associer au rôle.
<b>Connexion Smart Client au sein du profil de temps</b>	<p>Sélectionnez un profil de temps pour lequel l'utilisateur XProtect Smart Client associé à ce rôle est autorisé à se connecter.</p> <p>Si l'utilisateur XProtect Smart Client est connecté lorsque la période prend fin, il ou elle est alors déconnecté(e) automatiquement.</p> <p>Vous ne pouvez pas appliquer ceci au rôle d'<b>Administrateurs</b> par défaut.</p>
<b>Autoriser la connexion au Smart Client</b>	<p>Cochez la case pour permettre aux utilisateurs associés à ce rôle de se connecter au XProtect Smart Client.</p> <p>L'accès au Smart Client est autorisé par défaut. Décochez la case pour refuser l'accès au XProtect Smart Client.</p>
<b>Autoriser la connexion au client XProtect</b>	Cochez la case pour permettre aux utilisateurs associés à ce rôle de se connecter au client XProtect Mobile.

Nom	Description
<b>Mobile</b>	L'accès au client XProtect Mobile est autorisé par défaut. Décochez la case pour refuser l'accès au client XProtect Mobile.
<b>Autoriser la connexion au XProtect Web Client</b>	Cochez la case pour permettre aux utilisateurs associés à ce rôle de se connecter au XProtect Web Client. L'accès au XProtect Web Client est autorisé par défaut. Décochez la case pour refuser l'accès au XProtect Web Client.
<b>Autorisation de connexion requise</b>	Cochez la case pour associer l'autorisation de connexion au rôle. Cela signifie que, lorsque l'utilisateur se connecte, XProtect Smart Client ou le Management Client demande une deuxième autorisation, généralement par un superutilisateur ou responsable. Pour permettre aux administrateurs d'autoriser des utilisateurs, configurez le droit <b>Autoriser utilisateurs</b> du serveur de gestion dans l'onglet <b>Sécurité globale</b> . Vous ne pouvez pas appliquer ceci au rôle d' <b>Administrateurs</b> par défaut.
<b>Rendre les utilisateurs anonymes au cours des sessions PTZ</b>	Cochez la case pour masquer les noms des utilisateurs associés à ce rôle lorsqu'ils contrôlent des sessions PTZ.

### Onglet Utilisateur et Groupes (rôles)

Sur l'onglet **Utilisateur et Groupes**, vous attribuez des utilisateurs et des groupes à des rôles (voir Assigner et supprimer des utilisateurs et groupes aux/des rôles sur la page 373). Vous pouvez assigner des utilisateurs et groupes Windows ou des utilisateurs basiques (voir Utilisateurs (explications) sur la page 370).

Nom	Description
<b>Nom</b>	Affiche le nom de l'utilisateur ou du groupe assigné à ce rôle.
<b>Description</b>	Affiche la description que vous avez saisie lors de la création de l'utilisateur basique.



## Onglet Sécurité globale (rôles)

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

Dans l'onglet **Sécurité globale**, vous pouvez configurer les droits globaux des rôles. Pour chaque composant disponible dans votre système, définissez des droits d'accès pour les rôles en configurant **Autoriser** ou **Refuser**. Lorsqu'un rôle n'a pas accès à un composant, celui-ci n'est pas visible dans l'onglet **Sécurité globale** pour l'utilisateur dans ce rôle.



L'onglet **Sécurité générale** n'est pas disponible dans la version gratuite de XProtect Essential+.

Vous pouvez définir plus de droits d'accès pour XProtect Corporate que pour XProtect Expert, XProtect Professional+, et XProtect Express+. Cela tient au fait que vous pouvez seulement configurer des droits d'administrateur différents dans XProtect Corporate, tandis que vous pouvez configurer les droits globaux pour un rôle qui utilise un client XProtect Smart Client, XProtect Web Client ou XProtect Mobile dans tous les produits.



Les paramètres de sécurité globaux s'appliquent uniquement au site actuel.

Si vous associez un utilisateur à plusieurs rôles et que vous sélectionnez **Refuser** pour un paramètre de sécurité pour un rôle et **Autoriser** pour un autre, le **Refus** de permission prime sur l'**Autorisation** de permission.

Dans ce qui suit, les descriptions présentent ce qui se produit au niveau de chaque droit individuel pour les différents composants du système si vous sélectionnez **Autoriser** pour le rôle pertinent. Si vous utilisez XProtect Corporate, vous pouvez voir quels sont les paramètres disponibles **uniquement** pour votre système sous chaque composant du système.

Pour chaque composant ou fonction du système, l'administrateur système complet peut utiliser les cases **Autoriser** ou **Refuser** pour configurer les permissions de sécurité du rôle. Chaque permission de sécurité établie s'applique à l'ensemble du composant ou de la fonction du système. Ainsi, par exemple, si vous cochez la case **Refuser** pour les **Caméras**, toutes les caméras ajoutées sur le système sont indisponibles pour ce rôle. À l'inverse, si vous cochez la case **Autoriser**, le rôle peut voir toutes les caméras ajoutées sur le système. Suite à la sélection d'**Autoriser** ou **Refuser** sur vos caméras, les paramètres des caméras sur l'onglet **Périphérique** héritent alors des sélections que vous avez effectuées dans l'onglet **Sécurité globale** de façon à ce que toutes les caméras soient disponibles ou indisponibles pour le rôle en question.


Si vous souhaitez configurer des permissions de sécurité pour **chaque** caméra ou similaire, vous ne pouvez configurer ces permissions individuelles dans l'onglet du composant ou de la fonction correspondant que si vous avez **désactivé tous les paramètres globaux** pour le composant ou la fonction du système dans l'onglet **Sécurité globale**.



Les descriptions ci-dessous s'appliquent également aux droits que vous pouvez configurer par l'intermédiaire des MIP SDK.



Si vous souhaitez échanger votre licence de base XProtect Corporate contre une licence de l'un des autres produits, assurez-vous de retirer tous les droits de sécurité disponibles pour XProtect Corporate uniquement. Si vous ne supprimez pas ces droits, vous ne pourrez pas terminer l'échange.

## Management Server

Droit de sécurité	Description	XProtect Corporate
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
<b>Connecter</b>	<p>Permet aux utilisateurs de se connecter au Management Server.</p> <p>Cette permission est activée par défaut.</p> <p>Vous pouvez temporairement refuser une permission de connexion de rôles à des fins de maintenance puis réautoriser l'accès au système.</p> <div data-bbox="408 1066 1158 1196" style="background-color: #f9e79f; padding: 5px; border: 1px solid #ccc;">  Cette permission doit être sélectionnée afin d'autoriser l'accès au système.                 </div>	
<b>Lire</b>	<p>Active le droit d'accéder à un large éventail de fonctionnalités, y compris :</p> <ul style="list-style-type: none"> <li>• Se connecter avec le Management Client</li> <li>• Liste des tâches actuelles</li> <li>• Journaux des serveurs</li> </ul> <p>Il permet également d'accéder à :</p> <ul style="list-style-type: none"> <li>• Services de connexion à distance</li> <li>• Profils Smart Client</li> <li>• Profils Management Client</li> <li>• Matrix</li> <li>• Profils de temps</li> <li>• Serveurs enregistrés et API d'enregistrement de service</li> </ul>	Disponible uniquement


Droit de sécurité	Description	XProtect Corporate
<b>Modifier</b>	<p>Active le droit de modifier les données dans un large éventail de fonctionnalités, y compris :</p> <ul style="list-style-type: none"> <li>• Options</li> <li>• Gestion des licences</li> </ul> <p>Permet également aux utilisateurs de créer, de supprimer et de modifier les éléments suivants :</p> <ul style="list-style-type: none"> <li>• Services de connexion à distance</li> <li>• Groupes de périphériques</li> <li>• Matrix</li> <li>• Profils de temps</li> <li>• Profils de notification</li> <li>• Serveurs enregistrés</li> </ul> <div style="background-color: #e6f2ff; padding: 10px; margin-top: 10px;">  Active le droit de configurer des plages IP locales lors de la configuration du réseau sur le serveur d'enregistrement.         </div>	Disponible uniquement
<b>Moniteur système</b>	Active le droit de consulter les données du moniteur système.	Disponibles uniquement
<b>État API</b>	Active le droit d'exécuter des demandes concernant l'état API situé sur le serveur d'enregistrement. Cela signifie que le rôle pour lequel ce droit est activé dispose d'un accès suffisant pour lire l'état des éléments situés sur le serveur d'enregistrement.	
<b>Hiérarchie des sites fédérés</b>	<p>Active le droit d'ajouter ou de détacher le site actuel à d'autres sites dans une hiérarchie des sites fédérés.</p> <div style="background-color: #e6f2ff; padding: 10px; margin-top: 10px;">  Si vous autorisez uniquement l'accès à un site enfant, l'utilisateur peut toujours le connecter au site parent.         </div>	Disponibles uniquement

Droit de sécurité	Description	XProtect Corporate
<b>Sauvegarde de configuration</b>	Active le droit de création de sauvegardes de la configuration du système à l'aide de la fonction de sauvegarde et de restauration du système.	Disponible uniquement
<b>Autoriser des utilisateurs</b>	Active le droit d'autorisation d'utilisateurs lorsqu'une seconde authentification leur est demandée dans XProtect Smart Client ou Management Client. Vous déterminez si un rôle nécessite une autorisation de connexion dans l'onglet <b>Info</b> .	
<b>Gérer la sécurité</b>	Active le droit de gestion des permissions pour le serveur de gestion.  Permet également aux utilisateurs de créer, de supprimer et de modifier les fonctionnalités suivantes : <ul style="list-style-type: none"> <li>• Rôles</li> <li>• Utilisateurs</li> <li>• Profils Smart Client</li> <li>• Profils Management Client</li> </ul>	Disponible uniquement

### Serveurs d'enregistrement

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
<b>Modifier</b>	Active le droit de modification des propriétés sur les serveurs d'enregistrement, sauf pour les paramètres de configuration du réseau qui nécessitent un droit de modification sur le serveur de gestion.

Droit de sécurité	Description
Supprimer	<p>Active le droit de suppression des serveurs d'enregistrement. Pour ce faire, vous devez également octroyer les permissions de suppression d'utilisateurs sur :</p> <ul style="list-style-type: none"> <li>Les groupes de sécurité matérielle si vous avez ajouté du matériel au serveur d'enregistrement</li> </ul> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0; margin-top: 10px;">  <p>Si un des périphériques situés sur le serveur d'enregistrement contient des preuves verrouillées, vous pouvez uniquement supprimer le serveur d'enregistrement s'il est hors ligne.</p> </div>
Gérer le matériel	Active le droit d'ajouter du matériel sur les serveurs enregistrés.
Gérer le stockage	Active le droit d'administration des conteneurs de stockage sur le serveur d'enregistrement, c'est-à-dire le droit de créer, de supprimer, de déplacer et de vider des conteneurs de stockage.
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour des serveurs d'enregistrement.

### Serveurs de redondance

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
Lire	Active le droit d'accéder aux et de consulter les serveurs de basculement dans le Management Client.
Modifier	Active le droit de créer, mettre à jour, supprimer, déplacer et activer ou désactiver les serveurs de basculement dans le Management Client.
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour les serveurs de secours.


## Serveurs Mobile


Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
<b>Lire</b>	Active le droit d'accéder aux et de consulter les serveurs portables dans le Management Client.
<b>Modifier</b>	Active le droit de modifier et supprimer les serveurs portables dans le Management Client.
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour les serveurs mobiles.
<b>Créer</b>	Active le droit d'ajouter des serveurs mobiles sur le système.

## Matériel

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
<b>Modifier</b>	Active le droit de modification des propriétés du matériel.
<b>Supprimer</b>	<p>Active le droit de suppression de matériel.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;">  <p>Si un des dispositifs matériels contient des preuves verrouillées, vous pouvez uniquement supprimer le matériel lorsque le serveur d'enregistrement est hors ligne.</p> </div>

Droit de sécurité	Description
<b>Commandes du gestionnaire</b>	<p>Active le droit d'envoyer des commandes spécifiques aux gestionnaires, et contrôle donc les fonctionnalités et la configuration de l'appareil lui-même.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;">  <p>Le droit <b>Commandes du gestionnaire</b> est destiné à des modules d'extension MIP développés spécialement dans les clients uniquement. Il ne contrôle pas les tâches de configuration standard.</p> </div>
<b>Voir les mots de passe</b>	Établit le droit de voir les mots de passe sur les périphériques matériels dans la fenêtre de dialogue <b>Éditer matériel</b> .
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour le matériel.


## Caméras

Droit de sécurité	Description	XProtect Corporate
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
<b>Lire</b>	Active le droit de visualisation des caméras dans les clients et dans le Management Client.	
<b>Modifier</b>	Active le droit de modification des propriétés pour les caméras dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver une caméra.	Disponible uniquement
<b>Visualisation en direct</b>	Active le droit de consultation de vidéos en direct à partir des caméras dans les clients et dans le Management Client.	
<b>Lecture</b>	Active le droit de lecture de vidéos enregistrées à partir des caméras dans tous les clients.	

Droit de sécurité	Description	XProtect Corporate
<b>Rappeler les enregistrements à distance</b>	Active le droit de rappeler les enregistrements des clients depuis les caméras se trouvant dans des sites distants ou sur le stockage externe des caméras.	
<b>Lire les séquences</b>	Active le droit de lecture des informations séquentielles liées à la lecture de vidéo enregistrée dans les clients, par exemple.	
<b>Recherche avancée</b>	Active le droit d'utilisation de la fonction de recherche avancée dans les clients.	
<b>Exporter</b>	Active le droit d'exporter des enregistrements à partir des clients.	
<b>Créer des signets</b>	Active le droit de création de signet dans des vidéos enregistrées et en direct dans les clients.	
<b>Lire les signets</b>	Active le droit de recherche et de lecture des détails des signets dans les clients.	
<b>Modifier les signets</b>	Active le droit de modification des signets dans les clients.	
<b>Supprimer des signets</b>	Active le droit de suppression de signets dans les clients.	
<b>Créer et étendre la protection des preuves</b>	Active le droit de création et d'extension du verrouillage des preuves dans les clients.	Disponible uniquement
<b>Lire le verrouillage des preuves</b>	Active le droit de recherche et de lecture de preuves verrouillées dans les clients.	Disponible uniquement
<b>Supprimer et réduire le verrouillage des preuves</b>	Active le droit de suppression ou de réduction du verrouillage des preuves dans les clients.	Disponible uniquement
<b>Démarrer l'enregistrement manuel</b>	Active le droit de démarrer l'enregistrement manuel de la vidéo dans les clients.	



Droit de sécurité	Description	XProtect Corporate
<b>Arrêter l'enregistrement manuel</b>	Active le droit d'arrêter l'enregistrement manuel de la vidéo dans les clients.	
<b>Commandes AUX</b>	Active le droit d'utiliser des commandes auxiliaires (AUX) sur la caméra à partir des clients.  Les <b>commandes AUX</b> permettent aux utilisateurs de contrôler, par exemple, les essuie-glaces d'une caméra connectée via un encodeur vidéo. Les périphériques associés à la caméra, connectés via des connexions auxiliaires, sont contrôlés depuis le client.	
<b>Manuel PTZ</b>	Active le droit d'utilisation des fonctions PTZ sur les caméras PTZ dans les clients et dans le Management Client.	
<b>Activer des positions prédéfinies PTZ ou des profils de patrouille</b>	Active le droit de déplacer des caméras PTZ vers des positions prédéfinies, de démarrer et arrêter des profils de patrouille et de mettre des patrouilles en pause dans les clients et dans le Management Client.  Pour autoriser ce rôle à utiliser d'autres fonctions PTZ sur la caméra, activez le droit <b>PTZ manuel</b> .	
<b>Gérer les positions prédéfinies PTZ ou les profils de patrouille</b>	Active le droit d'ajouter, de modifier et d'effacer les positions et les profils de patrouille sur les caméras PTZ, dans les clients et dans le Management Client.  Pour autoriser ce rôle à utiliser d'autres fonctions PTZ sur la caméra, activez le droit <b>PTZ manuel</b> .	
<b>Verrouiller/Déverrouiller des positions prédéfinies PTZ</b>	Active le droit de bloquer et débloquer les positions PTZ prédéfinies dans le Management Client. Ceci empêche ou autorise d'autres utilisateurs à changer les positions prédéfinies dans les clients et dans le Management Client.	Disponible uniquement
<b>Réserver des sessions PTZ</b>	Active le droit de paramétrer les caméras PTZ en mode de session réservée dans les clients et dans le Management	Disponible uniquement

Droit de sécurité	Description	XProtect Corporate
	<p>Client.</p> <p>Dans une session PTZ réservée, d'autres utilisateurs dotés d'une priorité PTZ plus élevée ne peuvent pas prendre le contrôle.</p> <p>Pour autoriser ce rôle à utiliser d'autres fonctions PTZ sur la caméra, activez le droit <b>PTZ manuel</b>.</p>	
<b>Libérer les sessions PTZ</b>	<p>Active le droit de libérer les sessions PTZ d'autres utilisateurs du Management Client.</p> <p>Vous pouvez toujours libérer vos propres sessions PTZ, même sans cette permission.</p>	Disponible uniquement
<b>Supprimer des enregistrements</b>	<p>Active le droit de suppression des enregistrements vidéo stockés à partir du système via le Management Client.</p>	Disponible uniquement
<b>Enlever les masques de confidentialité</b>	<p>Active le droit de lever provisoirement les masques de confidentialité dans XProtect Smart Client. Il active également le droit d'autoriser les autres utilisateurs de XProtect Smart Client à lever les masques de confidentialité.</p> <div data-bbox="497 1196 1139 1518" style="border: 1px solid #0070C0; padding: 10px; background-color: #D9E1F2;">  <p>Le levage des masques de confidentialité s'applique uniquement aux masques de confidentialité configurés en tant que masques de confidentialité relevables dans Management Client.</p> </div>	
<b>Gérer la sécurité</b>	<p>Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client.</p>	Disponible uniquement

## Microphones

Droit de sécurité	Description	XProtect Corporate
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
<b>Lire</b>	Active le droit de visualisation des microphones dans les clients et dans le Management Client.	
<b>Modifier</b>	Active le droit de modification des propriétés pour les microphones dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver des microphones.	Disponible uniquement
<b>Écouter</b>	Active le droit d'écoute d'audio en direct à partir des microphones dans les clients et dans le Management Client.	
<b>Lecture</b>	Active le droit de lecture d'audio enregistré à partir des microphones dans les clients.	
<b>Rappeler les enregistrements à distance</b>	Active le droit de rappeler les enregistrements des clients depuis les microphones se trouvant dans des sites distants ou sur le stockage externe des caméras.	
<b>Lire les séquences</b>	Active le droit de lecture des informations séquentielles liées à l'onglet <b>Lecture</b> dans les clients, par exemple.	
<b>Exporter</b>	Active le droit d'exporter des enregistrements à partir des clients.	
<b>Créer des signets</b>	Active le droit de création de signets dans les clients.	
<b>Lire les signets</b>	Active le droit de recherche et de lecture des détails des signets dans les clients.	
<b>Modifier les signets</b>	Active le droit de modification des signets dans les clients.	
<b>Supprimer des signets</b>	Active le droit de suppression de signets dans les clients.	

Droit de sécurité	Description	XProtect Corporate
<b>Créer et étendre la protection des preuves</b>	Active le droit de création ou d'extension du verrouillage des preuves dans les clients.	Disponible uniquement
<b>Lire le verrouillage des preuves</b>	Active le droit de recherche et de lecture des détails des preuves verrouillées dans les clients.	Disponible uniquement
<b>Supprimer et réduire le verrouillage des preuves</b>	Active le droit de suppression ou de réduction du verrouillage des preuves dans les clients.	Disponible uniquement
<b>Démarrer l'enregistrement manuel</b>	Active le droit de démarrer l'enregistrement manuel de l'audio dans les clients.	
<b>Arrêter l'enregistrement manuel</b>	Active le droit d'arrêter l'enregistrement manuel de l'audio dans les clients.	
<b>Supprimer des enregistrements</b>	Active le droit de suppression des enregistrements stockés à partir du système.	Disponible uniquement
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour les microphones.	Disponible uniquement

## Haut-parleurs

Droit de sécurité	Description	XProtect Corporate
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
<b>Lire</b>	Active le droit de visualisation des haut-parleurs dans les clients	

Droit de sécurité	Description	XProtect Corporate
	et dans le Management Client.	
<b>Modifier</b>	Active le droit de modification des propriétés pour les haut-parleurs dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver des haut-parleurs.	Disponible uniquement
<b>Écouter</b>	Active le droit d'écoute d'audio en direct à partir des haut-parleurs dans les clients et dans le Management Client.	
<b>Parole</b>	Active le droit de parler dans les haut-parleurs au sein des clients.	
<b>Lecture</b>	Active le droit de lecture d'audio enregistré à partir des haut-parleurs dans les clients.	
<b>Rappeler les enregistrements à distance</b>	Active le droit de rappeler les enregistrements des clients depuis les haut-parleurs se trouvant dans des sites distants ou sur le stockage externe des caméras.	
<b>Lire les séquences</b>	Active le droit d'utilisation de la fonctionnalité Séquences tout en parcourant l'audio enregistré à partir des haut-parleurs dans les clients.	
<b>Exporter</b>	Active le droit d'export d'audio enregistré à partir des haut-parleurs dans les clients.	
<b>Créer des signets</b>	Active le droit de création de signets dans les clients.	
<b>Lire les signets</b>	Active le droit de recherche et de lecture des détails des signets dans les clients.	
<b>Modifier les signets</b>	Active le droit de modification des signets dans les clients.	
<b>Supprimer des signets</b>	Active le droit de suppression de signets dans les clients.	

Droit de sécurité	Description	XProtect Corporate
<b>Créer et étendre la protection des preuves</b>	Active le droit de création ou d'extension de la protection des preuves pour protéger l'audio enregistré dans les clients.	Disponible uniquement
<b>Lire le verrouillage des preuves</b>	Active le droit de consulter le son enregistré protégé par les protections des preuves dans les clients.	Disponible uniquement
<b>Supprimer et réduire le verrouillage des preuves</b>	Active le droit de suppression ou de réduction de protection des preuves sur l'audio enregistré dans les clients.	Disponible uniquement
<b>Démarrer l'enregistrement manuel</b>	Active le droit de démarrer l'enregistrement manuel de l'audio dans les clients.	
<b>Arrêter l'enregistrement manuel</b>	Active le droit d'arrêter l'enregistrement manuel de l'audio dans les clients.	
<b>Supprimer des enregistrements</b>	Active le droit de suppression des enregistrements stockés à partir du système.	Disponible uniquement
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour les haut-parleurs.	Disponible uniquement

## Métadonnées

Droit de sécurité	Description	XProtect Corporate
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	

Droit de sécurité	Description	XProtect Corporate
<b>Lire</b>	Active le droit de réception de métadonnées dans les clients.	
<b>Modifier</b>	Active le droit de modification des propriétés pour les métadonnées dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver des périphériques de métadonnées.	Disponible uniquement
<b>En direct</b>	Active le droit de réception de métadonnées en direct à partir des caméras dans les clients.	
<b>Lecture</b>	Active le droit de lecture de données enregistrées à partir des périphériques de métadonnées dans les clients.	
<b>Rappeler les enregistrements à distance</b>	Active le droit de rappeler les enregistrements des clients depuis les périphériques de métadonnées se trouvant dans des sites distants ou sur le stockage externe des caméras.	
<b>Lire les séquences</b>	Active le droit de lecture des informations séquentielles liées à l'onglet <b>Lecture</b> dans les clients, par exemple.	
<b>Exporter</b>	Active le droit d'exporter des enregistrements dans les clients.	
<b>Créer et étendre la protection des preuves</b>	Active le droit de création du verrouillage des preuves dans les clients.	Disponible uniquement
<b>Lire le verrouillage des preuves</b>	Active le droit de consultation du verrouillage des preuves dans les clients.	Disponible uniquement
<b>Supprimer et réduire le verrouillage des preuves</b>	Active le droit de suppression ou de réduction du verrouillage des preuves dans les clients.	Disponible uniquement
<b>Démarrer l'enregistrement</b>	Active le droit de démarrer l'enregistrement manuel des métadonnées dans les clients.	

Droit de sécurité	Description	XProtect Corporate
manuel		
<b>Arrêter l'enregistrement manuel</b>	Active le droit d'arrêter l'enregistrement manuel des métadonnées dans les clients.	
<b>Supprimer des enregistrements</b>	Active le droit de suppression des enregistrements stockés à partir du système.	Disponible uniquement
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour les métadonnées.	Disponible uniquement

## Entrées

Droit de sécurité	Description	XProtect Corporate
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	Disponible uniquement
<b>Lire</b>	Active le droit de visualisation des périphériques de saisie dans les clients et dans le Management Client.	
<b>Modifier</b>	Active le droit de modification des propriétés pour les périphériques d'entrée dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver un périphérique d'entrée.	Disponible uniquement
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour les périphériques de saisie.	Disponible uniquement

## Sortie



Droit de sécurité	Description	XProtect Corporate
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
<b>Lire</b>	Active le droit de visualisation des périphériques de sortie dans les clients.	
<b>Modifier</b>	Active le droit de modification des propriétés pour les périphériques de sortie dans le Management Client. Il permet également aux utilisateurs d'activer ou de désactiver un périphérique de sortie.	Disponible uniquement
<b>Activer</b>	Active le droit d'activation de sorties dans les clients.	
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour les périphériques de sortie.	Disponible uniquement

### Smart Wall

Les paramètres suivants sont uniquement disponibles dans XProtect Expert et XProtect Corporate.

Droit de sécurité	Description	XProtect Corporate
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
<b>Lire</b>	Active le droit de visualisation des Smart Walls dans les clients.	
<b>Modifier</b>	Active le droit de modification des propriétés pour le Smart Wall dans le Management Client.	Disponible uniquement
<b>Supprimer</b>	Active le droit de suppression des Smart Walls existants dans le Management Client.	Disponible uniquement
<b>Opérer</b>	Active le droit d'activer et de modifier les Smart Walls, par exemple pour modifier et activer des préréglages ou affecter des caméras à	

Droit de sécurité	Description	XProtect Corporate
	des vues dans les clients et dans le Management Client.	
<b>Créer un Smart Wall</b>	Active le droit de création de nouveaux Smart Walls dans le Management Client.	Disponible uniquement
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour le Smart Wall.	Disponible uniquement
<b>Lecture</b>	Active le droit de lecture de données enregistrées à partir des Smart Walls dans les clients.	

### Groupes de vues

Droit de sécurité	Description	XProtect Corporate
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
<b>Lire</b>	Active le droit de visualisation des groupes de vues dans les clients et dans le Management Client. Les groupes de vues sont créés dans le Management Client.	
<b>Modifier</b>	Active le droit de modification des propriétés pour les groupes de vues dans le Management Client.	Disponible uniquement
<b>Supprimer</b>	Active le droit de suppression des groupes de vues dans le Management Client.	
<b>Opérer</b>	Active le droit d'utilisation de groupes de vues dans XProtect Smart Client. Autrement dit, la création et la suppression de sous-groupes et de vues.	
<b>Créer un groupe de vues</b>	Active le droit de création des groupes de vues dans le Management Client.	Disponible uniquement
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour les groupes de vues.	Disponible uniquement

## Événements définis par l'utilisateur

Droit de sécurité	Description	XProtect Corporate
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	
<b>Lire</b>	Active le droit d'afficher des événements définis par les utilisateurs dans les clients.	
<b>Modifier</b>	Active le droit de modification des propriétés pour les événements définis par les utilisateurs dans le Management Client.	Disponible uniquement
<b>Supprimer</b>	Active le droit de visualiser des événements définis par les utilisateurs dans le Management Client.	Disponible uniquement
<b>Déclencher</b>	Active le droit de déclencher des événements définis par les utilisateurs dans les clients.	
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour les événements définis par les utilisateurs dans le Management Client.	Disponible uniquement
<b>Créer un événement défini par l'utilisateur</b>	Active le droit de création de nouveaux événements définis par les utilisateurs dans le Management Client.	Disponible uniquement

## Événement analytique

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
<b>Contrôle</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.

<b>Droit de sécurité</b>	<b>Description</b>
<b>total</b>	
<b>Lire</b>	Active le droit de visualiser des événements analytiques dans le Management Client.
<b>Modifier</b>	Active le droit de modifier des propriétés pour les événements analytiques dans le Management Client.
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité des événements analytiques dans le Management Client.

### Événements génériques

<b>Droit de sécurité</b>	<b>Description</b>
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
<b>Lire</b>	Active le droit de visualisation des événements génériques dans les clients et dans le Management Client.
<b>Modifier</b>	Active le droit de modifier des propriétés pour les événements génériques dans le Management Client.
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité des événements génériques dans le Management Client.

### Matrix

Droit de sécurité	Description	XProtect Corporate
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.	Disponible uniquement
<b>Lire</b>	Active le droit de sélectionner et d'envoyer une vidéo au destinataire Matrix à partir des clients.	
<b>Modifier</b>	Active le droit de modification des propriétés pour un Matrix dans le Management Client.	Disponible uniquement
<b>Supprimer</b>	Active le droit de suppression d'un Matrix dans le Management Client.	Disponible uniquement
<b>Créer un Matrix</b>	Active le droit de création d'un nouveau Matrix dans le Management Client.	Disponible uniquement
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour tous les Matrix.	Disponible uniquement

## Règles

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
<b>Lire</b>	Active le droit de visualiser des règles existantes dans le Management Client.
<b>Modifier</b>	Active le droit de modification des propriétés pour les règles et de définition du comportement des règles dans le Management Client. Il requiert également que l'utilisateur dispose de permissions de lecture sur tous les périphériques affectés par la règle.

Droit de sécurité	Description
<b>Supprimer</b>	Active le droit de suppression de règles dans le Management Client. Il requiert également que l'utilisateur dispose de permissions de lecture sur tous les périphériques affectés par la règle.
<b>Créer une règle</b>	Active le droit de création de nouvelles règles dans le Management Client. Il requiert également que l'utilisateur dispose de permissions de lecture sur tous les périphériques affectés par la règle.
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour toutes les règles.

## Sites

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
<b>Lire</b>	Active le droit de visualiser d'autres sites dans le Management Client. Les sites connectés sont connectés par le biais de Milestone Federated Architecture. Pour modifier les propriétés vous devez avoir des permissions de modification sur le serveur de gestion de chaque site.
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité sur tous les sites.

## Moniteur système

Les paramètres suivants sont uniquement disponibles dans XProtect Expert et XProtect Corporate.

Droit de sécurité	Description
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
<b>Lire</b>	Active le droit de visualisation des moniteurs système dans XProtect Smart Client.
<b>Modifier</b>	Active le droit de modification des propriétés des moniteurs système dans le Management Client.
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour tous les moniteurs système.

### Recherche de métadonnées

Les paramètres suivants sont uniquement disponibles dans XProtect Expert et XProtect Corporate.

Droit de sécurité	Description
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
<b>Lire</b>	Active le droit de voir les fonctionnalités <b>Utilisation des métadonnées</b> dans Management Client et ses paramètres connexes, mais sans activer le droit de modifier les paramètres.
<b>Modifier la configuration de la recherche de métadonnées</b>	Active le droit d'activer ou de désactiver les catégories de la recherche de métadonnées, par exemple, les métadonnées des personnes ou des véhicules dans le Management Client.
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour les recherches de métadonnées.

### Rechercher

Les paramètres suivants sont uniquement disponibles dans XProtect Expert et XProtect Corporate.


Droit de sécurité	Description
<b>Lire des recherches publiques</b>	Active le droit de consulter et ouvrir les recherches publiques sauvegardées dans XProtect Smart Client.
<b>Créer des recherches publiques</b>	Active le droit de sauvegarder nouvellement des recherches configurées comme recherches publiques dans XProtect Smart Client.
<b>Modifier des recherches publiques</b>	Active le droit de modifier les détails ou la configuration des recherches publiques sauvegardées dans XProtect Smart Client, le nom, la description, les caméras et les catégories de recherche, par exemple.
<b>Supprimer des recherches publiques</b>	Active le droit de supprimer les recherches publiques sauvegardées.
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour la caméra dans le Management Client pour la recherche.

## Alarmes

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
<b>Gestion</b>	Active le droit de gestion des alarmes dans le Management Client. Par exemple, modifiez les priorités des alarmes et réaffectez des alarmes à d'autres utilisateurs, acquittez les alarmes et modifiez l'état de plusieurs alarmes en même temps, pour les faire passer de Nouveau à Assigné, par exemple. Nouvelles définitions d'alarmes, sons d'alarmes, et paramètres de données d'alarmes.



Droit de sécurité	Description
	 L'onglet <b>Alarmes et événements</b> de la boîte de dialogue <b>Options</b> n'apparaît que lorsque vous choisissez d'autoriser cette fonction.
<b>Modifier</b>	Active le droit d'afficher les alarmes et d'imprimer les rapports d'alarme.
<b>Désactiver alarmes</b>	Active le droit de désactiver les alarmes.
<b>Recevoir des notifications</b>	Active le droit de recevoir des notifications à propos des alarmes dans les clients XProtect Mobile et XProtect Web Client.
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour les alarmes.
<b>Créer</b>	Active le droit de créer de nouvelles définitions d'alarmes dans le Management Client.

### Journaux des serveurs

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
<b>Lire les entrées du journal système</b>	Active le droit de lire les entrées du journal système.
<b>Lire les entrées du journal d'activité</b>	Active le droit de lire les entrées du journal d'activité.
<b>Lire les entrées du journal</b>	Active le droit de lire les entrées

Droit de sécurité	Description
déclenchées par une règle	du journal déclenchées par une règle.
Lire la configuration du journal	Active le droit de lire les paramètres du journal dans <b>Outils &gt; Options &gt; Journaux du serveur</b> .
Mettre à jour la configuration du journal	Active le droit de modifier les paramètres du journal dans <b>Outils &gt; Options &gt; Journaux du serveur</b> .
Gérer la sécurité	Active le droit de gérer les permissions de sécurité pour les alarmes.

### Contrôle d'accès

Les paramètres suivants sont uniquement disponibles dans XProtect Corporate.

Droit de sécurité	Description
Contrôle total	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
Modifier	Active le droit de modifier des propriétés pour les systèmes de contrôle d'accès dans le Management Client.
Utiliser le contrôle d'accès	Permet à l'utilisateur d'utiliser les fonctions relatives au contrôle d'accès dans les clients.
Voir la liste des détenteurs de cartes	Permet à l'utilisateur de voir la liste des détenteurs de cartes sur l'onglet <b>Contrôle d'accès</b> dans les clients.
Recevoir des notifications	Permet à l'utilisateur de recevoir des notifications concernant les demandes

Droit de sécurité	Description
	d'accès dans les clients.
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour tous les systèmes de contrôle d'accès.

## LPR

Si votre système fonctionne sous XProtect LPR, spécifiez les droits suivants pour l'utilisateur :

Droit de sécurité	Description
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
<b>Utiliser LPR</b>	Active le droit d'utiliser n'importe quelles fonctions relatives à LPR dans les clients
<b>Gérer les listes de correspondance de plaques d'immatriculation</b>	Active le droit d'ajouter, importer, modifier, exporter et supprimer les listes de correspondance de plaques d'immatriculation dans le Management Client.
<b>Lire les listes de correspondance de plaques d'immatriculation</b>	Active le droit d'afficher les listes de correspondance de plaques d'immatriculation.
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour toutes les définitions de transactions dans le Management Client.

## Sources de transactions

Droit de sécurité	Description
<b>Contrôle</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.

<b>Droit de sécurité</b>	<b>Description</b>
<b>total</b>	
<b>Lire</b>	Active le droit de visualisation des propriétés pour les sources de transactions dans le Management Client.
<b>Modifier</b>	Active le droit de modification des propriétés pour les sources de transactions dans le Management Client.
<b>Supprimer</b>	Active le droit de supprimer des sources de transactions dans le Management Client.
<b>Créer</b>	Active le droit de créer de nouvelles sources de transactions dans le Management Client.
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour toutes les sources de transactions dans le Management Client.

### Définitions des transactions

<b>Droit de sécurité</b>	<b>Description</b>
<b>Contrôle total</b>	Active le droit de gestion de toutes les entrées de sécurité sur cette partie du système.
<b>Lire</b>	Active le droit de visualisation des propriétés des définitions de transactions dans le Management Client.
<b>Modifier</b>	Active le droit de modification des propriétés des définitions de transactions dans le Management Client.
<b>Supprimer</b>	Active le droit de suppression des définitions de transactions dans le Management Client.
<b>Créer</b>	Active le droit de créer de nouvelles définitions de transactions dans le Management Client.
<b>Gérer la sécurité</b>	Active le droit de gérer les permissions de sécurité pour toutes les définitions de transactions dans le Management Client.

## Modules d'extension MIP

Au travers du MIP SDK, un vendeur tiers peut développer des modules d'extension personnalisés pour votre système, par exemple, l'intégration à des systèmes de contrôle d'accès externes ou similaires.

### Onglet Périphériques (rôles)

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

L'onglet **Périphérique** vous permet de spécifier quelles fonctions les utilisateurs/groupes avec le rôle sélectionné peuvent utiliser pour chaque périphérique (une caméra, par exemple) ou groupe de périphériques dans XProtect Smart Client.


N'oubliez pas de répéter cette procédure pour chaque périphérique. Vous pouvez également sélectionner un groupe de périphériques, et spécifier les droits du rôle pour tous les périphériques du groupe en même temps.


Vous avez toujours la possibilité de sélectionner ou de supprimer lesdites cases à cocher remplies d'un carré, cependant notez que votre choix s'applique dans ce cas à **tous** les périphériques d'un groupe de périphériques. Autre alternative, sélectionnez les périphériques individuels dans le groupe de périphériques afin de vérifier exactement à quel périphérique le droit pertinent s'applique.

### Droits relatifs aux caméras

Spécifiez les droits suivants pour les caméras :

Nom	Description
<b>Lire</b>	La ou les caméra(s) sélectionnée(s) seront visibles dans les clients.
<b>Visualisation en direct</b>	Permet de visionner les vidéos de la ou des caméra(s) sélectionnée(s) en direct dans les clients. Pour XProtect Smart Client, cette fonction exige également que le rôle ait reçu le droit de visualiser l'onglet <b>En direct</b> des clients. Le droit est attribué dans le cadre des droits sur les applications. Spécifiez le profil de temps ou conservez la valeur par défaut.
<b>Lecture &gt; Dans le profil de temps</b>	Permet la lecture des vidéos enregistrées de la ou des caméra(s) sélectionnée(s) en direct dans les clients. Spécifiez le profil de temps ou conservez la valeur par défaut.
<b>Lecture &gt; Limiter la lecture à</b>	Permet la lecture des vidéos enregistrées de la ou des caméra(s) sélectionnée(s) en direct dans les clients. Spécifiez une limite de lecture ou n'appliquez aucune restriction.


Nom	Description
<b>Lire les séquences</b>	Permet de lire des informations séquentielles liées à l'explorateur de séquence dans les clients, par exemple.
<b>Recherche avancée</b>	Permet à l'utilisateur d'utiliser la fonction de recherche avancée dans les clients.
<b>Exporter</b>	Permet à l'utilisateur d'exporter des enregistrements à partir des clients.
<b>Démarrer l'enregistrement manuel</b>	Permet de démarrer l'enregistrement manuel des vidéos de la ou des caméra(s) sélectionnée(s) en direct dans les clients.
<b>Arrêter l'enregistrement manuel</b>	Permet d'arrêter l'enregistrement manuel des vidéos de la ou des caméra(s) sélectionnée(s) en direct dans les clients.
<b>Lire les signets</b>	Permet de recherches et de lire des détails des signets dans les clients.
<b>Modifier les signets</b>	Permet de modifier des signets dans les clients.
<b>Créer des signets</b>	Permet d'ajouter des signets dans les clients.
<b>Supprimer des signets</b>	Permet de supprimer des signets dans les clients.
<b>Commandes AUX</b>	Permet d'utiliser les commandes auxiliaires à partir des clients.
<b>Créer et étendre la protection des preuves</b>	<p>Permet à l'utilisateur du client de :</p> <ul style="list-style-type: none"> <li>• Ajouter la caméra à un ou plusieurs verrouillages de preuves nouveaux ou existants</li> <li>• Étendre la durée d'expiration pour les preuves verrouillées existantes</li> <li>• Étendre l'intervalle protégé pour les preuves verrouillées existantes</li> </ul> <div style="background-color: #e6f2ff; padding: 10px; margin-top: 10px;">  Exige que les droits d'utilisateur associés à tous les périphériques soient inclus dans le verrouillage des preuves. </div>

Nom	Description
<b>Supprimer et réduire le verrouillage des preuves</b>	<p>Permet à l'utilisateur du client de :</p> <ul style="list-style-type: none"> <li>• Supprimer la caméra des verrouillages de preuves existants</li> <li>• Voir les preuves verrouillées existantes</li> <li>• Réduire la durée d'expiration pour les preuves verrouillées existantes</li> <li>• Réduire l'intervalle protégé pour les preuves verrouillées existantes</li> </ul> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #0070c0;">  Exige que les droits d'utilisateur associés à tous les périphériques soient inclus dans le verrouillage des preuves.                 </div>
<b>Lire le verrouillage des preuves</b>	Permet à l'utilisateur du client de rechercher et de lire les détails des preuves verrouillées.


### Droits relatifs aux microphones

Spécifiez les droits suivants pour les microphones :

Nom	Description
<b>Lire</b>	Le ou les microphone(s) sélectionné(s) seront visibles dans les clients.
<b>En direct &gt; Écouter</b>	<p>Permet d'écouter l'audio en direct du ou des microphone(s) sélectionné(s) dans les clients.</p> <p>Pour XProtect Smart Client, cette fonction exige également que le rôle ait reçu le droit de visualiser l'onglet <b>En direct</b> des clients. Le droit est attribué dans le cadre des droits sur les applications. Spécifiez le profil de temps ou conservez la valeur par défaut.</p>
<b>Lecture &gt; Dans le profil de temps</b>	Permet la lecture de l'audio enregistrées du ou des microphone(s) sélectionné(s) en direct dans les clients. Spécifiez le profil de temps ou conservez la valeur par défaut.
<b>Lecture &gt; Limiter la lecture à</b>	Permet la lecture de l'audio enregistrées du ou des microphone(s) sélectionné(s) en direct dans les clients. Spécifiez une limite de lecture ou n'appliquez aucune restriction.

Nom	Description
<b>Lire les séquences</b>	Permet de lire des informations séquentielles liées à l'explorateur de séquence dans les clients, par exemple.
<b>Exporter</b>	Permet à l'utilisateur d'exporter des enregistrements à partir des clients.
<b>Démarrer l'enregistrement manuel</b>	Permet de démarrer l'enregistrement manuel de l'audio du ou des microphone(s) sélectionné(s) en direct dans les clients.
<b>Arrêter l'enregistrement manuel</b>	Permet d'arrêter l'enregistrement manuel de l'audio du ou des microphone(s) sélectionné(s) en direct dans les clients.
<b>Lire les signets</b>	Permet de recherches et de lire des détails des signets dans les clients.
<b>Modifier les signets</b>	Permet de modifier des signets dans les clients.
<b>Créer des signets</b>	Permet d'ajouter des signets dans les clients.
<b>Supprimer des signets</b>	Permet de supprimer des signets dans les clients.
<b>Créer et étendre la protection des preuves</b>	<p>Permet à l'utilisateur du client de :</p> <ul style="list-style-type: none"> <li>• Ajouter le microphone à un ou plusieurs verrouillages de preuves nouveaux ou existants</li> <li>• Étendre la durée d'expiration pour les preuves verrouillées existantes</li> <li>• Étendre l'intervalle protégé pour les preuves verrouillées existantes</li> </ul> <div style="background-color: #e6f2ff; padding: 5px; margin-top: 10px;">  Exige que les droits d'utilisateur associés à tous les périphériques soient inclus dans le verrouillage des preuves. </div>
<b>Supprimer et réduire le verrouillage des preuves</b>	<p>Permet à l'utilisateur du client de :</p> <ul style="list-style-type: none"> <li>• Supprimer le microphone des verrouillages de preuves existants</li> <li>• Voir les preuves verrouillées existantes</li> </ul>





Nom	Description
	<ul style="list-style-type: none"> <li>• Réduire la durée d'expiration pour les preuves verrouillées existantes</li> <li>• Réduire l'intervalle protégé pour les preuves verrouillées existantes</li> </ul> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;">  Exige que les droits d'utilisateur associés à tous les périphériques soient inclus dans le verrouillage des preuves.                 </div>
<b>Lire le verrouillage des preuves</b>	Permet à l'utilisateur du client de rechercher et de lire les détails des preuves verrouillées.

### Droits relatifs aux haut-parleurs

Spécifiez les droits suivants pour les haut-parleurs :

Nom	Description
<b>Lire</b>	Le ou les haut-parleur(s) sélectionné(s) seront visibles dans les clients.
<b>En direct &gt; Écouter</b>	Permet d'écouter l'audio en direct du ou des haut-parleur(s) sélectionné(s) dans les clients. Pour XProtect Smart Client, cette fonction exige également que le rôle ait reçu le droit de visualiser l'onglet <b>En direct</b> des clients. Le droit est attribué dans le cadre des droits sur les applications. Spécifiez le profil de temps ou conservez la valeur par défaut.
<b>Lecture &gt; Dans le profil de temps</b>	Permet la lecture de l'audio enregistrées du ou des haut-parleur(s) sélectionné(s) en direct dans les clients. Spécifiez le profil de temps ou conservez la valeur par défaut.
<b>Lecture &gt; Limiter la lecture à</b>	Permet la lecture de l'audio enregistrées du ou des haut-parleur(s) sélectionné(s) en direct dans les clients. Spécifiez une limite de lecture ou n'appliquez aucune restriction.
<b>Lire les séquences</b>	Permet de lire des informations séquentielles liées à l'explorateur de séquence dans les clients, par exemple.

Nom	Description
<b>Exporter</b>	Permet à l'utilisateur d'exporter des enregistrements à partir des clients.
<b>Démarrer l'enregistrement manuel</b>	Permet de démarrer l'enregistrement manuel de l'audio du ou des haut-parleur(s) sélectionné(s) en direct dans les clients.
<b>Arrêter l'enregistrement manuel</b>	Permet d'arrêter l'enregistrement manuel de l'audio du ou des haut-parleur(s) sélectionné(s) en direct dans les clients.
<b>Lire les signets</b>	Permet de recherches et de lire des détails des signets dans les clients.
<b>Modifier les signets</b>	Permet de modifier des signets dans les clients.
<b>Créer des signets</b>	Permet d'ajouter des signets dans les clients.
<b>Supprimer des signets</b>	Permet de supprimer des signets dans les clients.
<b>Créer et étendre la protection des preuves</b>	<p>Permet à l'utilisateur du client de :</p> <ul style="list-style-type: none"> <li>• Ajouter le haut-parleur à un ou plusieurs verrouillages de preuves nouveaux ou existants</li> <li>• Étendre la durée d'expiration pour les preuves verrouillées existantes</li> <li>• Étendre l'intervalle protégé pour les preuves verrouillées existantes</li> </ul> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #0070c0;">  Exige que les droits d'utilisateur associés à tous les périphériques soient inclus dans le verrouillage des preuves.                 </div>
<b>Supprimer et réduire le verrouillage des preuves</b>	<p>Permet à l'utilisateur du client de :</p> <ul style="list-style-type: none"> <li>• Supprimer le haut-parleur des verrouillages de preuves existants</li> <li>• Voir les preuves verrouillées existantes</li> <li>• Réduire la durée d'expiration pour les preuves verrouillées existantes</li> <li>• Réduire l'intervalle protégé pour les preuves verrouillées existantes</li> </ul>

Nom	Description
	 Exige que les droits d'utilisateur associés à tous les périphériques soient inclus dans le verrouillage des preuves.
<b>Lire le verrouillage des preuves</b>	Permet à l'utilisateur du client de rechercher et de lire les détails des preuves verrouillées.

### Droits relatifs aux haut-parleurs

Spécifiez les droits suivants pour les périphériques à métadonnées :

Nom	Description
<b>Lire</b>	Active le droit de visualisation des périphériques à métadonnées et de récupération des données à partir de ces derniers dans les clients.
<b>Modifier</b>	Active le droit de modification des propriétés pour les métadonnées. Il permet également aux utilisateurs d'activer ou de désactiver les périphériques de métadonnées dans le Management Client et par le biais du MIP SDK.
<b>Visualisation en direct</b>	Active le droit de visualisation de métadonnées à partir des caméras dans les clients. Pour XProtect Smart Client, cette fonction exige également que le rôle ait reçu le droit de visualiser l'onglet <b>En direct</b> des clients. Le droit est attribué dans le cadre des droits sur les applications.
<b>Lecture</b>	Active le droit de lecture de données enregistrées à partir des périphériques de métadonnées dans les clients.
<b>Lire les séquences</b>	Active le droit d'utilisation de la fonctionnalité Séquences tout en parcourant les données enregistrées à partir des périphériques à métadonnées dans les clients.
<b>Exporter</b>	Active le droit d'export d'audio enregistré à partir des périphériques à métadonnées dans les clients.

Nom	Description
<b>Créer et étendre la protection des preuves</b>	Active le droit de création et d'extension du verrouillage des preuves sur les métadonnées dans les clients.
<b>Lire le verrouillage des preuves</b>	Active le droit de consultation du verrouillage des preuves sur les métadonnées dans les clients.
<b>Supprimer et réduire le verrouillage des preuves</b>	Active le droit de suppression ou de réduction du verrouillage des preuves sur les métadonnées dans les clients.
<b>Démarrer l'enregistrement manuel</b>	Active le droit de démarrer l'enregistrement manuel des métadonnées dans les clients.
<b>Arrêter l'enregistrement manuel</b>	Active le droit d'arrêter l'enregistrement manuel des métadonnées dans les clients.

### Droits relatifs aux entrées

Spécifiez les droits suivants pour les périphériques d'entrée :

Nom	Description
<b>Lire</b>	La ou les entrées sélectionnées seront visibles dans les clients.

### Droits relatifs aux sorties

Spécifiez les droits suivants pour les périphériques de sortie :

Nom	Description
<b>Lire</b>	La ou les sortie(s) sélectionnée(s) seront visibles dans les clients. Si visible, la sortie pourra être sélectionnée dans une liste dans les clients.
<b>Activer</b>	La ou les sortie(s) sélectionnée(s) peuvent être activées à partir du Management Client et des clients. Spécifiez le profil de temps ou conservez la valeur par défaut.

### Onglet PTZ (rôles)

Les droits relatifs aux caméras Pan/Tilt/Zoom (PTZ) peuvent être configurés dans l'onglet **PTZ**. Vous pouvez spécifier les fonctions que les utilisateurs/groupes peuvent utiliser dans les clients. Vous pouvez sélectionner des caméras PTZ individuelles ou des groupes de périphériques contenant des caméras PTZ.

Spécifiez les droits suivants pour les périphériques PTZ :

Nom	Description
<b>Manuel PTZ</b>	Détermine si le rôle sélectionné peut utiliser des fonctions PTZ et mettre une patrouille en pause sur la caméra sélectionnée.  Spécifiez un profil de temps, sélectionnez <b>Toujours</b> , ou laissez la valeur par défaut, qui suit le profil de temps par défaut définie dans l'onglet <b>Info</b> pour ce rôle.
<b>Activer des positions prédéfinies PTZ ou des profils de patrouille</b>	Détermine si le rôle sélectionné peut déplacer la caméra sélectionnée vers des positions prédéfinies, démarrer et arrêter des profils de patrouille et mettre des patrouilles en pause.  Spécifiez un profil de temps, sélectionnez <b>Toujours</b> , ou laissez la valeur par défaut, qui suit le profil de temps par défaut définie dans l'onglet <b>Info</b> pour ce rôle.  Pour autoriser ce rôle à utiliser d'autres fonctions PTZ sur la caméra, activez le droit <b>PTZ manuel</b> .
<b>Priorité PTZ</b>	Détermine la priorité des caméras PTZ. Lorsque plusieurs utilisateurs sur

Nom	Description
	<p>un système de surveillance veut contrôler la même caméra PTZ en même temps, des conflits peuvent survenir.</p> <p>Vous pouvez éviter une telle situation en spécifiant une priorité d'utilisation de la ou des caméra(s) PTZ par des utilisateurs/groupes ayant le rôle sélectionné. Spécifiez une valeur de priorité comprise entre 1 et 32 000, où 1 désigne la priorité la plus faible. La priorité par défaut est 3 000. Le rôle disposant du numéro de priorité le plus élevé est celui qui peut contrôler la ou les caméra(s) PTZ.</p>
<p><b>Gérer les positions prédéfinies PTZ ou les profils de patrouille</b></p>	<p>Détermine le droit d'ajouter, de modifier et d'effacer les positions prédéfinies PTZ et les profils de patrouille sur la caméra sélectionnée, dans Management Client et XProtect Smart Client.</p> <p>Pour autoriser ce rôle à utiliser d'autres fonctions PTZ sur la caméra, activez le droit <b>PTZ manuel</b>.</p>
<p><b>Verrouiller/Déverrouiller des positions prédéfinies PTZ</b></p>	<p>Détermine si le rôle peut verrouiller et déverrouiller des positions prédéfinies pour la caméra sélectionnée.</p>
<p><b>Réserver des sessions PTZ</b></p>	<p>Détermine le droit de mettre la caméra sélectionnée en mode session PTZ réservée.</p> <p>Dans une session PTZ réservée, d'autres utilisateurs ou sessions de patrouille dotés d'une priorité PTZ supplémentaire ne peuvent pas prendre le contrôle.</p> <p>Pour autoriser ce rôle à utiliser d'autres fonctions PTZ sur la caméra, activez le droit <b>PTZ manuel</b>.</p>
<p><b>Libérer les sessions PTZ</b></p>	<p>Détermine si le rôle sélectionné peut libérer les sessions PTZ d'autres utilisateurs du Management Client.</p> <p>Vous pouvez toujours libérer vos propres sessions PTZ, même sans cette permission.</p>

### Onglet Audio (rôles)

Pertinent uniquement vous utilisez des haut-parleurs sur votre système. Spécifiez les droits suivants pour les haut-parleurs :

Nom	Description
<b>Parole</b>	Détermine si les utilisateurs doivent être autorisé à parler par le biais du ou des haut-parleur(s) sélectionné(s). Spécifiez le profil de temps ou conservez la valeur par défaut.
<b>Priorité de parole</b>	<p>Lorsque plusieurs utilisateurs de clients souhaitent parler en même temps par l'intermédiaire du même haut-parleur, des conflits peuvent survenir.</p> <p>Pour résoudre ce problème, spécifier une priorité d'utilisation d'un ou plusieurs haut-parleurs par des utilisateurs/groupes ayant le rôle sélectionné. Indiquez une priorité comprise entre <b>Très faible</b> et <b>Très haute</b>. Le rôle doté de la priorité la plus élevée est autorisé à utiliser le haut-parleur avant les autres rôles.</p> <p>Si deux utilisateurs avec le même rôle souhaitent parler en même temps, la règle du premier arrivé premier servi s'applique.</p>

### Onglet Enregistrements à distance (rôles)

Indiquez les paramètres suivants relatifs aux enregistrements à distance :

Nom	Description
<b>Rappeler les enregistrements à distance</b>	Active le droit de rappeler les enregistrements des clients depuis les caméras, microphones, haut-parleurs et périphériques de métadonnées se trouvant dans des sites distants ou sur le stockage externe des caméras.

### Onglet Smart Wall (rôles)

Grâce aux rôles, vous pouvez accorder à vos utilisateurs de clients des droits d'utilisation relatifs à Smart Wall pour la fonction Smart Wall :

Nom	Description
<b>Lire</b>	Autorise les utilisateurs à afficher le Smart Wall sélectionné dans les clients.
<b>Modifier</b>	Autorise les utilisateurs à modifier le Smart Wall sélectionné dans le Management Client.
<b>Supprimer</b>	Autorise les utilisateurs à supprimer le Smart Wall sélectionné dans le Management Client.
<b>Opérer</b>	Autorise les utilisateurs à appliquer des dispositions sur le Smart Wall sélectionné dans le client et à activer le préréglage sélectionné.
<b>Lecture</b>	Autorise les utilisateurs à lire les données enregistrées à partir du Smart Wall sélectionné dans les clients.

### Onglet Événement externe (rôles)

Spécifiez les droits suivants relatifs aux événements externes :

Nom	Description
<b>Lire</b>	Autorise les utilisateurs à chercher et consulter les événements système externes sélectionnés dans les clients et dans le Management Client.
<b>Modifier</b>	Autorise les utilisateurs à modifier l'événement système externe sélectionné dans le Management Client.
<b>Supprimer</b>	Autorise les utilisateurs à supprimer l'événement système externe sélectionné dans le Management Client.
<b>Déclencher</b>	Autorise les utilisateurs à déclencher l'événement système externe sélectionné dans les clients.

### Onglet Groupe de vues (rôles)

Dans l'onglet **Groupe de vues**, vous pouvez spécifier quels groupes les utilisateurs et groupes d'utilisateurs dotés du rôle sélectionné sont autorisés à utiliser dans le client.



Spécifiez les droits suivants pour les groupes de vues :

Nom	Description
<b>Lire</b>	Active le droit de visualisation des groupes de vues dans les clients et dans le Management Client. Les groupes de vues sont créés dans le Management Client.
<b>Modifier</b>	Active le droit de modification des propriétés pour les groupes de vues dans le Management Client.
<b>Supprimer</b>	Active le droit de suppression des groupes de vues dans le Management Client.
<b>Opérer</b>	Active le droit d'utilisation de groupes de vues dans XProtect Smart Client. Autrement dit, la création de sous-groupes et de vues.

### Onglet Serveurs (rôles)

La spécification des droits d'un rôle dans l'onglet **Serveurs** n'est appropriée que si votre système fonctionne dans une configuration Milestone Federated Architecture.

Nom	Description
<b>Sites</b>	Active le droit de visualiser le site sélectionné dans le Management Client. Les sites connectés sont connectés par le biais de Milestone Federated Architecture.  Pour modifier les propriétés vous devez avoir des permissions de modification sur le serveur de gestion de chaque site.

Pour de plus amples informations, voir En cours de configuration de Milestone Federated Architecture sur la page 456.

### Onglet Matrix (rôles)

Si vous avez configuré des destinataires Matrix sur votre système, vous pouvez configurer des droits de rôle Matrix. À partir d'un client, vous pouvez envoyer la vidéo aux destinataires Matrix. Sélectionnez les utilisateurs qui peuvent la recevoir sur l'onglet Matrix.

Sont disponibles les droits suivants :

Nom	Description
<b>Lire</b>	Déterminez si les utilisateurs et groupes dotés du rôle sélectionné peuvent sélectionner et envoyer des vidéos au destinataire Matrix à partir des clients.

### Onglet alarmes (rôles)

Si vous utilisez des alarmes dans votre configuration système afin d'offrir une vue d'ensemble centrale et un meilleur contrôle de votre installation (incluant tout autre serveur XProtect), vous pouvez utiliser l'onglet **Alarmes** pour spécifier les droits d'alarme dont devraient disposer les utilisateurs/groupes dotés du rôle sélectionné, pour définir la façon de traiter les alarmes dans les clients, par exemple.

Spécifiez les droits suivants pour les alarmes :

Nom	Description
<b>Gestion</b>	Active le droit de gérer les alarmes, pour, par exemple, modifier les priorités des alarmes et réaffecter des alarmes à d'autres utilisateurs, acquitter les alarmes et modifier l'état de plusieurs alarmes en même temps, pour les faire passer de <b>Nouveau</b> à <b>Assigné</b> , par exemple.
<b>Vue</b>	Active le droit d'afficher les alarmes et d'imprimer les rapports d'alarme.
<b>Désactiver alarmes</b>	Active le droit de désactiver les alarmes.
<b>Recevoir des notifications</b>	Active le droit de recevoir des notifications à propos des alarmes dans les clients XProtect Mobile et XProtect Web Client.

### Onglet Contrôle d'accès (rôles)

Lorsque vous ajoutez ou modifiez des utilisateurs de base, des utilisateurs Windows ou des groupes, vous pouvez indiquer des paramètres de contrôle d'accès :

Nom	Description
<b>Utiliser le contrôle d'accès</b>	Permet à l'utilisateur d'utiliser les fonctions relatives au contrôle d'accès dans les clients.
<b>Voir la liste des détenteurs de cartes</b>	Permet à l'utilisateur de voir la liste des détenteurs de cartes sur l'onglet <b>Contrôle d'accès</b> dans les clients.
<b>Recevoir des notifications</b>	Permet à l'utilisateur de recevoir des notifications concernant les demandes d'accès dans les clients.

### Onglet LPR (rôles)

Si votre système fonctionne sous XProtect LPR, spécifiez les droits suivants pour les utilisateurs :

Nom	Description
<b>Utiliser LPR</b>	Active le droit d'utiliser n'importe quelles fonctions relatives à LPR dans les clients.
<b>Gérer les listes de correspondance de plaques d'immatriculation</b>	Active le droit d'ajouter, importer, modifier, exporter et supprimer les listes de correspondance de plaques d'immatriculation dans le Management Client.
<b>Lire les listes de correspondance de plaques d'immatriculation</b>	Active le droit d'afficher les listes de correspondance de plaques d'immatriculation.

### Onglet MIP (rôles)



Au travers du MIP SDK, un vendeur tiers peut développer des modules d'extension personnalisés pour votre système, par exemple, l'intégration à des systèmes de contrôle d'accès externes ou similaires.

Les paramètres que vous modifiez dépendent du module d'extension. Les paramètres personnalisés pour les modules d'extension sont indiqués dans l'onglet **MIP**.

## Utilisateurs basiques (explications)

Lorsque vous ajoutez un utilisateur de base sur votre système, vous créez un compte d'utilisateur de système de surveillance dédié avec une authentification par nom d'utilisateur de base et mot de passe pour l'utilisateur individuel. Contrairement à l'utilisateur Windows, ajouté avec Active Directory.

Lorsque vous travaillez avec des utilisateurs basiques, il est important de comprendre la différence entre un utilisateur basique et un utilisateur Windows.

-  Les utilisateurs basiques sont soumis à une authentification alliant un nom d'utilisateur et un mot de passe et sont spécifiques à un système. Même si les utilisateurs basiques ont le même nom d'utilisateur et mot de passe, un utilisateur basique créé sur l'un des sites fédérés n'a pas accès à un autre site fédéré
-  Les utilisateurs Windows sont authentifiés à partir de leurs identifiants de connexion Windows et sont spécifiques à une machine

## Créer des utilisateurs de base

Pour créer un utilisateur de base sur votre système :

1. Développez **Sécurité > Utilisateurs de base**.
2. Dans le volet **Utilisateurs basiques**, faites un clic droit et sélectionnez **Créer un utilisateur basique**.
3. Indiquez un nom d'utilisateur et un mot de passe et répétez-les pour être sûr de les avoir indiqués correctement.



Le mot de passe doit respecter les prérequis de complexité exigés par le système d'exploitation Windows sur l'ordinateur où est installé le service Management Server.

4. Cliquez sur **OK** pour créer l'utilisateur de base.

## Navigation sur le site : Tableau de bord système

Cet article décrit comment surveiller votre système, y compris comment créer des rapports et protéger des données.

### Tableau de bord du système (explications)

Le tableau de bord système vous offre des fonctions de surveillance de votre système et de ses composants.

Vous pouvez accéder aux fonctions suivantes :

Nom	Description
<b>Moniteur système</b>	Surveillez l'état de vos serveurs et caméras selon des paramètres définis par vos soins.
<b>Seuils du moniteur système</b>	Définissez des valeurs seuils pour les paramètres surveillés sur le serveur et surveillez les tuiles utilisées dans le moniteur système.
<b>Verrouillage des preuves</b>	Obtenez une vue d'ensemble de toutes les données protégées dans le système.
<b>Tâche actuelle</b>	Pour obtenir un aperçu des tâches en cours sur un serveur d'enregistrement sélectionné.
<b>Rapports de configuration</b>	Pour décider des éléments à inclure dans vos rapports de configuration système avant leur impression.

## Moniteur système (explication)

Le moniteur système vous offre une vue d'ensemble visuelle et rapide de l'état actuel des serveurs et caméras de votre système par le biais de tuiles colorées représentant le matériel du système. Par défaut, le système affiche des tuiles représentant tous les **Serveurs d'enregistrement**, **Tous les serveurs** et **Toutes les caméras**.

La couleur des tuiles :

Couleur des tuiles	Description
<b>Vert</b>	État <b>normal</b> . Tout fonctionne normalement.
<b>Jaune</b>	État d' <b>avertissement</b> . Un ou plusieurs paramètres de surveillance se trouvent au-dessus de la valeur de seuil (voir Seuils du Moniteur système (explication) sur la page 425) pour l'état <b>Normal</b> .
<b>Rouge</b>	État <b>critique</b> . Un ou plusieurs paramètres de surveillance se trouvent au-dessus de la valeur de seuil pour l'état <b>Normal</b> et l'état d' <b>Avertissement</b> .

Vous pouvez personnaliser les tuiles des serveurs et des caméras si vous souhaitez afficher plus ou moins de tuiles sur le tableau de bord. Par exemple, vous pouvez configurer des tuiles afin de représenter un serveur unique, une caméra individuelle, un groupe de caméras ou un groupe de serveurs. Vous pouvez également supprimer une tuile si vous ne souhaitez pas l'utiliser ou modifier ses paramètres de surveillance. Les paramètres de surveillance sont, par exemple, l'usage du processeur ou la mémoire disponible pour un serveur. Si vous supprimez ces paramètres de la tuile du serveur, la tuile ne surveille pas ces paramètres sur la tuile correspondante. Cliquez sur **Personnaliser** dans le coin supérieur droit de l'onglet pour ouvrir la fenêtre Personnaliser le tableau de bord. Voir [Personnaliser le tableau de bord](#) pour plus d'informations.

Les tuiles changent d'état et donc de couleur en fonction des valeurs de seuil définies dans les Seuils du moniteur système. Bien que le système définisse des valeurs de seuil par défaut, vous pouvez décider par vous-même de la valeur de seuil pour chacun des trois états. Pour configurer ou modifier les valeurs de seuil, vous pouvez utiliser des **Seuils du moniteur système**. Voir [Seuils du Moniteur système \(explication\)](#) sur la page 425.

Si une tuile change de couleur et si vous souhaitez savoir quel serveur/paramètre a entraîné son changement de couleur, il vous suffit de cliquer sur la tuile. Une vue d'ensemble s'ouvre alors en bas de l'écran et présente les couleurs rouge, jaune ou verte pour chaque paramètre de surveillance que vous avez activé pour votre tuile. Cliquez sur le bouton **Détails** pour obtenir des informations plus détaillées au sujet des raisons du changement d'état.



Si un signal d'alerte apparaît, en passant la souris dessus, un message d'erreur s'affichera.



La fonction moniteur système nécessite que le service Data Collector soit en fonctionnement.

## Personnaliser le tableau de bord

### Ajouter une nouvelle tuile de caméra ou de serveur :

1. Dans la fenêtre Moniteur système, cliquez sur **Personnaliser**.
2. Dans la fenêtre **Personnaliser le tableau de bord** qui s'ouvre, cliquez sur **Nouveau** sous **Tuiles de serveur** ou **Tuiles de caméras**.
3. Dans la fenêtre **Nouvelle tuile de serveur/Nouvelle tuile de caméra**, sélectionnez les caméras ou les serveurs à surveiller.
4. Dans **Paramètres de surveillance**, cochez ou décochez les cases correspondant aux paramètres à ajouter ou supprimer à partir de la tuile pertinente.
5. Cliquez sur **OK**. La nouvelle tuile de serveur ou de caméra est maintenant ajoutée aux tuiles affichées sur votre tableau de bord.

### Modifier les paramètres de surveillance :

1. Dans la fenêtre du tableau de bord du Moniteur système, cliquez sur **Personnaliser**.
2. Dans la fenêtre **Personnaliser le tableau de bord** qui s'ouvre, cliquez sur **Modifier** sous **Tuiles de serveur** ou **Tuiles de caméras**.
3. Dans la fenêtre **Modifier la tuile du serveur** ou **Modifier la tuile de la caméra**, sélectionnez le composant du serveur ou les caméras que vous souhaitez modifier.
4. Dans la case **Paramètres de surveillance**, cochez ou décochez les cases correspondant aux paramètres de surveillance à ajouter ou supprimer à partir de la tuile pertinente.
5. Cliquez sur **OK**. Les paramètres de surveillance ainsi modifiés font maintenant partie de la tuile correspondante ou en ont disparu.



Vous pouvez activer et désactiver des données d'historique sur le système à votre guise. Si vous désactivez ces données, vous ne pourrez pas afficher les graphiques de comportement de système précédant. Si vous voulez réduire la charge sur le SQL Server et la base des données ou sur la bande passante, vous pouvez réduire l'intervalle d'échantillonnage des données d'historique. Si vous réduisez l'intervalle d'échantillonnage des données d'historique, les graphiques contiendront moins de détails.

### Détails du moniteur système (explications)

Si vous cliquez sur un serveur ou une tuile de caméras, vous pouvez consulter l'état de chaque paramètre de surveillance sélectionné sous le tableau de bord.

State	Name	Live FPS	Recording FPS	Used space	
	Panasonic SPxxx/SFxxx/SWxxx no I/O Camera Series	<div style="width: 100%; height: 10px; background-color: yellow;"></div>	<div style="width: 100%; height: 10px; background-color: green;"></div>	<div style="width: 100%; height: 10px; background-color: green;"></div>	Details

Exemple : Les paramètres de surveillance FPS en direct d'une caméra a atteint l'état d'Avertissement.

Le champ **État** affiche l'état de la caméra. Par exemple, un avertissement apparaît en rouge si la connexion avec le périphérique est rompue. L'icône comprend une astuce avec une brève description du problème à l'origine de l'avertissement.

Le champ **Espace utilisé** présente des données d'autres serveurs d'enregistrement sur lesquels ce périphérique a des enregistrements, si le périphérique était précédemment situé sur d'autres serveurs d'enregistrement, par exemple.

Si vous cliquez sur le bouton **Détails** correspondant à la caméra/au serveur concerné, vous pouvez consulter des informations système et créer des rapports au sujet de :

Composant	Description
<b>Serveur de gestion</b>	Présente des données provenant du serveur de gestion sélectionné
<b>Serveur(s) d'enregistrement</b>	Présente des données provenant du serveur d'enregistrement sélectionné. Vous pouvez les afficher en fonction du : <ul style="list-style-type: none"> <li>• Disque</li> <li>• Stockage</li> <li>• Réseau</li> <li>• Caméra</li> </ul>
<b>Serveurs d'enregistrement de redondance</b>	Présente des données provenant du serveur d'enregistrement de redondance sélectionné.
<b>Serveurs supplémentaires</b>	Affiche les données sur le serveur de journaux, les serveurs d'événements et bien plus encore.
<b>Caméras</b>	Affiche les données de toute caméra de n'importe quel groupe au sein de votre configuration.

Chacun de ces éléments est un espace sur lequel vous pouvez cliquer et que vous pouvez agrandir. Lorsque vous cliquez dans cet espace, vous obtenez des données dynamiques pertinentes au sujet de ce serveur ou de cette caméra.

La barre **Caméras** contient une liste des groupes de caméras sélectionnables. Une fois qu'un groupe est sélectionné, choisissez une caméra spécifique et affichez ses données dynamiques. Tous les serveurs affichent des informations sur l'utilisation CPU et la mémoire disponibles. Les serveurs d'enregistrement affichent également des informations sur l'état de connexion. Vous pouvez trouver dans chaque vue le lien **Historique**. Cliquez sur ce lien pour afficher les données et les rapports historiques (pour afficher des rapports sur une caméra, cliquez sur le nom de la caméra). Pour chaque rapport historique, vous pouvez visualiser les données des 24 dernières heures, 7 jours ou 30 jours. Pour enregistrer et / ou imprimer des rapports, cliquez sur l'icône **Envoyer vers un PDF**. Utilisez les icônes < et Accueil pour naviguer dans le moniteur système.



Vous ne pouvez créer des rapports historiques qu'avec des données provenant du serveur d'enregistrement sur lequel le périphérique se trouve actuellement.





Si vous accédez aux détails du moniteur système à partir d'un système d'exploitation serveur, il est possible qu'un message sur la **Configuration de sécurité améliorée d'Internet Explorer** apparaisse. Suivez les instructions dans le message pour ajouter la page du **Moniteur système** à la **Zone des sites de confiance** avant de continuer.

## Seuils du Moniteur système (explication)

Les seuils du moniteur système vous permettent de configurer et d'ajuster les seuils généraux à partir desquels les tuiles du moniteur système devraient indiquer par un signal visuel que votre matériel change d'état, lorsque l'usage du processeur d'un serveur passe d'un état normal (vert) à un état d'avertissement (jaune) par exemple.

Le système est configuré avec des valeurs de seuil par défaut. Vous pouvez donc commencer à surveiller le matériel de votre système dès que votre système est configuré. Pour modifier les valeurs de seuil, voir Définir les seuils du moniteur système sur la page 427

Par défaut, le système est configuré de façon à afficher les valeurs de seuil pour toutes les unités d'un matériel particulier, comme, par exemple, toutes les caméras ou tous les serveurs. Vous pouvez également configurer des valeurs de seuil pour des serveurs et caméras individuels ou pour une partie de ceux-ci. Par exemple, il est conseillé d'établir des valeurs de seuil pour des serveurs ou caméras individuels si certaines caméras doivent être autorisées à utiliser un **FPS en direct** ou un **FPS d'enregistrement** plus élevé que les autres caméras.

Vous pouvez configurer les valeurs de seuil pour des serveurs, des caméras, des disques et des espaces de stockage. Si vous souhaitez modifier les valeurs de seuil, vous pouvez utiliser le curseur de contrôle des seuils. Le curseur de contrôle des seuils vous permet d'accroître ou de réduire les valeurs de seuil en faisant glisser les poignées séparant les différents états vers le haut ou le bas. Le curseur de contrôle des seuils est divisé en différentes couleurs similaires à celles affichées sur les tuiles de serveurs ou de caméras de votre Moniteur système (voir Seuils du Moniteur système (explication) sur la page 425).

Pour vous assurer de ne pas observer d'état **Critique** ou **Avertissement** dans les cas où l'usage ou la charge du matériel de votre système atteint une valeur de seuil élevée pendant une seconde ou une période similaire, utilisez la fonctionnalité **Intervalle de calcul**. La fonctionnalité Intervalle de calcul répartit l'effet de changements brefs ou fréquents de l'état d'un matériel du système. Dans la pratique, cela signifie que la fonctionnalité Intervalle de calcul nivelle les effets des changements du matériel au fil de temps, de sorte que vous ne receviez pas d'alerte à chaque fois qu'un seuil est dépassé.

Par exemple, vous pouvez fixer la fonctionnalité **Intervalle de calcul** sur une (1) minute, pour vous assurer de ne recevoir d'alertes que lorsque la valeur moyenne de la minute entière dépasse le seuil. L'avantage de ce système est que vous évitez de recevoir des alertes au sujet de changements fréquents et potentiellement non pertinents pour ne recevoir que les alertes reflétant des problèmes récurrents au niveau de l'usage du processeur ou de la mémoire, par exemple. Pour changer les valeurs des intervalles de calcul, voir Définir les seuils du moniteur système sur la page 427

## Seuils de serveur

Seuil	Description	Unité
<b>Utilisation unité centrale</b>	Les seuils correspondant à l'usage du processeur sur les serveurs que vous surveillez.	%
<b>Mémoire disponible</b>	Les seuils correspondant à la mémoire RAM utilisée sur les serveurs que vous surveillez.	Mo
<b>Décodage NVIDIA</b>	Les seuils correspondant à l'usage du décodeur NVIDIA sur les serveurs que vous surveillez.	%
<b>Mémoire NVIDIA</b>	Les seuils correspondant à la mémoire NVIDIA RAM utilisée sur les serveurs que vous surveillez.	%
<b>Rendu de NVIDIA</b>	Les seuils correspondant au rendu NVIDIA sur les serveurs que vous surveillez.	%

## Seuils de caméras

Seuil	Description	Unité
<b>FPS en direct</b>	Les seuils pour le FPS des caméras en cours d'utilisation lorsque des vidéos en direct sont diffusées sur les caméras que vous surveillez.	%
<b>FPS d'enregistrement</b>	Les seuils pour le FPS des caméras en cours d'utilisation lorsque le système enregistre des vidéos sur les caméras que vous surveillez.	%
<b>Espace utilisé</b>	Les seuils correspondant à l'espace utilisé par les caméras que vous surveillez.	Go

## Seuils de disques

Seuil	Description	Unité
Espace libre	Les seuils correspondant à l'espace disponible sur les disques que vous surveillez.	Go

## Seuils de stockage

Seuil	Description	Unité
Durée de rétention	Le seuil présentant une prédiction du moment où votre stockage ne disposera plus d'espace libre. L'état indiqué est basé sur la configuration de votre système et est mis à jour deux fois par jour.	Jours

Vous pouvez également configurer des règles (voir Règles sur la page 338) afin d'effectuer des actions spécifiques ou d'activer des alarmes (voir Tableau de bord du système (explications) sur la page 420) lorsqu'un seuil passe d'un état à un autre.

## Définir les seuils du moniteur système

1. Dans le volet de **Navigation sur le site**, sélectionnez **Seuils du moniteur système**.
2. Cochez la case **Activer** du matériel pertinent si vous ne l'avez pas encore fait. La figure ci-dessous illustre un exemple.

The screenshot shows the 'System monitor thresholds' configuration interface. On the left, a sidebar lists 'Server', 'Camera', 'Disk', and 'Storage'. The 'CPU usage' section is selected. It features a 'CPU thresholds' chart with three horizontal bars: a red bar for 'Critical' at 80%, a yellow bar for 'Warning' at 60%, and a green bar for 'Normal'. The 'Enabled' checkbox is checked. To the right, the 'Calculation interval' is set to 300 seconds. At the bottom right, there are 'Advanced' and 'Create rule...' buttons.

3. Faites glisser le curseur de contrôle des seuils vers le haut ou le bas afin d'accroître ou de réduire la valeur du seuil. Il y a deux curseurs disponibles pour chaque périphérique matériel présenté dans le contrôle des seuils, qui séparent les niveaux **Normal**, **Avertissement** et **Critique**.
4. Indiquez la valeur de l'intervalle de calcul ou conservez la valeur par défaut.
5. Si vous souhaitez définir les valeurs sur des périphériques individuels, cliquez sur **Avancé**.
6. Si vous souhaitez spécifier des règles pour certains événements ou au sein d'intervalles de temps spécifiques, cliquez sur **Créer une règle**.
7. Une fois que vous avez réglé les différents niveaux de seuils et intervalles de calcul, sélectionnez **Fichier > Enregistrer** dans le menu.

Exemple de paramètre de seuil :



- Rouge : indique vous avez atteint l'état Critique
- Jaune : il s'agit d'un état d'avertissement indiquant que vous avez presque atteint l'état Critique
- Vert : indique un déroulement normal, au sein des valeurs de seuil sélectionnées

## Protection des preuves (explications)



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



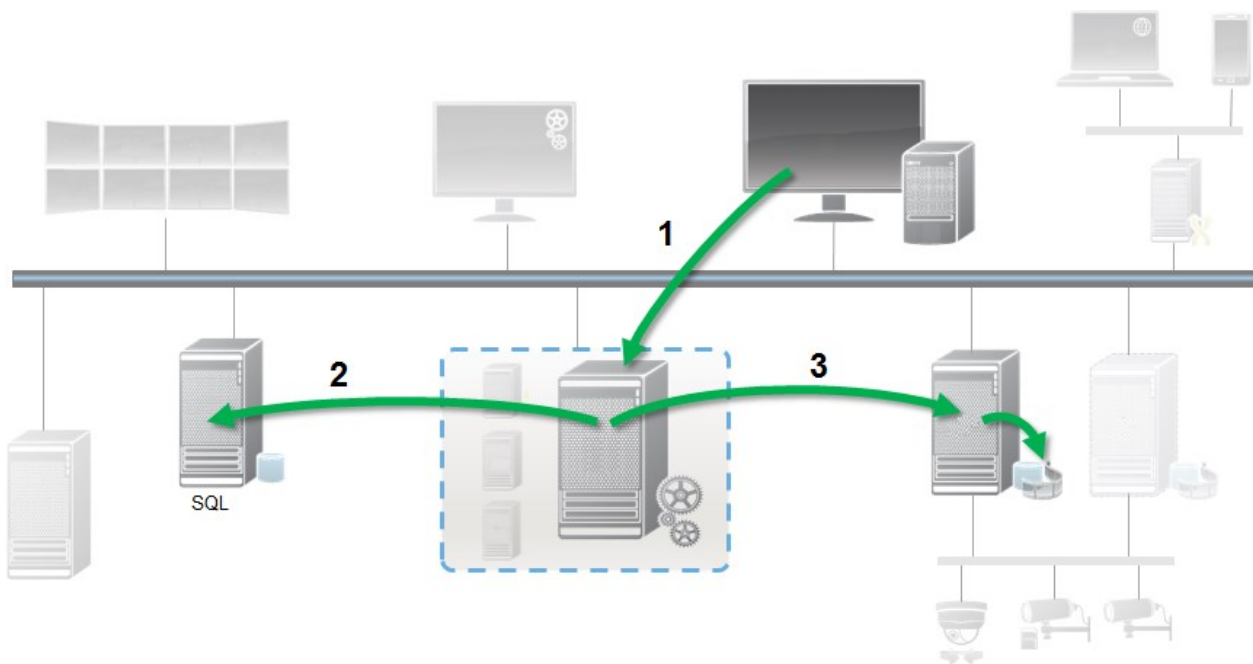
À partir de la version 2020 R2 de VMS XProtect, lorsque vous mettez à niveau le serveur de gestion vers une version plus récente, celui-ci ne pourra plus créer ou modifier la protection des preuves associées aux serveurs d'enregistrement de la version 2020 R1 ou une version antérieure, jusqu'à leur mise à niveau.

Par ailleurs, il est impossible de créer ou modifier la protection des preuves si le matériel a été transféré d'un serveur d'enregistrement (2020 R1 ou d'une version antérieure) à un autre serveur d'enregistrement et qu'il contient des enregistrements.

Avec la fonctionnalité de protection des preuves, les opérateurs du client peuvent protéger des séquences vidéo, y compris l'audio et d'autres données, contre toute suppression, si nécessaire, par exemple, lorsqu'une enquête ou un procès est en cours. Pour plus d'informations sur la façon de protéger des preuves, référez-vous à la documentation XProtect Smart Client.

Lorsque les données sont protégées, elles ne peuvent pas être supprimées, ni automatiquement par le système après le temps de rétention par défaut du système ou dans d'autres situations, ni manuellement par les utilisateurs du client. Le système ou un utilisateur ne peut pas supprimer les données tant qu'un utilisateur disposant des droits d'utilisateur suffisants ne déverrouille pas la protection de la preuve.

Organigramme pour la protection des preuves :



1. L'utilisateur crée une protection des preuves dans XProtect Smart Client. Des informations sont envoyées au serveur de gestion.
2. Management Server stocke les informations au sujet de la protection des preuves sur la base de données SQL.
3. Le serveur de gestion informe le serveur d'enregistrement qu'il faut stocker et protéger les enregistrements protégés dans la base de données.

Lorsque l'opérateur crée une protection des preuves, les données protégées restent dans l'espace de stockage des enregistrements dans lequel elles ont été enregistrées et sont déplacées vers des disques d'archivage en même temps que les données non protégées, mais les données protégées :

- Se conforment à la durée de rétention configurée pour la protection des preuves. Potentiellement indéfiniment
- Conservent la qualité d'origine des enregistrements, même si la réduction a été configurée pour les données non protégées

Lorsqu'un opérateur crée des protections, la taille minimum d'une séquence est la durée choisie par la base de données pour diviser les fichiers enregistrés. Par défaut, cette durée est fixée à une heure. Vous pouvez modifier ce paramètre, mais vous devrez alors personnaliser le fichier RecorderConfig.xml sur le serveur d'enregistrement. Si une petite séquence s'étend sur deux périodes d'une heure, le système verrouille les enregistrements des deux périodes.

Dans le journal d'activité du Management Client, vous pouvez voir à quel moment un utilisateur crée, modifie ou supprime des protections des preuves.

Lorsqu'un disque est à court d'espace libre, cela n'affecte aucunement les données protégées. Ce sont alors les données non protégées les plus anciennes qui sont supprimées. S'il n'y a plus de données non protégées à supprimer, le système s'arrête d'enregistrer. Vous pouvez créer des règles et des alarmes déclenchées par des événements disque plein, de façon à en être informé automatiquement.

À l'exception des cas où plus de données sont stockées sur une longue période et ont un impact potentiel sur l'espace de stockage du disque, la fonction de protection des preuves en elle-même n'influe pas sur la performance du système.

Si vous déplacez du matériel (voir Déplacer le matériel sur la page 500) vers un autre serveur d'enregistrement :

- Les enregistrements protégés par la protection des preuves restent sur l'ancien serveur d'enregistrement conformément à la durée de rétention fixée pour la protection des preuves lors de sa création
- L'utilisateur XProtect Smart Client peut continuer à protéger les données à l'aide de la protection des preuves sur les enregistrements effectués sur une caméra avant qu'elle n'ait été déplacée vers un autre serveur d'enregistrement. Ceci est vrai même si vous déplacez la caméra plusieurs fois et si les enregistrements sont stockés sur de multiples serveurs d'enregistrement

Par défaut, tous les opérateurs ont un profil de protection des données par défaut qui leur est assigné, mais ne disposent pas des droits d'accès de l'utilisateur à cette fonction. Pour indiquer les droits d'accès à la protection des preuves d'un rôle, voir l'Onglet Périphériques (rôles) sur la page 405 pour les paramètres de rôle. Pour indiquer le profil de la protection des preuves d'un rôle, voir l'Onglet Info (rôles) sur la page 374 pour les paramètres de rôle.

Dans le Management Client, vous pouvez modifier les propriétés du profil de protection des preuves par défaut et créer des profils de protection de preuves supplémentaires et les affecter aux rôles à la place.

**Protection des preuves** sous **Tableau de bord du système** affiche un aperçu de toutes les données protégées sur le système de surveillance actuel :

- La date de début et de fin pour les données protégées
- L'utilisateur qui a protégé la preuve
- Le moment où la preuve n'est plus protégée
- L'endroit où les données sont stockées
- La taille de chaque preuve protégée

Toutes les informations affichées dans **Protection des preuves** sont des captures d'écran. Appuyez sur F5 pour actualiser.

## Tâches actuelles (explications)

Le nœud **Tâches actuelles** affiche un aperçu des tâches sous un serveur d'enregistrement sélectionné, leur heure de début, l'heure de fin estimée et la progression. Toutes les informations affichées dans les **tâches actuelles** sont des captures d'écran. Vous pouvez les rafraîchir en cliquant sur le bouton **Actualiser** en bas à droite du volet **Propriétés**.

## Rapports de configuration (explications)

Lors de la création de rapports de configuration au format PDF, vous pouvez inclure n'importe quel élément de votre système dans le rapport. Vous pouvez par exemple y inclure des licences, la configuration d'un périphérique, la configuration des alarmes et bien plus encore. Vous pouvez également personnaliser votre mise en page et votre police et inclure une page de couverture personnalisée.

## Créer un rapport de configuration

1. Développez le **Tableau de bord système**, puis cliquez sur **Rapports de configuration**. Cela génère la page de configuration du rapport.
2. Sélectionnez les éléments que vous souhaitez inclure à votre rapport.
3. **Facultatif** : Cliquez sur **Page de couverture** afin de personnaliser votre première page. Dans la fenêtre qui s'affiche, complétez les informations requises. Sélectionnez la **Page de couverture** comme un élément à inclure dans votre rapport, sinon la première page que vous personnalisez ne sera pas intégrée à votre rapport.
4. Cliquez sur **Formatage** afin de personnaliser votre police, votre mise en page et vos marges. Dans la fenêtre qui s'affiche, sélectionnez les paramètres désirés.
5. Une fois que vous êtes prêt à exporter, cliquez sur **Exporter**, sélectionnez un nom et sauvegardez l'emplacement de votre rapport.

## Configurer les détails du rapport

Les éléments suivants sont accessibles lors de la configuration des rapports :

Nom	Description
<b>Sélectionner tout</b>	Sélectionne tous les éléments de la liste.
<b>Effacer tout</b>	Efface tous les éléments de la liste.
<b>Page de</b>	Pour personnaliser la page de couverture du rapport.

Nom	Description
<b>couverture</b>	
<b>Formatage</b>	Pour formater le rapport.
<b>Exporter</b>	Pour sélectionner un emplacement d'enregistrement du rapport et créer un fichier PDF.

## Navigation sur le site : Journaux des serveurs

Cet article décrit comment changer les paramètres de connexion, les journaux de filtre, et la création d'exportations.

### Journaux (explications)

Les journaux sont un enregistrement détaillé de l'activité des utilisateurs, des événements, des actions, et des erreurs au sein du système.

Pour afficher les journaux, accédez au volet **Navigation sur le site** et sélectionnez **Journaux des serveurs**.

Type de journaux	Quels éléments sont-ils enregistrés ?
<b>Journaux système</b>	Informations associées au système
<b>Journaux d'audit</b>	Activité des utilisateurs
<b>Journaux déclenchés par les règles</b>	Les règles dans lesquelles les utilisateurs ont spécifié l'action <b>Créer une &lt;entrée au journal&gt;</b> . Pour plus d'informations sur l'action <entrée au journal>, voir Actions et actions d'arrêt (explications) sur la page 314.

Pour afficher les journaux dans une autre langue, voir Onglet Général (options) sur la page 123 sous **Options**.

Pour exporter les journaux en tant que fichiers présentant des valeurs séparées par des virgules (.csv), consultez la rubrique Exporter les journaux sur la page 434.



Pour modifier les paramètres des journaux, reportez-vous à l'Onglet Journaux de serveurs (options) sur la page 126.

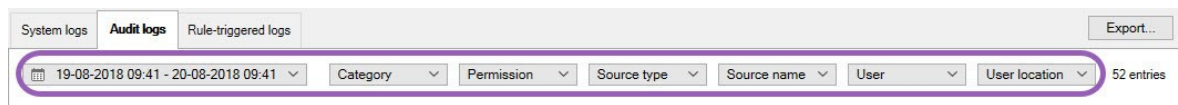
## Filtrer les journaux

Chaque fenêtre de journal vous permet d'appliquer des filtres pour afficher les entrées en fonction d'une échelle chronologique, un périphérique ou un utilisateur spécifique.

1. Dans le volet **Navigation sur le site**, sélectionnez **Journaux des serveurs**. Par défaut, l'onglet **Journaux système** s'affiche.

Sélectionnez un autre onglet pour naviguer entre les types de journaux.

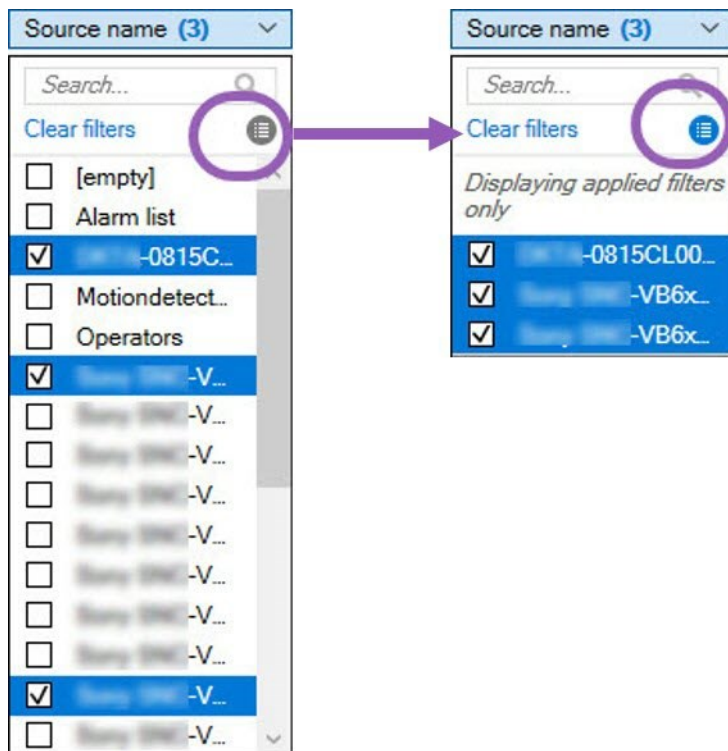
2. Dans les onglets, sélectionnez un groupe de filtres, par exemple, **Catégorie**, **Type de source**, ou **Utilisateur**.



Une liste de filtres s'affiche.

3. Sélectionnez un filtre pour l'appliquer. Sélectionnez le filtre à nouveau pour le supprimer.

Facultatif : Dans une liste de filtres, sélectionnez **Afficher les filtres appliqués uniquement** pour n'afficher que les filtres que vous avez appliqués.





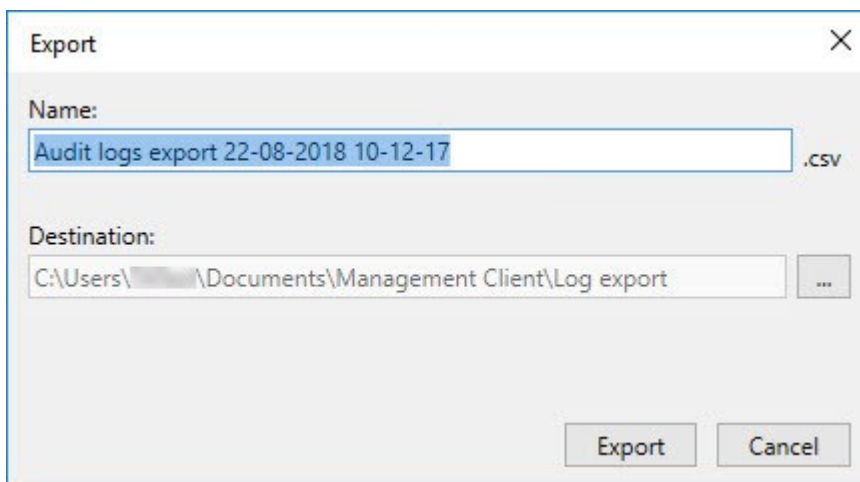
Le contenu de votre exportation est modifié en fonction des filtres appliqués. Pour obtenir des informations sur votre exportation, voir Exporter les journaux sur la page 434.

## Exporter les journaux

L'exportation de journaux vous permet d'enregistrer les entrées des journaux au-delà de la durée de rétention des journaux par exemple. Vous pouvez exporter les journaux sous forme de fichiers présentant des valeurs séparées par des virgules (.csv).

Pour exporter un journal :

1. Sélectionnez **Exporter** dans le coin supérieur droit. La fenêtre **Exporter** s'ouvre.



2. Dans la fenêtre **Exporter**, dans le champ **Nom**, indiquez un nom pour le fichier journal.
3. Par défaut, les fichiers de journaux exportés sont sauvegardés dans votre dossier **Exportation de journaux**. Pour spécifier un emplacement différent, sélectionnez **...** à droite du champ **Destination**.
4. Sélectionnez **Exporter** pour exporter le journal.



Le contenu de votre exportation est modifié en fonction des filtres appliqués. Pour obtenir des informations sur votre exportation, voir Filtrer les journaux sur la page 433.

## Autoriser la version 2018 R2 et les composants antérieurs à écrire dans les journaux

La version 2018 R3 du serveur de journaux intègre l'authentification pour renforcer la sécurité. Ainsi, les versions 2018 R2 et les composants antérieurs ne peuvent pas écrire dans les journaux sur le nouveau serveur de journaux.

Composants affectés :

- XProtect Smart Client
- Plug-in XProtect LPR
- LPR Server
- Modules d'extension du contrôle d'accès
- Event Server
- Module d'extension de l'alarme

Si vous utilisez la version 2018 R2 ou une version antérieure des composants énumérés ci-dessus, vous devez déterminer si vous autorisez le composant à écrire sur les journaux dans le nouveau serveur de journaux :

1. Sélectionnez **Outils > Options**.
2. Dans la boîte de dialogue **Options**, au bas de l'onglet **Journaux des serveurs**, trouvez la case **Autoriser la version 2018 R2 et les composants antérieurs à écrire dans les journaux**.
  - Cochez la case Autoriser la version 2018 R2 et les composants antérieurs à écrire dans les journaux
  - Décochez la case si vous ne souhaitez pas autoriser la version 2018 R2 et les composants antérieurs à écrire dans les journaux

## Journaux système (propriétés)

Chaque ligne dans un journal représente une entrée de journal. Une entrée de journal contient un certain nombre de champs d'informations :

Nom	Description
Niveau de journal	Info, avertissement, ou erreur.
Heure locale	Horodaté en heure locale du serveur de votre système.
Texte du message	Numéro d'identification de l'incident journalisé.
Catégorie	Type d'incident journalisé.
Type de source	Type d'équipement sur lequel l'incident journalisé est intervenu, par exemple,

Nom	Description
	serveur ou périphérique.
<b>Nom de la source</b>	Nom de l'équipement sur lequel l'incident journalisé est intervenu.
<b>Type d'événement</b>	Type d'événement correspondant à l'incident journalisé.

## Journaux d'activité (propriétés)

Chaque ligne dans un journal représente une entrée de journal. Une entrée de journal contient un certain nombre de champs d'informations :

Nom	Description
<b>Heure locale</b>	Horodaté en heure locale du serveur de votre système.
<b>Texte du message</b>	Affiche une description de l'incident journalisé.
<b>Autorisation</b>	Informations indiquant si l'action de l'utilisateur distant était autorisée ou non.
<b>Catégorie</b>	Type d'incident journalisé.
<b>Type de source</b>	Type d'équipement sur lequel l'incident journalisé est intervenu, par exemple, serveur ou périphérique.
<b>Nom de la source</b>	Nom de l'équipement sur lequel l'incident journalisé est intervenu.
<b>Utilisateur</b>	Nom de l'utilisateur distant ayant causé l'incident journalisé.
<b>Emplacement de l'utilisateur</b>	Adresse IP ou nom d'hôte de l'ordinateur utilisé par l'utilisateur distant ayant causé l'incident journalisé.

## Journaux déclenchés par les règles (propriétés)

Chaque ligne dans un journal représente une entrée de journal. Une entrée de journal contient un certain nombre de champs d'informations :

Nom	Description
Heure locale	Horodaté en heure locale du serveur de votre système.
Texte du message	Affiche une description de l'incident journalisé.
Catégorie	Type d'incident journalisé.
Type de source	Type d'équipement sur lequel l'incident journalisé est intervenu, par exemple, serveur ou périphérique.
Nom de la source	Nom de l'équipement sur lequel l'incident journalisé est intervenu.
Type d'événement	Type d'événement correspondant à l'incident journalisé.
Nom de la règle	Nom de la règle qui déclenche la journalisation de l'entrée.
Nom du service	Nom du service sur lequel l'incident journalisé est intervenu.

## Navigation sur le site : utilisation des métadonnées

Dans cet article, vous apprendrez à configurer la façon dont votre système de vidéosurveillance utilise les métadonnées.



Pour gérer et configurer les périphériques de métadonnées, voir Périphériques métadonnées (explications) sur la page 220.

## Définition des métadonnées

Les métadonnées sont des informations sur les données, par exemple, des données qui décrivent l'image vidéo, le contenu ou les objets de l'image, ou la localisation de l'endroit où l'image a été enregistrée.

Les métadonnées peuvent être générées par :

- Le périphérique lui-même en fournissant les données. Par exemple une caméra qui diffuse la vidéo
- Un système tiers ou une intégration via un pilote de métadonnées générique

## Recherche de métadonnées (explications)

La recherche de métadonnées est toute recherche d'enregistrements vidéo dans XProtect Smart Client qui utilisent des catégories de recherche et des filtres de recherche liés aux métadonnées.

Les catégories de recherche de métadonnées de Milestone par défaut sont :

- Localisation
- Personnes
- Véhicules

### Critères de la recherche de métadonnées

Pour obtenir des résultats de recherche, vous devez respecter l'un des critères suivants :

- Avoir au moins un périphérique dans votre système de vidéosurveillance pouvant effectuer des analyse vidéo et étant correctement configuré
- Avoir un service de traitement vidéo dans votre système de vidéosurveillance qui génère des métadonnées

Dans tous les cas, les métadonnées doivent être au format de métadonnées requis.

Pour plus d'informations, voir la [documentation pour Intégration de la recherche de métadonnées](#).

## Afficher ou masquer les catégories et les filtres de recherche de métadonnées dans XProtect Smart Client

Les utilisateurs de XProtect Management Client ayant des droits d'administrateur peuvent afficher ou masquer les catégories de recherche de métadonnées et les filtres de recherche de Milestone par défaut dans XProtect Smart Client. Ces catégories et ces filtres de recherche sont masqués par défaut. Leur affichage est utile si votre système de vidéosurveillance répond aux [critères de recherche de métadonnées](#).

Ce paramètre affecte tous les utilisateurs de XProtect Smart Client.

Ce paramètre n'affecte pas la visibilité de :



- Tout autre catégorie et filtre de recherche de données qui ne sont pas des métadonnées Milestone, par exemple **Mouvement**, **Signets**, **Alarmes** et **Événements**
- Tout autre catégorie et filtre de recherche tiers

1. Dans XProtect Management Client, dans le volet **Navigation sur site**, sélectionnez **Utilisation des métadonnées > Recherche de métadonnées**.
2. Dans le volet **Recherche de métadonnées**, sélectionnez la catégorie de recherche pour laquelle vous souhaitez modifier les paramètres de visibilité.
3. Pour activer la visibilité d'une catégorie de recherche ou d'un filtre recherche, cochez la case correspondante. Pour désactiver la visibilité d'une catégorie de recherche ou d'un filtre recherche, décochez la case correspondante.

## Navigation sur le site : Alarmes

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

### Alarmes (explications)



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

Basée sur les fonctions gérées par un serveur d'événements, la fonction des alarmes centralise la visualisation, le contrôle et le dimensionnement des alarmes dans un nombre illimité d'installations (y compris tous les autres systèmes XProtect) au sein d'une même entreprise. Vous pouvez configurer cette fonction afin qu'elle génère des alarmes en fonction des éléments suivants :

- **Événements internes liés au système**

Par exemple, mouvement, réponse ou non-réponse d'un serveur, anomalie d'archivage, manque d'espace sur un volume de stockage, etc.

- **Événements externes intégrés**

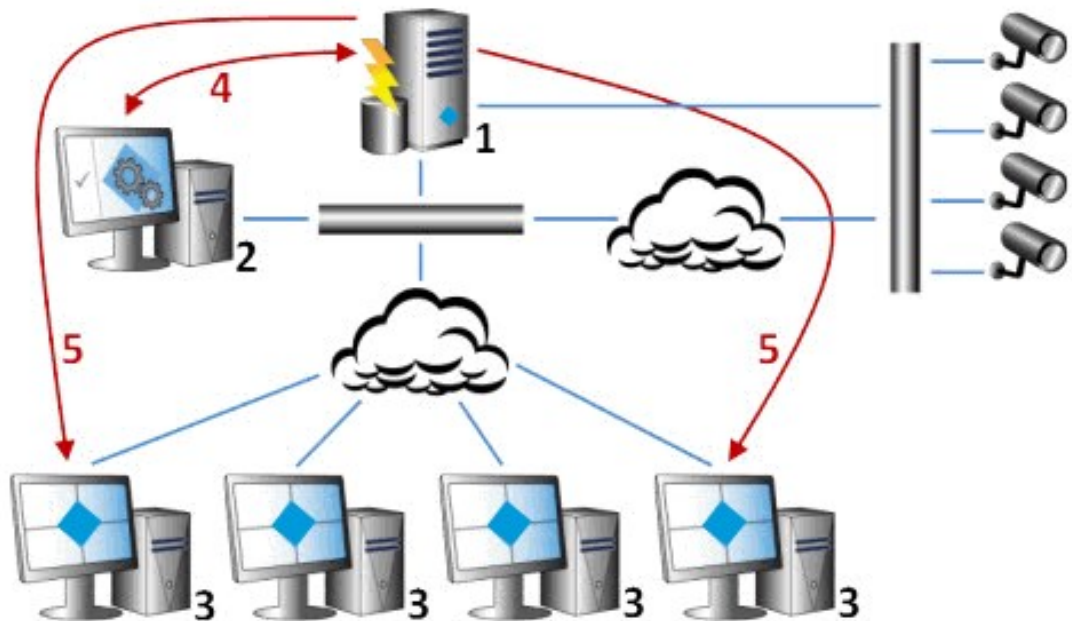
Ce groupe peut être composé de plusieurs types d'événements externes :

- **Événements analytiques**

Généralement, les données reçues de la part de fournisseurs d'analyses de contenus vidéo (VCA) tiers externes.

- **Événements du module d'extension MIP**

Au travers du MIP SDK, un vendeur tiers peut développer des modules d'extension personnalisés (par exemple, l'intégration à des systèmes de contrôle d'accès externes ou semblables) pour votre système.



Légende :

1. Système de surveillance
2. Management Client
3. XProtect Smart Client
4. Configuration de l'alarme
5. Flux des données de l'alarme

Les alarmes sont gérées et déléguées dans la liste d'alarmes sous XProtect Smart Client. Vous pouvez également intégrer des alarmes à l'aide de la fonctionnalité de smart map et de plan de XProtect Smart Client.

## Configuration des alarmes (explications)

La configuration des alarmes comprend les éléments suivants :



- La configuration dynamique de la gestion des alarmes basée sur un rôle spécifique
- Une vue d'ensemble technique centrale de tous les composants : serveurs, caméras et unités externes
- La configuration de la journalisation centralisée de toutes les alarmes entrantes et des informations du système
- La prise en charge des modules d'extension, permettant ainsi l'intégration personnalisée d'autres systèmes, par exemple des systèmes de contrôle d'accès externe ou des systèmes basés sur VCA

En règle générale, les alarmes sont contrôlées par la visibilité de l'objet déclenchant l'alarme. Cela signifie que quatre aspects potentiels peuvent jouer un rôle en matière d'alarmes et de la personne pouvant les contrôler/gérer et dans quelle mesure :

Nom	Description
<b>Visibilité de la source/périphérique</b>	Si le périphérique qui génère l'alarme n'est pas configuré pour être visible dans un rôle d'utilisateur, l'utilisateur ne peut pas voir l'alarme dans la liste des alarmes dans XProtect Smart Client.
<b>Le droit de déclencher des événements définis par l'utilisateur</b>	Ce droit détermine si le rôle de l'utilisateur peut déclencher les événements sélectionnés définis par l'utilisateur dans XProtect Smart Client.
<b>Modules d'extension externes</b>	Si des modules d'extension externes sont configurés dans votre système, ils peuvent contrôler les droits des utilisateurs relatifs à la gestion des alarmes.
<b>Droits généraux des rôles</b>	Déterminent si l'utilisateur peut uniquement voir les alarmes, ou également les gérer. Ce qu'un utilisateur d' <b>alarmes</b> peut faire avec les alarmes dépend du rôle de l'utilisateur et des paramètres configurés pour ce rôle en particulier.

L'onglet **Alarmes et événements** vous permet de spécifier dans **Options** les paramètres des alarmes, des événements et des journaux.

## Définitions des alarmes

Lorsque votre système enregistre un événement, vous pouvez le configurer afin qu'il génère une alarme dans XProtect Smart Client. Vous devez définir les alarmes avant de les utiliser et elles sont définies à partir des événements enregistrés sur les serveurs de votre système. Vous pouvez également utiliser des événements définis par l'utilisateur pour déclencher des alarmes et utiliser le même événement pour déclencher plusieurs alarmes différentes.

## Ajout d'une alarme

Pour définir une alarme, vous devez créer une définition d'alarme, dans laquelle vous spécifiez, par exemple, ce qui déclenche l'alarme, des instructions quant aux actions que l'opérateur devrait prendre, ce qui peut arrêter l'alarme et à quel moment. Pour obtenir des informations détaillées au sujet des paramètres, voir [Définitions des alarmes \(propriétés\)](#).

1. Dans le **volet Navigation du site**, agrandissez **Alarmes** et faites un clic droit sur **Définitions d'alarme**.
2. Sélectionnez **Ajouter nouveau**.
3. Remplissez ces propriétés :
  - **Nom** : Saisissez un nom pour la définition d'alarme. Le nom de la définition d'alarme apparaît dès que la définition d'alarme est répertoriée.
  - **Instructions** : Vous pouvez rédiger des instructions pour l'opérateur recevant l'alarme.
  - **Déclenchement de l'événement** : Utilisez les menus déroulants pour sélectionner un type d'événement et un message d'événement à utiliser lors du déclenchement de l'alarme.



*Une liste d'événements déclencheurs pouvant être sélectionnés. L'événement en surbrillance est créé et personnalisé à l'aide d'événements analytiques.*

- **Sources** : Sélectionnez les caméras et/ou autres dispositifs qui devraient être à l'origine de l'événement afin de déclencher l'alarme. Vos options dépendent du type d'événements que vous avez sélectionné.
  - **Profil de temps** : Si vous souhaitez que l'alarme soit activée au cours d'un intervalle de temps spécifique, sélectionnez le bouton radio puis un profil de temps dans le menu déroulant.
  - **Basé sur l'événement** : Si vous souhaitez que l'alarme soit activée par un événement, sélectionnez le bouton radio et spécifiez l'événement qui déclenchera l'alarme. Vous devez également spécifier l'événement qui arrêtera l'alarme.
4. Dans le menu déroulant **Limite de temps**, spécifiez une limite de temps pour les mesures que l'opérateur devrait prendre.
  5. Dans le menu déroulant **Événements déclenchés**, indiquez quel événement devrait être déclenché une fois la limite de temps écoulée.
  6. Spécifiez des paramètres supplémentaires, tels que les caméras associées et le propriétaire de l'alarme initiale, par exemple.

## Définitions d'alarmes (Propriétés)

### Paramètres de définition d'alarme :

Nom	Description
<b>Activer</b>	Par défaut, la définition de l'alarme est activée. Pour la désactiver, décochez la case.
<b>Nom</b>	Les noms d'alarme ne sont pas nécessairement uniques, mais utiliser des noms et des descriptions d'alarme uniques peut s'avérer avantageux dans de nombreuses situations.
<b>Instructions</b>	Saisissez un texte descriptif à propos de l'alarme et la manière de résoudre le problème qui a déclenché cette alarme.  Le texte s'affiche dans XProtect Smart Client lorsque l'utilisateur gère l'alarme.
<b>Événement déclencheur</b>	Sélectionnez le message d'événement à utiliser en cas de déclenchement de l'alarme. Choisissez dans les deux menus déroulants : <ul style="list-style-type: none"> <li>Le premier menu déroulant : Sélectionnez le type d'événement, comme un événement analytique ou des événements système, par exemple</li> <li>Le second menu déroulant : Sélectionnez le message d'événement spécifique à utiliser. Les messages disponibles dépendent du type d'événement sélectionné par vos soins dans le premier menu déroulant</li> </ul>
<b>Sources</b>	Spécifie les sources dont proviennent les événements. En dehors des caméras ou autres périphériques, les sources peuvent également être des sources définies par des modules d'extension, telles que VCA et MIP, par exemple. Les options dépendent du type d'événements que vous avez sélectionné.

### Déclencheur d'alarme :


Nom	Description
<b>Profil temporel</b>	Sélectionnez le bouton radio <b>Profil de temps</b> pour sélectionner l'intervalle de temps au cours

Nom	Description
	duquel la définition d'alarme est active. Seuls les profils de temps que vous avez définis dans le nœud <b>Règles et événements</b> figurent dans la liste. Si aucun profil de temps n'est défini, seule l'option <b>Toujours</b> est disponible.
<b>Basée sur l'événement</b>	Si vous souhaitez que l'alarme soit basée sur un événement, sélectionnez ce bouton radio. Une fois sélectionné, choisissez l'événement de démarrage et d'arrêt. Vous pouvez sélectionner des événements matériels définis sur les caméras, serveurs vidéo et entrées. Voir également Vue d'ensemble des événements sur la page 326. Vous pouvez aussi utiliser les définitions de l'événement global/manuel. Voir également Événements définis par l'utilisateur sur la page 356.

#### Action requise de la part de l'opérateur :

Nom	Description
<b>Limite de temps</b>	Sélectionnez une limite de temps relative au moment où une action de l'opérateur est nécessaire. La valeur par défaut est 1 minute. La limite de temps n'est pas active tant que vous n'avez pas attaché d'événement dans le menu déroulant <b>Événements déclenchés</b> .
<b>Événements déclenchés</b>	Sélectionnez l'événement à déclencher lorsque la limite de temps est dépassée.

#### Plans :

Nom	Description
<b>Vue Gestionnaire d'alarme</b>	<p>Assignez une Smart Map ou un plan à l'alarme lorsque celle-ci apparaît dans XProtect Smart Client &gt; <b>Gestionnaire d'alarme</b>.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;">  <p>Une smart map affiche les alarmes si celles-ci sont déclenchées par une caméra et si cette dernière est ajoutée à une smart map. Pour plus d'informations sur l'ajout des caméras à la smart map, voir Ajout, modification ou suppression de liens sur une smart map.</p> </div>

**Autre :**

Nom	Description
<b>Caméras associées</b>	Sélectionnez jusqu'à 15 caméras à inclure dans la définition des alarmes même si ces caméras ne sont pas directement responsables du déclenchement de l'alarme. Cela peut être utile, par exemple, si vous avez sélectionné un message d'événement externe (tel que l'ouverture d'une porte) comme élément déclencheur de l'alarme. En définissant une ou plusieurs caméras à proximité de la porte, vous pouvez associer les enregistrements de l'incident par les caméras à l'alarme.
<b>Propriétaire de l'alarme initiale</b>	Sélection d'un utilisateur par défaut responsable de l'alarme.
<b>Priorité initiale de l'alarme</b>	Sélectionnez une priorité pour l'alarme. Utilisez ces priorités dans XProtect Smart Client pour définir l'importance d'une alarme.
<b>Catégorie d'alarme</b>	Sélectionnez une catégorie pour l'alarme, par exemple <b>Fausse alarme</b> ou <b>Investigation requise</b> .
<b>Événements déclenchés par l'alarme</b>	Définissez un événement que l'alarme peut déclencher dans XProtect Smart Client.
<b>Alarme de fermeture automatique</b>	Si vous souhaitez qu'un événement particulier arrête automatiquement l'alarme, cochez cette case. Les événements ne peuvent pas tous déclencher des alarmes. Décochez la case pour désactiver le lancement de la nouvelle alarme.
<b>Alarme assignée au Administrateurs</b>	Cochez la case à cocher pour inclure des utilisateurs dans un rôle d'administrateur dans la liste <b>Assigné à</b> . La liste <b>Assigné à</b> se trouve dans les détails de l'alarme dans l'onglet <b>Gestion des alarmes</b> dans XProtect Smart Client. Décochez la case à cocher pour filtrer les utilisateurs ayant un rôle d'administrateur depuis la liste <b>Assigné à</b> pour réduire la liste.

## Paramètres des données de l'alarme

Lorsque vous configurez les paramètres des données d'alarme, indiquez les propriétés suivantes :

## Onglet niveaux de données d'alarme

### Priorités

Nom	Description
Niveau	Ajoutez de nouvelles priorités avec des chiffres de niveau de votre choix ou utilisez/modifiez les niveaux de priorité par défaut (chiffres 1, 2 ou 3). Ces niveaux de priorité servent à configurer le paramètre de <b>Priorité initiale de l'alarme</b> .
Nom	Saisissez un nom pour l'entité. Vous pouvez en créer autant que vous le souhaitez.
Son	Sélectionnez le son à associer à l'alarme. Utilisez un des sons par défaut ou ajoutez-en plus dans <b>Paramètres de son</b> .
Répéter le son	Décidez si le son ne doit être joué qu'une fois, ou plusieurs fois jusqu'à ce que l'opérateur dans XProtect Smart Client clique sur l'alarme dans la liste d'alarmes.
Activez les notifications sur le bureau	Vous pouvez activer ou désactiver les notifications sur le bureau pour chaque priorité d'alarme. Si vous utilisez un XProtect VMS qui prend en charge les profils Smart Client, vous devez également activer les notifications sur les profils Smart Client requis. Voir Onglet Gestionnaire d'alarme (profils Smart Client) sur la page 304.

### États

Nom	Description
Niveau	Vous pouvez, en plus des niveaux d'état par défaut (numéros <b>1, 4, 9</b> et <b>11</b> , qui ne peuvent être ni modifiés ni réutilisés), ajouter de nouveaux états avec les numéros de niveaux de votre choix. Ces niveaux d'états ne sont visibles que dans la <i>Liste des alarmes</i> du XProtect Smart Client.

### Catégories

Nom	Description
Niveau	Ajoutez de nouvelles catégories avec les numéros de niveau de votre choix. Ces niveaux de catégorie servent à configurer les paramètres de <b>Catégorie initiale de l'alarme</b> .
Nom	Saisissez un nom pour l'entité. Vous pouvez en créer autant que vous le souhaitez.

## Onglet Configuration de la liste d'alarme

Nom	Description
<b>Colonnes disponibles</b>	Utilisez > pour sélectionner les colonnes à mettre la disposition dans la <i>Liste des alarmes</i> du XProtect Smart Client. Utilisez < pour effacer la sélection. Une fois que vous avez terminé, les <b>Colonnes sélectionnées</b> doivent comporter les éléments à intégrer.

## Onglet Raisons de la fermeture

Nom	Description
<b>Activer</b>	Toutes les alarmes doivent se voir attribuer une raison de fermeture avant de les fermer.
<b>Raison</b>	Ajoutez des raisons de fermeture pour que l'utilisateur puisse choisir entre plusieurs lors de la fermeture des alarmes. Par exemple <i>Problème résolu</i> ou <i>Fausse alarme</i> . Vous pouvez en créer autant que vous le souhaitez.

## Paramètres sons

Lorsque vous configurez des paramètres de son, indiquez les propriétés suivantes :

Nom	Description
<b>Sons</b>	Sélectionnez le son à associer à l'alarme. La liste de sons intègre un certain nombre de sons Windows par défaut. Vous pouvez également ajouter de nouveaux son (.wav ou .mp3).
<b>Ajouter</b>	Ajouter des sons. Naviguez dans les fichiers son pour télécharger un ou plusieurs fichiers .wav ou mp3.
<b>Supprimer</b>	Supprimer un son sélectionné dans la liste des sons ajoutés manuellement. Les sons par défaut ne peuvent être supprimés.
<b>Test</b>	Tester le son. Sélectionnez le son dans la liste. Le son est diffusé une fois.

## 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 70.

#### Pré-requis :

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

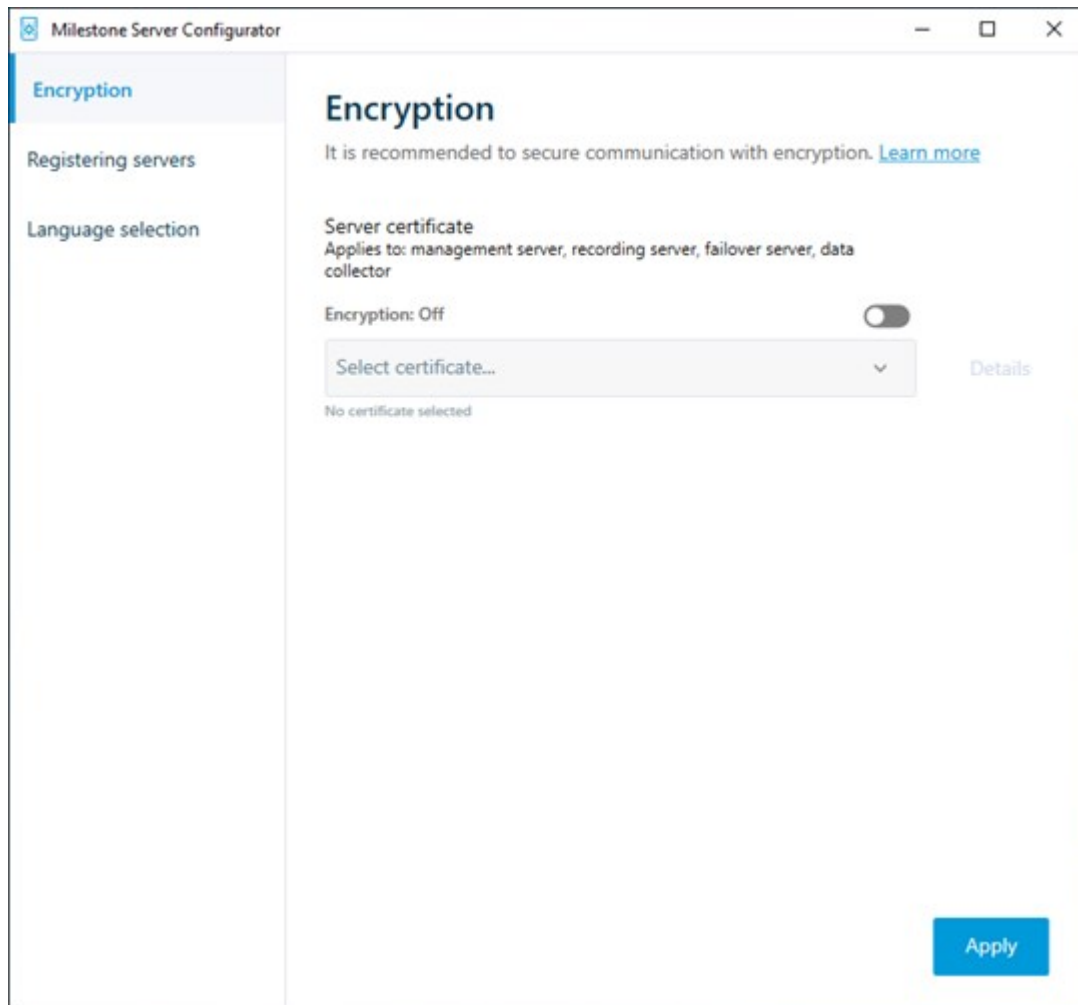
D'abord, vous devez activer le cryptage sur le serveur de gestion.

Étapes :

1. Sur un ordinateur où est installé le serveur de gestion, ouvrez le **Server Configurator** à partir de :
  - Le menu Démarrer de Windowsou
  - 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 449.

## 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 72 et **Cryptage entre le serveur de gestion et le Data Collector Server (explications)** sur la page 73.

**Pré-requis :**

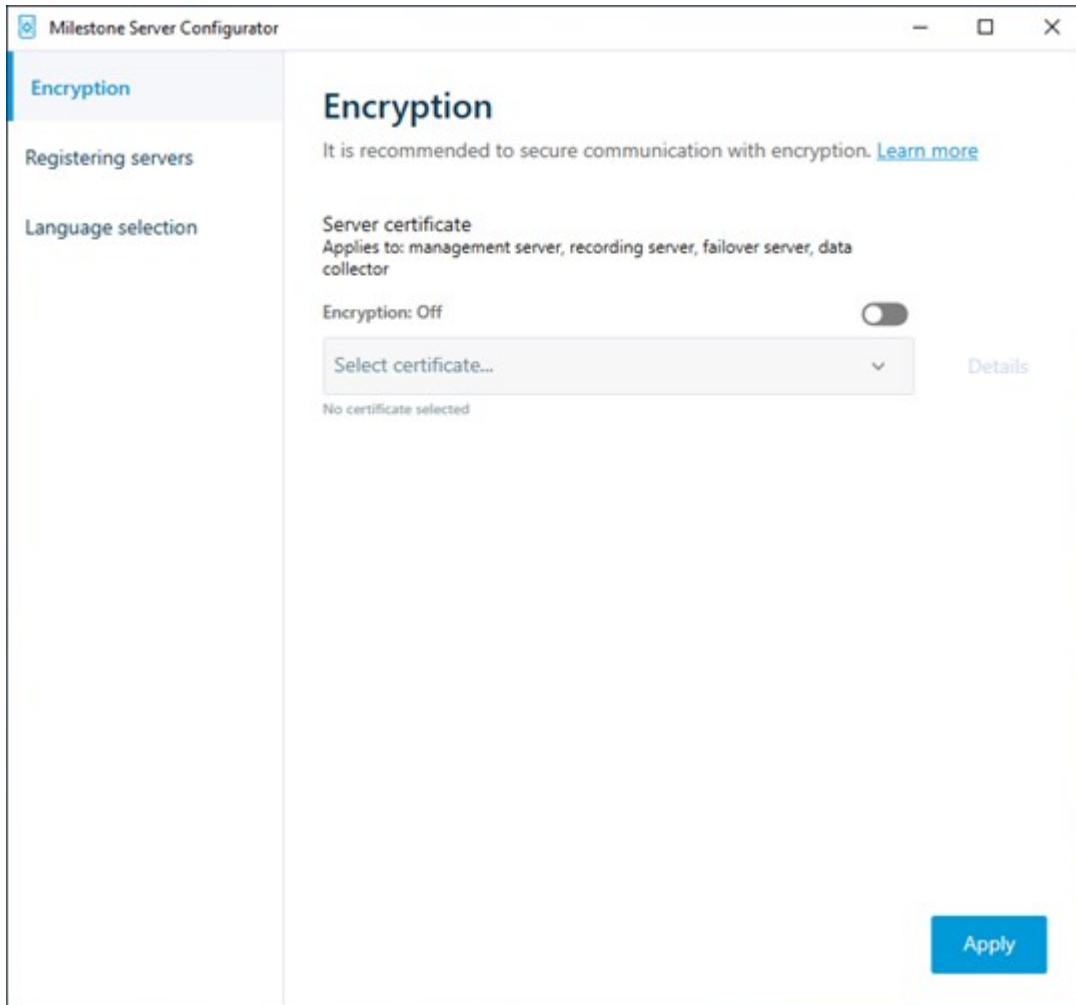
- Vous avez activé le cryptage sur le serveur de gestion, voir **Activer le cryptage** sur la page 448

Étapes :

1. Sur un ordinateur où est installé le serveur d'enregistrement, ouvrez le **Server Configurator** à partir de :
  - Le menu Démarrer de Windowsou
  - 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 74.

**Pré-requis :**

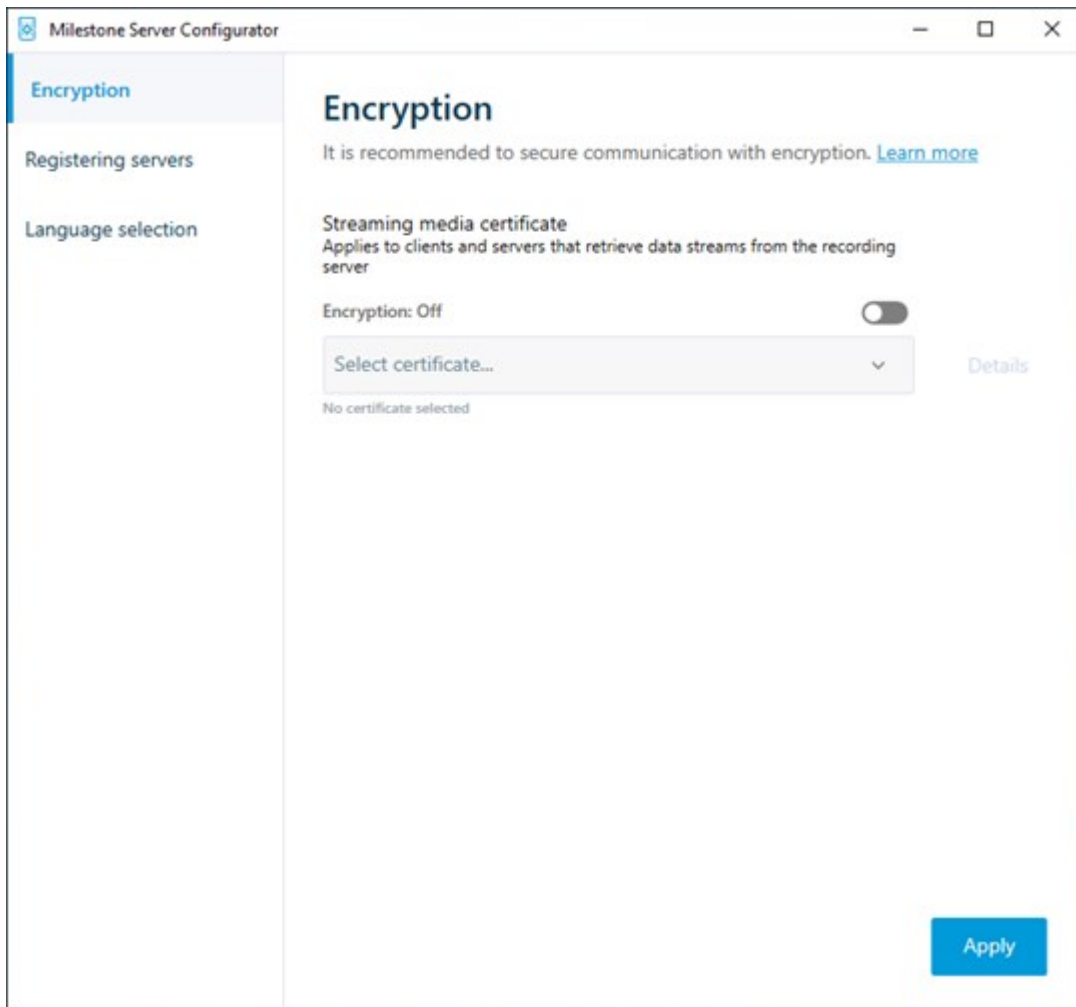
- Le certificat d'authentification du serveur à utiliser est fiable sur tous les ordinateurs exécutant des services qui collectent des flux de données depuis le serveur d'enregistrement
- XProtect Smart Client et tous les services récupérant des flux de données pour le serveur d'enregistrement doivent 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 Windowsou
  - 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 77 et [Exigences du cryptage du serveur mobile pour les clients](#) sur la page 78.



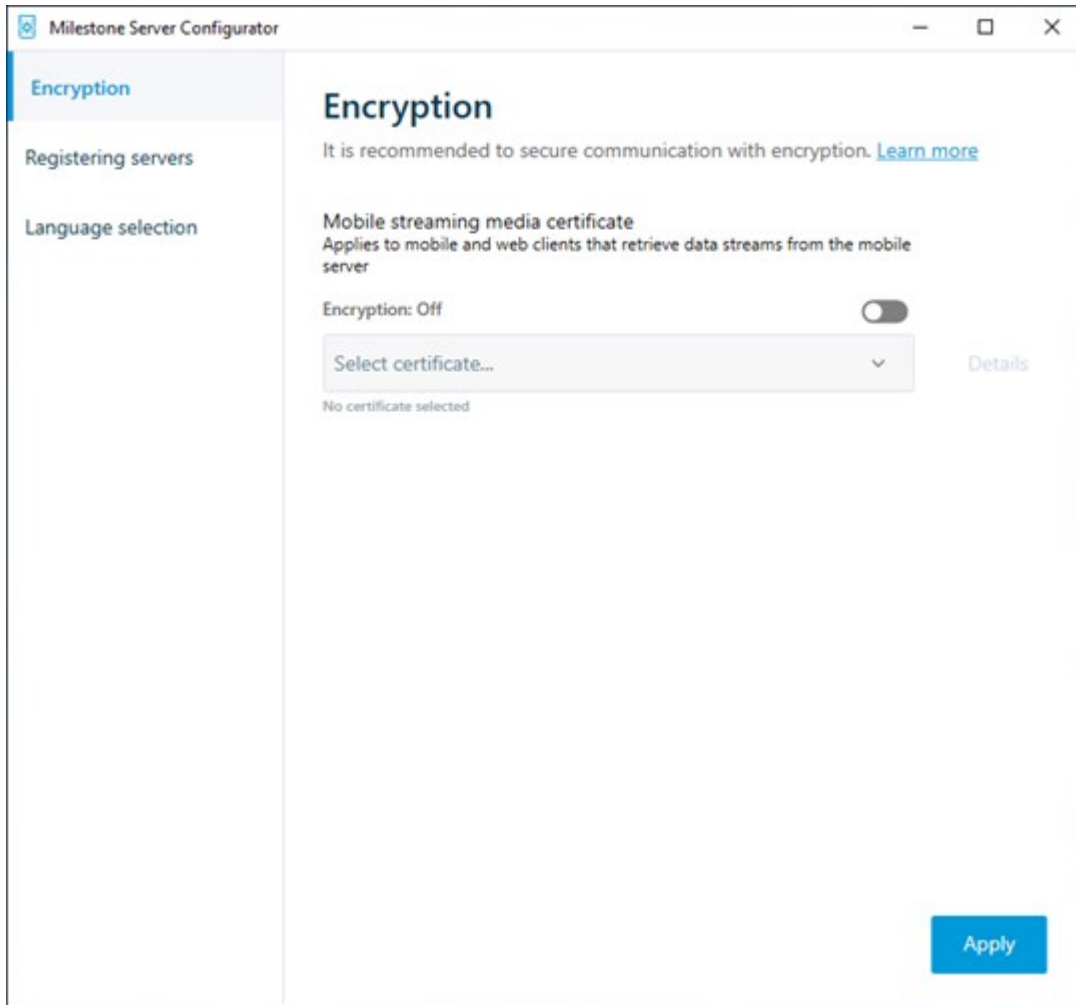
Les certificats émis par l'AC (Autorité de certification) comportent une chaîne de certificats, et le certificat racine de l'AC se trouve à la racine de cette chaîne. Lorsqu'un périphérique ou un navigateur détecte ce certificat, il compare son certificat racine aux certificats préinstallés sur le système 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 Windowsou
  - 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.

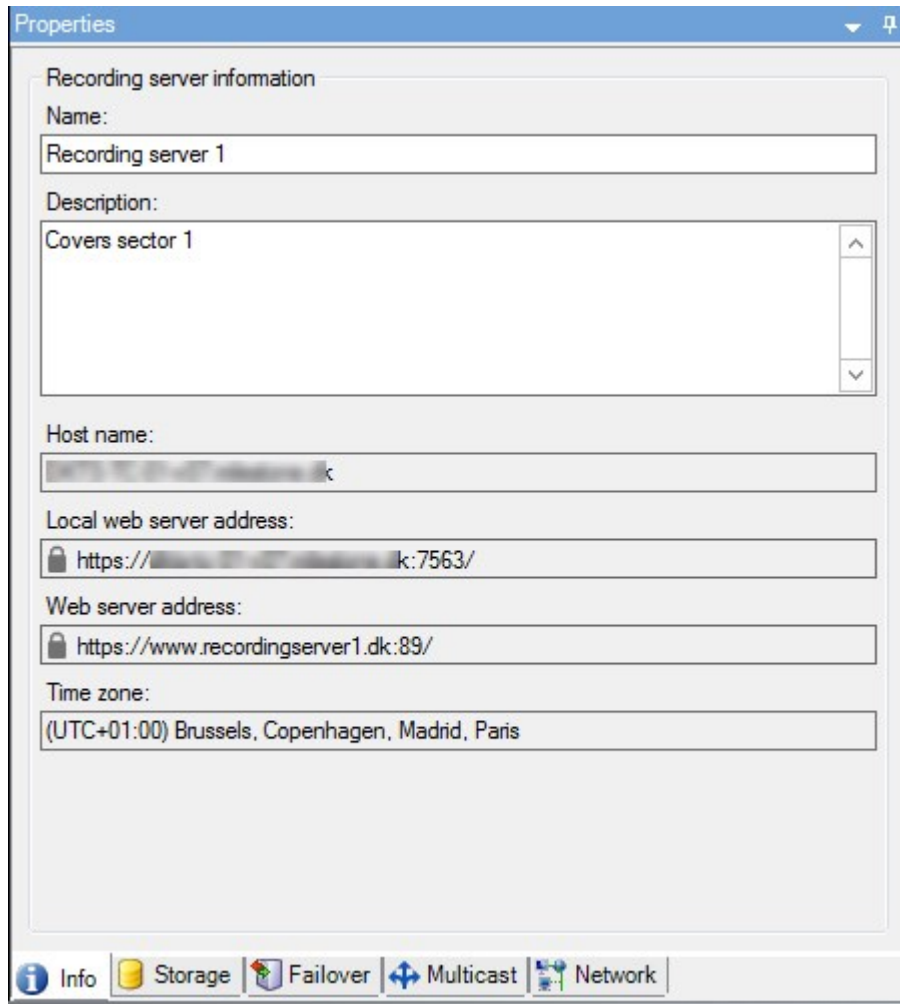
## Voir le status du cryptage vers les clients

Pour vérifier si votre serveur d'enregistrement crypte les connexions :

1. Ouvrez le Management Client.
2. Dans le panneau **Navigation du site**, sélectionnez **Serveurs > Serveurs d'enregistrement**. Cette commande ouvre une liste de serveurs d'enregistrement.

3. Dans le volet **Vue d'ensemble**, sélectionnez le serveur d'enregistrement concerné, puis allez sur l'onglet **Info**.

Si le cryptage est activé vers les clients et serveurs récupérant des flux de données depuis le serveur d'enregistrement, une icône représentant un cadenas apparaîtra devant l'adresse du serveur Web local et l'adresse du serveur Web optionnel.



## En cours de configuration de Milestone Federated Architecture



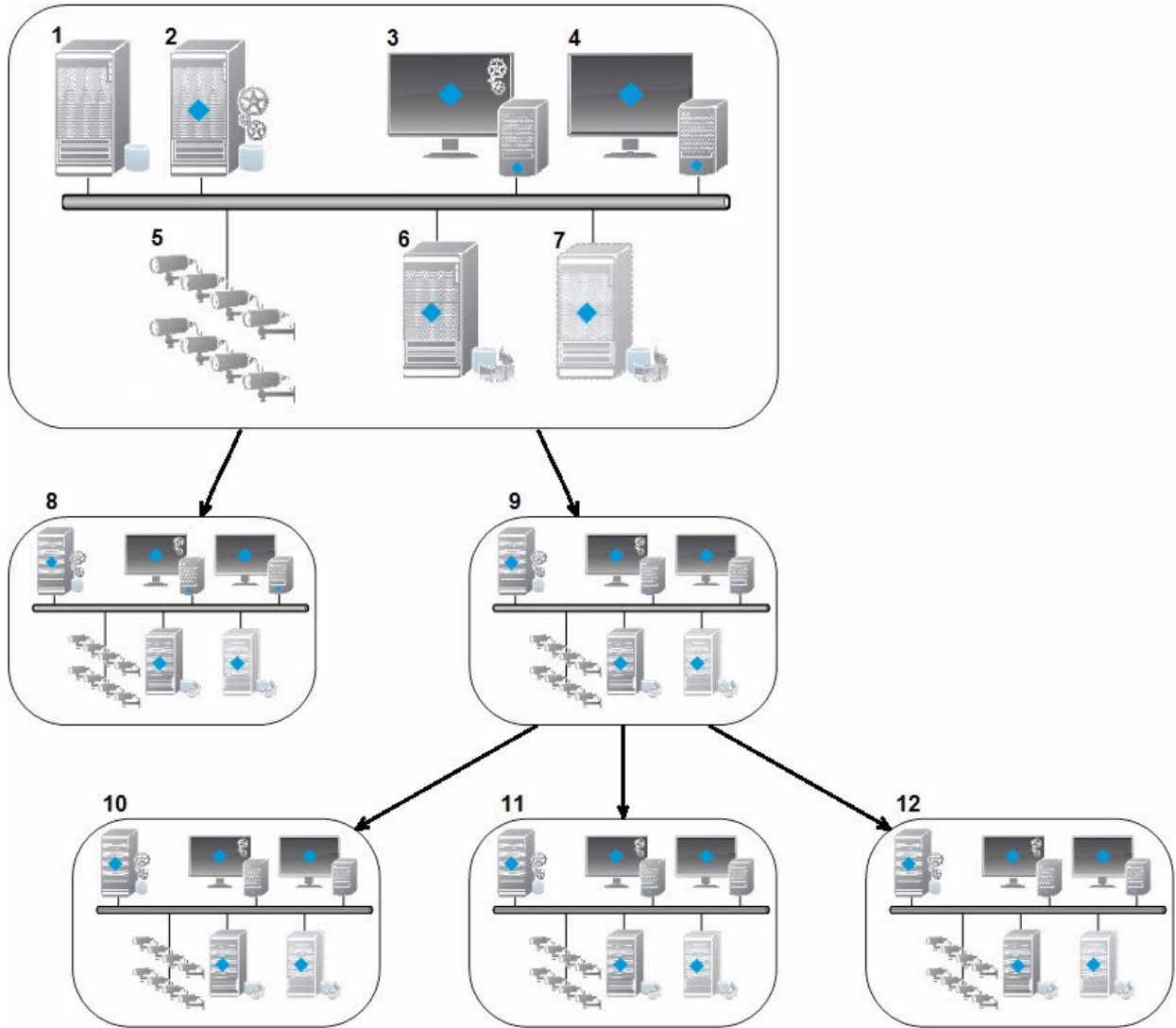
XProtect Expert ne peuvent être fédérés qu'en tant que sites enfants.

Milestone Federated Architecture relie de multiples systèmes standard individuels pour créer une hiérarchie de sites fédérés, composée de sites parents/enfants. Les utilisateurs du client dotés de droits suffisants bénéficient d'un accès transparent aux vidéos, fichiers audio et autres ressources via les sites individuels. Les administrateurs peuvent gérer de manière centralisée tous les sites depuis la version 2018 R1 ou plus récente dans la hiérarchie fédérée se basant sur les droits de l'administrateur pour les sites individuels.



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

Milestone Federated Architecture est configuré avec un seul site central (site supérieur) et un nombre illimité de sites fédérés (voir Configurer votre système pour exécuter des sites fédérés sur la page 460). Lorsque vous êtes connecté à un site, vous pouvez accéder à des informations concernant tous ses sites enfants et les sites enfants de ses sites enfants. Le lien entre deux sites est établi lorsque vous demandez le lien à partir du site parent (voir Ajouter un site à la hiérarchie sur la page 462). Un site enfant ne peut être relié qu'à un seul site parent. Si vous n'êtes pas l'administrateur du site enfant lorsque vous l'ajoutez à la hiérarchie des sites fédérés, la demande doit être acceptée par l'administrateur du site enfant.



Composants d'une configuration Milestone Federated Architecture :

1. Serveur avec SQL Server
2. Serveur de gestion
3. Management Client
4. XProtect Smart Client
5. Caméras
6. Serveur d'enregistrement
7. Serveur d'enregistrement de redondance
8. à 12. Sites fédérés

### Synchronisation de la hiérarchie

Un site parent contient une liste mise à jour de tous les sites enfants qui y sont attachés à présent, ainsi que de tous les sites enfants des sites enfants, etc. La hiérarchie des sites fédérés inclut une synchronisation programmée entre les sites, ainsi qu'une synchronisation déclenchée par la direction à chaque fois qu'un site est ajouté ou supprimé par l'administrateur système. La synchronisation de la hiérarchie par le système a lieu niveau par niveau. Chaque niveau transmet et retourne des messages jusqu'à ce qu'il atteigne le serveur demandant les informations. Le système envoie moins de 1 Mo à chaque fois. En fonction du nombre de niveaux, les modifications apportées à une hiérarchie peuvent mettre du temps à apparaître dans le Management Client. Vous ne pouvez pas planifier vos propres synchronisations.

### Trafic des données

Le système envoie des communications ou des données de configuration lorsqu'un utilisateur ou un administrateur consulte des vidéos enregistrées ou en direct, ou qu'il configure un site. La quantité de données dépend de la quantité et du contenu visualisé ou configuré.

### Milestone Federated Architecture avec d'autres produits

- Si le site central utilise XProtect Smart Wall, vous pouvez également utiliser les fonctionnalités XProtect Smart Wall dans la hiérarchie des sites fédérés. Voir Configurer les Smart Wall sur la page 286 pour savoir comment configurer XProtect Smart Wall
- Si le site central utilise XProtect Access et qu'un utilisateur XProtect Smart Client se connecte à un site dans une hiérarchie des sites fédérés, les notifications de demande d'accès envoyées par les sites fédérés apparaissent également dans XProtect Smart Client
- Vous pouvez ajouter des systèmes XProtect Expert 2013 (ou des versions plus récentes) à la hiérarchie des sites fédérés en tant que sites enfants, et non en tant que sites parents
- Milestone Federated Architecture ne nécessite aucune licence supplémentaire
- Pour plus d'informations sur les applications et les avantages de ce système, voir le [livre blanc sur Milestone Federated Architecture](#).

## Établir une hiérarchie de sites fédérés

Avant de commencer à bâtir la hiérarchie dans le Management Client, Milestone vous recommande de planifier les liaisons entre vos sites.

Vous installez et configurez chaque site au sein d'une hiérarchie fédérée comme un système autonome normal avec des standards en termes de composants système, paramètres, règles, programmations, administrateurs, utilisateurs et droits d'utilisateurs. Si vous avez déjà installé et configuré les sites et qu'il ne vous reste plus qu'à les combiner au sein d'une hiérarchie de sites fédérés, vos systèmes sont prêts à être configurés.

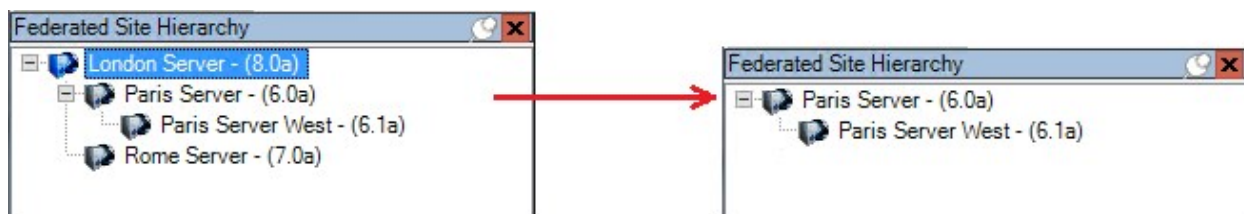
Une fois les sites individuels installés, vous devez les configurer afin qu'ils fonctionnent en tant que sites fédérés (voir Configurer votre système pour exécuter des sites fédérés sur la page 460).

Pour commencer la hiérarchie, vous pouvez vous connecter au site que vous souhaitez utiliser en tant que site central et ajouter (voir Ajouter un site à la hiérarchie sur la page 462) le premier site fédéré. Lorsque le lien est établi, les deux sites créent automatiquement une hiérarchie de sites fédérés dans le volet **Hiérarchie des sites fédérés** du Management Client et vous pouvez y ajouter d'autres sites pour développer la hiérarchie fédérée.

Lorsque vous avez créé la hiérarchie des sites fédérés, les utilisateurs et administrateurs peuvent se connecter à un site pour y accéder et accéder à tout site fédéré dont il dispose. L'accès aux sites fédérés dépend des droits de l'utilisateur.






Vous pouvez ajouter un nombre illimité de sites à une hiérarchie fédérée. En outre, vous pouvez lier un site fonctionnant sur une version plus ancienne du produit à une version plus récente et vice versa. Les numéros de version apparaissent automatiquement et ne peuvent pas être supprimés. Le site auquel vous êtes connecté est toujours en haut du volet de la **Hiérarchie des sites fédérés** et s'appelle le site d'origine.

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



## Icônes d'état dans Milestone Federated Architecture

Les icônes représentent les états possibles d'un site :

Description	Icône
Le site supérieur de l'ensemble de la hiérarchie est opérationnel.	
Le site supérieur de l'ensemble de la hiérarchie est encore opérationnel, mais un ou plusieurs problèmes nécessitent votre attention. Affiché par-dessus l'icône du site supérieur.	
Le site est opérationnel.	
Le site est en attente d'acceptation dans la hiérarchie.	
Le site est attaché mais n'est pas encore opérationnel.	

## Configurer votre système pour exécuter des sites fédérés

Afin de préparer votre système pour Milestone Federated Architecture, vous devez effectuer certains choix lors de l'installation du serveur de gestion. Selon la façon dont votre infrastructure informatique est configurée, choisissez parmi les trois alternatives suivantes.

### Alternative 1 : Connecter des Sites d'un même Domaine (ayant un utilisateur de Domaine Commun)

Avant d'installer le serveur de gestion, vous devez créer un utilisateur de domaine commun et l'utiliser en tant qu'administrateur sur tous les serveurs impliqués dans la hiérarchie des sites fédérés. La manière dont vous connectez les sites dépend du compte utilisateur créé.

#### Avec un compte utilisateur Windows

1. Commencez l'installation du produit sur le serveur devant être utilisé comme serveur de gestion et sélectionnez **Personnalisé**.
2. Sélectionnez afin d'installer le service Management Server en utilisant un compte utilisateur. Le compte utilisateur sélectionné doit être l'administrateur sur l'ensemble des serveurs de gestion. Vous devez utiliser le même compte utilisateur lorsque vous installez les autres serveurs de gestion dans la hiérarchie des sites fédérés.
3. Terminez l'installation. Répétez les étapes 1 à 3 afin d'installer tout autre système que vous souhaitez ajouter à la hiérarchie des sites fédérés.
4. Ajouter un site à la hiérarchie (voir Ajouter un site à la hiérarchie sur la page 462).

#### Avec un compte utilisateur intégré de Windows (service réseau)

1. Commencez l'installation du produit sur le premier serveur devant être utilisé comme serveur de gestion et sélectionnez **Ordinateur unique** ou **Personnalisation**. Ceci installe le serveur de gestion en utilisant un compte de service réseau. Répétez cette étape pour tous les sites de votre hiérarchie de sites fédérés.

2. Connectez-vous au site que vous souhaitez utiliser en tant que site central dans la hiérarchie de sites fédérés.
3. Dans le Management Client, développez **Sécurité > Rôles > Administrateurs**.
4. Dans l'onglet **Utilisateurs et groupes**, cliquez sur **Ajouter** et sélectionnez **Utilisateur Windows**.
5. Dans la fenêtre de dialogue, sélectionnez **Ordinateurs** en tant que type d'objet, saisissez le nom du serveur du site fédéré, puis cliquez sur **OK** pour ajouter le serveur au rôle d'**Administrateur** du site central. Répétez cette étape jusqu'à ce que tous les sites fédérés soient ajoutés de cette façon puis quittez l'application.
6. Connectez-vous à chaque site fédéré et ajoutez les serveurs suivants au rôle d'**Administrateur**, comme indiqué ci-dessus :
  - Le serveur du site parent.
  - Les serveurs du site enfant que vous souhaitez connecter directement à ce site fédéré.
7. Ajouter un site à la hiérarchie (voir Ajouter un site à la hiérarchie sur la page 462).

#### Alternative 2 : Connecter des sites de différents domaines

Afin de pouvoir vous connecter aux sites sur l'ensemble des domaines, assurez-vous que ces domaines se font mutuellement confiance. Configurez les domaines de façon à ce qu'ils se fassent mutuellement confiance dans la configuration du domaine de Microsoft Windows. Lorsque vous avez établi une relation de confiance entre les différents domaines de chaque site de la hiérarchie des sites fédérés, procédez comme indiqué au paragraphe Alternative 1. Pour plus d'informations sur la façon de configurer les domaines fiables, voir le site web de Microsoft ([https://docs.microsoft.com/previous-versions/windows/it-pro/windows-2000-server/cc961481\(v=technet.10\)](https://docs.microsoft.com/previous-versions/windows/it-pro/windows-2000-server/cc961481(v=technet.10))).



Milestone recommande Milestone Interconnect pour la création de systèmes à sites multiples avec plusieurs domaines.

#### Alternative 3 : Connecter des sites dans un ou plusieurs groupes de travail

Lorsque vous connectez des sites à l'intérieur de groupes de travail, le même compte d'administrateur doit être présent sur tous les serveurs que vous souhaitez connecter à la hiérarchie des sites fédérés. Vous devez définir le compte d'administrateur avant d'installer le système.

1. Connectez-vous à **Windows** en utilisant un compte administrateur commun.
2. Commencez à installer le produit et cliquez sur **Personnaliser**.
3. Sélectionnez pour installer le service Management Server en utilisant le compte administrateur commun.
4. Terminez l'installation. Répétez les étapes 1 à 4 pour installer tous les autres systèmes que vous souhaitez connecter. Vous devez installer tous ces systèmes en utilisant le compte administrateur commun.
5. Ajouter un site à la hiérarchie (voir Ajouter un site à la hiérarchie sur la page 462).



Milestone recommande Milestone Interconnect pour la création de systèmes à sites multiples avec plusieurs domaines.



multiples connectés lorsque les sites ne font pas partie d'un domaine.





Vous ne pouvez pas mélanger domaine(s) et groupe(s) de travail. Cela signifie que vous ne pouvez pas connecter les sites d'un domaine aux sites d'un groupe de travail et vice versa.

## Ajouter un site à la hiérarchie


Au fur et à mesure de l'expansion de votre système, vous pouvez ajouter des sites à votre site supérieur et à ses sites enfants aussi longtemps que le système est correctement configuré.

1. Sélectionnez le panneau **Hiérarchie des sites fédérés**.
2. Sélectionnez le site auquel vous souhaitez ajouter un site enfant, faites un clic droit et cliquez sur **Ajouter un site à la hiérarchie**.
3. Saisissez l'URL du site requis dans la fenêtre **Ajouter un site à la hiérarchie** et cliquez sur **OK**.
4. Le site parent envoie une demande de liaison au site enfant et, après quelques temps, un lien entre les deux sites est ajouté dans le panneau **Hiérarchie des sites fédérés**.
5. Si vous pouvez établir le lien vers le site enfant sans avoir à obtenir l'acceptation de l'administrateur du site enfant, passez à l'étape 7.

Si ce n'est pas **pas** le cas, le site enfant voit s'afficher l'icône  d'attente d'acceptation jusqu'à ce que l'administrateur du site enfant autorise la demande.

6. Assurez-vous que l'administrateur du site enfant autorise la demande de liaison de la part du site parent (voir Accepter les ajouts dans la hiérarchie sur la page 462).
7. Le nouveau lien parent/enfant est établi et le panneau **Hiérarchie des sites fédérés** est mis à jour avec l'icône  pour le nouveau site enfant.


## Accepter les ajouts dans la hiérarchie

Quand un site enfant reçoit une demande de liaison à partir d'un site parent potentiel où l'administrateur n'a pas de droits administrateur sur le site enfant, l'icône  en attente d'acceptation s'affiche.

Pour accepter une demande de liaison :

1. Connectez-vous au site.
2. Dans le panneau **Hiérarchie des sites fédérés**, cliquez avec le bouton droit sur le site et cliquez sur **Accepter les ajouts dans la hiérarchie**.

Si le site exécute la version XProtect Expert, faites un clic droit sur le site dans le panneau **Navigation du site**.

3. Cliquez sur **Oui**.
4. Le nouveau lien parent/enfant est établi et le panneau **Hiérarchie des sites fédérés** est mis à jour avec l'icône  de site normale pour le site sélectionné.

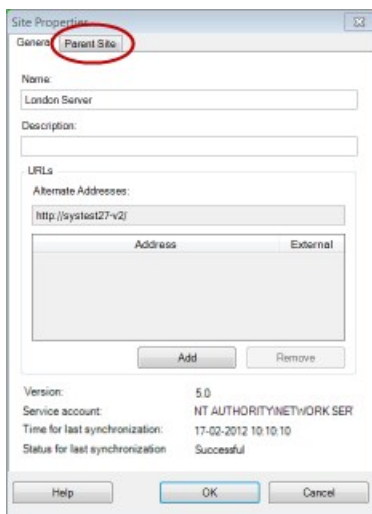


Les modifications apportées aux sites enfants situés à distance du site parent peuvent mettre du temps à se voir reflétées dans le panneau **Hiérarchie des sites fédérés**.

## Définir les propriétés du site

Vous pouvez voir et, le cas échéant, modifier les propriétés de votre site d'accueil et de ses enfants.

1. Dans le Management Client, dans le panneau **Hiérarchie des sites fédérés**, sélectionnez le site concerné, faites un clic droit et sélectionnez **Propriétés**.



2. Le cas échéant, modifiez ce qui suit :

Onglet **Général** (voir Onglet Généralités sur la page 465)

Onglet **Site parent** (voir Onglet Site parent sur la page 465) (**disponible sur les sites enfants uniquement**)



Pour des questions de synchronisation, toute modification apportée à un enfant distant peut mettre du temps à se voir reflété dans le **panneau Navigation du Site**.

## Actualiser la hiérarchie des sites

Le système procède régulièrement à une synchronisation automatique de la hiérarchie à tous les niveaux de votre configuration parent/enfant. Vous pouvez l'actualiser manuellement, si vous souhaitez voir les modifications reflétées instantanément dans la hiérarchie, et si vous ne souhaitez pas attendre la prochaine synchronisation automatique.

Vous devez être connecté(e) sur un site pour effectuer une actualisation manuelle. Seules les modifications sauvegardées par ce site depuis la dernière synchronisation sont affichées par le biais d'une actualisation. Par conséquent, les modifications apportées à des niveaux inférieurs dans la hiérarchie pourraient ne pas être affichées par le biais d'une mise à jour manuelle, si les changements n'ont pas encore atteint le site.

1. Connectez-vous au site pertinent.
2. Cliquez avec le bouton droit sur le site supérieur dans le panneau **Hiérarchie des sites fédérés** et cliquez sur **Rafraîchir la hiérarchie des sites**.

Cela prendra quelques secondes.

## Connexion à d'autres sites de la hiérarchie



Vous pouvez vous connecter à d'autres sites et les gérer. Le site auquel vous êtes connecté est votre site d'origine.

1. Dans le volet **Hiérarchie des sites fédérés**, cliquez avec le bouton droit sur le site auquel vous souhaitez vous connecter.
2. Cliquez sur **Se connecter au site**.  
Le Management Client de ce site s'ouvre.
3. Saisissez les informations de connexion et cliquez sur **OK**.
4. Une fois la connexion effectuée, vous êtes prêt à procéder à vos tâches administratives sur ce site.

## Détacher un site de la hiérarchie

Lorsque vous détachez un site de son site parent, le lien entre les sites est aboli. Vous pouvez détacher des sites à partir du site central, du site en lui-même ou de son site parent.

1. Dans le volet **Hiérarchie des sites fédérés**, cliquez avec le bouton droit sur le site et cliquez **Détacher le site de la hiérarchie**.
2. Cliquez sur **Oui** pour mettre à jour le volet **Hiérarchie des sites fédérés**.

Si le site détaché a des sites enfants, il devient le nouveau site supérieur pour cette branche de la hiérarchie et l'icône de site normal  se transforme en une icône de site supérieur .

3. Cliquez sur **OK**.



Les modifications apportées à la hiérarchie sont reflétées après une actualisation manuelle ou une synchronisation automatique.

## Propriétés des sites fédérés

Cette section décrit l'onglet **Général** et l'onglet **Site Parental**.

### Onglet Généralités

Vous pouvez modifier certaines informations liées au site auquel vous êtes actuellement connecté.

Nom	Description
<b>Nom</b>	Saisissez le nom du site.
<b>Description</b>	Saisissez une description du site.
<b>URL</b>	Utilisez la liste pour ajouter et supprimer des URL pour ce site et indiquez si elles sont externes ou non. Les adresses externes peuvent être atteintes depuis l'extérieur du réseau local.
<b>Version</b>	Le numéro de version du serveur de gestion du site.
<b>Compte service</b>	Le compte service sous lequel fonctionne le serveur de gestion.
<b>Temps de la dernière synchronisation</b>	Date et heure de la dernière synchronisation de la hiérarchie.
<b>État pour la dernière synchronisation</b>	L'état de la dernière synchronisation de la hiérarchie. Cela peut être soit <b>Réussi</b> , soit <b>Échoué</b> .

### Onglet Site parent

Cet onglet présente des informations concernant le site parent du site auquel vous êtes actuellement connecté. L'onglet n'est pas visible si votre site n'a pas de site parent.

Nom	Description
Nom	Affiche le nom du site parent.
Description	Affiche une description du site parent (facultatif).
URL	Répertorie les URL pour le site parent et indique si elles sont externes ou non. Les adresses externes peuvent être atteintes depuis l'extérieur du réseau local.
Version	Le numéro de version du serveur de gestion du site.
Compte service	Le compte service sous lequel fonctionne le serveur de gestion.
Temps de la dernière synchronisation	Date et heure de la dernière synchronisation de la hiérarchie.
État pour la dernière synchronisation	L'état de la dernière synchronisation de la hiérarchie. Cela peut être soit <b>Réussi</b> , soit <b>Échoué</b> .

## En cours de configuration de Milestone Interconnect

Cette section décrit Milestone Interconnect et comment configurer cette fonctionnalité.

### Sélectionner Milestone Interconnect ou Milestone Federated Architecture (explications)

Dans un système à distribution physique où les utilisateurs d'un site central doivent pouvoir accéder à la vidéo sur le site distant, vous pouvez choisir entre Milestone Interconnect™ et Milestone Federated Architecture™.

Milestone recommande Milestone Federated Architecture lorsque :

- La connexion réseau entre les sites centraux et fédérés est stable
- Le réseau utilise le même domaine
- Il y a très peu de sites importants
- La bande passante est suffisante pour l'utilisation requise

Milestone recommande Milestone Interconnect lorsque :

- La connexion réseau entre les sites centraux et distants est instable
- Vous ou votre organisation souhaitez utiliser un autre produit XProtect sur les sites distants
- Le réseau utilise différents domaines ou groupes de travail
- Il y a beaucoup de sites de petite taille

## Milestone Interconnect et les licences

Pour exécuter Milestone Interconnect, vous avez besoin de licences de caméra Milestone Interconnect sur votre site central pour voir les vidéos des périphériques sur les sites distants. Seul XProtect Corporate peut servir de site central.

L'état de vos licences de caméra Milestone Interconnect s'affiche sur la page **Renseignements sur la licence** du site central.

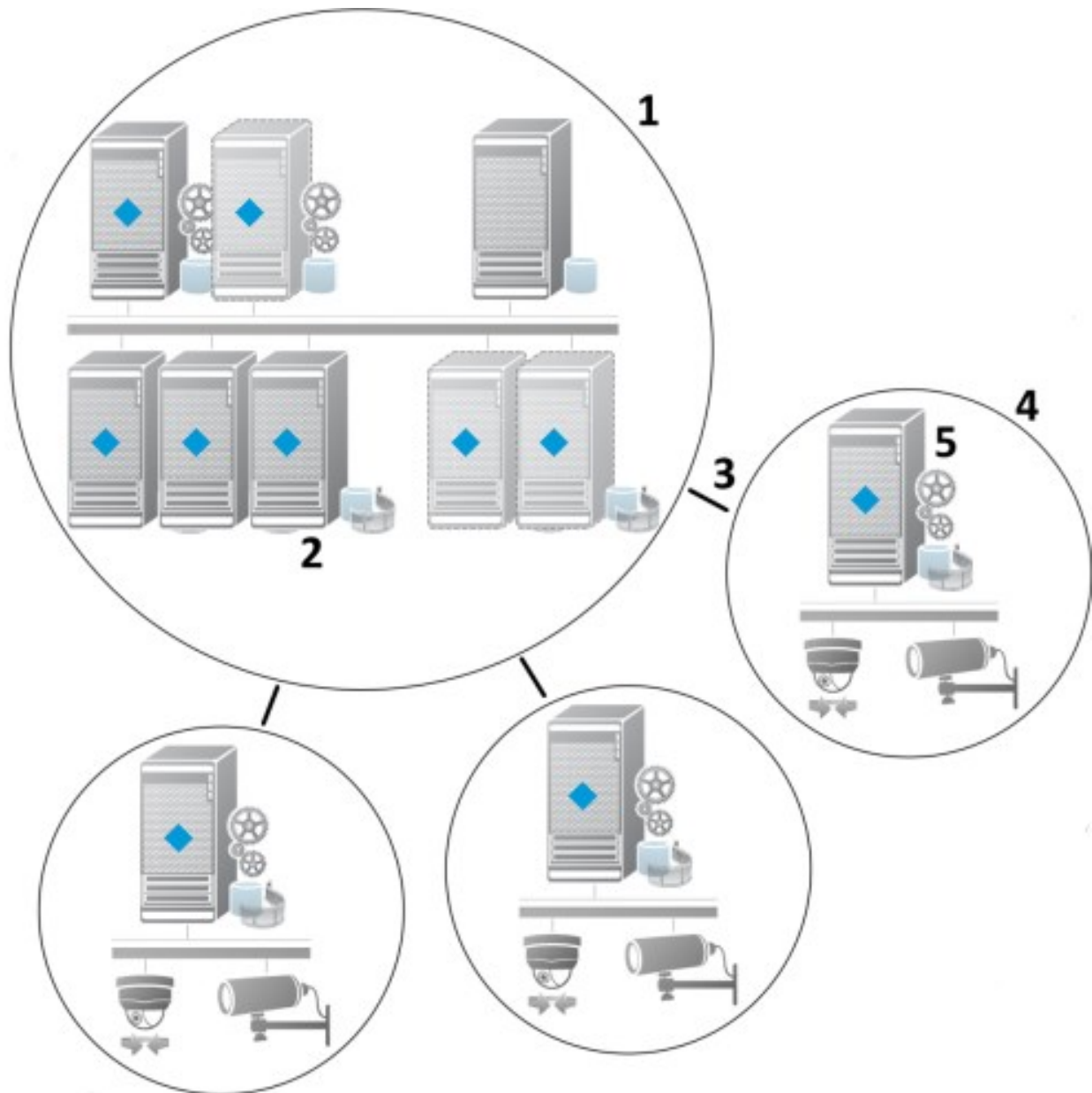
## Milestone Interconnect (explications)



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

Milestone Interconnect™ vous permet d'intégrer un nombre d'installations plus petites, physiquement fragmentées et des installations XProtect distantes avec un site central XProtect Corporate. Vous pouvez installer ces sites plus petits, appelés sites distants, sur des unités mobiles, par exemple des bateaux, des bus ou des trains. Cela signifie que ces sites n'ont pas besoin d'être connectés en permanence à un réseau.

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



1. Site Milestone Interconnect central XProtect Corporate
2. Les pilotes Milestone Interconnect (établissant la connexion entre les serveurs d'enregistrement des sites centraux et le site distant, et devant être sélectionnés dans la liste de pilotes lorsque l'on ajoute des systèmes à distance par le biais de l'assistant **Ajouter du matériel**)
3. Connexion Milestone Interconnect
4. Site distant Milestone Interconnect (le site distant complet avec installation du système, utilisateurs, caméras, etc.)
5. Système à distance Milestone Interconnect (l'installation technique sur le site distant)

Vous ajoutez des sites distants à votre site central à l'aide de l'assistant **Ajouter du matériel** sur le site central (voir Ajouter un site distant à votre site Milestone Interconnect central sur la page 470).

Chaque site distant fonctionne indépendamment et peut effectuer n'importe quelle tâche de surveillance normale. Selon les connexions réseau et les droits d'utilisateur appropriés (voir Attribuer des droits d'utilisateur sur la page 472), Milestone Interconnect vous offre une fonction de lecture en direct à partir des caméras des sites distants et de lecture des enregistrements des sites distants à partir du site central.

Le site central ne peut seulement voir et accéder aux périphériques auxquels le compte d'utilisateur spécifié a accès (lors de l'ajout du site distant). Ceci permet aux administrateurs de systèmes locaux de contrôler les périphériques devant être mis à la disposition du site central et de ses utilisateurs.

Sur le site central, vous pouvez afficher l'état du système pour les caméras interconnectées, mais pas directement l'état du site distant. Pour contrôler le site distant, vous pouvez utiliser les événements du site distant pour déclencher des alarmes ou d'autres notifications sur le site central (voir Configurer votre site central pour répondre aux événements des sites distants sur la page 474).

Il vous permet également de transférer les enregistrements des sites distants vers le site central en fonction d'événements, de règles/calendriers, ou de demandes manuelles des utilisateurs XProtect Smart Client.

Seuls les systèmes XProtect Corporate peuvent fonctionner en tant que sites centraux. Tous les autres produits peuvent servir de sites distants, y compris XProtect Corporate. La prise en charge diffère d'une configuration à une autre, de la version considérée, du nombre de caméras et de la façon dont les périphériques et les événements provenant du site distant sont traités (le cas échéant) par le site central. Pour de plus amples informations sur la façon dont des produits XProtect spécifiques communiquent dans une configuration Milestone Interconnect, rendez-vous sur le site Web Milestone Interconnect (<https://www.milestonesys.com/solutions/hardware-and-add-ons/milestone-addons/interconnect/>).

## Configurations Milestone Interconnect (explications)

Il existe trois façons d'exécuter Milestone Interconnect. La façon dont vous exécutez votre configuration dépend de votre connexion au réseau, de la manière dont vous revoyez les enregistrements et du fait que vous rappeliez ou non des enregistrements à distance et de l'ampleur de ces activités.

La section suivante décrit les trois configurations les plus probables :

### **Lecture directe à partir des sites distants (bonne connexion réseau) :**

La configuration la plus simple. Le site central est toujours en ligne et connecté à ses sites distants et les utilisateurs du site central lisent les enregistrements à distance directement à partir des sites distants. Cela nécessite l'utilisation de l'option **Lire les enregistrements à partir du système à distance** (voir Activer la lecture directe à partir de la caméra du site distant sur la page 473).

## Récupération des séquences d'enregistrement à distance sélectionnées basé sur des règles ou sur XProtect Smart Client à partir des sites distants (connexions au réseau limitées périodiquement)

Utilisé lorsque des séquences d'enregistrement sélectionnées (provenant de sites distants) doivent être stockées au niveau central pour garantir leur indépendance vis-à-vis des sites distants. Cette indépendance est cruciale en cas de panne de réseau ou de restrictions affectant le réseau. Vous pouvez configurer les paramètres de récupération d'enregistrements à distance sur l'onglet **Récupération à distance** (voir Onglet Rappel à distance sur la page 216).

La récupération des enregistrements à distance peut être déclenchée à partir du XProtect Smart Client en cas de besoin. Il est également possible de configurer une règle. Dans certains scénarios, les sites distants sont en ligne. Dans d'autres cas, ils sont hors ligne la plupart du temps. Ce paramètre dépend bien souvent du secteur d'activité. Dans certains secteurs, le site central est généralement en ligne et connecté à ses sites distants en permanence (par exemple, un QG commercial (site central) et plusieurs magasins (sites distants)). Dans d'autres secteurs, tels que les transports, les sites distants sont mobiles (il peut s'agir, par exemple, de bus, de trains, de bateaux, etc.) et ne peuvent établir une connexion au réseau que de façon aléatoire. En cas d'échec de connexion au réseau au cours d'un rappel d'enregistrements à distance déjà entamé, la tâche se poursuit lorsque l'occasion se présente à nouveau.

Si le système détecte une récupération automatique ou une demande de récupération à partir du XProtect Smart Client en dehors de l'intervalle de temps que vous avez spécifié dans l'onglet **Récupération à distance**, elle est acceptée, mais n'est pas commencée avant d'avoir atteint l'intervalle de temps sélectionné. Les nouvelles demandes de rappel d'enregistrements à distance seront mises en attente et ne débiteront que lorsque l'intervalle de temps autorisé aura pris fin. Vous pouvez visualiser les tâches de rappel d'enregistrement à distance en instance à partir du **Tableau de bord système** -> **Tâches actuelles**.

## Après un échec de connexion, les enregistrements à distance manquants sont récupérés par défaut à partir des sites distants

Utilise des sites distants comme un serveur d'enregistrement utilise le stockage externe sur une caméra. Généralement, les sites distants sont en ligne et connectés à leur site central, et lui diffusent un flux en direct que le site central enregistre. En cas de défaillance du réseau pour quelque raison que ce soit, le site central ne peut pas accéder aux séquences d'enregistrement. Cependant, une fois que le réseau est rétabli, le site central rappelle automatiquement les enregistrements à distance couvrant la période d'arrêt de la connexion. Cela nécessite l'activation de l'option **Récupérer automatiquement les enregistrements à distance lorsque la connexion est rétablie** (voir Rappeler les enregistrements à distance de la caméra du site distant sur la page 473) dans l'onglet **Enregistrer** pour la caméra en question.

Vous pouvez recourir à un mélange des solutions ci-dessus afin de répondre aux besoins spécifiques à votre organisation.

## Ajouter un site distant à votre site Milestone Interconnect central

Ajoutez des sites distants au site central à l'aide de l'assistant **Ajouter du matériel**.

### Configuration

- Nombre suffisant de licences de caméra Milestone Interconnect (voir Milestone Interconnect et les licences sur la page 467)
- Un autre système XProtect configuré et fonctionnel compatible comprenant un compte d'utilisateur (utilisateur basique, utilisateur Windows local ou utilisateur Windows Active Directory) doté de droits pour les périphériques auquel le système central XProtect Corporate peut accéder
- Connexion réseau entre le site central XProtect Corporate et les sites distants avec un accès ou un port redirigeant vers les ports utilisés sur les sites distants

Pour ajouter un site distant :

1. Sur le site central, agrandissez **Serveurs** et sélectionnez **Serveurs d'enregistrement**.
2. Dans le volet de vue d'ensemble, agrandissez le serveur d'enregistrement en question et faites un clic droit.
3. Sélectionnez **Ajouter su matériel** pour lancer l'assistant d'installation.
4. Sur la première page, sélectionnez **Analyse de la plage d'adresses** ou **Manuel** et cliquez sur **Suivant**.
5. Précisez les noms d'utilisateur et mots de passe. Le compte d'utilisateur doit être prédéfini sur le système à distance. Vous pouvez ajouter autant de noms d'utilisateurs et de mots de passe que nécessaire en appuyant sur le bouton **Ajouter**. Lorsque vous avez fini, cliquez sur **Suivant**.
6. Sélectionnez les pilotes à utiliser lors de votre analyse. Dans ce cas, choisissez l'un des pilotes Milestone. Cliquez sur **Suivant**.
7. Précisez l'adresse IP et les numéros de port que vous souhaitez analyser. Le port par défaut est 80. Cliquez sur **Suivant**.

Attendez que votre système détecte les sites distants. L'indicateur d'état présente le processus de détection. Si un site est détecté, un message de **Réussite** apparaît dans la colonne **État**. Si vous n'arrivez pas à ajouter un système, vous pouvez cliquer sur le message d'erreur **Échec** pour découvrir pourquoi la détection a échoué.

8. Choisissez d'activer ou de désactiver les systèmes correctement détectés. Cliquez sur **Suivant**.
9. Attendez que votre système détecte un matériel et recueille les informations spécifiques au périphérique. Cliquez sur **Suivant**.
10. Choisissez d'activer ou de désactiver les périphériques et matériel correctement détectés. Cliquez sur **Suivant**.
11. Sélectionner un groupe par défaut. Cliquez sur **Terminer**.
12. Une fois l'installation terminée, vous pouvez voir le système et ses périphériques dans le panneau **Vue d'ensemble**.

Selon les droits d'utilisateur de l'utilisateur sélectionné sur le site distant, le site central a accès à toutes les caméras et fonctions ou à une partie de celles-ci.

## Attribuer des droits d'utilisateur

On configure les droits d'utilisateur pour une caméra interconnectée de la même manière que pour d'autres caméras, en créant un rôle et en attribuant un accès à des fonctions.

1. Sur le site central, dans le volet **Navigation du site**, développez **Sécurité** et sélectionnez **Rôles**.
2. Dans le volet Vue d'ensemble, cliquez sur le rôle administrateur intégré avec le bouton droit de votre souris et sélectionnez **Ajouter un rôle** (voir Ajouter et gérer un rôle sur la page 372).
3. Nommez le rôle et configurez les paramètres dans l'onglet **Périphérique** (voir Paramètres des rôles sur la page 374) et l'onglet **Enregistrements à distance** (voir Paramètres des rôles sur la page 374).

## Mise à jour du matériel du site distant

Si la configuration a été modifiée sur un site distant, par exemple si des caméras ou événements ont été ajoutés, il vous faudra mettre à jour la configuration du site central pour qu'elle corresponde à celle du site distant.

1. Sur le site central, agrandissez **Serveurs** et sélectionnez **Serveurs d'enregistrement**.
2. Dans le volet Vue d'ensemble, agrandissez le serveur d'enregistrement requis et sélectionnez le système à distance concerné. Cliquez dessus à l'aide du bouton droit de votre souris.
3. Sélectionnez **Mettre le matériel à jour**. Cela ouvre la boîte de dialogue **Mise à niveau du matériel**.
4. La boîte de dialogue présente tous les changements (périphériques supprimés, mis à jour et ajoutés) dans le système à distance depuis la création ou le dernier rafraîchissement de votre configuration Milestone Interconnect. Cliquez sur **Confirmer** pour mettre votre site central à jour avec ces changements.

## Établir une connexion à distance entre le bureau et un système à distance

Vous pouvez vous connecter à distance aux systèmes dans votre configuration Milestone Interconnect.

### Configuration

Les connexions distantes du bureau à l'ordinateur que vous souhaitez faire fonctionner à distance doivent être installées et activées.

1. Sur le site central, agrandissez **Serveurs** et sélectionnez **Serveurs d'enregistrement**.
2. Dans le volet Vue d'ensemble, agrandissez le serveur d'enregistrement requis et sélectionnez le système à distance concerné.
3. Dans le volet Propriétés, sélectionnez l'onglet **Info**.
4. Dans la zone **Administration à distance**, saisissez le nom d'utilisateur Windows et le mot de passe appropriés.
5. Une fois que vous avez sauvegardé le nom d'utilisateur et le mot de passe, cliquez sur **Connexion** pour établir une connexion à distance sur le bureau.
6. Dans la boîte à outils, cliquez sur **Enregistrer**.



## Activer la lecture directe à partir de la caméra du site distant

Si votre site central est toujours en ligne et connecté à ses sites distants, vous pouvez configurer votre système pour que les utilisateurs effectuent la lecture des enregistrements directement sur les sites distants. Pour plus d'informations, voir Configurations Milestone Interconnect (explications) sur la page 469.

1. Sur le site central, agrandissez **Serveurs** et sélectionnez **Serveurs d'enregistrement**.
2. Dans le volet Vue d'ensemble, agrandissez le serveur d'enregistrement requis et sélectionnez le système à distance concerné. Sélectionnez la caméra interconnectée pertinente.
3. Dans le volet Propriétés, sélectionnez l'onglet **Enregistrer**, puis sélectionnez l'option **Lire les enregistrements à partir du système à distance**.
4. Dans la boîte à outils, cliquez sur **Enregistrer**.

Dans une configuration Milestone Interconnect, le site central ignore les masques de confidentialité défini dans un site distant. Si vous souhaitez utiliser les mêmes masques de confidentialité, vous devez les redéfinir sur le site central.

## Rappeler les enregistrements à distance de la caméra du site distant

Si votre site central **n'est pas** connecté en permanence à ses sites distants, vous pouvez configurer votre système pour sauvegarder les enregistrements de manière centralisée et vous pouvez configurer le rappel des enregistrements à distance lorsque la connexion du réseau est optimale. Pour plus d'informations, voir Configurations Milestone Interconnect (explications) sur la page 469.

Pour permettre aux utilisateurs de récupérer des enregistrements, vous devez activer l'autorisation pour le rôle pertinent (voir Paramètres des rôles sur la page 374).

Pour configurer votre système :

1. Sur le site central, agrandissez **Serveurs** et sélectionnez **Serveurs d'enregistrement**.
2. Dans le volet Vue d'ensemble, agrandissez le serveur d'enregistrement requis et sélectionnez le système à distance concerné. Sélectionnez serveur à distance pertinent.
3. Dans le volet Propriétés, sélectionnez l'onglet **Récupération à distance** et mettez à jour les paramètres (voir Onglet Rappel à distance sur la page 216).

En cas de défaillance du réseau pour quelque raison que ce soit, le site central ne peut pas accéder à certaines séquences d'enregistrement. Vous pouvez configurer votre système pour que le site central récupère automatiquement les enregistrements à distance pour couvrir la période d'arrêt une fois que le réseau est rétabli.

1. Sur le site central, agrandissez **Serveurs** et sélectionnez **Serveurs d'enregistrement**.
2. Dans le volet Vue d'ensemble, agrandissez le serveur d'enregistrement requis et sélectionnez le système à distance concerné. Sélectionnez la caméra pertinente.

3. Dans le panneau Propriétés, sélectionnez l'onglet **Enregistrer**, puis sélectionnez l'option **Récupérer automatiquement les enregistrements à distance lorsque la connexion est rétablie** (voir Périphériques prenant la mise en mémoire-tampon préalable en charge sur la page 240).
4. Dans la boîte à outils, cliquez sur **Enregistrer**.

Autrement, vous pouvez utiliser des règles ou commencer à rappeler des enregistrements à distance à partir du XProtect Smart Client en fonction de vos besoins.

Dans une configuration Milestone Interconnect, le site central ignore les masques de confidentialité défini dans un site distant. Si vous souhaitez utiliser les mêmes masques de confidentialité, vous devez les redéfinir sur le site central.

## Configurer votre site central pour répondre aux événements des sites distants

Vous pouvez utiliser les événements définis sur les sites distants pour déclencher des règles et des alarmes sur votre site central et ainsi répondre immédiatement aux événements des sites distants. Les sites distants doivent être connectés et en ligne. Le nombre et type d'événements dépendent des événements configurés et prédéfinis dans les sites distants.

La liste des événements pris en charge est disponible sur le site Web Milestone (<https://www.milestonesys.com/>).

Vous ne pouvez pas supprimer les événements prédéfinis.

### Exigences :

- Si vous voulez utiliser des événements manuels ou définis par l'utilisateur sur les sites distants en tant qu'événements à déclenchement, vous devez d'abord les créer sur les sites distants
- Assurez-vous d'avoir une liste à jour des événements des sites distants (voir Mise à jour du matériel du site distant sur la page 472)

### Ajouter un événement manuel ou défini par l'utilisateur depuis un site distant :

1. Sur le site central, agrandissez **Serveurs** et sélectionnez **Serveurs d'enregistrement**.
2. Dans le volet Vue d'ensemble, sélectionnez le serveur distant en question et l'onglet **Événements**.
3. La liste contient les événements prédéfinis. Cliquez sur **Ajouter** pour inclure les événements manuels ou définis par l'utilisateur sur le site distant dans la liste.

### Utiliser un événement sur un site distant pour déclencher une alarme sur le site central :

1. Sur le site central, agrandissez **Alarmes** et sélectionnez **Définitions d'alarmes**.
2. Dans le volet Vue d'ensemble, faites un clic droit sur **Définitions d'alarmes** et cliquez sur **Ajouter nouveau**.
3. Saisissez les valeurs nécessaires.

4. Dans le champ **Événement à déclenchement**, vous pouvez sélectionner les événements prédéfinis ou définis par l'utilisateur.
5. Dans le champ **Sources**, sélectionnez le serveur à distance représentant le site distant dont vous voulez les alarmes.
6. Enregistrez la configuration une fois terminé.

#### Utiliser un événement sur un site distant pour déclencher une action basée sur des règles sur le site central :

1. Sur le site central, développez **Règles et événements** et sélectionnez **Règles**.
2. Dans le volet Vue d'ensemble, faites un clic droit sur **Règles** et cliquez sur **Ajouter un règle**.
3. Dans l'assistant, sélectionnez **Réaliser une action lors de l'événement**.
4. Dans la zone **Modifier la description de la règle**, cliquez sur **événement** et sélectionnez les événements prédéfinis ou définis par l'utilisateur. Cliquez sur **OK**.
5. Cliquez sur **périphériques/serveur d'enregistrement/serveur de gestion** et sélectionnez le serveur à distance représentant le site distant sur lequel vous voulez que le site central réalise une action. Cliquez sur **OK**.
6. Cliquez sur **Suivant** pour passer à la page suivante de l'assistant.
7. Sélectionnez les conditions que vous voulez appliquer pour cette règle. Si vous ne sélectionnez aucune condition, la règle s'applique toujours. Cliquez sur **Suivant**.
8. Sélectionnez une action et précisez les détails dans la zone **Modifier la description de la règle**. Cliquez sur **Suivant**.
9. Sélectionnez un critère d'arrêt si nécessaire. Cliquez sur **Suivant**.
10. Sélectionnez une action d'arrêt si nécessaire. Cliquez sur **Terminer**.

## Configuration des services de connexion à distance



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

La fonction Services de connexion à distance bénéficie de la technologie de connexion à la caméra Axis One-click, développée par Axis Communications. Elle active le système pour récupérer des vidéos (et audio) des caméras extérieures où les pare-feu et / ou une configuration de réseaux de routeurs empêche toute tentative de connexion à ces caméras. La communication réelle a lieu par les serveurs de tunnel sécurisés (serveurs ST). Les serveurs ST utilisent un VPN. Seuls les périphériques détenant une clé valide fonctionnent avec un VPN. Ceci offre un tunnel de sécurité où les réseaux publics peuvent échanger des données en toute sécurité.

**Les services de connexion à distance vous permettent de**

- Modifier les données de connexion au sein du service de répartition d'Axis
- Ajouter, modifier et retirer les serveurs ST
- Enregistrer/désenregistrer et modifier les caméras Axis One-click
- Atteindre le matériel relatif à la caméra Axis One-Click

Avant de pouvoir bénéficier de la connexion à la caméra Axis One-click, commencez par installer un environnement approprié avec un serveur ST. Pour travailler avec les environnements de serveurs de tunnel sécurisé (serveur ST) et des caméras Axis One-click, veuillez contacter au préalable votre fournisseur de système pour obtenir le nom d'utilisateur et le mot de passe exigés pour les services de répartition Axis.

## Installer un environnement STS pour une connexion à la caméra One-click

### Configuration

- Contactez le fournisseur de votre système pour obtenir le nom d'utilisateur et le mot de passe requis pour les services de répartition d'Axis
  - Assurez-vous que votre/vos caméra(s) prennent en charge Axis Video Hosting System. Allez sur le site Web d'Axis pour voir les périphériques pris en charge (<https://www.axis.com/products/axis-guardian>)
  - Si nécessaire, actualisez vos caméras Axis avec le nouveau firmware. Allez sur le site Web d'Axis pour télécharger le firmware (<https://www.axis.com/techsup/firmware.php/>)
1. Sur la page d'accueil de chaque caméra, allez sur **Configuration de base, TCP/IP**, et sélectionnez **Activer AVHS** et **Toujours**.
  2. Dans le serveur de gestion, accédez à la page de téléchargement de Milestone (<https://www.milestonesys.com/downloads/>) et téléchargez le logiciel **AXIS One-click**. Exécutez le programme permettant de configurer une infrastructure appropriée de tunnel sécurisé d'Axis.

## Ajouter/Modifier des STS

1. Procédez comme suit :
  - Pour ajouter un serveur ST, cliquez sur le nœud principal **Serveurs de tunnel sécurisé Axis** avec le bouton droit de votre souris et sélectionnez **Ajouter serveur de tunnel sécurisé Axis**
  - Pour modifier un serveur ST, cliquez dessus avec le bouton droit de votre souris et sélectionnez **Modifier serveur de tunnel sécurisé Axis**
2. Dans la fenêtre qui s'ouvre, saisissez les informations nécessaires.
3. Si vous avez choisi d'utiliser des identifiants de connexion lorsque vous avez installé le **composant Axis One-Click Connection**, cochez la case **Utiliser les certificats** et utilisez exactement le même nom d'utilisateur et le même mot de passe que pour le **composant Axis One-Click Connection**.
4. Cliquez sur **OK**.

## Enregistrer une nouvelle caméra Axis One-Click

1. Pour enregistrer une caméra sous un serveur ST, cliquez dessus avec le bouton droit de votre souris et sélectionnez **Enregistrer caméra Axis One-Click**.
2. Dans la fenêtre qui s'ouvre, saisissez les informations nécessaires.
3. Cliquez sur **OK**.
4. La caméra apparaît alors sous le serveur ST pertinent.

La caméra peut avoir les codes couleur suivants :

Couleur	Description
Rouge	État initial. Enregistrée, mais pas connectée au serveur ST.
Jaune	Enregistrée. Connectée au serveur ST, mais pas ajoutée en tant que matériel.
Vert	Ajoutée en tant que matériel. Peut être connectée au serveur ST ou non.

Lorsque vous ajoutez une nouvelle caméra, son état est toujours vert. L'état de connexion est reflété par l'option **Périphériques** sur **Serveurs d'enregistrement** dans le volet **Vue d'ensemble**. Dans le volet **Vue d'ensemble**, vous pouvez regrouper vos caméras pour pouvoir les examiner plus facilement. Si vous choisissez de **ne pas** enregistrer votre caméra sur le service de répartition Axis à ce moment-là, vous pouvez le faire par la suite à l'aide du menu apparaissant lorsque vous cliquez sur le bouton droit de la souris, en sélectionnant **Modifier caméra Axis One-click**.

## Propriété de connexion à la caméra Axis One-Click

Nom	Description
Mot de passe de la caméra	Saisir/modifier. Fourni avec votre caméra lors de l'achat. Pour de plus amples informations, consultez le manuel de votre caméra ou rendez-vous sur le site Web d'Axis <a href="https://www.axis.com/">https://www.axis.com/</a> .
Utilisateur de la caméra	Voir les détails concernant le <b>Mot de passe caméra</b> .

Nom	Description
<b>Description</b>	Saisissez/modifiez une description pour la caméra.
<b>Adresse externe</b>	Saisissez/modifiez l'adresse Web du serveur ST auquel est/sont connectée(s) la/les caméra(s).
<b>Adresse interne</b>	Saisissez/modifiez l'adresse Web du serveur ST auquel est connecté le serveur d'enregistrement.
<b>Nom</b>	Si besoin, modifiez le nom de l'élément.
<b>Clé d'identification du propriétaire</b>	Voir <b>Mot de passe caméra</b> .
<b>Mots de passe</b> (pour Dispatch Server)	Entrer le mot de passe. Doit être identique à celui fourni par le fournisseur de votre système.
<b>Mots de passe</b> (pour serveur ST)	Entrer le mot de passe. Doit être identique à celui saisi lors de la création du <b>composant Axis One-Click Connection</b> .
<b>Enregistrement/Dé-recensement sur le service de répartition Axis</b>	Indiquez si vous souhaitez enregistrer votre caméra Axis avec le service de répartition Axis. Peut être effectué au moment de la création ou à une date ultérieure.
<b>Numéro de série</b>	Numéro de série du matériel tel que spécifié par le fabricant. Le numéro de série est souvent, mais pas toujours, identique à l'adresse MAC.
<b>Utiliser les identifiants de connexion</b>	Cochez la case si vous avez décidé d'utiliser des identifiants de connexion lors de l'installation du serveur ST.
<b>Nom d'utilisateur</b> (pour Dispatch Server)	Entrez un nom d'utilisateur. Le nom d'utilisateur doit être identique à celui fourni par le fournisseur de votre système.
<b>Nom d'utilisateur</b> (pour serveur ST)	Entrez un nom d'utilisateur. Doit être identique à celui saisi lors de la création du <b>composant Axis One-Click Connection</b> .

## Configuration de Smart Map

Cette section décrit comment :

- Configurer l'arrière-plan géographique choisi pour votre smart map
- Activer l'édition des smart map, y compris les caméras, dans XProtect Smart Client
- Configurer votre smart map avec Milestone Federated Architecture

## Arrière-plans géographiques (explications)

Avant de sélectionner un arrière-plan géographique dans XProtect Smart Client, vous devez d'abord configurer les arrière-plans géographiques dans XProtect Management Client.

- **Carte du monde basique** - Utilisez l'arrière-plan géographique standard fourni dans XProtect Smart Client. Aucune configuration n'est requise. Ce plan a été conçu pour servir de référence générale et ne contient pas de fonctions comme frontières, villes ou autres détails. Cependant, comme les autres arrière-plans géographiques, il contient des données de géo-référence
- **Bing Maps** - Connectez-vous à Bing Maps
- **Google Maps** - Connectez-vous à Google Maps
- **OpenStreetMap** vous offre trois options :
  - Vous connecter à un serveur de tuile commercial de votre choix
  - Vous connecter à votre propre serveur de tuile local



Les options Bing Maps et Google Maps nécessitent un accès Internet, et vous devez acheter une clé à Microsoft ou Google.

À moins que vous n'utilisiez votre propre serveur de tuile local, OpenStreetMap nécessite également un accès Internet.

Par défaut, Bing Maps et Google Maps affichent des images satellitaires (Satellite). Vous pouvez modifier les images dans XProtect Smart Client, en choisissant par exemple aérien ou terrain, pour voir différents détails.

## Acquérir une clé API pour Google Maps ou Bing Maps

### Google Maps

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

Une fois que vous avez la clé API, vous devez l'entrer dans le XProtect Management Client. Voir Activer Bing Maps ou Google Maps dans Management Client sur la page 480.

Pour plus d'informations, voir :

- Plate-forme Google Maps - Démarrer : <https://cloud.google.com/maps-platform/>
- Guide de plate-forme de facturation Google Maps : <https://developers.google.com/maps/billing/gmp-billing>
- Guide du développeur de l'API Maps Static : <https://developers.google.com/maps/documentation/maps-static/dev-guide>

## Bing Maps

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

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

Une fois que vous avez la clé API, vous devez l'entrer dans le XProtect Management Client. Voir Activer Bing Maps ou Google Maps dans Management Client sur la page 480.

## Activer Bing Maps ou Google Maps dans Management Client

Vous pouvez rendre la clé disponible à plusieurs utilisateurs en la saisissant pour un profil Smart Client dans Management Client. Tous les utilisateurs étant assignés au profil utiliseront cette clé.

Étapes :

1. Dans Management Client, dans le panneau **Navigation de site**, cliquez sur **Profil Smart Client**.
2. Dans le volet **Smart Client Profils**, sélectionnez le profil Smart Client concerné.
3. Dans le volet **Propriétés**, cliquez sur l'onglet **Smart Map** :
  - Pour Bing Maps, saisissez votre clé basique ou d'entreprise dans le champ **Clé Bing Maps**
  - Pour Google Maps, saisissez votre clé API Maps Static dans le champ **Clé privée pour Google Maps**
4. Pour empêcher les utilisateurs de XProtect Smart Client d'utiliser une autre clé, cochez la case **Verrouillée**.

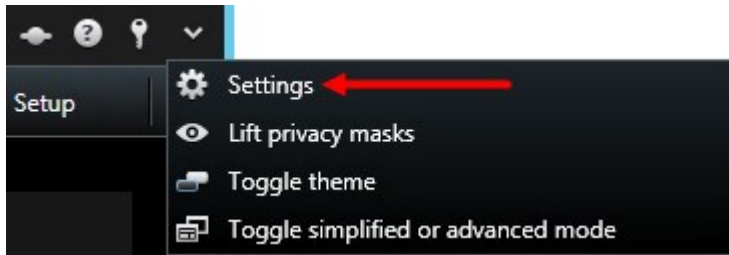
## Activer Bing Maps ou Google Maps dans XProtect Smart Client

Pour permettre aux opérateurs de XProtect Smart Client d'utiliser une clé différente à celle du profil Smart Client, vous devez saisir la clé dans les paramètres dans XProtect Smart Client.

Étapes :



1. Dans XProtect Smart Client, ouvrez la fenêtre **Paramètres**.



2. Cliquez sur **Smart Map**.
3. En fonction du service de plan que vous voulez utiliser, faites comme suit :
  - Pour Bing Maps, saisissez votre clé dans le champ **Clé Bing Maps**
  - Pour Google Maps, saisissez votre clé dans le champ **Clé privée pour Google Maps**

## Spécifier le serveur de tuile OpenStreetMap

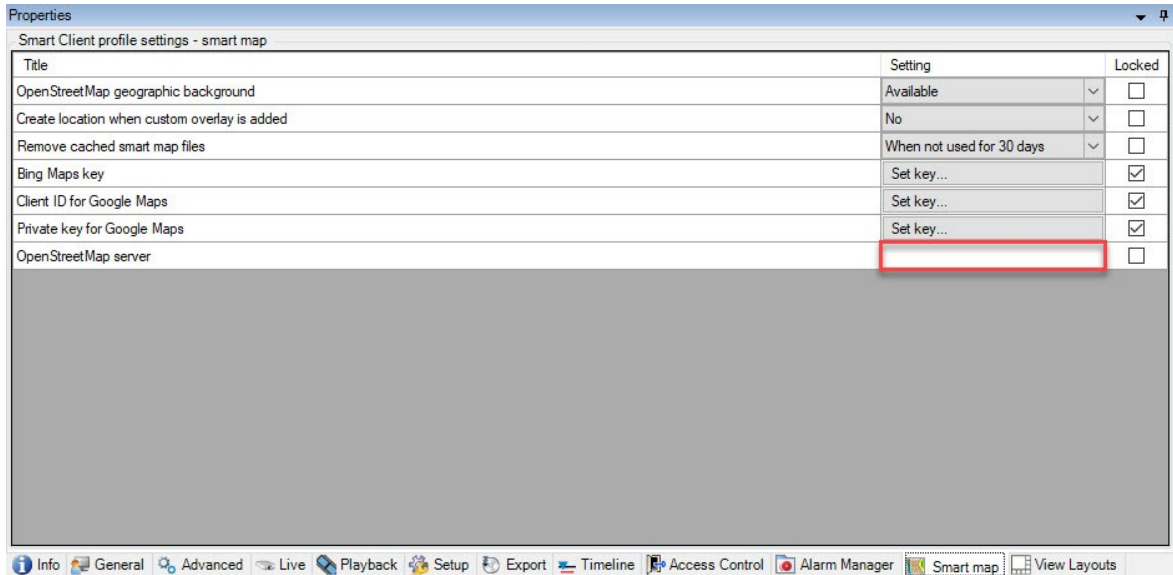
Si vous utilisez l'option **OpenStreetMap** en tant qu'arrière-plan géographique pour votre smart map, vous devez indiquer l'emplacement à partir duquel les images en tuile seront récupérées. Pour ce faire, il vous suffit de préciser l'adresse du serveur de tuile, que ce soit un serveur de tuile commercial ou local, par exemple, si votre organisation dispose de ses propres plans pour des zones telles que des aéroports ou des ports.



Vous pouvez également spécifier l'adresse du serveur de tuile dans la fenêtre **Paramètres** dans XProtect Smart Client.

Étapes :

1. Dans le panneau **Navigation du site**, développez le nœud **Client** et cliquez sur **Profils Smart Client**.
2. Dans le panneau Vue d'ensemble, sélectionnez le profil Smart Client pertinent.
3. Dans le volet **Propriétés**, cliquez sur l'onglet **Smart Map**.



4. Dans le champ **Serveur OpenStreetMap**, saisissez l'adresse du serveur de tuile.
5. Pour activer ce paramètre dans XProtect Smart Client, cochez la case **Verrouillé**. Les opérateurs de XProtect Smart Client ne pourront plus modifier l'adresse.
6. Sauvegardez les modifications apportées.

## Fichiers smart map en cache supprimés (explications)



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

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

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

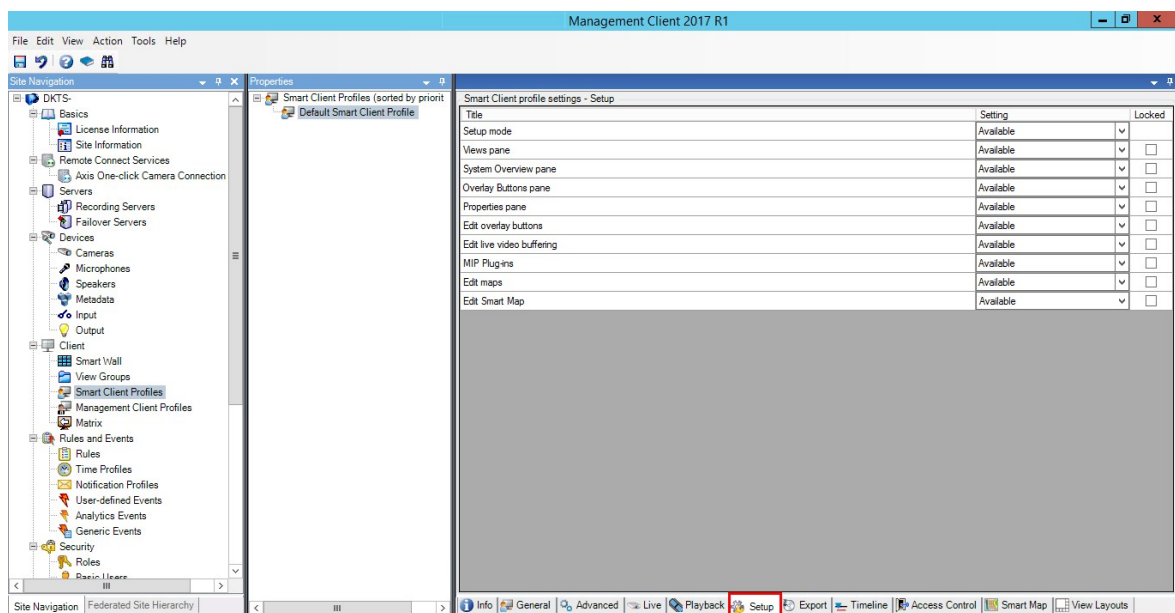
Lorsque vous modifiez l'adresse du serveur de tuile, un nouveau répertoire de cache est automatiquement créé. Les fichiers des plans précédents sont conservés dans le répertoire de cache correspondant sur votre ordinateur local.

## Activer la modification de la smart map

Les opérateurs peuvent modifier les smart maps dans XProtect Smart Client en mode configuration, uniquement si la modification est activée dans Management Client. Si cette option n'est pas déjà activée, vous devez activer la modification pour chaque profil Smart Client pertinent.

Étapes :

1. Dans le panneau **Navigation du site**, développez le nœud **Client**.
2. Cliquez sur **Smart Client Profiles**.



3. Dans le panneau Vue d'ensemble, sélectionnez le profil Smart Client pertinent.
4. Dans le volet **Propriétés**, cliquez sur l'onglet **Configuration**.
5. Dans la liste **Modifier les smart maps**, choisissez **Disponible**.
6. Répétez ces étapes pour chaque profil Smart Client pertinent.
7. Sauvegardez vos modifications. La prochaine fois que les utilisateurs assignés au profil Smart Client que vous avez sélectionné se connecteront au XProtect Smart Client, ils pourront modifier les smart maps.



Pour désactiver la modification, dans la liste **Modifier les smart maps**, choisissez **Indisponible**.

## Activer l'édition des caméras sur smart map

Afin de permettre aux opérateurs de positionner une caméra sur la smart map, régler le champ de visualisation ainsi que la direction, vous devez activer l'édition des caméras par rôle.

### Configuration

Avant de commencer, assurez-vous que la modification du Smart Map a été activée (voir Activer la modification de la smart map sur la page 483). Vous effectuez ces opérations dans le profil Smart Client auquel le rôle de l'opérateur est assigné.

Étapes :

1. Développez le noeud **Sécurité > Rôles**.
2. Dans le volet **Rôles**, sélectionnez le rôle auquel votre opérateur est associé.
3. Pour accorder les droits d'édition de rôles :
  - Cliquez sur l'onglet **Sécurité globale**, puis sélectionnez **Caméras** dans le panneau **Paramètres des rôles**
  - Dans la colonne **Autoriser**, cochez la case **Contrôle total** ou **Modifier**
4. Sauvegardez les modifications apportées.



Les étapes ci-dessus donnent au rôle le droit de modifier toutes les caméras. Pour activer la modification des différentes caméras, allez à l'onglet **Périphérique**, puis sélectionnez la caméra pertinente.

## Définissez la position de la caméra, la direction, le champ de visualisation et la profondeur (smart map)

Pour vous assurer qu'une caméra est positionnée correctement sur la smart map, vous pouvez définir les coordonnées géographiques, la direction de la caméra, le champ de visualisation et la profondeur de vue. Ce faisant, la caméra s'ajoute automatiquement à la smart map la prochaine fois où un opérateur la charge dans XProtect Smart Client.

Étapes :

1. Dans Management Client, développez le noeud **Périphériques** et sélectionnez **Caméras**.
2. Dans le volet **Périphériques**, sélectionnez le groupe de caméras pertinent ainsi que la caméra.
3. Sur l'onglet **Infos**, défilez vers le bas jusqu'à **Informations sur la position**.

**Properties**

**Device information**

Name: 10.100.x.xxx\_camera1

Short name: Back entry

Description:

Hardware name: Back entry

Port number: 2

**Positioning information**

Geo coordinates: 55.6553634527205, 12.43028007233498  
(Example: -33.856900, 151.215100)

Direction (a): 87,75 Degrees

Field of view (b): 150 Degrees

Depth (c): 112,36 Meter

Illustration:

Preview position in browser...

Info Settings Streams Record Motion Fisheye Lens Client Privacy Mask

4. Spécifiez la latitude et la longitude dans le champ **Coordonnées géographiques**, dans cet ordre. Utilisez un point comme séparateur et une virgule pour séparer les valeurs.
5. Dans le champ **Direction**, saisissez une valeur comprise dans la plage allant de 0 à 360 degrés.
6. Dans le champ **Champ de visualisation**, saisissez une valeur comprise entre 0 et 360 degrés.

7. Dans le champ **Profondeur**, saisissez la profondeur de vue en mètres ou en pieds.
8. Sauvegardez les modifications apportées.



Vous pouvez également définir les propriétés sur les serveurs d'enregistrement.

## Configuration d'une Smart Map avec Milestone Federated Architecture

Si vous utilisez un Smart Map dans une Milestone Federated Architecture, toutes les caméras des sites connectés apparaîtront sur ce Smart Map. Cette section décrit les différentes étapes de configuration d'une Smart Map dans une architecture fédérée.



Pour une présentation générale de Milestone Federated Architecture, voir En cours de configuration de Milestone Federated Architecture sur la page 456.

1. Avant de vous connecter au site supérieur et ses sites enfants, vérifiez que les coordonnées géographiques sont bien spécifiées sur toutes les caméras de tous les sites. Les coordonnées géographiques s'ajoutent automatiquement lorsque l'on positionne une caméra sur la smart map par le biais de XProtect Smart Client, mais vous pouvez aussi les ajouter manuellement dans Management Client, dans les propriétés des caméras. Pour plus d'informations, voir Définissez la position de la caméra, la direction, le champ de visualisation et la profondeur (smart map) sur la page 484.
2. Vous devez ajouter les opérateurs Smart Client comme utilisateurs Windows sur le site parent et tous les sites fédérés. Au moins sur le site supérieur, les utilisateurs Windows doivent avoir les droits de modification de Smart Map. Ils pourront ainsi modifier la Smart Map du site supérieur et de tous les sites enfants. Vous devrez ensuite déterminer si les utilisateurs Windows des sites enfants doivent avoir les droits de modifier une Smart Map. Dans Management Client, vous créez d'abord les utilisateurs Windows sous **Rôles**, puis vous activez la modification de Smart Map. Pour plus d'informations, voir Activer la modification de la smart map sur la page 483.
3. Sur le site supérieur, ajoutez les sites enfants en tant qu'utilisateurs Windows à un rôle détenant des droits d'administrateur. Lorsque vous spécifiez le type d'objet, cochez la case **Ordinateurs**.
4. Sur chacun des sites enfants, ajoutez le site supérieur en tant qu'utilisateur Windows au même rôle administrateur utilisé sur le site supérieur. Lorsque vous spécifiez le type d'objet, cochez la case **Ordinateurs**.
5. Sur le site supérieur, vérifiez que la fenêtre **Hiérarchie des sites fédérés** s'affiche. Dans Management Client, allez dans **Aperçu** et sélectionnez **Hiérarchie des sites fédérés**. Ajoutez tous les sites enfants au site supérieur. Pour en savoir plus, voir Ajouter un site à la hiérarchie sur la page 462.

6. Vous pouvez maintenant tester si cela fonctionne sur XProtect Smart Client. Connectez-vous au site supérieur en tant qu'administrateur ou opérateur, et ouvrez un aperçu contenant la Smart Map. Si la configuration a été correctement effectuée, toutes les caméras du site supérieur et des sites enfants apparaîtront sur la Smart Map. Si vous vous connectez à l'un des sites enfants, vous ne verrez que les caméras de ce site et ses sites enfants.



Pour modifier les caméras d'une smart map, par exemple l'emplacement ou l'angle d'une caméra, l'utilisateur doit disposer du droit de modification des caméras.

# Maintenance

## Sauvegarde et restauration de la configuration système

Milestone vous recommande de faire des sauvegardes régulières de la configuration de votre système comme mesure préventive de la récupération d'urgence. Bien que la perte de votre configuration soit un phénomène rare, cela peut arriver dans des circonstances malheureuses. Il est important de protéger vos sauvegardes par le biais de mesures techniques ou organisationnelles.

### Sauvegarde et de la restauration de la configuration de votre système (explications)

Le système offre une fonctionnalité intégrée qui sauvegarde toute la configuration du système que vous pouvez définir dans le Management Client. La base de données du serveur de journaux et les fichiers journaux, y compris les fichiers de journal d'activité, ne sont pas inclus dans cette sauvegarde.

Si votre système est grand, Milestone vous recommande de définir des sauvegardes planifiées. Cela se fait avec l'outil tiers : Microsoft® SQL Server Management Studio. Cette sauvegarde contient les mêmes données qu'une sauvegarde manuelle.

Lors d'une sauvegarde, le système reste en ligne.

La sauvegarde de votre configuration peut prendre un certain temps. La durée de sauvegarde dépend de :

- Votre configuration système
- Votre matériel
- Si vous avez installé le composant SQL Server, Event Server et le composant Management Server sur un seul ou sur plusieurs serveurs

Chaque fois que vous effectuez une sauvegarde à la fois manuelle et programmée, le fichier journal de transaction de la base de données SQL est vidé. Pour plus d'informations sur comment purger le fichier journal de transaction, voir Journal des transactions de la base de données SQL (explications) sur la page 58.



Assurez-vous de connaître les paramètres de votre mot de passe de configuration système lorsque vous créez une sauvegarde.





Pour les systèmes conformes aux normes FIPS 140-2 comportant des exportations et des bases de données multimédias archivées à partir des versions de VMS XProtect antérieures à 2017 R3 qui sont cryptées avec un cryptage non-conforme aux normes FIPS, il est nécessaire d'archiver les données dans un emplacement auquel il est possible d'accéder après l'activation du mode FIPS.

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

## Sélectionner le fichier de sauvegarde partagé

Avant de sauvegarder et de restaurer une configuration système, vous devez créer un fichier de sauvegarde à cette fin.

1. Cliquez droit sur l'icône de service du Management Server de la zone de notification et sélectionnez **Sélectionner le répertoire de sauvegarde partagé**.
2. Dans la fenêtre qui s'affiche, naviguez vers l'emplacement de fichier désiré.
3. Cliquez deux fois sur **OK**.
4. S'il vous est demandé si vous souhaitez supprimer des fichiers dans le fichier de sauvegarde actuel, cliquez sur **Oui** ou **Non** en fonction de vos besoins.

## Sauvegarde manuelle de la configuration système

1. À partir de la barre de menu, sélectionnez **Fichier > Configuration de sauvegarde**.
2. Lisez la note dans la boîte de dialogue et cliquez sur **Sauvegarder**.
3. Entrez un nom de fichier pour le fichier .cnf.
4. Saisissez un dossier de destination et cliquez sur **Enregistrer**.
5. Attendez que la sauvegarde soit terminée, puis cliquez sur **Fermer**.



Tous les fichiers de configuration du système concernés sont regroupés dans un seul fichier .cnf, qui est sauvegardé à un emplacement spécifique. Pendant la sauvegarde, tous les fichiers de sauvegarde sont d'abord exportés vers un dossier de sauvegarde temporaire du système sur le serveur de gestion. Vous pouvez sélectionner un autre répertoire temporaire par un clic droit sur l'icône du service du Management Server de la zone de notification, et en sélectionnant **Sélectionner le répertoire de sauvegarde partagé**.

## Restauration d'une configuration système à partir d'une sauvegarde manuelle

### Informations importantes

- L'utilisateur qui installe et celui qui restaure doivent tous les deux être des administrateurs locaux de la base de données SQL de la configuration de votre système sur le serveur de gestion **et** sur le SQL Server
- À l'exception de vos serveurs d'enregistrement, votre système est complètement éteint pendant la durée de la restauration, qui peut prendre plusieurs minutes
- Une sauvegarde ne peut être restaurée que sur l'installation du système où elle a été créée. Assurez-vous que la configuration est aussi similaire que possible au moment où la sauvegarde a été effectuée. Autrement, la restauration peut échouer
- Si, lors de la restauration, vous êtes invité à saisir un mot de passe de configuration système, vous devez alors fournir le mot de passe de configuration système qui était valide au moment de la création de la sauvegarde. Sans ce mot de passe, il vous est impossible de restaurer votre configuration à partir de la sauvegarde.
- Si vous sauvegardez la base de données SQL et la restaurez sur un SQL Server propre, les erreurs de la base de données ne fonctionneront pas et vous ne recevrez que des messages d'erreurs généraux du SQL Server. Pour éviter cela, réinstallez d'abord votre système XProtect à l'aide du SQL Server propre et restaurez la sauvegarde par-dessus
- Si la restauration échoue au cours de la phase de validation, vous pouvez redémarrer l'ancienne configuration parce que vous n'avez apporté aucun changement  
En cas d'échec de la restauration à un autre endroit du processus, vous ne pouvez pas revenir à l'ancienne configuration  
Tant que le fichier de sauvegarde n'est pas corrompu, vous pouvez effectuer une autre restauration
- La restauration remplace la configuration actuelle. Cela signifie que toute modification apportée à la configuration depuis la perte de la dernière sauvegarde est perdue
- Aucun journal, y compris les journaux d'audit, n'est restauré
- Une fois que la restauration a commencé, vous ne pouvez pas l'annuler

## Restauration

1. Cliquez droit sur l'icône de service du Management Server de la zone de notification et sélectionnez **Restaurer la configuration**.
2. Lisez la note importante et cliquez sur **Restaurer**.
3. Dans la boîte de dialogue d'ouverture de fichier, naviguez vers l'emplacement du fichier de configuration de sauvegarde du système, sélectionnez-le, et cliquez sur **Ouvrir**.



Le fichier de sauvegarde se trouve sur l'ordinateur Management Client. Si le Management Client est installé sur un autre serveur, copiez le fichier de sauvegarde de ce serveur avant de sélectionner la destination.

4. La fenêtre **Restaurer la configuration** s'affiche. Attendez la fin de la restauration et cliquez sur **Fermer**.

## Mot de passe de configuration système (explications)

Vous pouvez choisir de protéger la configuration système globale en attribuant un mot de passe de configuration système. Une fois que vous attribuez un mot de passe de configuration système, les sauvegardes de cette dernière sont protégées par ce mot de passe. Les paramètres du mot de passe sont stockés dans un dossier sécurisé de l'ordinateur qui exécute le serveur de gestion. Vous aurez besoin de ce mot de passe pour :

- Restaurer la configuration à partir d'une sauvegarde de configuration qui a été créée avec des paramètres de mot de passe différents à ceux du mot de passe actuel
- Déplacer ou installer le serveur de gestion sur un autre ordinateur en raison d'une panne matérielle (récupération)
- Configurer un serveur de gestion additionnel dans un système en grappe



Vous pouvez attribuer le mot de passe de configuration système avant ou après l'installation. Il doit respecter les exigences en matière de complexité de Windows, lesquelles sont définies par la politique de Windows concernant les mots de passe.



Il est important que les administrateurs système enregistrent ce mot de passe dans un emplacement sécurisé. Si vous avez attribué un mot de passe de configuration système et que vous effectuez la restauration d'une sauvegarde, vous pourriez être invité à fournir le mot de passe de configuration système. Sans ce mot de passe, il vous est impossible de restaurer votre configuration à partir de la sauvegarde.

## Paramètres du mot de passe de configuration système

Vous pouvez modifier les paramètres du mot de passe de configuration système. Dans les paramètres du mot de passe de configuration système, vous pouvez :

- Choisir de protéger par un mot de passe la configuration système en attribuant un mot de passe de configuration système
- Modifier un mot de passe de configuration système
- Choisir de ne pas protéger par un mot de passe la configuration système en supprimant tout mot de passe de configuration système attribué

## Modifier les paramètres du mot de passe de configuration système



Lorsque vous changez le mot de passe, il est important que les administrateurs système enregistrent les mots de passe associés aux différentes sauvegardes dans un emplacement sécurisé. Si vous effectuez la restauration d'une sauvegarde, vous pourriez être invité à saisir le mot de passe de configuration système qui était valide au moment de la création de la sauvegarde. Sans ce mot de passe, il vous est impossible de restaurer votre configuration à partir de la sauvegarde.



Vous devez redémarrer les services du serveur de gestion pour appliquer les changements.

1. Accédez à l'icône du serveur de gestion dans la barre d'état et vérifiez que le service s'exécute normalement.
2. Effectuez un clic droit sur l'icône de service du Management Server de la zone de notification et sélectionnez **Modifier les paramètres du mot de passe de configuration système**.
3. La boîte de dialogue pour modifier les paramètres du mot de passe de configuration système s'affiche.

### Attribuer un mot de passe

1. Saisissez le nouveau mot de passe dans le champ **Nouveau mot de passe**.
2. Saisissez à nouveau le nouveau mot de passe dans le champ **Confirmer le nouveau mot de passe** puis sélectionnez **Entrer**.
3. Lisez la notification qui s'affiche puis cliquez sur **Oui** pour accepter le changement.
4. Attendez de recevoir la confirmation du changement puis sélectionnez **Fermer**.
5. Vous devez redémarrer les services du serveur de gestion pour appliquer les changements.
6. Après le redémarrage, vérifiez que le serveur de gestion s'exécute normalement.

### Supprimer la protection par mot de passe

Vous pouvez annuler la protection par mot de passe si vous n'en avez pas besoin :

1. Cochez la case : **Je choisis de ne pas utiliser de mot de passe de configuration système et je comprends que la configuration système ne sera pas cryptée** puis cliquez sur **entrer**.
2. Lisez la notification qui s'affiche puis cliquez sur **oui** pour accepter le changement.

3. Attendez de recevoir la confirmation du changement puis sélectionnez **Fermer**.
4. Vous devez redémarrer les services du serveur de gestion pour appliquer les changements.
5. Après le redémarrage, vérifiez que le serveur de gestion s'exécute normalement.

## Entrer les paramètres du mot de passe de configuration système (récupération)

Si le fichier contenant les paramètres du mot de passe est supprimé en raison d'une panne matérielle ou toute autre raison, il vous faudra saisir les paramètres du mot de passe de configuration système pour accéder à la base de données hébergeant la configuration système. Lors de son installation sur un nouvel ordinateur, vous serez invité à entrer les paramètres du mot de passe de configuration système.

Cependant, si le fichier contenant les paramètres du mot de passe est supprimé ou corrompu, et que l'ordinateur exécutant le serveur de gestion n'a pas d'autres problèmes, vous pouvez entrer les paramètres du mot de passe de configuration système :

1. Accédez à l'icône du serveur de gestion dans la barre d'état.
2. Effectuez un clic droit sur l'icône de service du Management Server de la zone de notification et sélectionnez **Entrer le mot de passe de configuration système**.
3. La boîte de dialogue pour entrer les paramètres du mot de passe de configuration système s'affiche.

### La configuration système est protégée par un mot de passe

1. Saisissez le mot de passe dans le champ **mot de passe** puis sélectionnez **Entrer**.
2. Attendez que le mot de passe ait bien été accepté. Sélectionnez **Fermer**.
3. Vérifiez que le serveur de gestion s'exécute normalement.

### La configuration système n'est pas protégée par un mot de passe

1. Cochez la case : **Ce système n'utilise pas de mot de passe de configuration système** puis sélectionnez **entrer**.
2. Attendez que le paramètre ait bien été accepté. Sélectionnez **Fermer**.
3. Vérifiez que le serveur de gestion s'exécute normalement.

## Sauvegarde manuelle de la configuration de votre système (explications)

Si vous souhaitez effectuer une sauvegarde manuelle de la configuration de la base de données SQL du serveur de gestion contenant la configuration du système, assurez-vous que votre système reste en ligne. Le nom par défaut de la base de données SQL du serveur de gestion est **Surveillance**.

Voici quelques éléments à considérer avant de commencer la sauvegarde :

- Vous ne pouvez pas utiliser une sauvegarde de la base de données SQL pour copier des configurations de votre système pour d'autres systèmes
- La sauvegarde de la base de données SQL peut prendre un certain temps. Cela dépend de la configuration de votre système, de votre matériel, et si votre SQL Server, votre serveur de gestion et Management Client sont installés sur le même ordinateur
- Les journaux, y compris les journaux d'audit, sont stockés sur la base de données SQL du serveur de journaux, et ne font ainsi **pas** partie d'une sauvegarde de la base de données SQL du serveur de gestion. Le nom par défaut de la base de données SQL du serveur de journaux est **SurveillanceLogServerV2**. Vous sauvegardez les deux base de données SQL en même temps.

## Sauvegarde et restauration de la configuration du serveur d'événements (explications)

Le contenu de la configuration de votre serveur d'événements est inclus lorsque vous sauvegardez et restaurez la configuration du système.

La première fois que vous exécutez le serveur d'événements, tous ses fichiers de configuration sont automatiquement déplacés sur la base de données SQL. Vous pouvez appliquer la configuration restaurée au serveur d'événements sans avoir besoin de redémarrer le serveur d'événements, et le serveur d'événements peut démarrer et d'arrêter toutes les communications externes pendant que la restauration de la configuration est en cours de chargement.

## Sauvegarde et restauration programmées de la configuration du système (explications)

Le serveur de gestion sauvegarde la configuration de votre système dans une base de données SQL. Milestone vous recommande de programmer régulièrement des sauvegardes de cette base de données SQL comme mesure préventive de la récupération d'urgence. Bien que la perte de la configuration de votre système soit un phénomène rare, cela peut arriver dans des circonstances malheureuses. Heureusement, la sauvegarde ne prend qu'une minute et elle offre également l'avantage de purger le journal de transaction de la base de données SQL.

Si vous avez une configuration plus petite et n'avez pas besoin de sauvegardes programmées, vous pouvez sauvegarder la configuration de votre système manuellement. Pour de plus amples instructions, voir Sauvegarde manuelle de la configuration de votre système (explications) sur la page 493.

Lorsque vous sauvegardez/restaurez le serveur de gestion, assurez-vous que la base de données SQL comportant la configuration du système est incluse dans la sauvegarde/restauration.

### Conditions préalables pour l'utilisation de la sauvegarde et la restauration programmées

Microsoft® SQL Server Management Studio, un outil à télécharger gratuitement depuis leur site Web (<https://www.microsoft.com/downloads/>).

Outre la gestion des SQL Server et leurs bases de données, l'outil comprend des fonctions de sauvegarde et de restauration faciles à utiliser. Téléchargez et installez l'outil sur votre serveur de gestion.

## Sauvegarder la configuration du système avec une sauvegarde programmée

1. Lancez Microsoft® SQL Server Management Studio depuis le menu Windows.
2. Lors de la connexion, spécifiez le nom du SQL Server requis. Utilisez le compte sous lequel vous avez créé la base de données SQL.
  1. Localisez la base de données SQL qui contient toute votre configuration du système, incluant le serveur d'événements, les serveurs d'enregistrement, les caméras, les entrées, les sorties, les utilisateurs, les règles, les profils de patrouille, entre autres. Le nom par défaut de la base de données SQL est **Surveillance**.
  2. Faites une sauvegarde de la base de données SQL et assurez-vous de :
    - Vérifiez que la base de données SQL sélectionnée est la correcte
    - Vérifiez que le type de sauvegarde est **complète**
    - Établissez la programmation pour la sauvegarde récurrente. Vous pouvez obtenir de plus amples informations sur les sauvegardes programmées et automatiques sur le site Web de Microsoft (<https://docs.microsoft.com/en-us/sql/relational-databases/logs/the-transaction-log-sql-server?view=sql-server-2017>)
    - Vérifier que le chemin proposé est satisfaisant ou de sélectionner un autre chemin
    - Sélectionner **Vérifier la sauvegarde en fin d'opération** et **Effectuer une somme de contrôle avant d'écrire sur le support**
3. Suivez les instructions de l'outil jusqu'à la fin.

Envisagez également la sauvegarde de la base de données SQL du serveur de journaux en procédant de la même manière. Le nom par défaut de la base de données SQL du serveur de journaux est **SurveillanceLogServerV2**.

## Restauration d'une configuration système à partir d'une sauvegarde programmée

### Configuration

Afin d'empêcher les modifications de configuration du système pendant que vous restaurez la base de données SQL de la configuration du système, arrêtez le :

- Service Management Server (voir Services du serveur de gestion sur la page 509)
- Event Server service (peut être effectué depuis les **Services** de Windows (recherchez **services.msc** sur votre machine. Dans **Services**, localisez **Milestone XProtect Event Server**))
- World Wide Web Publishing Service, également connu sous le nom d'Internet Information Service (IIS). Pour découvrir comment arrêter l'IIS ([https://technet.microsoft.com/library/cc732317\(ws.10\).aspx/](https://technet.microsoft.com/library/cc732317(ws.10).aspx/))

Ouvrez Microsoft® SQL Server Management Studio depuis le menu Windows .

Dans l'outil, procédez comme suit :

1. Lors de la connexion, spécifiez le nom du SQL Server requis. Utilisez le compte utilisateur sous lequel la base de données SQL a été créée.
2. Localisez la base de données SQL (son nom par défaut est **Surveillance**) qui contient toute votre configuration du système, incluant le serveur d'événements, les serveurs d'enregistrement, les caméras, les entrées, les sorties, les utilisateurs, les règles, les profils de patrouille, entre autres.
3. Faites une restauration de la base de données SQL et assurez-vous de :
  - Sélectionner Sauvegarder **à partir** d'un périphérique
  - Sélectionner sauvegarde du support de type **fichier**
  - Localisez et sélectionnez votre fichier de sauvegarde (**.bak**)
  - Sélectionner pour **écraser la base de données existante**
4. Suivez les instructions de l'outil jusqu'à la fin.

Utilisez la même méthode pour restaurer la base de données SQL du serveur des journaux avec vos journaux. Le nom par défaut de la base de données SQL du serveur de journaux est **SurveillanceLogServerV2**.



Le système ne fonctionne pas tant que le service Management Server est arrêté. Il est important de se rappeler de démarrer tous les services une fois que vous avez terminé la restauration de la base de données.

## Sauvegarder la base de données SQL du serveur de journaux

Gérer la base de données SQL du serveur des journaux en utilisant la méthode que vous utilisez lorsque vous gérez la configuration du système comme décrit précédemment. La base de données SQL du serveur des journaux contient tous les journaux système, y compris les erreurs reportées par les serveurs d'enregistrement et les caméras. Le nom par défaut de la base de données SQL du serveur de journaux est **SurveillanceLogServerV2**.

La base de données SQL se trouve sur la SQL Server du serveur des journaux. En général, les bases de données SQL du serveur des journaux et du serveur de gestion se trouvent sur le même SQL Server. La sauvegarde de la base de données SQL n'est pas vitale car elle ne contient aucune configuration du système. Toutefois, il est possible que vous appréciez éventuellement d'avoir accès aux journaux système précédant la restauration/sauvegarde du serveur de gestion.

## Scénarios de problèmes et d'échecs de sauvegarde/restauration (explications)

- Si, après votre dernière sauvegarde de la configuration du système, vous avez déplacé le serveur d'événements ou d'autres services enregistrés tels que le serveur de journaux, vous devez sélectionner la configuration du service enregistrée que vous souhaitez pour le nouveau système. Vous pouvez décider de conserver la nouvelle configuration après que le système ait été restauré avec l'ancienne configuration. Vous choisissez en regardant les noms d'hôte des services.



- Si votre restauration de la configuration du système échoue parce que le serveur d'événements ne se trouve pas à la destination spécifiée (par exemple, si vous avez choisi l'ancienne configuration de service enregistrée), effectuez une nouvelle restauration.
- Si vous restaurez une sauvegarde de configuration et que vous saisissez un mot de passe de configuration système incorrect, vous devez alors fournir le mot de passe de configuration système qui était valide au moment de la création de la sauvegarde.

## Déplacer le serveur de gestion

Le serveur de gestion sauvegarde votre configuration du système dans une base de données SQL. Si vous déplacez le serveur de gestion d'un serveur physique à un autre, il est primordial que vous vous assuriez que votre nouveau serveur de gestion a également accès à cette base de données SQL. La base de données SQL de la configuration du système peut être enregistrée de deux manières différentes :

- **Réseau SQL Server** : Si vous enregistrez votre configuration du système dans une base de données SQL sur un SQL Server de votre réseau, vous pouvez identifier l'emplacement de la base de données SQL sur le SQL Server lors de l'installation du logiciel du serveur de gestion sur votre nouveau serveur de gestion. Dans ce cas, seul applique le paragraphe suivant sur le nom d'hôte et l'adresse IP du serveur de gestion et vous pouvez ignorer le reste de ce sujet :

**Nom d'hôte et adresse IP du serveur de gestion** : Lorsque vous déplacez le serveur de gestion d'un serveur physique à un autre serveur physique, la solution la plus facile consiste à donner au nouveau serveur le même nom d'hôte et la même adresse IP que l'ancien serveur. Ceci s'explique par le fait que le serveur d'enregistrement se connecte automatiquement au nom d'hôte et à l'adresse IP de l'ancien serveur de gestion. Si vous donnez au nouveau serveur de gestion un nouveau nom d'hôte et/ou une nouvelle adresse IP, le serveur d'enregistrement ne peut trouver le serveur de gestion et vous devez alors arrêter manuellement chaque service Recording Server dans votre système, changer l'URL de leur serveur de gestion, réenregistrer le serveur d'enregistrement et une fois fait, démarrer le service Recording Server.

- **Local SQL Server** : Si vous enregistrez votre configuration du système dans une base de données SQL sur un SQL Server directement sur le serveur de gestion, il est important que vous sauvegardiez la base de données de configuration du système du serveur de gestion existant avant le déplacement. En sauvegardant la base de données SQL et ensuite, en la restaurant sur un SQL Server sur le nouveau serveur de gestion, vous évitez d'avoir à reconfigurer vos caméras, règles, profils de temps etc. après le déplacement



Si vous déplacez le serveur de gestion, vous aurez besoin du mot de passe de configuration système afin de restaurer la sauvegarde, voir Mot de passe de configuration système (explications) sur la page 491.

## Configuration

- **Votre fichier d'installation logicielle pour installation sur le nouveau serveur de gestion**
- **Votre fichier de licence logicielle (.lic)**, que vous avez reçu lors de l'achat et de l'installation initiale de votre système. Vous ne devriez pas utiliser le fichier de licence logicielle activé que vous avez reçu après une activation manuelle des licences hors ligne. Un fichier de licence logicielle contient des informations relatives au serveur spécifique sur lequel le système est installé. Par conséquent un fichier de licence logicielle activé ne peut pas être réutilisé lors du déplacement vers un nouveau serveur

Si vous mettez également à jour le logiciel de votre système conjointement au déplacement, vous aurez reçu un nouveau fichier de licence logicielle. Il vous suffira alors d'utiliser ce dernier.

- **SQL Server local réservé aux utilisateurs : Microsoft® SQL Server Management Studio**
- Que se passe-t-il lorsque le serveur de gestion est indisponible ? Serveurs de gestion indisponibles (explications) sur la page 498)
- Copier la base de données du serveur de journaux (voir Sauvegarder la base de données SQL du serveur de journaux sur la page 496)

## Serveurs de gestion indisponibles (explications)

- **Les serveurs d'enregistrement peuvent encore enregistrer** : Tout serveur d'enregistrement en cours de fonctionnement a reçu une copie de sa configuration du serveur de gestion, donc il peut fonctionner et sauvegarder les enregistrements automatiquement pendant que le serveur de gestion est hors service. Par conséquent, l'enregistrement programmé et par détection de mouvement fonctionne, et l'enregistrement déclenché par les événements fonctionne également sous réserve d'être basé sur des événements associés au serveur de gestion ou tous autres serveurs d'enregistrement puisque ces derniers passent par le serveur de gestion
- **Les serveurs d'enregistrement sauvegardent temporairement les données de journaux localement** : Ils envoient automatiquement les données de journaux au serveur de gestion lorsqu'il redevient disponible :
  - **Les clients ne peuvent pas s'identifier** : L'accès des clients est autorisé via le serveur de gestion. Sans le serveur de gestion, les clients ne peuvent se connecter
  - **Les clients qui sont déjà connectés peuvent rester connectés pendant une heure** : Lorsque les clients se connectent, ils sont autorisés par le serveur de gestion et peuvent communiquer avec les serveurs d'enregistrement pour une durée d'une heure. Si vous pouvez organiser le nouveau serveur de gestion et le faire fonctionner en une heure, beaucoup de vos utilisateurs ne sont pas affectés
  - **Impossible de configurer le système** : Sans le serveur de gestion, vous ne pouvez pas modifier la configuration du système

Milestone vous recommande que vous informiez vos utilisateurs du risque de perte de contact avec le système de surveillance pendant que le serveur de gestion est hors service.

## Déplacer la configuration du système

Déplacer votre configuration système est un processus en trois étapes :

1. Faites une sauvegarde de votre configuration système. Il s'agit de la même procédure que pour programmer une sauvegarde programmée. Voir également Sauvegarder la configuration du système avec une sauvegarde programmée sur la page 495.
2. Installez le nouveau serveur de gestion sur le nouveau serveur. Voir sauvegarde programmée, étape 2.
3. Restaurez la configuration de votre système sur le nouveau système. Voir également Restauration d'une configuration système à partir d'une sauvegarde programmée sur la page 495.

## Remplacer un serveur d'enregistrement

Si un serveur d'enregistrement fonctionne mal et que vous souhaitez le remplacer par un nouveau serveur qui hérite des paramètres de l'ancien serveur d'enregistrement, procédez comme suit :

1. Récupérez l'identifiant du serveur d'enregistrement auprès de l'ancien serveur d'enregistrement :
  1. Sélectionnez **Serveurs d'enregistrement**, puis dans le volet **Vue d'ensemble**, sélectionnez l'ancien serveur d'enregistrement.
  2. Sélectionnez l'onglet **Stockage**.
  3. Appuyez sur la touche CTRL de votre clavier et maintenez-la enfoncée tout en sélectionnant l'onglet **Infos**.
  4. Copiez l'identifiant du serveur d'enregistrement indiqué dans la partie inférieure de l'onglet **Infos**. Ne copiez pas le terme *ID*, mais seulement le numéro.



2. Remplacez l'identifiant du serveur d'enregistrement sur le nouveau serveur d'enregistrement :
  1. Arrêtez le service Recording Server sur l'ancien serveur d'enregistrement, puis dans les **Services** de Windows, configurez le **Type de démarrage** des services à **Désactiver**.



Il est très important de ne pas démarrer simultanément deux serveurs d'enregistrement dotés d'identifiants identiques.

2. Sur le nouveau serveur d'enregistrement, ouvrez l'explorateur et allez sur *C:\ProgramData\Milestone\XProtect Serveur d'enregistrement* ou le chemin d'accès pour l'endroit où se situe votre serveur d'enregistrement.
3. Ouvrez le fichier *RecorderConfig.xml*.

4. Effacez l'identifiant indiqué entre les balises `<id>` et `</id>`.

```
- <recorderconfig>
- <recorder>
  <id>ff0b388d2-4b1b-4e00-8000-00003f4c337d3</id>
```



5. Collez l'identifiant du serveur d'enregistrement copié entre les balises `<id>` et `</id>`. Enregistrez le fichier `RecorderConfig.xml`.
  6. Allez au répertoire : `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VideoOS\Recorder\Installation`.
  7. Ouvrez **RecorderIDOnMachine** et changez l'ancien ID du serveur d'enregistrement au profit du nouvel ID.
3. Enregistrez le nouveau serveur d'enregistrement sur le serveur de gestion. Pour ce faire, effectuez un clic droit avec votre souris sur l'icône Recording Server Manager de la barre, puis cliquez sur **Enregistrer**. Pour plus d'informations, voir Enregistrer un serveur d'enregistrement sur la page 150.
  4. Redémarrez le service Recording Server. Dès que le nouveau service Recording Server démarre, le serveur d'enregistrement hérite de tous les paramètres de l'ancien serveur d'enregistrement.

## Déplacer le matériel

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

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

- Le système les supprime à l'expiration de la durée de rétention. Les enregistrements que quelqu'un a protégés à l'aide de la protection des preuves (voir Protection des preuves (explications) sur la page 428) ne sont pas supprimés tant que la durée de rétention de la protection des preuves n'a pas expiré. C'est vous qui définissez la durée de rétention de la protection des preuves lorsque vous la créez. La durée de rétention des preuves peut potentiellement ne jamais expirer
- Vous les supprimez du nouveau serveur d'enregistrement de chaque périphérique dans l'onglet **Enregistrer**

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



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

Vous pouvez utiliser la fonction Déplacer du matériel pour :

- **Équilibrer les charges** : Si, par exemple, le disque du serveur d'enregistrement est surchargé, vous pouvez ajouter un nouveau serveur d'enregistrement et déplacer une partie de votre matériel
- **Mettre à jour** : Par exemple, si vous devez remplacer le serveur hébergeant le serveur d'enregistrement par un nouveau modèle, vous pouvez installer un nouveau serveur d'enregistrement et déplacer le matériel de l'ancien serveur vers le nouveau serveur
- **Remplacer un serveur d'enregistrement défectueux** : Si, par exemple, le serveur est hors ligne et ne va jamais revenir en ligne, vous pouvez déplacer le matériel vers d'autres serveurs d'enregistrement et ainsi permettre au système de continuer à fonctionner. Vous ne pouvez pas accéder aux anciens enregistrements. Pour plus d'informations, voir Remplacer un serveur d'enregistrement sur la page 499.

## Enregistrements à distance

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

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

## Déplacer du matériel (Assistant)

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

### Configuration

Avant de démarrer l'assistant :

- Assurez-vous que le nouveau serveur d'enregistrement peut accéder à la caméra physique par le biais du réseau
- Installez le serveur d'enregistrement sur lequel vous souhaitez déplacer le matériel (voir XProtect Installer les nouveaux composants sur la page 94 ou XProtect Installer les nouveaux composants sur la page 94)
- Installez la même version des pilotes de périphériques sur le nouveau serveur d'enregistrement exécuté sur le serveur existant (voir Pilotes de périphériques (explications) sur la page 69)

Pour exécuter l'assistant :

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

3. Sélectionnez **Déplacer du matériel**.



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

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

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



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

### Diagnostic des problèmes de déplacement du matériel

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

Type d'erreur	Dépannage
Le serveur d'enregistrement n'est pas connecté ou est en mode de redondance.	Assurez-vous que le serveur d'enregistrement est bien en ligne. Vous aurez peut-être à l'enregistrer.  Si le serveur est en mode de redondance, patientez et réessayez.
La version du serveur d'enregistrement n'est pas la plus récente.	Mettez le serveur d'enregistrement à jour de façon à ce qu'il utilise la même version que le serveur de gestion.
Impossible de trouver le serveur d'enregistrement dans la configuration.	Assurez-vous de bien avoir autorisé le serveur d'enregistrement ou vérifiez qu'il n'a pas été supprimé.
Échec de la mise à jour de la configuration ou de la communication avec la base de données de configuration.	Assurez-vous que votre SQL Server et la base de données soient connectés et qu'ils fonctionnent.
Échec d'arrêt du matériel sur le serveur d'enregistrement actuel	Il est possible qu'un autre processus ait verrouillé le serveur d'enregistrement ou que le serveur d'enregistrement soit en mode erreur.  Assurez-vous que le serveur d'enregistrement fonctionne et réessayez.
Le matériel n'existe pas.	Assurez-vous que le matériel que vous essayez de déplacer n'a pas été simultanément supprimé du système par un autre utilisateur. Ce scénario est relativement improbable.
Le serveur d'enregistrement à partir duquel le matériel a été déplacé est à nouveau en ligne, mais vous avez choisi d'ignorer cette possibilité lorsqu'il était en ligne.	Vous avez sans doute accepté que l'ancien serveur d'enregistrement ne soit plus jamais en ligne lorsque vous avez lancé l'assistant <b>Déplacer du matériel</b> mais, au cours du déplacement, le serveur est revenu en ligne.  Redémarrez l'assistant et sélectionnez <b>Non</b> lorsqu'on vous demande de confirmer si le serveur va être en ligne à nouveau.
Le stockage d'enregistrement source n'est pas disponible.	Vous tentez de déplacer du matériel avec des périphériques configurés avec un stockage d'enregistrement actuellement hors ligne.  Un stockage d'enregistrement est hors ligne si le disque est

Type d'erreur	Dépannage
	<p>hors ligne ou indisponible.</p> <p>Assurez-vous que le stockage d'enregistrement en bien connecté et réessayez.</p>
<p>Tous les stockages des enregistrements disponibles sur le serveur d'enregistrement cible doivent être disponibles.</p>	<p>Vous tentez de déplacer du matériel vers un serveur d'enregistrement où une ou plusieurs stockages des enregistrements sont actuellement hors ligne.</p> <p>Assurez-vous que tous les stockages des enregistrement sur le serveur d'enregistrement cible sont en ligne.</p> <p>Un stockage d'enregistrement est hors ligne si le disque est hors ligne ou indisponible.</p>

## Remplacer le matériel

Lorsque vous remplacez un périphérique par un autre périphérique sur votre réseau, vous devez connaître l'adresse IP, le port, le nom d'utilisateur et le mot de passe du nouveau périphérique.

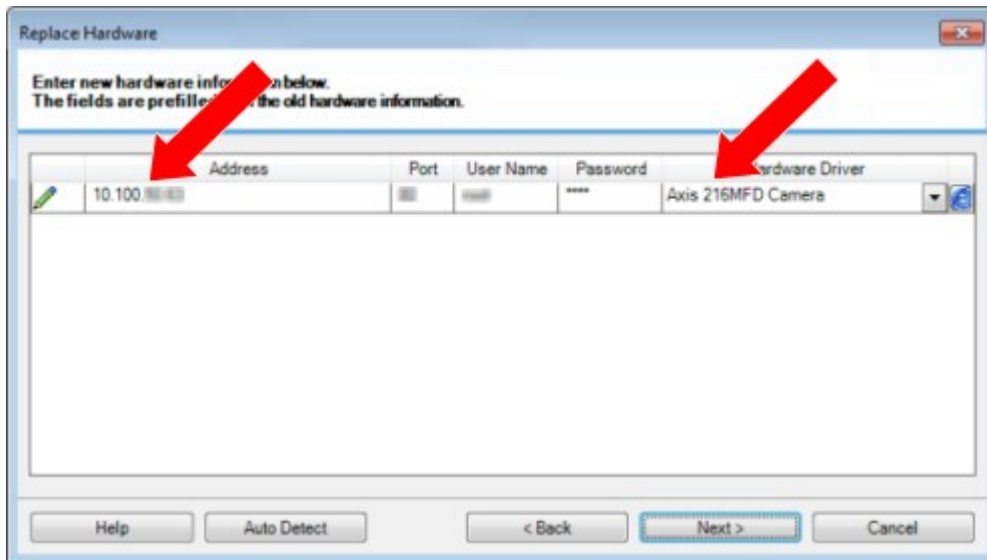


Si vous n'avez pas activé l'Informations sur la licence sur la page 140 et si vous avez utilisé tous les changements apportés aux périphériques sans activation (voir Informations sur la licence sur la page 140), vous devez activer manuellement vos licences **après** avoir remplacé les périphériques. Si le nombre de périphériques dépasse le nombre total de licences de périphérique, vous devrez acheter de nouvelles licences.

1. Agrandissez le serveur d'enregistrement requis et faites un clic droit sur le matériel que vous souhaitez remplacer.
2. Sélectionnez **Remplacer le matériel**.
3. L'assistant **Remplacer le matériel** apparaît. Cliquez sur **Suivant**.



4. Dans l'assistant, saisissez l'adresse IP du nouveau matériel dans le champ **Adresse** (marqué par une flèche rouge dans l'illustration). Si vous le connaissez, sélectionnez le pilote pertinent dans la liste déroulante **Pilote matériel**. Autrement, sélectionnez **Détection automatique**. Si le port, le nom d'utilisateur ou le mot de passe sont différents pour le nouveau matériel, corrigez ces informations **avant de lancer le processus de détection automatique, le cas échéant**.



L'assistant contient déjà les données relatives au matériel existant. Si vous le remplacez par un périphérique similaire, vous pouvez réutiliser certaines de ces informations, comme, par exemple, les informations concernant le port et le pilote.

5. Procédez comme suit :

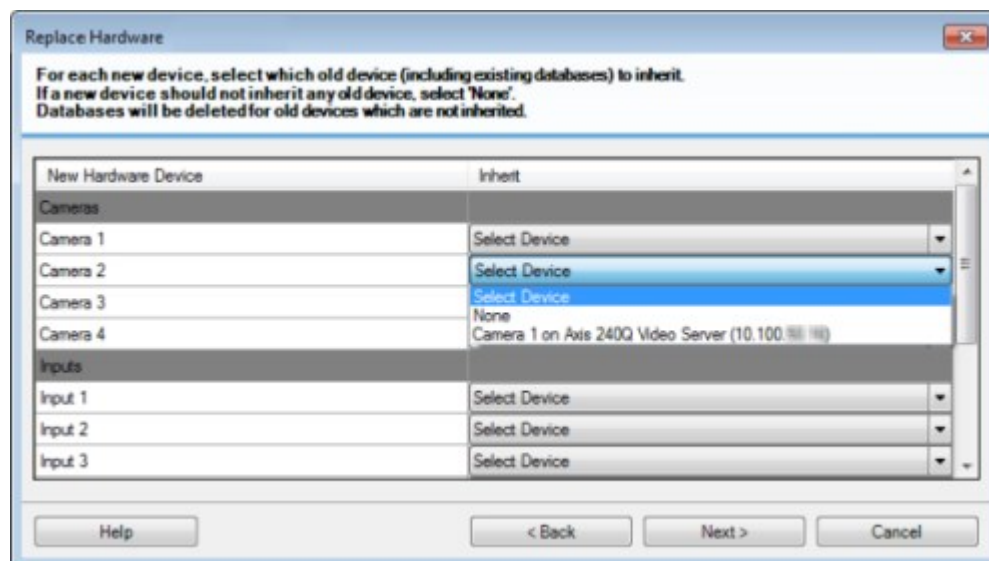
- Si vous avez sélectionné le pilote de périphérique requis directement dans la liste, cliquez sur **Suivant**
- Si vous avez sélectionné **Détection automatique** dans la liste, cliquez sur le bouton **Détection automatique**, attendez que ce processus se termine correctement (cela sera indiqué par un ✓ à gauche), cliquez sur **Suivant**

Cette étape est conçue pour vous aider à cartographier vos périphériques et leurs bases de données, en fonction du nombre de caméras, micros, entrées et sorties individuels, etc., connectés respectivement à l'ancien périphérique et au nouveau.

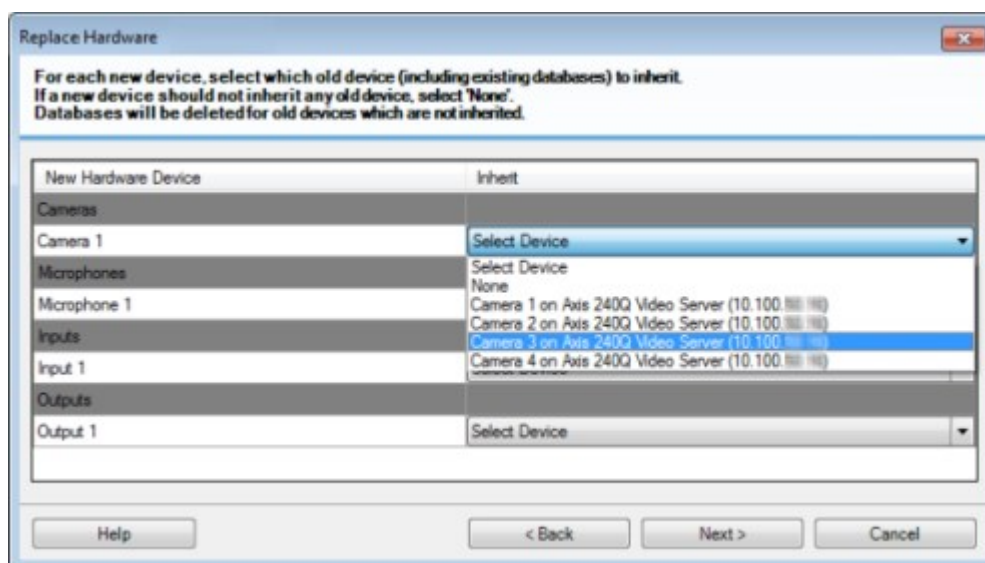
Il est important de réfléchir à la **façon** de cartographier les bases de données de l'ancien périphérique avec celles du nouveau périphérique. Vous pouvez cartographier des périphériques individuels, etc. en sélectionnant une caméra, un micro, une entrée, une sortie correspondante ou **Aucune** dans la colonne de droite.



Assurez-vous de cartographier **tous** les microphones, caméras, entrées, sorties, etc. Le contenu cartographié sur **Aucun** est **perdu**.



Exemple d'un ancien périphérique ayant plus de périphériques individuels que le nouveau :



Cliquez sur **Suivant**.

- Une liste s'affiche alors. Elle contient une liste de matériel à ajouter, remplacer ou supprimer. Cliquez sur **Confirmer**.
- L'étape finale est un résumé des périphériques ajoutés, remplacés et hérités et de leurs paramètres. Cliquez sur **Copier dans le presse-papier** pour copier le contenu vers le presse-papier Windows ou/et **Fermer** pour mettre fin à l'assistant.

## Gérer le SQL Server et les bases de données

### Modifier les adresses du SQL Server et de la base de données (explications)

Lorsque vous installez un système dans sa version d'essai, ou si vous restructurez une grande installation, vous devrez peut-être utiliser un SQL Server différent ou une base de données différente. Vous pouvez le faire avec l'outil **Mettre à jour l'adresse du SQL Server**.

Avec l'outil, vous pouvez modifier l'adresse du SQL Server et de la base de données utilisée par le serveur de gestion et par le serveur d'événements, ainsi que l'adresse du SQL Server et de la base de données utilisée par le serveur des journaux. La seule limite vient du fait que vous ne pouvez pas changer les adresses SQL du serveur de gestion et du serveur d'événements en même temps que les adresses SQL du serveur de journaux. Vous pouvez le faire l'une après l'autre.

Vous devez changer les adresses du SQL Server et de la base de données localement sur les ordinateurs où vous avez installé le serveur de gestion, le serveur d'événements et le serveur de journaux. Si votre serveur de gestion et votre serveur d'événement sont installés sur des ordinateurs séparés, vous devez exécuter l'outil **Mettre à jour l'adresse de SQL Server** sur les deux ordinateurs.



Vous devez copier les bases de données SQL avant de poursuivre.

## Modifier le SQL Server et la base de données du serveur des journaux

1. Allez sur l'ordinateur où votre serveur de gestion est installé et copiez le dossier *%ProgramFiles%\Milestone\XProtect Management Server\Tools\ChangeSqlAddress\* (et son contenu) vers un dossier temporaire sur le serveur d'événements.
2. Collez le dossier que vous avez copié sur un emplacement temporaire de l'ordinateur sur lequel le serveur de journaux est installé et exécutez le fichier inclus : *VideoOS.Server.ChangeSqlAddress.exe*. La boîte de dialogue **Mettre à jour l'adresse du SQL Server** s'affiche.
3. Sélectionnez **Log Server** et cliquez sur **Suivant**.
4. Entrez l'adresse du nouveau SQL Server et cliquez sur **Suivant**.
5. Sélectionnez la nouvelle base de données SQL et cliquez sur **Sélectionner**.
6. Patientez pendant que la modification de l'adresse a lieu. Cliquez sur **OK** pour confirmer.

## Modifier les adresses de la base de données SQL du serveur de gestion et du serveur d'événements

Le serveur de gestion et le serveur d'événements utilisent la même base de données SQL.

1. Si votre serveur de gestion et votre serveur d'événements sont situés :
  1. ensemble sur le même ordinateur et que vous souhaitez mettre à jour les adresses SQL, allez sur l'ordinateur où le serveur de gestion est installé.
  2. sur différents ordinateurs et que vous souhaitez mettre à jour l'adresse SQL du serveur de gestion (puis l'adresse SQL du serveur d'événements), allez sur l'ordinateur où le serveur de gestion est installé.
  3. sur différents ordinateurs et que vous souhaitez mettre à jour uniquement l'adresse SQL du serveur d'événements (ou que vous l'avez déjà mise à jour sur le serveur de gestion), allez sur l'ordinateur où votre serveur de gestion est installé et copiez le répertoire *%ProgramFiles%\Milestone\XProtect Management Server\Tools\ChangeSqlAddress\* (et son contenu) vers un répertoire temporaire sur le serveur d'événements.
2. Si vous sélectionnez :
  1. les étapes **1.1** et **1.2**, allez dans la zone de notification de la barre d'état. Cliquez avec le bouton droit sur l'icône **Serveur de gestion**, puis sélectionnez **Mettre à jour l'adresse SQL**. Vous devez répéter cette procédure pour mettre à jours l'adresse SQL du serveur d'événements.
  2. l'étape **1.3**, collez le répertoire que vous avez copié sur un emplacement temporaire de l'ordinateur sur lequel le serveur d'événements est installé et exécutez le fichier inclus : *VideoOS.Server.ChangeSqlAddress.exe*.

3. La boîte de dialogue **Mettre à jour l'adresse du SQL Server** s'affiche. Sélectionnez **Services Management Server** et cliquez sur **Suivant**.
4. Entrez l'adresse du nouveau SQL Server et cliquez sur **Suivant**.
5. Sélectionnez la nouvelle base de données SQL et cliquez sur **Sélectionner**.
6. Patientez pendant que la modification de l'adresse a lieu. Lorsqu'un message de confirmation s'affiche, cliquez sur **OK**.














## Services du serveur de gestion





Sur l'ordinateur qui exécute les services du serveur, vous trouvez les icônes de barre d'état du Gestionnaire de serveur dans la zone de notification. Avec ces icônes, vous pouvez accéder aux informations relatives aux services et effectuer certaines tâches. Par exemple, ceci peut inclure la vérification de l'état des services, la consultation des journaux ou encore des messages d'état, ainsi que le démarrage et l'arrêt des services.

### Icônes de la barre des tâches du serveur de gestion (explication)

Les icônes de la barre des tâches affichent les différents états des services exécutés sur le serveur de gestion, le serveur d'enregistrement, le serveur d'enregistrement de redondance et le serveur d'événements. Elles sont visibles sur les ordinateurs où sont installés les serveurs, dans la zone de notification :

Management Server Manager icône de la barre des tâches	Recording Server Manager icône de la barre des tâches	Event Server Manager icône de la barre des tâches	Failover Recording Server Manager icône de la barre des tâches	Description
				<p><b>En cours</b></p> <p>S'affiche lorsqu'un service du serveur est activé et a démarré.</p>

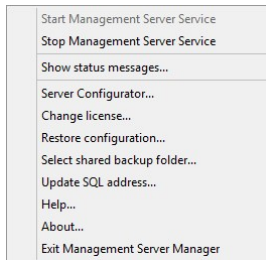
<b>Management Server Manager</b> icône de la barre des tâches	<b>Recording Server Manager</b> icône de la barre des tâches	<b>Event Server Manager</b> icône de la barre des tâches	<b>Failover Recording Server Manager</b> icône de la barre des tâches	<b>Description</b>
				<div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;">  <p>Si le service Failover Recording Server est en cours d'exécution, il peut prendre le relais si les serveurs d'enregistrement standards échouent.</p> </div>
				<p><b>Arrêté</b></p> <p>S'affiche quand le service du serveur s'arrête.</p> <div style="background-color: #e6f2ff; padding: 10px; border: 1px solid #0070c0;">  <p>Si le service Failover Recording Server s'arrête, il ne peut prendre le relais si les serveurs d'enregistrement standards échouent.</p> </div>
				<p><b>Démarrage</b></p> <p>S'affiche quand un service du serveur est en cours de démarrage. Dans des circonstances normales, l'icône de la barre des tâches passe peu après à <b>En cours</b>.</p>
				<p><b>Arrêt en cours</b></p> <p>S'affiche quand un service du serveur est en</p>

Management Server Manager icône de la barre des tâches	Recording Server Manager icône de la barre des tâches	Event Server Manager icône de la barre des tâches	Failover Recording Server Manager icône de la barre des tâches	Description
				cours d'arrêt. Dans des circonstances normales, l'icône de la barre des tâches passe peu après à <b>Arrêté</b> .
				<b>Dans un état indéterminé</b> S'affiche lorsque le service du serveur est initialement chargé et jusqu'à ce que les premières informations soient reçues, à la suite de quoi l'icône de la barre des tâches, dans des circonstances normales, changera au profit de l'icône <b>Démarrage</b> , puis de l'icône <b>En cours</b> .
				<b>Fonctionnement hors ligne</b> S'affiche généralement lorsque le service Serveur d'enregistrement ou Serveur d'enregistrement de redondance est en cours de fonctionnement, mais pas le service Management Server.

## Démarrer ou arrêter le service Management Server

L'icône de la barre d'état Management Server Manager indique l'état du service du Management Server, par exemple **Exécution en cours**. Par le biais de cette icône, vous pouvez démarrer ou arrêter le service Management Server. Si vous arrêtez le service Management Server, vous ne pourrez pas utiliser le Management Client.

1. Dans la zone de notification, cliquez avec le bouton droit sur l'icône de la barre d'état Management Server Manager. Un menu contextuel s'affiche.



2. Si le service s'est arrêté, cliquez sur **Démarrer le service Management Server** pour le lancer. L'icône de la barre des tâches reflète son nouvel état.
3. Pour arrêter le service, cliquez sur **Arrêter le service Management Server**.

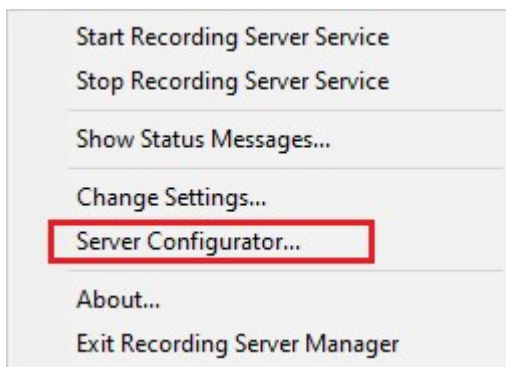


Pour obtenir de plus amples informations sur les icônes de la barre d'état, voir [Icônes de la barre des tâches du serveur de gestion \(explication\)](#) sur la page 509.

## Démarrer ou arrêter le service Recording Server

L'icône de la barre d'état Recording Server Manager indique l'état du service du Recording Server, par exemple **Exécution en cours**. Par le biais de cette icône, vous pouvez démarrer ou arrêter le service Recording Server. Si vous arrêtez le service Recording Server, votre système ne peut pas interagir avec les périphériques connectés au serveur. Cela signifie que vous ne pouvez pas visualiser la vidéo en direct ou enregistrer des vidéos.

1. Dans la zone de notification, cliquez avec le bouton droit sur l'icône de la barre d'état Recording Server Manager. Un menu contextuel s'affiche.



2. Si le service s'est arrêté, cliquez sur **Démarrer le service Recording Server** pour le lancer. L'icône de la barre des tâches reflète son nouvel état.
3. Pour arrêter le service, cliquez sur **Arrêter le service Recording Server**.

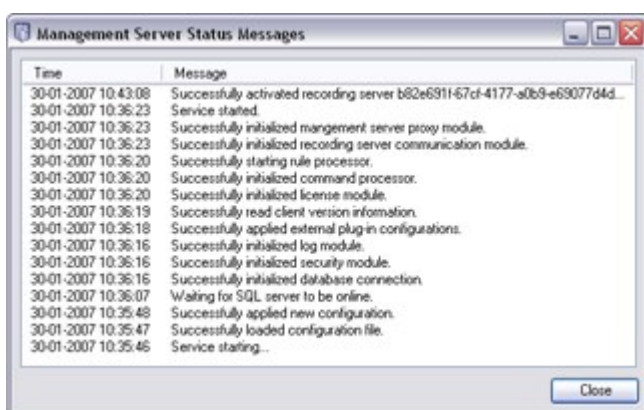




Pour obtenir de plus amples informations sur les icônes de la barre d'état, voir  **Icônes de la barre des tâches du serveur de gestion (explication)**  sur la page 509.

## Consulter les messages d'état relatifs au serveur de gestion ou au serveur d'enregistrement

1. Dans la zone de notification, cliquer avec le bouton droit sur l'icône pertinente de la barre des tâches. Un menu contextuel s'affiche.
2. Sélectionnez **Afficher les messages d'état**. En fonction du type de serveur, s'affiche soit la fenêtre **Messages d'état du serveur de gestion** soit la fenêtre **Messages d'état du serveur d'enregistrement**, établissant la liste des messages d'état horodatés :



## Gérer le cryptage avec le Server Configurator

Utilisez le Server Configurator pour sélectionner des certificats sur les serveurs locaux pour la communication cryptée et enregistrez les services du serveur afin qu'ils puissent communiquer avec les serveurs.

Ouvrez le Server Configurator depuis le menu Démarrer de Windows ou depuis l'icône de la barre des tâches du serveur de gestion.

Avant d'activer le cryptage, vous devez installer des certificats de sécurité sur l'ordinateur où se trouve le serveur de gestion et sur tous les ordinateurs où figurent les serveurs d'enregistrement. Pour plus d'informations, voir le [guide des certificats sur comment sécuriser votre installation de VMS XProtect](#).

Dans la rubrique **Cryptage** du Server Configurator, configurez le cryptage des types de certificats suivants :

- **Certificat du serveur**

Sélectionnez le certificat à utiliser pour crypter une connexion bidirectionnelle entre le serveur de gestion, les collecteurs de données et les serveurs d'enregistrement.



Le cryptage de Mobile Server s'active depuis la barre de tâche de Mobile Server.

- **Certificat de flux de multimédia**

Sélectionnez le certificat à utiliser pour crypter la communication entre les serveurs d'enregistrement et tous les clients, serveurs et intégrations récoltant des flux de données depuis les serveurs d'enregistrement.

- **Certificat de flux de multimédia mobile**

Sélectionnez le certificat à utiliser pour crypter la communication entre le serveur mobile et les clients mobiles et Web récupérant les flux de données depuis le serveur mobile.

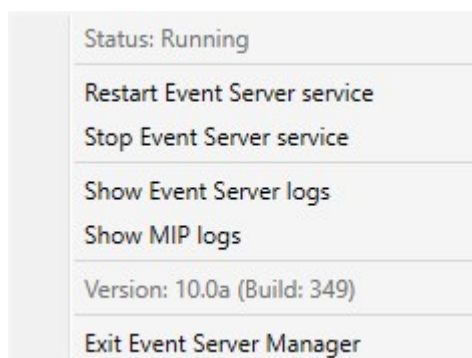
Dans la rubrique **Enregistrement des serveurs** de Server Configurator, enregistrez les serveurs qui s'exécutent sur l'ordinateur avec le serveur de gestion sélectionné.

Pour enregistrer les serveurs, vérifiez l'adresse du serveur de gestion, puis sélectionnez **Enregistrer**.

## Démarrer, arrêter ou redémarrer le service Event Server

L'icône de la barre d'état Event Server Manager indique l'état du service du Event Server, par exemple **Exécution en cours**. Par le biais de cette icône, vous pouvez démarrer, arrêter ou redémarrer le service Event Server. Si vous arrêtez le service, certaines parties du système ne fonctionneront pas, et notamment les événements et les alarmes. Cependant, vous pourrez continuer à afficher et enregistrer des vidéos. Pour de plus informations, voir Arrêt du service Event Server sur la page 515.

1. Dans la zone de notification, cliquez avec le bouton droit sur l'icône de la barre d'état Event Server Manager. Un menu contextuel s'affiche.



2. Si le service s'est arrêté, cliquez sur **Démarrer le service Event Server** pour le lancer. L'icône de la barre des tâches reflète son nouvel état.
3. Pour redémarrer ou arrêter le service, cliquez sur **Redémarrer le service Event Server** ou **Arrêter le service Event Server**.



Pour obtenir de plus amples informations sur les icônes de la barre d'état, voir Icônes de la barre des tâches du serveur de gestion (explication) sur la page 509.

## Arrêt du service Event Server

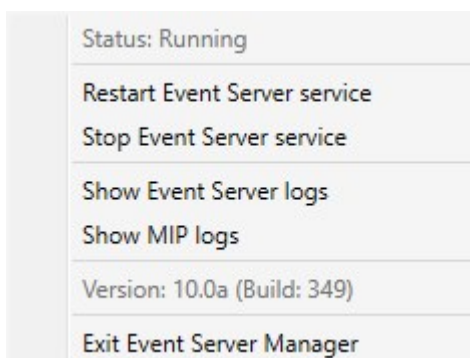
Lors de l'installation de modules d'extension MIP sur le serveur d'événements, vous devez d'abord arrêter le service Event Server puis le redémarrer une fois la procédure terminée. Cependant, lorsque le service sera à l'arrêt, de nombreuses parties du système VMS ne fonctionneront pas :

- Aucun événement ou alarme ne sera stocké dans le serveur d'événements. Cependant, les événements système et les événements de périphériques déclencheront encore des actions, telles que le démarrage de l'enregistrement
- Les modules complémentaires ne fonctionnent pas dans XProtect Smart Client et ne peuvent être configurés depuis le Management Client.
- Les événements analytiques ne fonctionnent pas
- Les événements génériques ne fonctionnent pas
- Aucune alarme n'est déclenchée
- Dans XProtect Smart Client, les éléments de vue du plan, les éléments de vue de la liste d'alarmes et l'espace de travail du gestionnaire d'alarmes ne fonctionnent pas
- Les modules d'extension MIP dans le serveur d'événements ne peuvent pas fonctionner
- Les modules d'extension MIP dans Management Client et XProtect Smart Client ne fonctionnent pas correctement

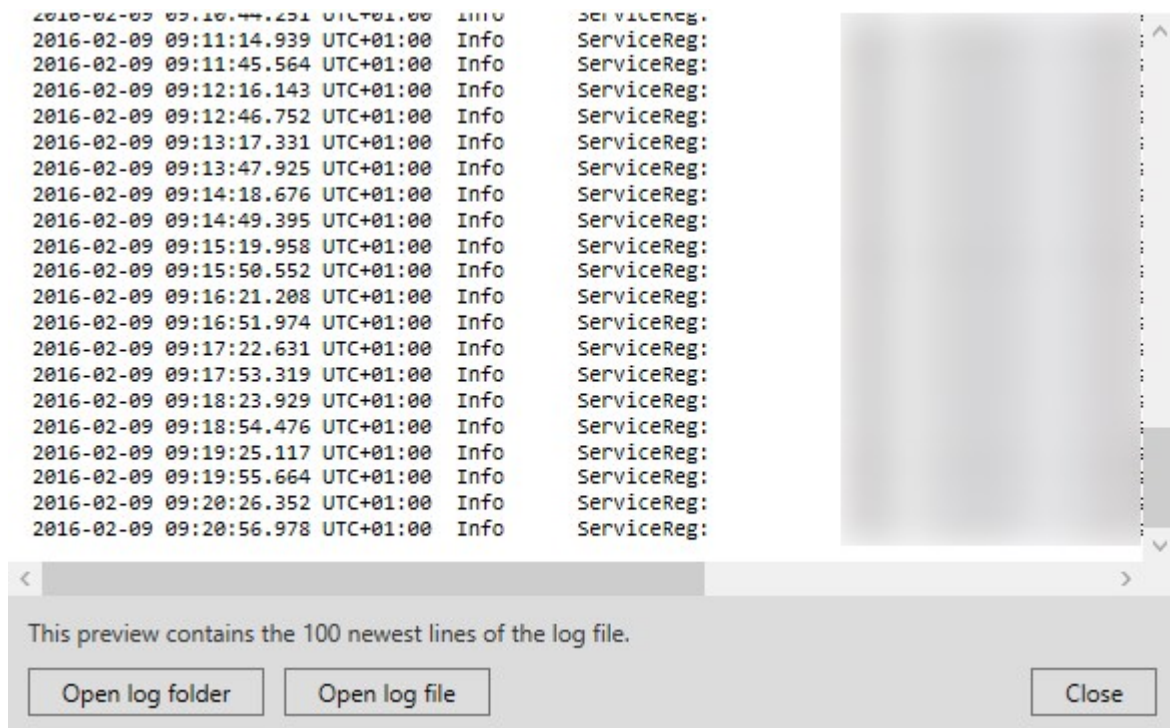
## Consulter le Event Server ou les journaux MIP

Vous pouvez consulter des informations horodatées au sujet des activités du serveur d'événements dans le journal du serveur d'événements. Des informations au sujet des intégrations tierces sont consignées dans le journal MIP, dans un sous-répertoire du répertoire **Serveur d'événements**.

1. Dans la zone de notification, cliquez avec le bouton droit sur l'icône de la barre d'état Event Server Manager. Un menu contextuel s'affiche.



2. Pour afficher les 100 lignes les plus récentes du journal du serveur d'événements, cliquez sur **Afficher les journaux du serveur d'événements**. Un programme d'affichage des journaux s'affiche.



1. Pour consulter le journal, cliquez sur **Ouvrir le journal**.
2. Pour ouvrir le répertoire du journal, cliquez sur **Ouvrir le répertoire du journal**.
3. Pour consulter les 100 lignes les plus récentes du journal MIP, revenez au menu contextuel et cliquez sur **Afficher les journaux MIP**. Un programme d'affichage des journaux s'affiche.



Si quelqu'un supprime les journaux du répertoire des journaux, les éléments du menu sont grisés. Pour ouvrir le programme d'affichage des journaux, vous devez d'abord copier les journaux dans l'un de ces répertoires : `C:\ProgramData\Milestone\XProtect Event Server\logs` ou `C:\ProgramData\Milestone\XProtect Event Server\logs\MIPLogs`.

## Gérer les services enregistrés

Occasionnellement, il y a des serveurs et/ou des services qui devraient pouvoir communiquer avec le système même s'ils ne font pas directement partie du système. Certains services (et non pas tous) peuvent s'enregistrer automatiquement dans le système. Les services pouvant être automatiquement enregistrés sont :

- Service Event Server
- Service Log Server

Les services automatiquement enregistrés apparaissent dans la liste des services enregistrés.

Il est possible de préciser manuellement les serveurs/services dans le Management Client comme services enregistrés.

## Ajouter et modifier des services enregistrés

1. Dans la fenêtre **Ajouter/Supprimer des services enregistrés**, cliquez sur le bouton **Ajouter** ou **Modifier**, en fonction de vos besoins.
2. Dans la fenêtre **Ajouter un service enregistré** ou **Modifier un service enregistré** (en fonction de votre sélection précédente), spécifiez ou modifiez les paramètres.
3. Cliquez sur **OK**.

## Gérer la configuration du réseau

Avec les paramètres de configuration réseau, vous pouvez indiquer les adresses serveur WAN et LAN du serveur de gestion afin que le serveur de gestion et les serveurs fiables puissent communiquer.

1. Dans la fenêtre **Ajouter/supprimer des services enregistrés**, cliquez sur **Réseau**.
2. Spécifiez l'adresse IP LAN et/ou WAN du serveur de gestion.

Si tous les serveurs concernés (le serveur de gestion et les serveurs approuvés) sont sur votre réseau local, vous pouvez simplement spécifier l'adresse LAN. Si un ou plusieurs serveurs concernés accèdent au système par le biais d'une connexion Internet, vous devez également spécifier l'adresse WAN.



3. Cliquez sur **OK**.

## Propriétés des services enregistrés

Dans la fenêtre **Ajouter un service enregistré** ou **Modifier un service enregistré**, spécifiez les éléments suivants :

Composant	Exigences
Type	Champ pré-rempli.
Nom	Nom du service enregistré. Le nom est utilisé à des fins d'affichage dans le Management

Composant	Exigences
	Client.
URL	<p>Cliquez sur <b>Ajouter</b> pour ajouter l'adresse IP ou le nom d'hôte du service enregistré. Si vous spécifiez un nom d'hôte comme partie intégrante d'une URL, l'hôte en question doit exister et être accessible sur le réseau. Les URL doivent commencer par <i>http://</i> ou <i>https://</i> et ne doivent contenir aucun des caractères suivants : &lt; &gt; &amp; ' " * ?   [ ]".</p> <p><b>Exemple</b> d'un format typique d'URL : <i>http://ipaddress:port/directory</i> (où le port et le répertoire sont facultatifs). Vous pouvez ajouter plusieurs URL le cas échéant.</p>
De confiance	<p>Sélectionnez si le service enregistré doit être reconnu immédiatement (c'est souvent le cas, mais l'option vous donne la possibilité d'ajouter le service enregistré puis de le marquer comme fiable en modifiant le service enregistré ultérieurement).</p> <p>Modifier l'état de confiance modifie également l'état des autres services enregistrés partageant une ou plusieurs URL définies pour le service enregistré pertinent.</p>
Description	Description du service enregistré. La description est utilisée à des fins d'affichage dans le Management Client.
Avancés	<p>Lorsqu'un service est avancé, il dispose de son propre modèle d'URI (par exemple, HTTP, HTTPS, TCP, ou UDP) qui doit être configuré pour chaque adresse d'hôte que vous définissez. Une adresse d'hôte a donc de multiples extrémités, ayant chacune leur propre modèle, adresse d'hôte et port IP pour ce modèle.</p>

## Supprimer des pilotes de périphériques (explications)

Si vous souhaitez supprimer des pilotes de périphériques de votre ordinateur, vous pouvez supprimer les packs de périphérique de votre système. Pour ce faire, suivez la procédure Windows standard pour la suppression de programmes.

Si vous possédez plusieurs packs de pilotes de périphériques installés et rencontrez des problèmes pour supprimer les fichiers, vous pouvez utiliser le script du dossier d'installation du pack de pilotes de périphériques pour les supprimer totalement.

Si vous supprimez des pilotes de périphériques, le serveur d'enregistrement et les périphériques de type caméra ne pourront plus communiquer entre eux. Ne supprimez pas les packs de périphériques lorsque vous procédez à une mise à niveau parce que vous installez une nouvelle version en la superposant à une ancienne. Le pack de périphériques ne doit être supprimé qu'en cas de désinstallation du système complet.

## Supprimer un serveur d'enregistrement



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

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

## Supprimer tous les périphériques matériels sur un serveur d'enregistrement



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

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

## Dépannage

### Problème : Le changement des adresses de SQL Server et de la base de données empêche l'accès à la base de données

Si les adresses de SQL Server et de la base de données sont modifiées, en changeant le nom d'hôte de l'ordinateur exécutant le SQL Server, par exemple, l'accès du serveur d'enregistrement à la base de données est perdue.

**Solution : Utilisez l'outil d'adresse SQL trouvé en cliquant sur l'icône de la barre d'état du Recording Server Manager.**

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

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

#### Service SMTP : Vérification et solutions

Pour vérifier si le Service SMTP est installé :

1. Depuis le menu **Démarrage** de Windows, sélectionnez **Panneau de configuration**.
2. Dans le **Panneau de configuration**, effectuez un double-clic sur **Ajouter ou supprimer des programmes**.
3. À gauche de la fenêtre **Ajouter ou supprimer des programmes**, cliquez sur **Ajouter/Supprimer des fonctionnalités Windows**.
4. Dans l'assistant **Composants Windows**, sélectionnez **Internet Information Services (IIS)**, et cliquez sur le bouton **Détails**.
5. Dans la fenêtre **Internet Information Services (IIS)**, vérifiez si la case **Service SMTP** est cochée ou non. Si oui, le Service SMTP est installé.

Si le Service SMTP est installé, choisissez une des solutions suivantes :

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

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

1. Depuis le menu **Démarrage** de Windows, sélectionnez **Panneau de configuration**.
2. Dans le **Panneau de configuration**, effectuez un double-clic sur **Outils d'administration**.
3. Dans la fenêtre **Outils administratifs**, double-cliquez sur **Services**.



4. Dans la fenêtre **Services**, double-cliquez sur **Simple Mail Transfer Protocol (SMTP)**.
5. Dans la fenêtre **Propriétés SMTP**, cliquez sur **Arrêt**, puis réglez **Type de démarrage** sur **Manuel** ou **Désactivé**.

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

6. Cliquez sur **OK**.

### Solution 2 : Supprimez le Service SMTP

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

1. Depuis le menu **Démarrage** de Windows, sélectionnez **Panneau de configuration**.
2. Dans la fenêtre du **Panneau de configuration**, effectuez un double-clic sur **Ajouter ou supprimer des programmes**.
3. À gauche de la fenêtre **Ajouter ou supprimer des programmes**, cliquez sur **Ajouter/Supprimer des fonctionnalités Windows**.
4. Dans l'assistant **Composants Windows**, sélectionnez l'élément **Internet Information Services (IIS)**, et cliquez sur le bouton **Détails**.
5. Dans la fenêtre **Internet Information Services (IIS)**, décochez la case **Service SMTP**.
6. Cliquez sur **OK**, **Suivant** et **Terminer**.

## Problème : Recording Server est mis hors tension lors du basculement du nœud en grappe de Management Server

Si vous configurez une grappe Microsoft pour la redondance de Management Server, le Recording Server ou Recording Server seront mis hors tension lors du basculement de Management Server entre les nœuds en grappe.

Pour le corriger, modifiez les paramètres de configuration suivants :

Dans les nœuds Management Server :

- Dans `C:\ProgramData\Milestone\XProtectManagement Server\ServerConfig.xml` :

```
<AuthorizationServerUri>http://ClusterRoleAddress/IDP</AuthorizationServerUri>
```

- Dans `C:\Program Files\Milestone\XProtectManagement Server\IIS\IDP\appsettings.json` :

```
« Authority » : « http://ClusterRoleAddress/IDP »
```

Dans les Recording Server, vérifiez que l'adresse du serveur d'autorisation est également configurée sur l'adresse du rôle en grappe :

Dans `C:\ProgramData\Milestone\XProtectRecording Server\RecorderConfig.xml` :

```
<authorizationserveraddress>http://ClusterRoleAddress/IDP</authorizationserveraddress>
```

## Mise à niveau

### Mise à niveau (explications)

Lorsque vous procédez à la mise à niveau, tous les composants actuellement installés dans l'ordinateur sont mis à jour. Il n'est pas possible de supprimer des composants installés lors d'une mise à niveau. Si vous souhaitez supprimer des composants installés, utilisez la fonctionnalité **Ajouter ou supprimer des programmes** de Windows avant ou après une mise à niveau. Lors d'une mise à niveau, tous les composants à l'exception de la base de données du serveur de gestion sont automatiquement supprimés et remplacés. Cela inclut vos pilotes de périphériques.

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



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

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



Si vous effectuez une mise à niveau à partir de la version 2017 R3 ou antérieure vers la version 2018 R1 ou ultérieure, et si votre système est équipé de caméras plus anciennes, vous devez télécharger manuellement les pilotes de périphériques avec les anciens pilotes disponibles sur la page de téléchargement de notre site web (<https://www.milestonesys.com/downloads/>). Pour voir si vous avez des caméras qui utilisent des pilotes dans le pack de pilotes de périphériques ancienne génération, visitez cette page sur notre site web (<https://www.milestonesys.com/community/business-partner-tools/device-packs/>).



Si vous passez de la version 2018 R1 ou antérieure à la version 2018 R2 ou ultérieure, il est important auparavant de mettre à niveau tous les serveurs d'enregistrement de votre système à l'aide d'un patch de sécurité. Si vous changez de version sans le correctif de sécurité, les serveurs d'enregistrement ne répondront pas.



Vous trouverez les instructions d'installation du correctif de sécurité sur vos serveurs d'enregistrement, sur notre site internet <https://supportcommunity.milestonesys.com/s/article/XProtect-VMS-NET-security-vulnerability-hotfixes-for-2016-R1-2018-R1/>.



Lorsque tous les serveurs d'enregistrement dans votre système sont mis à niveau vers la version 2019 R2 ou une version plus récente, Milestone recommande de configurer UseRemoting to False dans le fichier de configuration du serveur de gestion. Pour plus d'informations sur comment sécuriser vos installations de VMS XProtect contre les cyberattaques, voir le [guide de durcissement](#).



Si vous souhaitez crypter la connexion entre le serveur de gestion et les serveur d'enregistrement, tous les serveurs d'enregistrement doivent être mis à jour vers 2019 R2 ou une version plus récente.

## Conditions préalables de mise à niveau

- Ayez votre fichier de licence logicielle (voir Licences (explications) sur la page 50) (.lic) prêt :
  - **Mise à jour du Service Pack** : Au cours de l'installation du serveur de gestion, l'assistant vous demandera peut-être de préciser l'emplacement du fichier de licence logicielle. Vous pouvez utiliser le fichier de licence logicielle que vous avez reçu après l'achat de votre système (ou après la dernière mise à jour) ou celui que vous avez reçu suite à la dernière activation de votre licence
  - **Mise à jour de la version** : Après avoir acheté la nouvelle version, vous recevrez un nouveau fichier de licence logicielle. Au cours de l'installation du serveur de gestion, l'assistant vous demandera de préciser l'emplacement du fichier de licence logicielle

Le système vérifie votre fichier de licence logicielle avant que vous puissiez poursuivre. Les périphériques matériels et autres périphériques déjà ajoutés nécessitant une licence passent en période d'évaluation. Si vous n'avez pas activé l'activation automatique des licences (voir Activer l'activation automatique des licences sur la page 145), n'oubliez pas d'activer vos licences manuellement avant l'expiration de la période d'évaluation. Si vous n'avez pas de fichier de licence logicielle, veuillez contacter votre revendeur XProtect.

- Assurez-vous d'avoir le logiciel de la **nouvelle version de votre produit** à disposition. Vous pouvez la télécharger depuis la page de téléchargement sur le site web Milestone.
- N'oubliez pas de sauvegarder la configuration du système (voir Sauvegarde et de la restauration de la configuration de votre système (explications) sur la page 488)

Le serveur de gestion sauvegarde la configuration du système dans une base de données SQL. La base de données SQL peut se situer dans un SQL Server sur le serveur de gestion sur la machine ou sur un SQL Server sur le réseau.

Si vous utiliser une base de données SQL dans SQL Server situé sur votre réseau, le serveur de gestion doit disposer de droits d'administrateur sur le SQL Server lorsque vous souhaitez créer, déplacer ou actualiser la base de données SQL. Pour une utilisation et en entretien réguliers de la base de données SQL, le serveur de gestion nécessite uniquement d'être le propriétaire de la base de données SQL.

- Si vous voulez activer le cryptage lors de l'installation, les certificats nécessaires doivent être installés et fiables sur les ordinateurs concernés. Pour plus d'informations, voir Communication sécurisée (explications) sur la page 70

Lorsque vous êtes prêt à commencer la mise à niveau, suivez les procédures indiquées dans Mise à jour des meilleures pratiques sur la page 526.

## Mettre à jour VMS XProtect pour un fonctionnement conforme au mode FIPS 140-2

Depuis la version 2020 R3, VMS XProtect est configuré pour s'exécuter en n'utilisant uniquement des instances d'algorithmes certifiées conformes aux normes FIPS 140-2.

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



Pour les systèmes conformes aux normes FIPS 140-2 comportant des exportations et des bases de données multimédias archivées à partir des versions de VMS XProtect antérieures à 2017 R3 qui sont cryptées avec un cryptage non-conforme aux normes FIPS, il est nécessaire d'archiver les données dans un emplacement auquel il est possible d'accéder après l'activation du mode FIPS.

Les étapes ci-dessous décrivent les prérequis nécessaires pour configurer le fonctionnement de VMS XProtect conforme au mode FIPS 140-2 :

1. Désactivez la politique de configuration du mode Windows FIPS sur tous les composants faisant partie du VMS, y compris l'ordinateur qui héberge le serveur SQL.

Lorsque vous effectuez la mise à jour, vous ne pouvez pas installer VMS XProtect si le mode FIPS est activé sur le système d'exploitation Windows.

2. Assurez-vous que les intégrations autonomes tierces peuvent s'exécuter dans un système d'exploitation Windows où est activé le mode FIPS.

Une intégration autonome qui ne s'exécute pas conformément aux normes FIPS 140-2, ne pourra pas s'exécuter une fois le système d'opération Windows configuré pour fonctionner en mode FIPS.

Pour y pallier :

- Répertoriez tous vos intégrations autonomes de VMS XProtect
  - Contactez le fournisseurs desdites intégrations et demandez-lui si elle sont conformes au mode FIPS 140-2
  - Déployez les intégrations autonomes conformes aux normes FIPS 140-2
3. Assurez-vous que les pilotes et donc leur communication avec les périphériques, sont conformes aux normes FIPS 140-2.

VMS XProtect est garanti et peut assurer le respect du mode FIPS 140-2 de l'opération si les critères suivants sont respectés :

- Les périphériques utilisent uniquement des pilotes testés pour se connecter à VMS XProtect

Voir la section de conformité aux normes FIPS 140-2 dans le [guide de durcissement](#) pour plus d'information sur les pilotes qui peuvent assurer et appliquer la conformité.



Les modules du pilote ne peuvent pas garantir le respect des normes FIPS 140-2 d'une connexion HTTP. La connexion peut être conforme, mais rien ne garantit sa conformité.

- Les périphériques utilisent des packs de pilotes de périphériques version 11.1 ou ultérieures  
Les pilotes des packs d'ancienne génération ne peuvent pas garantir une connexion conforme aux normes FIPS 140-2.
  - Les périphériques se connectent via HTTPS et sur le protocole Secure Real-Time Transport Protocol (SRTP) ou le protocole Real Time Streaming Protocol (RTSP) via HTTPS pour le flux vidéo
  - L'ordinateur exécutant le serveur d'enregistrement exécute Windows OS avec le mode FIPS activé
4. Assurez-vous que les données des bases de données multimédia sont cryptées avec un cryptage conforme aux normes FIPS 140-2.

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

5. Avant d'activer le mode FIPS sur le système d'exploitation Windows et après avoir configuré votre système VMS XProtect et vous être assuré que tous les composants et les périphériques peuvent s'exécuter dans un environnement conforme aux normes FIPS, mettez à jour vos mots de passe logiciels existants sur le XProtect Management Client.

Pour ce faire, dans le Management Client, effectuez un clic droit sur le serveur d'enregistrement sélectionné dans le nœud **Serveurs d'enregistrement**, puis sélectionnez **Ajouter un matériel...** Suivez les indications de l'assistant **Ajouter un matériel**. Cela mettra à jour tous les identifiants actuels et les cryptera conformément aux normes FIPS.

Vous pouvez activer le mode FIPS uniquement après avoir mis à jour l'intégralité du VMS, y compris tous les clients.

## Mise à jour des meilleures pratiques

Consultez les conditions préalables de mise à niveau (voir Conditions préalables de mise à niveau sur la page 523), y compris la sauvegarde de la base de données SQL, avant de démarrer la mise à niveau.



Les pilotes de périphériques sont désormais répartis en deux device packs : le device pack classique équipé des pilotes plus récents et un périphérique d'ancienne génération doté de pilotes plus anciens. Les pilotes de périphériques classiques s'installent toujours automatiquement lors d'une mise à jour ou d'une mise à niveau. Si vous disposez de caméras plus anciennes qui sont équipées de pilotes de périphériques du pack de périphérique d'ancienne génération, et si ce dernier n'est pas encore installé, le système n'installera pas automatiquement le pack de périphérique d'ancienne génération.



Si votre système est équipé de caméras plus anciennes, Milestone vous recommande de vérifier sur cette page si ces dernières utilisent des pilotes de périphériques ancienne génération (<https://www.milestonesys.com/community/business-partner-tools/device-packs/>). Pour vérifier si le pack hérité est déjà installé sur votre système, cherchez dans les dossiers système de XProtect. Si vous devez télécharger les pilotes de périphériques ancienne génération, accédez à la page de téléchargement (<https://www.milestonesys.com/downloads/>).

Si votre système est un système **Ordinateur unique**, vous pouvez installer le nouveau programme sur l'installation existante.

Dans un système Milestone Interconnect ou Milestone Federated Architecture, vous devez commencer en mettant à jour le site central, puis les sites à distance.

Dans un système distribué, exécutez la mise à jour dans cette ordre :

1. Mettre à niveau le serveur de gestion avec l'option **Personnalisée** dans l'assistant d'installation (voir Installer votre système - option personnalisée sur la page 89).
  1. Sur la page de l'assistant où vous choisissez les composants, tous les composants des serveurs de gestion sont présélectionnés.
  2. Spécifiez le SQL Server et la base de données. Choisissez si vous souhaitez conserver la base de données SQL que vous utilisez et conserver les données existantes dans la base de données.



Lorsque vous démarrez l'installation, vous perdez la fonction de serveur de basculement (voir Serveurs d'enregistrement de redondance (explications) sur la page 185).



Si vous activez le cryptage sur le serveur de gestion, les serveurs d'enregistrement sont hors ligne jusqu'à leur mise à niveau et vous avez activé le cryptage sur le serveur de gestion (voir Avant de commencer l'installation sur la page 59).

2. Mettez à jour serveurs d'enregistrement de redondance. Depuis votre page Web de téléchargement du serveur de gestion (contrôlé par Download Manager), installez Recording Server.



Si vous voulez activer le cryptage sur des serveurs d'enregistrement de redondance, et que vous désirez conserver la fonctionnalité de redondance, mettez à jour le serveur d'enregistrement de redondance sans cryptage et activez-le après avoir mis à jour les serveurs d'enregistrement.

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

3. Si vous voulez activer le cryptage depuis les serveurs d'enregistrement ou les serveurs d'enregistrement de redondance vers les clients, et qu'il est important que les clients puissent continuer à récolter des données lors de la mise à jour, mettez à jour tous les clients et services qui recueillent des flux de streaming depuis les serveurs d'enregistrement avant de mettre à jour les serveurs d'enregistrement. Ces clients et services sont :
  - XProtect Smart Client
  - Management Client
  - Management Server
  - Serveur XProtect Mobile
  - XProtect Event Server
  - DLNA Server Manager

- Milestone Open Network Bridge
  - Les sites collectant des flux de donnée depuis le serveur d'enregistrement par le biais de Milestone Interconnect
  - Quelques intégrations tierces de MIP SDK
4. Mettre à niveau les serveurs d'enregistrement. Vous pouvez installer les serveurs d'enregistrement à l'aide de l'assistant d'installation (voir XProtect Installer les nouveaux composants sur la page 94) ou silencieusement (voir XProtect Installer les nouveaux composants sur la page 94). L'avantage d'une installation silencieuse est qu'elle peut être effectuée à distance.



Si vous activez le cryptage et que le certificat de l'authentification du serveur sélectionné n'est pas fiable sur tous les ordinateurs l'exécutant, ils seront déconnectés. Pour plus d'informations, voir Avant de commencer l'installation sur la page 59.

Continuez ces étapes pour les autres sites de votre système.

## Mise à niveau dans une configuration de groupe de travail

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

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

Pour les installations avec groupes de travail, reportez-vous à la section Installation pour les groupes de travail sur la page 104.

## Mise à jour dans une grappe

Assurez-vous d'avoir une copie de sauvegarde de la base de données avant de mettre la grappe à niveau.



1. Arrêtez les services Management Server sur tous les serveurs de gestion de la grappe.
2. Désinstallez le serveur de gestion sur tous les serveurs de la grappe.
3. Utilisez la procédure d'installation de serveurs de gestion multiples dans une grappe, comme décrite dans la section Installation dans une grappe. Se reporter à la section Installer un nouveau système XProtect sur la page 79.



Lors de l'installation, assurez-vous de réutiliser le SQL Server existant et la base de données SQL existante qui stockent actuellement la configuration du système. La configuration du système est automatiquement mise à jour.



[helpfeedback@milestone.dk](mailto: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/>.

