



Guide d'utilisation de l'appareil Streamvault™

Cliquez [ici](#) pour obtenir la dernière version de ce document.

Dernière mise à jour du document : 5 juin 2025

Mentions légales

©2025 Genetec Inc. Tous droits réservés.

Genetec Inc. distribue ce document avec un logiciel qui comprend un contrat de licence, qui est fourni sous licence et qui ne peut être utilisé qu'en conformité avec les conditions énumérées dans le contrat de licence. Le contenu de ce document est protégé par la loi sur la propriété intellectuelle.

Le contenu de ce manuel n'est fourni qu'à titre indicatif et peut être modifié sans avis préalable. Genetec Inc. décline toute responsabilité en relation avec d'éventuelles erreurs ou imprécisions pouvant figurer dans le contenu de ce manuel.

Il est interdit de copier, modifier ou reproduire cette publication sous toute forme et à toute fin que ce soit, ou de créer toute œuvre dérivée de celle-ci, sans autorisation écrite préalable de Genetec Inc.

Genetec Inc. se réserve le droit de modifier et d'améliorer ses produits comme bon lui semble. Ce document décrit l'état d'un produit au moment de la dernière révision du document et peut ne pas refléter le produit à tout moment à l'avenir.

Genetec Inc ne pourra en aucun cas être tenu pour responsable envers tout individu ou entité de toute perte ou de tout dommage fortuit ou consécutif résultant de l'utilisation des instructions fournies dans ce document ou dans les produits logiciels ou matériels décrits dans celui-ci.

Genetec^{MC}, AutoVu^{MC}, AutoVu MLC^{MC}, Citywise^{MC}, Cloud Link Roadrunner^{MC}, Community Connect^{MC}, Curb Sense^{MC}, Federation^{MC}, Flexreader^{MC}, Genetec Airport Sense^{MC}, Genetec Citigraf^{MC}, Genetec Clearance^{MC}, Genetec ClearID^{MC}, Genetec Cloudlink^{MC}, Genetec Mission Control^{MC}, Genetec Motoscan^{MC}, Genetec Patroller^{MC}, Genetec Retail Sense^{MC}, Genetec Traffic Sense^{MC}, KiwiVision^{MC}, KiwiSecurity^{MC}, Omnicast^{MC}, Privacy Protector^{MC}, Sipelia^{MC}, Stratocast^{MC}, Streamvault^{MC}, Streamvault Edge^{MC}, Synergis^{MC}, Valcri^{MC}, leurs logos respectifs ainsi que le logo Mobius Strip sont des marques commerciales de Genetec Inc. qui peuvent être déposées ou en instance de dépôt dans différents pays.

Les autres marques commerciales citées dans ce document appartiennent à leurs fabricants ou éditeurs respectifs.

Brevet en instance. Genetec^{MC} Security Center, Omnicast^{MC}, AutoVu^{MC}, Stratocast^{MC}, Genetec Citigraf^{MC}, Genetec Clearance^{MC} et les autres produits Genetec^{MC} font l'objet de dépôts de brevets en attente et peuvent faire l'objet de brevets déposés, aux États-Unis et dans d'autres juridictions dans le monde.

Toutes les spécifications sont sujettes à modification sans avis préalable.

Informations sur le documents

Titre du document : Guide d'utilisation de l'appareil Streamvault^{MC}

Numéro du document d'origine : EN.803.003

Numéro de document : FR.803.003

Date de mise à jour du document : 5 juin 2025

Vous pouvez envoyer vos commentaires, corrections et suggestions concernant ce guide à l'adresse documentation@genetec.com.

À propos de ce guide

Ce guide décrit la manière d'installer et de configurer votre appareil Streamvault pour le contrôle d'accès et la vidéosurveillance dans Security Center à l'aide de la dernière version du Tableau de bord SV. Ce guide complète le Guide de l'administrateur Security Center et le Guide de configuration des appareils Synergis^{MC}.

Ce guide s'adresse à l'intégrateur qui effectue la configuration initiale de l'appareil SV. Il part du principe que vous comprenez la terminologie et les notions utilisées dans Security Center.

Notes et avertissements

Les avis et avertissements suivants peuvent être utilisés dans ce guide :

- **Conseil** : Suggère une manière d'appliquer les informations d'un thème ou d'une étape.
- **Note** : Décrit un dossier particulier, ou développe un point important.
- **Important** : Souligne une information critique concernant un thème ou une étape.
- **Attention** : Indique qu'une action ou étape peut entraîner la perte de données, des problèmes de sécurité ou des problèmes de performances.
- **Avertissement** : Indique qu'une action ou une étape peut entraîner des dommages physiques, ou endommager le matériel.

IMPORTANT : Le contenu de ce guide peut faire référence à des informations publiées sur des sites Web de tiers qui étaient correctes au moment de leur publication. Toutefois, ces informations peuvent changer sans notification préalable de la part de Genetec Inc.

Table des matières

Preface

Mentions légales.	ii
À propos de ce guide.	iii

Chapitre 1 : Présentation de votre appareil Streamvault

Mise en route de votre appareil Streamvault.	2
Ports par défaut utilisés par Streamvault.	4
À propos de la mise à jour du logiciel SV dans SV Control Panel.	7
Connexion des composants d'un appareil Streamvault.	8
Cartes de codage analogiques Genetec.	8
Désactiver les entrées de caméra sur les cartes de codage d'un appareil Streamvault.	9
Entrées et sorties d'alarme d'un appareil Streamvault.	10
À propos des comptes utilisateur Streamvault.	12
Informations de connexion pour les comptes utilisateur par défaut sur un appareil Streamvault.	12
Se connecter à un appareil Streamvault.	14
À propos du service Streamvault.	15
À propos du renforcement Streamvault.	16
Appareils dotés de capacités de gestion renforcement.	16

Chapitre 2 : Prise en main de SV Control Panel

À propos du SV Control Panel.	19
Configuration de votre appareil dans SV Control Panel.	19
Activer votre licence Security Center sur un appareil.	22
Activer manuellement une licence depuis Server Admin.	24
Activer System Availability Monitor.	26
Activer les fonctionnalités vidéo et de contrôle d'accès Security Center.	27
À propos de l'outil Inscription d'unités.	30
Ouvrir l'Outil d'inscription d'unités.	30
Configurer les réglages d'inscription des unités.	30
Ajouter des unités.	31
Effacer les unités ajoutées.	31
Ignorer des unités.	32
Supprimer des unités de la liste des unités ignorées.	32
Configurer les réglages par défaut des caméras.	33
Créer des horaires d'enregistrement personnalisés.	35
À propos de la sauvegarde et de la restauration.	36
Sauvegarder la base de données du Répertoire.	37
Restaurer la base de données du Répertoire.	38
Choisir la méthode de création des rôles Archiveur et des partitions.	39
Ajouter des rôles Archiveur dans SV Control Panel.	40
Ajout manuel de rôles et de partitions Archiveur.	41
Chiffrer le lecteur du SE.	44
Création d'une clé de récupération.	45
Collecte des journaux d'assistance.	48

Chapitre 3 : Prise en main du module externe Streamvault Maintenance

À propos du module externe Streamvault Maintenance.	51
Téléchargement et installation du module externe.	52
Privileges Genetec Streamvault.	53
Création du rôle de module externe.	55
Configuration de l'entité de surveillance de matériel Streamvault.	56
Configurer une entité Gestionnaire Streamvault.	60
À propos de l'onglet Gestion.	63
Analyser l'état de fonctionnement d'un appareil Streamvault.	64
Colonnes du volet de rapport de la tâche Matériel Streamvault..	65
Créer des mécanismes événement-action pour les dysfonctionnements de Streamvault.	66

Chapitre 4 : Référence SV Control Panel

Page d'accueil de SV Control Panel.	69
Page Configuration de SV Control Panel.	71
Page Sécurité de SV Control Panel.	74
Page À propos du SV Control Panel.	78

Chapitre 5 : Ressources complémentaires

Garantie de votre appareil Streamvault.	81
Configurer le mot de passe du BIOS.	82
Modifier le mot de passe iDRAC par défaut.	85
Ajouter un nouvel utilisateur iDRAC avec des privilèges d'administrateur.	86
Désactiver l'utilisateur root iDRAC.	87
Réappliquer une image à un appareil Streamvault.	88
Recherche de l'ID système et de la version d'image d'un appareil Streamvault.	89
Autoriser le partage de fichiers sur un appareil Streamvault.	90
Autoriser les connexions Bureau à distance à un appareil Streamvault.	91

Chapitre 6 : Dépannage

Rétablir les réglages d'usine sur un appareil tout-en-un Streamvault.	93
Créer une clé USB de réinitialisation d'usine pour un appareil tout-en-un Streamvault.	93
Réinitialisation de l'image logicielle sur un appareil tout-en-un.	95
Rétablir les réglages d'usine sur un appareil Streamvault poste de travail ou serveur.	103
Créer une clé USB de réinitialisation d'usine pour un appareil de type poste de travail ou serveur Streamvault.	104
Réinitialiser l'image logicielle sur un appareil de type poste de travail ou serveur Streamvault.	106
Les contrôleurs Mercury EP restent hors ligne lorsque TLS 1.1 est désactivé.	108
Activer Transport Layer Security (TLS).	109
Le Bureau à distance ne peut pas se connecter à un appareil Streamvault.	112
Suppression des restrictions des comptes utilisateur non administrateurs.	116
Les comptes locaux ne peuvent pas accéder au Bureau à distance, au service de partage de fichier et à la gestion à distance.	117
Activer les services connexes à la carte à puce.	118
Activation de la prise en charge des contrôleurs 1.x.x du micrologiciel Mercury EP ou LP.	119
Activer la prise en charge de l'intégration Synergis IX.	121
Modifier les objets de stratégie de groupe locaux pour les comptes utilisateur non-administrateurs.	122
Désactiver le pare-feu Windows.	125

Chapitre 7 : Assistance technique

Contacter le centre d'assistance technique de Genetec.	128
Contacter le GTAC par téléphone.	128
Contacter le GTAC par l'intermédiaire du GTAP.	129
Contacter le GTAC par l'intermédiaire du chat en direct.	129
Assistance logicielle.	131
Assistance matérielle.	132
Spécifications pour Streamvault.	133
Conditions générales de l'assistance Streamvault.	134
Glossaire	135
Où trouver les informations sur les produits	137

Présentation de votre appareil Streamvault

Cette section aborde les sujets suivants:

- ["Mise en route de votre appareil Streamvault"](#), page 2
- ["Ports par défaut utilisés par Streamvault"](#), page 4
- [" À propos de la mise à jour du logiciel SV dans SV Control Panel "](#), page 7
- ["Connexion des composants d'un appareil Streamvault"](#), page 8
- ["À propos des comptes utilisateur Streamvault"](#), page 12
- ["Se connecter à un appareil Streamvault "](#), page 14
- ["À propos du service Streamvault"](#), page 15
- [" À propos du renforcement Streamvault"](#), page 16

Mise en route de votre appareil Streamvault

Vous pouvez déployer votre appareil Streamvault^{MC} avec Security Center en suivant une succession d'étapes.

Présentation du déploiement

Étape	Tâche	Informations complémentaires
Comprendre les prérequis et les problèmes clés avant le déploiement		
1	Ouvrez les ports réseau requis pour connecter les systèmes centraux dans Security Center et les modules Streamvault. Connectez les périphériques tels que le moniteur, le clavier, la carte de codage analogique et les périphériques aux entrées et aux sorties. Connectez l'appareil à votre réseau.	<ul style="list-style-type: none"> • Ports par défaut utilisés par Streamvault, page 4. • Connexion des composants d'un appareil Streamvault, page 8. • Cartes de codage analogiques Genetec, page 8. • Désactiver les entrées de caméra sur les cartes de codage d'un appareil Streamvault, page 9. • Entrées et sorties d'alarme d'un appareil Streamvault, page 10.
2	Avant de déployer votre appareil, renseignez-vous sur le contenu de votre version d'image.	<ul style="list-style-type: none"> • Contenu de chaque version d'image de Streamvault.
3	Connectez-vous à Windows en tant qu'administrateur avec le mot de passe imprimé sur votre appareil, puis modifiez le mot de passe.	<ul style="list-style-type: none"> • Se connecter à un appareil Streamvault, page 14.
4	Configurez le mot de passe du BIOS sur votre appareil.	<ul style="list-style-type: none"> • Configurer le mot de passe du BIOS, page 82.
5	Si votre appareil prend en charge iDRAC, modifiez immédiatement le mot de passe iDRAC par défaut. Pour renforcer la sécurité, il est recommandé de créer un compte utilisateur secondaire avec des privilèges d'administrateur et de désactiver le compte utilisateur racine.	<ul style="list-style-type: none"> • Modifier le mot de passe iDRAC par défaut, page 85. • Ajouter un nouvel utilisateur iDRAC avec des privilèges d'administrateur, page 86. • Désactiver l'utilisateur root iDRAC, page 87.
Suivez les assistants de configuration		
6	Terminez l' <i>Assistant de configuration Streamvault Control Panel</i> . REMARQUE : Le bureau distant est désactivé par défaut. Pour activer le bureau à distance, activez le paramètre Service Bureau à distance sur la page <i>Sécurité</i> du SV Control Panel.	<ul style="list-style-type: none"> • Configuration de votre appareil dans SV Control Panel, page 19. • Autoriser les connexions Bureau à distance à un appareil Streamvault, page 91.
7	Activez votre licence Security Center. <ul style="list-style-type: none"> • Si l'appareil est connecté à Internet, activez votre licence via l'assistant d'activation <i>Streamvault Control Panel</i>. 	<ul style="list-style-type: none"> • Activer votre licence Security Center sur un appareil, page 22. • Activer manuellement une licence depuis Server Admin, page 24.

Étape Tâche	Informations complémentaires
<ul style="list-style-type: none"> • Si l'appareil n'est pas connecté à Internet, activez votre licence manuellement depuis Server Admin. 	
8 Activez System Availability Monitor.	<ul style="list-style-type: none"> • Activer System Availability Monitor, page 26.
9 Configurez Genetec ^{MC} Update Service afin d'obtenir la dernière version de Security Center et de SV Control Panel. S'il existe des mises à jour, installez-les.	<ul style="list-style-type: none"> • Configurer Genetec Update Service.
10 Si SV Control Panel indique que d'autres mises à jour sont disponibles, installez-les maintenant.	<ul style="list-style-type: none"> • À propos de la mise à jour du logiciel SV dans SV Control Panel, page 7.
11 Chiffrez le lecteur du SE sur votre appareil avec BitLocker, et créez une clé de récupération.	<ul style="list-style-type: none"> • Chiffrer le lecteur du SE, page 44.
12 Pour un appareil Archiveur, créez le nombre de rôles Archiveur nécessaire pour prendre en charge le nombre de caméras et la bande passante prévue pour votre déploiement.	<ul style="list-style-type: none"> • Pour les séries SV-1000E, SV-2000E, SV-4000E : Ajouter des rôles Archiveur dans SV Control Panel, page 40. • Pour la série SV-7000EX et pour un appareil tout-en-un : Ajout manuel de rôles et de partitions Archiveur, page 41.
13 Connectez-vous à Config Tool et configurez les fonctionnalités vidéo et de contrôle d'accès de Security Center.	<ul style="list-style-type: none"> • Activer les fonctionnalités vidéo et de contrôle d'accès Security Center, page 27. • Configurer les réglages d'inscription des unités, page 30.
14 Sauvegarder la configuration de Security Center.	<ul style="list-style-type: none"> • Sauvegarder la base de données du Répertoire, page 37.

Ports par défaut utilisés par Streamvault

Les ports réseau requis doivent être ouverts pour permettre aux composants Streamvault^{MC} suivants de fonctionner correctement.

Ports requis du module externe Streamvault^{MC} Maintenance

Le port suivant doit être ouvert sur un pare-feu externe pour le trafic entrant afin que le module externe Streamvault^{MC} Maintenance puisse communiquer avec le matériel Streamvault. Cette exigence ne s'applique que si les trois conditions suivantes sont réunies :

- La connexion de passerelle entre le SE interne et l'iDRAC est désactivée
- L'iDRAC utilise un port LAN dédié
- Il y a un pare-feu entre le réseau iDRAC et le réseau hôte

Dans toutes les autres situations, cette exigence peut être ignorée.

Module	Port entrant	Utilisation du port
Surveillance de matériel Streamvault ^{MC}	65116	Utilisé pour les communications HTTPS entre Security Center et le contrôleur de gestion de la carte de base iDRAC du matériel Streamvault via le réseau.

Ports requis SV Control Panel

Les ports de trafic sortant répertoriés ci-dessous doivent être ouverts pour permettre aux composants de Streamvault Control Panel de se connecter aux services Cloud de Genetec^{MC}.

Port sortant	Utilisation du port	URL de destination
TCP 443	Communication HTTPS avec les services de sauvegarde de Genetec	svbackupservices.genetec.com genetecbackupservice.blob.core.windows.net

Ports requis de CylancePROTECT

Les ports de trafic sortant répertoriés ci-dessous qui doivent être ouverts pour que l'agent de bureau CylancePROTECT communique avec la console de gestion de Genetec et recevoir les mises à jour de l'agent.

Port sortant	Utilisation du port	URL de destination
TCP 443	Communication HTTPS en Amérique du Nord	cement.cylance.com data.cylance.com protect.cylance.com update.cylance.com api.cylance.com download.cylance.com venueapi.cylance.com

Port sortant	Utilisation du port	URL de destination
TCP 443	Communication HTTPS en Asie-Pacifique Nord-Est	cement-apne1.cylance.com data-apne1.cylance.com protect-apne1.cylance.com update-apne1.cylance.com api.cylance.com download.cylance.com venueapi-apne1.cylance.com
TCP 443	Communication HTTPS en Asie-Pacifique Sud-Est	cement-au.cylance.com cement-apse2.cylance.com data-au.cylance.com protect-au.cylance.com update-au.cylance.com api.cylance.com download.cylance.com venueapi-au.cylance.com
TCP 443	Communication HTTPS en Europe centrale	cement-euc1.cylance.com data-euc1.cylance.com protect-euc1.cylance.com update-euc1.cylance.com api.cylance.com download.cylance.com venueapi-euc1.cylance.com
TCP 443	Communication HTTPS en Amérique du Sud	cement-sae1.cylance.com data-sae1.cylance.com protect-sae1.cylance.com update-sae1.cylance.com api.cylance.com download.cylance.com venueapi-sae1.cylance.com
TCP 443	Communication HTTPS dans GovCloud	cement.us.cylance.com data.us.cylance.com protect.us.cylance.com update.us.cylance.com api.us.cylance.com download.cylance.com download.us.cylance.com

Port sortant	Utilisation du port	URL de destination
		venueapi.us.cylance.com
TCP 443	Communication HTTPS pour activer Cylance après réinstallation	svservices.genetec.com

REMARQUE : Si vous ne souhaitez pas ouvrir les connexions sortantes susmentionnées, CylancePROTECT peut être mis en mode déconnecté. En mode déconnecté, CylancePROTECT reçoit les mises à jour de l'agent à partir du service Genetec^{MC} Update Service (GUS).

Pour plus d'informations sur les modes de communication de l'appareil Streamvault avec les services de gestion de Genetec, voir [Page Sécurité de SV Control Panel](#), page 74.

À propos de la mise à jour du logiciel SV dans SV Control Panel

Genetec^{MC} Update Service (GUS) est intégré dans SV Control Panel pour vous aider à vérifier que les composants logiciels de votre appareil sont à jour.

Lorsque des mises à jour sont disponibles, le bouton **Afficher les mises à jour** est affiché et une pastille indique le nombre de mises à jour disponibles. Lorsque vous cliquez sur le bouton **Afficher les mises à jour**, GUS est lancé dans un navigateur.

REMARQUE : La couleur de la pastille dépend de l'importance des mises à jour. Une pastille orange indique des mises à jour recommandées, tandis qu'une pastille rouge indique une mise à jour critique.



Voici les principales caractéristiques de GUS :

- Mettre à jour vos produits Genetec^{MC} lors de la sortie de nouvelles versions.
- Rechercher des mises à jour à intervalles réguliers.
- Configurer le téléchargement des mises à jour en arrière-plan, bien qu'une intervention manuelle reste nécessaire.
- Consulter la date de la dernière vérification.
- Actualiser automatiquement la licence en arrière-plan pour qu'elle soit valable et que la date d'expiration soit mise à jour.
- Activer diverses fonctionnalités, comme le Programme d'amélioration Genetec.
- Analyser automatiquement votre micrologiciel et recommander des mises à niveau ou vous avertir en cas de vulnérabilités.

Pour en savoir plus sur l'utilisation de GUS, reportez-vous au [Guide de l'utilisateur de Genetec^{MC} Update Service](#) sur TechDoc Hub.

Connexion des composants d'un appareil Streamvault

Pour préparer votre appareil Streamvault, vous devez connecter les périphériques obligatoires (moniteur, clavier et souris), les périphériques facultatifs, le réseau ainsi qu'une source d'alimentation.

Avant de commencer

Libérez l'espace autour du bouton d'alimentation. Pour éviter d'éteindre accidentellement l'appareil, veillez à ce que rien ne touche ou ne soit trop près du bouton d'alimentation.

Procédure

- 1 Connectez le câble du moniteur à une entrée vidéo prise en charge : prise VGA, HDMI ou DisplayPort. Vous devez connecter au moins un moniteur à l'appareil. Vous pouvez connecter jusqu'à trois moniteurs au même appareil.
- 2 Branchez le moniteur dans une prise secteur et allumez-le.
- 3 Connectez le clavier et la souris à un port USB disponible.
- 4 Connectez les périphériques facultatifs :
 - Haut-parleurs
 - [Caméras analogiques](#)
 - [Entrées et sorties d'alarmes](#)
- 5 Connectez un câble Ethernet au port Ethernet de l'appareil. Connectez l'autre extrémité du câble à la prise RJ-45 du réseau IP.
- 6 Pour les appareils Streamvault^{MC} SV-100E, insérez la fiche CC dans la prise d'entrée 19,5 V de l'appareil et l'autre extrémité dans le bloc d'alimentation. Branchez le cordon du bloc sur une prise électrique.
- 7 Pour allumer l'appareil Streamvault, appuyez sur le bouton de mise sous tension.

Lorsque vous avez terminé

[Pour vous connecter à votre appareil Streamvault :](#)

Cartes de codage analogiques Genetec

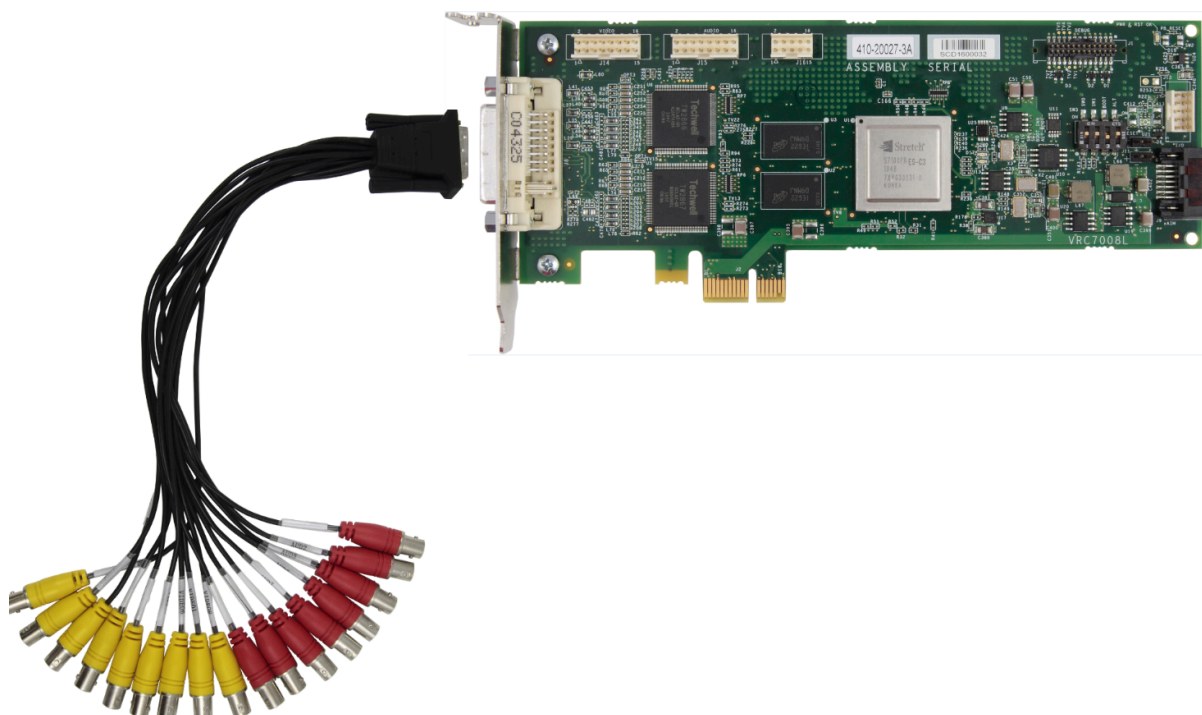
Si vous utilisez un appareil Streamvault pour déployer un système de gestion vidéo avec des caméras analogiques, vous devez connecter les caméras à la carte de codage analogique Genetec^{MC} de l'appareil.

Spécifications de la carte de codage analogique

Les spécifications suivantes s'appliquent aux appareils Streamvault incluant la carte vidéo analogique :

- 8 ou 16 entrées vidéo analogiques, en fonction de la carte installée
- Résolution vidéo max. 4CIF
- Débit d'images maximum : 30 images/s
- Prend en charge le format de compression H.264

Limitation : Pour que la carte de codage analogique puisse enregistrer, votre appareil Streamvault doit disposer d'une connexion réseau. Si une connexion réseau n'est pas disponible, vous devez configurer une interface de bouclage pour que la carte de codage puisse fonctionner correctement.



À propos de la connexion de caméras analogiques

Si votre appareil Streamvault comprend la carte de codage analogique Genetec, un câble de dérivation avec des connecteurs BNC est fourni. Les connecteurs sont utilisés pour connecter les caméras analogiques directement à la carte de codage intégrée.

A propos de l'ajout de caméras analogiques dans Security Center

Pour ajouter des caméras analogiques dans Security Center, vous devez utiliser l'outil d'inscription d'unités. Pour en savoir plus, voir [À propos de l'outil d'inscription d'unités](#).

Tenez compte des éléments suivants lors de l'ajout de caméras analogiques :

- Vous ne pouvez pas ajouter de caméras analogiques dans Security Center à l'aide de la méthode *Ajout manuel*. Utilisez l'outil d'inscription d'unités.
- Pour découvrir de nouvelles unités et utiliser l'outil d'inscription d'unités, vous devez vous connecter à Config Tool localement.
- Lors de la sélection du fabricant de la caméra dans l'outil d'inscription d'unités, toutes les caméras analogiques sont répertoriées sous la *carte de codage Genetec* du fabricant.

Désactiver les entrées de caméra sur les cartes de codage d'un appareil Streamvault

Pour mettre à niveau une licence de connexion de caméra d'analogique à IP, vous devez désactiver les entrées de caméra sur la carte de codage.

Procédure

- 1 Sur la page d'accueil de Config Tool, cliquez sur l'onglet *À propos*.
- 2 Cliquez sur l'onglet **Omnicast^{MC}** et repérez le nombre de caméras en regard de *Nombre de caméras et de moniteurs analogiques*.

Par exemple : 16 / 16.

- 3 Ouvrez la tâche *Vidéo*.
 - 4 Dans l'arborescence des entités, cliquez sur l'unité vidéo correspondant à la carte encodeur.
 - 5 Cliquez sur l'onglet **Périphériques**, puis sélectionnez les caméras à désactiver.
Vous pouvez sélectionner plusieurs caméras en appuyant sur Ctrl puis en cliquant sur les caméras.
 - 6 Au bas de la page *Périphériques*, cliquez sur le cercle rouge (●) pour désactiver les caméras, puis cliquez sur **Appliquer**.
Les caméras désactivées sont grisées, et un point rouge est affiché à gauche de chaque caméra désactivée dans la liste.
 - 7 Sur la page *À propos*, vérifiez que le nombre de caméras est exact.
Vous devrez peut-être redémarrer Config Tool pour actualiser le nombre de caméras.
- REMARQUE :** Si une caméra que vous avez désactivée a enregistré une vidéo, la caméra apparaît dans l'arborescence des entités de la tâche *Surveillance* de Security Desk. Vous pouvez visionner la vidéo depuis cette caméra.

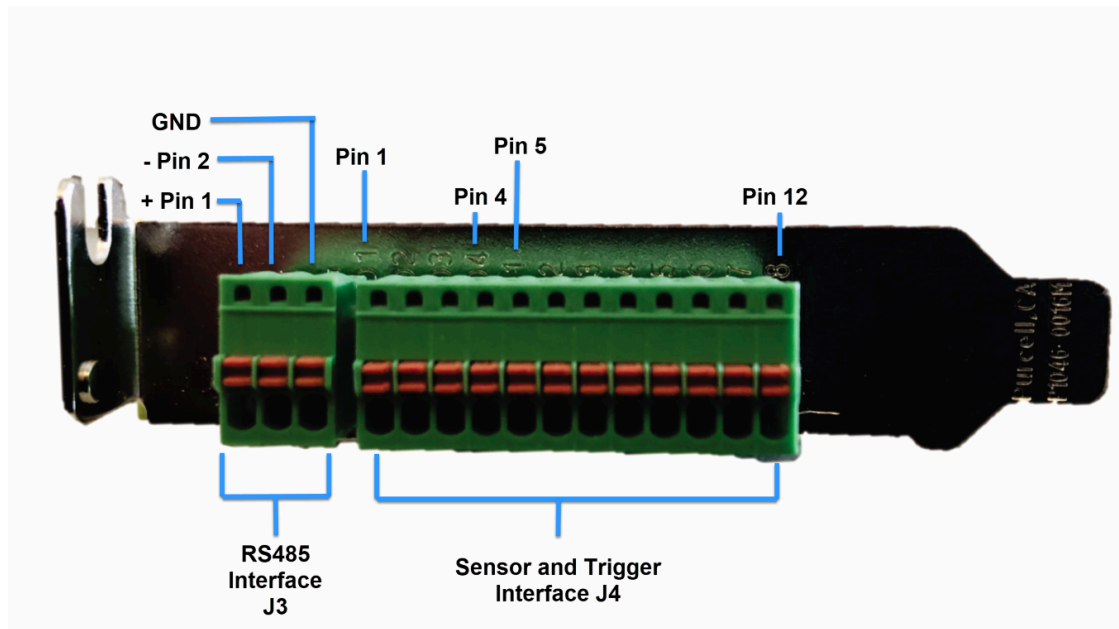
Entrées et sorties d'alarme d'un appareil Streamvault

Si vous utilisez un appareil Streamvault pour déployer un système de contrôle d'accès, vous pouvez utiliser la carte d'E/S pour connecter directement les entrées d'alarme matérielles à l'appareil, puis contrôler les sorties à l'aide du mécanisme événement-action dans Security Center.

Spécifications de carte E/S

Les spécifications suivantes s'appliquent aux modèles Streamvault incluant la carte E/S analogique :

- 4 sorties de déclenchement
- 8 entrées d'alarme
- Port de communication RS-485



À propos de la connexion des entrées E/S

Vous pouvez connecter les fils des entrées et sorties des périphériques matériels directement à la carte d'E/S à l'arrière de l'appareil Streamvault. Les câbles doivent être insérés à l'aide d'un petit tournevis à tête plate pour enfoncer les pinces de tension sur le connecteur.

À propos de la création du mécanisme événement-action

Pour plus d'informations sur la manière de créer des mécanismes événement-action pour Streamvault, voir [Créer des mécanismes événement-action](#) sur le TechDoc Hub.

À propos des comptes utilisateur Streamvault

Il existe deux types de comptes utilisateur Streamvault^{MC} : administrateur local et non-administrateur local. Selon le type de compte utilisateur avec lequel vous vous connectez à SV Control Panel, vous ne voyez que les fonctionnalités qui vous intéressent.

Administrateur local

Le compte utilisateur administrateur local (Admin) est créé par défaut. Une personne connectée en tant qu'administrateur dispose de tous les droits administratifs sur SV Control Panel. L'administrateur peut configurer tous les paramètres liés au système et à la sécurité dans SV Control Panel et peut créer des comptes utilisateur non administrateurs.

Non-administrateur local

Le compte utilisateur non administrateur local par défaut pour les appareils tout-en-un et les postes de travail est le compte Opérateur. Une personne connectée en tant qu'opérateur a un accès restreint aux fonctionnalités de SV Control Panel. L'opérateur peut lancer Config Tool et Security Desk, afficher les informations sur le système et les licences et accéder à la documentation du produit.

Une personne connectée en tant qu'administrateur peut créer d'autres comptes non administrateurs, qui ont également un accès limité à SV Control Panel.

REMARQUE : Il est possible de supprimer les restrictions d'accès par défaut imposées à tous les comptes utilisateur non administrateurs. Pour plus d'informations sur la façon de procéder, consultez [Suppression des restrictions des comptes utilisateur non administrateurs](#), page 116.

Informations de connexion pour les comptes utilisateur par défaut sur un appareil Streamvault

Au premier démarrage de votre appareil Streamvault, les comptes utilisateur d'administrateur et d'opérateur Windows sont créés. Ces comptes ont des droits d'accès différents et des mots de passe par défaut. Server Admin a également un mot de passe par défaut.

Les mots de passe par défaut suivants sont destinés à la connexion initiale. Pendant la configuration, vous créez votre propre mot de passe pour Config Tool et Security Desk.

Nom d'utilisateur	Mot de passe par défaut	Accès accordé à	Accès refusé pour
Admin	admin	Accès complet au système : <ul style="list-style-type: none"> Windows : toutes les fonctionnalités système et administratives Security Center SV Control Panel 	Non applicable
Opérateur	opérateur	<ul style="list-style-type: none"> Corbeille Bibliothèques Mon ordinateur C: lecteur Page d'accueil du tableau de bord SV, page de configuration, paramètres 	<ul style="list-style-type: none"> Windows: arrêter et redémarrer Paramètres système Partition vidéo

Nom d'utilisateur	Mot de passe par défaut	Accès accordé à	Accès refusé pour
		régionaux seulement, page À propos <ul style="list-style-type: none"> Server Admin : nécessite un mot de passe administrateur pour tous les droits 	
Non applicable	genetecfactory	Server Admin	REMARQUE : Cette option n'est pas disponible pour les appareils de type poste de travail.

Pour modifier le mot de passe de votre compte utilisateur Windows, de votre application cliente ou de Server Admin, connectez-vous à SV Control Panel avec votre compte d'administrateur Windows. Sur la page *Sécurité*, dans la section *Informations d'identification*, vous pouvez gérer tous vos mots de passe.

REMARQUE : Le compte Opérateur n'est pas créé avec un modèle. Si vous créez un nouveau compte utilisateur, il n'aura pas les mêmes restrictions par défaut.

Security Center Server Admin

- Seuls les utilisateurs Administrateurs peuvent se connecter à Server Admin.
- Pour vous connecter à partir de votre ordinateur local, cliquez sur le raccourci **Server Admin** disponible sur votre bureau.
- Pour vous connecter à Server Admin à distance, vous avez besoin du nom DNS ou l'adresse IP du serveur, ainsi que du port du serveur Web et du mot de passe du serveur. Lorsque vous entrez le mot de passe par défaut, vous êtes invité à le modifier.

IMPORTANT : Pour assurer la sécurité de votre système, modifiez immédiatement tous les mots de passe par défaut. Utilisez les bonnes pratiques du secteur pour créer des mots de passe fiables.

Rubriques connexes

[Modifier les objets de stratégie de groupe locaux pour les comptes utilisateur non-administrateurs](#), page 122

Se connecter à un appareil Streamvault

Au premier démarrage de votre appareil Streamvault^{MC}, vous êtes invité à modifier le mot de passe d'administrateur par défaut. Modifiez aussi le mot de passe par défaut de l'opérateur. Vous pourrez ensuite vous connecter en tant qu'opérateur ou administrateur.

Avant de commencer

[Découvrez les droits des comptes Operator et Admin.](#)

À savoir

Connectez-vous également en tant qu'utilisateur Admin pour configurer votre appareil dans SV Control Panel.

IMPORTANT : Le mot de passe doit répondre aux exigences suivantes :

- 14 caractères minimum

La longueur minimale est de 10 caractères pour les appareils avec des versions d'image qui ne disposent pas du service Streamvault. Pour en savoir plus sur les appareils équipés du service Streamvault et ceux qui ne le sont pas, voir [Appareils dotés de capacités de gestion renforcement](#), page 16.

- Au moins trois caractères issus des quatre catégories suivantes :

- Lettres majuscules
- lettres minuscules
- Chiffres en base 10 (0-9)
- Caractères non alphanumériques (tels que \$,%,!)

Procédure

- 1 Mettez l'appareil sous tension.
- 2 Connectez-vous avec le nom d'utilisateur Admin et le mot de passe par défaut inscrits sur l'appareil.
- 3 Entrez un nouveau mot de passe d'administrateur.
Vous êtes connecté en tant qu'utilisateur administrateur.
REMARQUE : Certains modèles disposent uniquement du compte Admin par défaut.
- 4 Déconnectez-vous, puis reconnectez-vous avec le nom d'utilisateur Operator et le mot de passe par défaut inscrits sur l'appareil.
- 5 Entrez un nouveau mot de passe d'opérateur.
Vous êtes connecté en tant qu'utilisateur opérateur.
- 6 Poursuivez avec la session opérateur, ou déconnectez-vous et reconnectez-vous en tant qu'utilisateur administrateur.

Lorsque vous avez terminé

[Lancez la configuration initiale de votre appareil.](#)

À propos du service Streamvault

Le service Streamvault est un service Windows qui permet aux utilisateurs de configurer un appareil Streamvault^{MC}, par exemple en appliquant des profils de renforcement.

Le service Streamvault peut appliquer les profils de renforcement suivants sur les appareils :

- Lignes directrices de sécurité Microsoft
- Lignes directrices de sécurité Microsoft avec le profil de niveau 1 du Center for Internet Sécurité (CIS)
- Lignes directrices de sécurité Microsoft avec le profil CIS niveau 2
- Lignes directrices de sécurité Microsoft avec le profil Sécurité Technical Implementation Guide (STIG)

Voir [À propos du renforcement Streamvault](#), page 16 pour plus d'informations sur les profils de renforcement.

Lorsqu'un utilisateur administrateur sélectionne un profil de renforcement dans SV Control Panel, le service Streamvault applique le profil à l'appareil.

Des mises à jour du service Streamvault sont disponibles périodiquement et peuvent être appliquées via le Genetec^{MC} Update Service^{MC} (GUS) ou le portail d'assistance technique Genetec (GTAP). Lorsqu'une mise à jour est disponible, une notification apparaît dans SV Control Panel. L'application des mises à jour est facultative, mais recommandée pour accéder aux nouvelles versions des profils de renforcement.

À propos du renforcement Streamvault

Le renforcement améliore la sécurité de votre appareil Streamvault^{MC} en appliquant un ensemble spécifique de paramètres de sécurité.

Lorsque vous renforcez votre appareil, vous l'optimisez pour plus de sécurité, mais potentiellement au détriment de la facilité d'utilisation ou des performances. Le degré de renforcement de votre appareil dépend de votre modèle de menace et de la sensibilité de vos informations.

Le renforcement est appliqué sur la page *Sécurité* de SV Control Panel. Vous avez le choix entre quatre profils de renforcement prédéfinis.

Par défaut, tous les appareils sont livrés avec le profil de renforcement Microsoft CIS de niveau 2 appliqué.

Profil de renforcement	Description
Microsoft (uniquement)	Ce profil de renforcement applique les lignes directrices de sécurité Microsoft à votre système. Les lignes directrices de sécurité Microsoft sont un groupe de paramètres de configuration recommandés par Microsoft qui sont basés sur les commentaires des équipes d'ingénierie de sécurité, des groupes de produits, des partenaires et des clients Microsoft. Les lignes directrices Microsoft déployées sur les appareils Streamvault sont la ligne de base Windows et la ligne de base Microsoft Edge.
Microsoft avec CIS niveau 1	Ce profil de renforcement applique les lignes directrices de sécurité Microsoft et le profil Center for Internet Sécurité (CIS) niveau 1 (CIS L1) à votre système. Le CIS L1 fournit des exigences de sécurité essentielles qui peuvent être mises en œuvre sur n'importe quel système avec peu ou pas d'impact sur les performances ou des fonctionnalités réduites.
Microsoft avec CIS niveau 2	Ce profil de renforcement applique les lignes directrices de sécurité Microsoft et les profils CIS L1 et niveau 2 (L2) à votre système. Le profil CIS L2 offre le plus haut niveau de sécurité et est destiné aux organisations pour lesquelles la sécurité est de la plus haute importance. La sécurité stricte apportée par ce profil de renforcement peut réduire les fonctionnalités du système et rendre la gestion du serveur à distance plus difficile.
Microsoft avec STIG	Ce profil de renforcement applique les lignes directrices de sécurité Microsoft et les guides de mise en œuvre technique de Sécurité (STIG) de la Defense Information Systems Agency (DISA) à votre système. Les STIG DISA sont basés sur les normes du National Institute of Standards and Technology (NIST) et offrent une protection de sécurité avancée pour les systèmes Windows du ministère de la Défense américain.

REMARQUE : Les profils de renforcement ne sont disponibles que sur les appareils dotés du [Service Streamvault](#). Pour en savoir plus, voir [À propos du service Streamvault](#), page 15.

Appareils dotés de capacités de gestion renforcement

Seuls les appareils dotés du service Streamvault^{MC} disposent de capacités de gestion renforcement. Le type d'appareil et l'image déterminent si le service Streamvault est disponible.

Le tableau ci-dessous indique quels appareils disposent du service Streamvault et lesquels n'en disposent pas.

Type d'appareil	Versions d'images avec le service Streamvault	Versions d'images sans le service Streamvault
Tout-en-un	<ul style="list-style-type: none"> 11.2024.2 	<ul style="list-style-type: none"> 16 17 18 19
SVW	<ul style="list-style-type: none"> 11.2024.2 	<ul style="list-style-type: none"> 0010.4 0011.2 0012.2 0013.2
SVA	<ul style="list-style-type: none"> 11.2024.2 	<ul style="list-style-type: none"> 0010.4 0011.2 0012.2 0013.2
SVR	<ul style="list-style-type: none"> 10.2021.2 11.2024.2 	<ul style="list-style-type: none"> 0012.2.X
Autres appareils Streamvault	<ul style="list-style-type: none"> WS.2022.1 	<ul style="list-style-type: none"> 2016.1.B 2016.1.C 2019.1 2019.4.C 2022.1.C

REMARQUE : Pour plus d'informations sur la recherche de la version d'image de votre appareil, consultez [Recherche de l'ID système et de la version d'image d'un appareil Streamvault](#), page 89.

Prise en main de SV Control Panel

La prise en main vous présente SV Control Panel et vous décrit la procédure de configuration de votre appareil Streamvault.

Cette section aborde les sujets suivants:

- ["À propos du SV Control Panel"](#), page 19
- [" Activer votre licence Security Center sur un appareil "](#), page 22
- [" Activer manuellement une licence depuis Server Admin "](#), page 24
- ["Activer System Availability Monitor"](#), page 26
- [" Activer les fonctionnalités vidéo et de contrôle d'accès Security Center "](#), page 27
- ["À propos de l'outil Inscription d'unités"](#), page 30
- [" Configurer les réglages par défaut des caméras "](#), page 33
- [" Créer des horaires d'enregistrement personnalisés "](#), page 35
- [" À propos de la sauvegarde et de la restauration "](#), page 36
- [" Choisir la méthode de création des rôles Archiveur et des partitions "](#), page 39
- [" Chiffrer le lecteur du SE "](#), page 44
- [" Collecte des journaux d'assistance "](#), page 48

À propos du SV Control Panel

Le SV Control Panel est une application qui vous permet de configurer rapidement un appareil Streamvault^{MC} pour qu'il fonctionne avec Security Center pour le contrôle d'accès et la vidéosurveillance.

ATTENTION : Les modifications de configuration que vous effectuez dans SV Control Panel remplaceront les modifications de configuration effectuées en dehors de SV Control Panel, y compris les paramètres Windows personnalisés.

Le SV Control Panel peut être exécuté comme suit :

- Mode Extension pour les configurations s'exécutant sur un serveur d'extension.
- Mode Client pour les configurations s'exécutant sur des appareils de type poste de travail.
- Mode Répertoire pour les configurations exécutées sur le serveur primaire.

Le SV Control Panel inclut les fonctionnalités suivantes :

- Assistant *Configuration du Streamvault Control Panel* pour configurer rapidement votre appareil.
- Assistant *Activation du tableau de bord Streamvault* pour vous aider à activer votre appareil.
- L'Assistant d'installation de Security Center que vous pouvez utiliser pour configurer Security Center.
- Assistants de *sauvegarde du tableau de bord Streamvault* et de *restauration du tableau de bord Streamvault* pour vous aider à créer des sauvegardes de la base de données du Répertoire et des fichiers de configuration, et à les restaurer en cas de besoin.
- Genetec^{MC} Update Service (GUS) qui recherche régulièrement les mises à jour logicielles.
- Raccourcis vers les tâches courantes dans Config Tool et Security Desk.
- Liens vers le portail d'assistance technique Genetec (GTAP) et la documentation produit.
- L'option permettant de choisir le mode de fonctionnement du logiciel antivirus Cylance fourni avec votre appareil Streamvault^{MC}. Les options sont répertoriées sur la page de configuration *Sécurité*.
- La capacité de créer des partitions et rôles Archiveur supplémentaires pour les configurations sur les serveurs d'extension.

REMARQUE :

- Ce guide s'applique à la version 3.2.1 de SV Control Panel, que vous pouvez télécharger à partir de GTAP.
- SV Control Panel versions 3.0 et versions ultérieures sont compatibles avec les appareils qui ne disposent pas du service Streamvault. Cependant, ces appareils n'auront pas accès aux profils de renforcement.

Configuration de votre appareil dans SV Control Panel

Lors de la première connexion à votre appareil Streamvault^{MC}, SV Control Panel ouvre l'assistant de *configuration du tableau de bord Streamvault* pour vous guider pas à pas.


Avant de commencer

Connectez l'appareil à Internet.

À savoir

- Les réglages appliqués dans l'assistant peuvent être modifiés par la suite sur la page *Configuration* de SV Control Panel.
- Vous n'êtes pas invité à modifier les mots de passe utilisateur sur les appareils Archiveur, Analyses, Poste de travail ou tout autre appareil configuré en tant que serveur d'extension Security Center.

Procédure

- 1 Démarrez votre appareil.
SV Control Panel démarre et l'assistant de *configuration du tableau de bord Streamvault* apparaît.
REMARQUE : SV Control Panel ne s'ouvre automatiquement que lors du premier démarrage de l'appareil. Lors des redémarrages suivants, les utilisateurs doivent se connecter avec leurs identifiants d'administrateur et démarrer SV Control Panel.
- 2 Sur la page de *Présentation*, cliquez sur **Suivant**.
- 3 Sur la page *Réseau*, configurez les réglages de connexion IP :
 - a) Si vous utilisez le DHCP pour obtenir une adresse IP automatiquement (valeur par défaut) et que l'adresse IP est manquante, cliquez sur **Actualiser**  pour obtenir une nouvelle adresse IP. Cliquez ensuite sur **Réessayer**.
 - b) Si le champ **État** affiche autre chose que « Connecté à Internet », cliquez sur **Réessayer**.
 - c) Lorsque le champ **État** affiche « Connecté à Internet », cliquez sur **Suivant**.
- 4 Sur la page *Configuration d'ordinateur*, renseignez les champs dans les sections *Informations générales* et *Paramètres régionaux*.
- 5 Pour modifier la langue de l'interface utilisateur :
 - a) Dans **Langue du produit**, sélectionnez votre langue.
 - b) Redémarrez le SV Control Panel.
 - c) Lorsque l'assistant de *configuration du tableau de bord Streamvault* s'ouvre à nouveau, cliquez sur **Suivant** sur la page *Configuration d'ordinateur*.
- 6 Sur la page *Configurer CylancePROTECT*, sélectionnez un mode de communication :
 - **En ligne (recommandé) :** L'agent CylancePROTECT communique avec Genetec pour signaler les nouvelles menaces, mettre à jour l'agent et envoyer des données qui contribuent à l'amélioration des modèles mathématiques. Cette option offre un niveau de protection maximal.
 - **Déconnecté :** Le mode déconnecté est destiné aux appareils dépourvus de connexion Internet. Dans ce mode, CylancePROTECT ne peut pas se connecter ni envoyer des informations aux services de gestion de Genetec dans le cloud. Votre appareil est protégé contre la plupart des menaces. Les opérations de maintenance et les mises à jour sont disponibles à travers le service Genetec^{MC} Update Service (GUS).
 - **Désactiver :** Sélectionnez ce mode pour désinstaller définitivement CylancePROTECT de votre appareil. Votre appareil utilisera les fonctions de protection et de détection des menaces de Microsoft Defender. Évitez de désactiver CylancePROTECT si l'appareil ne peut pas recevoir les mises à jour des définitions de virus pour Microsoft Defender.
- 7 Cliquez sur **Activer la gestion de la quarantaine** pour ajouter des fonctionnalités supplémentaires à l'icône Cylance dans la barre des tâches, y compris l'option **Supprimer la quarantaine** pour supprimer les fichiers que Cylance a mis en quarantaine.
- 8 Sur la page *Informations d'identification*, cliquez sur **Modifier le mot de passe** pour configurer les mots de passe pour les applications suivantes :
 - **Security Center (utilisateur Admin) :** Le mot de passe de l'utilisateur administrateur pour Security Desk, Config Tool et Genetec^{MC} Update Service.
 - **Server Admin :** Le mot de passe pour l'application Genetec^{MC} Server Admin.

Si votre appareil est un serveur d'extension Security Center , vous n'êtes pas invité à modifier les mots de passe. Sélectionnez **Ignorer cette étape** si vous ne souhaitez pas définir de nouveaux mots de passe.
- 9 Sur la page *Renforcement*, sélectionnez l'un des profils de renforcement suivants :
 - **Microsoft (uniquement) :** Ce profil de renforcement applique les lignes directrices de sécurité Microsoft à votre système. Les lignes directrices de sécurité Microsoft sont un groupe de paramètres de configuration recommandés par Microsoft qui sont basés sur les commentaires des équipes d'ingénierie de sécurité, des groupes de produits, des partenaires et des clients Microsoft.
 - **Microsoft avec CIS niveau 1 :** Ce profil de renforcement applique les lignes directrices de sécurité Microsoft et le profil Center for Internet Sécurité (CIS) niveau 1 (CIS L1) à votre système. Le CIS L1

fournit des exigences de sécurité essentielles qui peuvent être mises en œuvre sur n'importe quel système avec peu ou pas d'impact sur les performances ou des fonctionnalités réduites.

- **Microsoft avec CIS niveau 2** : Ce profil de renforcement applique les lignes directrices de sécurité Microsoft et les profils CIS L1 et niveau 2 (L2) à votre système. Le profil CIS L2 offre le plus haut niveau de sécurité et est destiné aux organisations pour lesquelles la sécurité est de la plus haute importance.

REMARQUE : La sécurité stricte apportée par ce profil de renforcement peut réduire les fonctionnalités du système et rendre la gestion du serveur à distance plus difficile.

- **Microsoft avec STIG** : Ce profil de renforcement applique les lignes directrices de sécurité Microsoft et les guides de mise en œuvre technique de Sécurité (STIG) de la Defense Information Systems Agency (DISA) à votre système. Les STIG DISA sont basés sur les normes du National Institute of Standards and Technology (NIST) et offrent une protection de sécurité avancée pour les systèmes Windows du ministère de la Défense américain.

REMARQUE : La page *Renforcement* est disponible uniquement pour les appareils dotés du service Streamvault.

10 Sur la page *System Availability Monitor*, sélectionnez une méthode de collecte de données :

- **Ne pas recueillir de données** : Le System Availability Monitor Agent est installé, mais ne recueillera pas de données.
- **Les données seront recueillies de façon anonyme** : Aucun code d'activation n'est requis. Les données de fonctionnement sont envoyées à un service de surveillance de l'état dédié, les noms des entités étant masqués et intraquables. Ces données ne sont utilisées que par Genetec Inc. à des fins statistiques, et ne sont pas accessibles via GTAP.
- **Les données seront recueillies et associées à mon système** : Un code d'activation est requis. Les données de fonctionnement recueillies sont liées à un système répertorié avec un contrat de maintenance applicative (CMA) actif.

11 Lisez l'accord de confidentialité, cochez la case **J'accepte les termes de cet accord de confidentialité**, puis cliquez sur **Appliquer**.

12 Sur la page *Conclusion*, cliquez sur **Fermer**.

L'option **Lancer l'assistant d'activation après l'installation** est cochée par défaut. Si vous l'effacez, vous êtes invité à activer le produit.

Lorsque vous avez terminé

[Activez votre appareil](#) avant de l'utiliser.

Activer votre licence Security Center sur un appareil

L'assistant *Activation de Streamvault Control Panel* vous aide à activer votre licence Security Center sur votre appareil Streamvault^{MC}.

Avant de commencer

- Connectez votre appareil à Internet.
- Munissez-vous de l'ID système et du mot de passe qui vous ont été envoyés à l'achat de votre licence.

À savoir

- Cette tâche ne concerne que les appareils dotés d'une connexion à Internet. Pour les appareils sans Internet, [activez votre licence Security Center manuellement dans Server Admin](#).
- Vous devez activer la licence Security Center uniquement sur un appareil qui héberge le rôle Répertoire et non sur des appareils tels que des serveurs d'extension ou des postes de travail.

Procédure

- 1 Dans SV Control Panel, cliquez sur **Le système n'est pas activé. Cliquez ici pour activer**.
L'assistant d'activation du *Streamvault Control Panel* apparaît.
REMARQUE : Si vous voyez le message *Un accès à Internet est nécessaire pour l'activation*, cela signifie que votre appareil n'est pas actuellement connecté à Internet. Connectez votre appareil maintenant, ou activez votre licence manuellement dans Server Admin.
- 2 Sur la page *Activation*, cliquez sur **ID système**, puis cliquez sur **Suivant**.
- 3 Sur la page *ID système*, entrez votre ID système et votre mot de passe, puis cliquez sur **Suivant**.
- 4 Sur la page *Résumé*, vérifiez que vous avez saisi le bon ID système, puis cliquez sur **Activer**.
La page *Résultat* vous indique ensuite si l'activation a réussi.
- 5 Cliquez sur **Suivant**.
- 6 (Facultatif) Sur la page *Mises à jour*, procédez de l'une des manières suivantes :
 - Si aucune mise à jour n'est disponible, cliquez sur **Ouvrir l'assistant d'installation Security Center**.
 - Si des mises à jour sont disponibles, cliquez sur **Afficher les mises à jour** pour ouvrir le Genetec^{MC} Update Service, puis installez les mises à jour.
 - Si la recherche de mises à jour échoue parce que le Répertoire ne répond pas, cliquez sur **Ouvrir Server Admin** et vérifiez que le Répertoire est prêt.**REMARQUE :** Si le service de mise à jour Genetec n'était pas prêt, la vérification de la mise à jour pourrait échouer. Le message *Impossible de rechercher des mises à jour pour l'instant. Nous réessayerons plus tard. s'affiche*.
- 7 Sur la page *Fonctionnalités complémentaires*, activez ou désactivez Synergis^{MC} Softwire et Genetec^{MC} Mobile. Ces fonctionnalités s'affichent uniquement si elles sont installées sur votre appareil. La fonction Genetec Mobile est uniquement disponible pour Security Center 5.8 et versions antérieures.
- 8 Fermez l'assistant d'activation du *Streamvault Control Panel*.

Lorsque vous avez terminé

- (Facultatif) [Activez l'agent de System Availability Monitor](#).
- [Configurer les paramètres de Security Center à l'aide de l'assistant du programme d'installation de Security Center](#)

Rubriques connexes

[Activer manuellement une licence depuis Server Admin](#), page 24

[Page À propos du SV Control Panel](#), page 78

Activer manuellement une licence depuis Server Admin

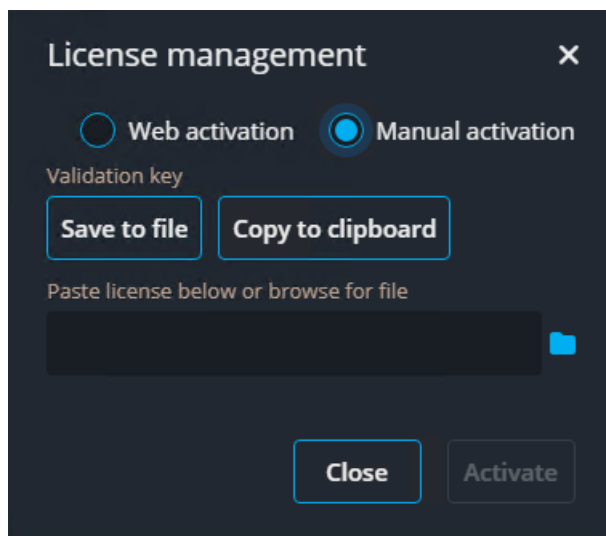
Si votre appareil Streamvault^{MC} n'a pas accès à Internet, vous pouvez activer votre licence Security Center manuellement depuis Server Admin.

Procédure

- 1 Enregistrez la clé de validation :
 - a) Depuis votre appareil, ouvrez le SV Control Panel.
 - b) Sur la page d'accueil, cliquez sur l'icône **Server Admin**.
 - c) Connectez-vous à Server Admin.

Si le mot de passe Server Admin est différent du mot de passe d'administrateur Windows, connectez-vous à Server Admin avec les identifiants que vous avez spécifiés dans l'assistant de *configuration du tableau de bord Streamvault*.
 - d) Sur la page *Licence*, cliquez sur **Modifier**.
 - e) Dans la boîte de dialogue *Gestion des licences*, sélectionnez **Activation manuelle** > **Enregistrer dans un fichier**.

Le nom par défaut du fichier est *validation.vk*.



- f) Copiez le fichier *validation.vk* sur une clé USB.
- g) Éjectez la clé USB de l'ordinateur.

- 2 Obtenez la licence sur le portail d'assistance technique Genetec^{MC} (GTAP) :
 - a) Branchez la clé USB sur un autre ordinateur doté d'un accès à Internet.
 - b) Connectez-vous à [GTAP](#).
 - c) Sur la page de *connexion GTAP*, entrez l'ID système et mot de passe qui vous ont été affectés à l'achat de votre licence, puis cliquez sur **Connexion**.
 - d) Dans la page *Informations système*, cliquez sur **Activer la licence** dans la section *Informations de licence*.
 - e) Dans la boîte de dialogue qui apparaît, collez la clé de validation, ou naviguez jusqu'au fichier.
 - f) Dans la boîte de dialogue *Activation*, naviguez jusqu'au fichier *validation.vk* sur la clé USB, puis cliquez sur **Envoyer**.
Le message *Votre licence a été activée avec succès* apparaît.
 - g) Cliquez sur **Télécharger la licence**, puis enregistrez la clé de licence.
Le nom de fichier par défaut est votre ID système suivi de *_Directory_License.lic*.
 - h) Copiez le fichier *_Directory_License.lic* sur la clé USB.
 - i) Éjectez la clé USB de l'ordinateur.
- 3 Activez votre licence :
 - a) Branchez la clé USB sur votre appareil.
 - b) Revenez à Server Admin.
 - c) Sur la page *Licence*, cliquez sur **Modifier**.
 - d) Dans la boîte de dialogue *Gestion de licences*, sélectionnez **Activation manuelle**.
 - e) Collez vos informations de licence à partir du fichier *License.lic* (que vous ouvrez dans un éditeur de texte), ou naviguez jusqu'au fichier *License.lic*, puis cliquez sur **Ouvrir**.
 - f) Cliquez sur **Activer**.

Rubriques connexes

[Activer votre licence Security Center sur un appareil](#), page 22

Activer System Availability Monitor

Pour surveiller la disponibilité et le bon fonctionnement du système sur GTAP, vous pouvez configurer System Availability Monitor pour la collecte de données concernant votre appareil et les envoyer au service de surveillance de l'état.

Avant de commencer

Pour recueillir et rapporter des informations sur l'état de votre appareil, vous devez générer un code d'activation sur [GTAP](#). Pour plus d'informations, voir [Générer des codes d'activation pour System Availability Monitor Agent](#) sur le TechDoc Hub.

Procédure

- 1 Ouvrez SV Control Panel.
- 2 Sur la page *Configuration*, cliquez sur **Configurer** dans la section *System Availability Monitor*.
- 3 Dans la fenêtre *Genetec System Availability Monitor Agent*, cliquez sur **Modifier**.
- 4 Vérifiez que la case **Les données seront recueillies et associées à mon système** est cochée.
- 5 Dans le champ **Code d'activation**, tapez le code pour votre appareil.
- 6 Cliquez sur **OK**.

Activer les fonctionnalités vidéo et de contrôle d'accès Security Center

L'Assistant d'installation de Security Center vous guide tout au long du processus de configuration des principales fonctionnalités de gestion vidéo et de contrôle d'accès.

À savoir

Les réglages que vous appliquez dans l'assistant peuvent être modifiés ultérieurement dans Config Tool.

S'applique à : Les appareils qui hébergent le rôle Répertoire, comme les appareils tout-en-un.

Procédure

- 1 Connectez-vous en tant qu'utilisateur Admin.

CONSEIL : Si votre mot de passe Security Center est différent du mot de passe d'administrateur Windows, connectez-vous à Security Center avec les identifiants spécifiés dans l'assistant de *configuration du tableau de bord Streamvault*.

L'Assistant d'installation de Security Center s'ouvre.

- 2 Lorsque vous avez lu la page de *présentation*, cliquez sur **Suivant**.

- 3 Sur la page de *Fonctionnalités disponibles*, sélectionnez les fonctionnalités qui vous intéressent, puis cliquez sur **Suivant**.

Les fonctionnalités de base sont activées par défaut. Vous pouvez ultérieurement activer et désactiver des fonctionnalités sur la page *Fonctionnalités* de la vue **Paramètres généraux** de la tâche **Système**.

REMARQUE : Si votre licence ne prend pas en charge une fonctionnalité, celle-ci n'apparaît pas dans la liste.

- 4 Sur la page *Sécurité des caméras*, spécifiez le nom d'utilisateur et mot de passe par défaut utilisés pour toutes vos caméras, puis cliquez sur **Suivant**.

CONSEIL : Pour renforcer la sécurité, sélectionnez **Utiliser HTTPS**.

- 5 Sur la page *Réglages de qualité des caméras*, configurez les options suivantes :

- **Résolution :**

- **Élevée :** 1280x720 ou plus
- **Standard :** Supérieur à 320x240 et inférieur à 1280x720
- **Faible :** 320x240 ou moins
- **Par défaut :** Réglages par défaut du fabricant


La caméra utilise toujours la résolution la plus élevée qu'elle prend en charge dans la catégorie sélectionnée. Si la caméra ne prend pas en charge une résolution de la catégorie sélectionnée, elle utilise la résolution la plus élevée de la catégorie précédente. Par exemple, si la caméra ne prend pas en charge une résolution élevée, elle utilise la résolution la plus élevée de la catégorie Standard.

Les réglages sur cette page peuvent être modifiés ultérieurement sur la page *Réglages par défaut des caméras* du rôle Archiveur.

- 6 Sur la page *Réglages d'enregistrement*, sélectionnez les réglages d'enregistrement par défaut que vous souhaitez appliquer à toutes les caméras.
 - **Désactivé** : L'enregistrement est arrêté.
 - **Continu** : Les caméras enregistrent en continu. Ce sont les paramètres par défaut.
 - **Sur mouvement / manuel** : Les caméras enregistrent en cas de déclenchement par une action (comme Démarrer l'enregistrement, Ajouter un signet ou Déclencher l'alarme), de détection de mouvement ou d'intervention manuelle d'un utilisateur.
 - **Manuel** : Les caméras enregistrent en cas de déclenchement par une action (comme Démarrer l'enregistrement, Ajouter un signet ou Déclencher l'alarme) ou d'intervention manuelle d'un utilisateur.

REMARQUE : Lorsque le réglage **Manuel** est utilisé, le mouvement ne déclenche pas d'enregistrement.

 - **Personnalisé** : Vous pouvez définir un horaire pour le déclenchement de l'enregistrement.
- 7 Cliquez sur **Suivant**.
- 8 Sur la page *Sécurité des unités de contrôle d'accès*, spécifiez le nom d'utilisateur et mot de passe par défaut pour toutes vos unités de contrôle d'accès, puis cliquez sur **Suivant**.
- 9 Sur la page *Titulaires de cartes*, sélectionnez la manière d'ajouter vos identifiants (cartes) et titulaires de cartes.
 - a) Spécifiez si vous souhaitez ajouter les titulaires de cartes (à la fermeture de l'assistant d'installation Security Center) à l'aide de la tâche *Gestion des titulaires de cartes* ou à l'aide de l'outil d'importation.
 - b) Cliquez sur **Suivant**.
- 10 Sur la page *Utilisateurs*, ajoutez des utilisateurs à votre système :
 - a) Entrez le nom d'utilisateur.
 - b) Sélectionnez le **Type d'utilisateur** :
 - **Opérateur** : Un opérateur peut utiliser la tâche *Surveillance*, afficher de la vidéo et gérer les visiteurs dans Security Desk.
 - **Rapports** : Un utilisateur des rapports peut utiliser l'application Security Desk et effectuer les tâches de base, à l'exclusion des tâches de RAPI AutoVu^{MC}. Un utilisateur doté des seuls privilèges de reporting ne peut pas visionner de vidéo, contrôler des appareils physiques ou signaler des incidents.
 - **Enquêteur** : Un enquêteur peut utiliser la tâche *Surveillance*, contrôler les caméras PTZ, enregistrer et exporter de la vidéo, ajouter des signets et incidents, utiliser les tâches d'investigation, gérer les alarmes et les visiteurs, ignorer les horaires de déverrouillage de portes, enregistrer les tâches, etc.
 - **Superviseur** : Un superviseur peut utiliser la tâche *Surveillance*, contrôler les caméras PTZ, enregistrer et exporter de la vidéo, ajouter des signets et incidents, utiliser les tâches d'investigation, gérer les alarmes et les visiteurs, ignorer les horaires de déverrouillage de portes, enregistrer les tâches, etc. Un superviseur peut également utiliser les tâches de maintenance, gérer les titulaires de cartes et les identifiants, modifier les champs personnalisés, définir les niveaux de risque, bloquer les caméras et utiliser le comptage d'individus.
 - **Approvisionnement** : Un utilisateur de provisionnement est doté de la plupart des privilèges de configuration, à l'exception des suivants : gestion des rôles, macros, utilisateurs, groupes d'utilisateurs, événements personnalisés, historiques d'activité, niveaux de risque et fichiers audio. L'utilisateur de provisionnement est généralement l'installateur du système.
 - **Opérateur AutoVu de base** : Ce type d'utilisateur est destiné aux opérateurs qui utilisent la RAPI AutoVu. Les utilisateurs AutoVu de base peuvent utiliser les tâches de RAPI, configurer des entités de RAPI, créer des règles de RAPI, surveiller les événements de RAPI, etc.
 - **Utilisateur Patroller** : Ce type d'utilisateur est destiné aux utilisateurs de Genetec Patroller^{MC} qui utilisent la RAPI AutoVu. L'utilisateur Patroller peut utiliser les tâches de RAPI, configurer les entités de RAPI, créer des règles de RAPI, surveiller des événements de RAPI, etc. Un utilisateur Patroller n'a pas accès aux autres applications Security Center, par exemple Config Tool et Security Desk. L'utilisateur Patroller ne peut pas modifier les rapports ni modifier le mot de passe Patroller.

- 11 Entrez et confirmez le **Mot de passe**, puis cliquez sur **Ajouter**.
Le nouvel utilisateur est ajouté à la liste des utilisateurs dans la partie droite de la boîte de dialogue. Pour supprimer un utilisateur, sélectionnez-le dans la liste et cliquez sur .
Vous pouvez modifier les profils des utilisateurs dans la vue **Utilisateurs** de la tâche *Gestion des utilisateurs*. Pour en savoir plus, voir le [Guide de l'administrateur Security Center](#) sur TechDoc Hub.
- 12 Cliquez sur **Suivant**.
- 13 Vérifiez les informations affichées sur la page *Résumé*, puis cliquez sur **Appliquer**, ou cliquez sur **Précédent** pour corriger d'éventuelles erreurs.
- 14 Sur la page *Conclusion*, cliquez sur **Redémarrer**.
Config Tool redémarre pour appliquer vos réglages.
REMARQUE : L'option **Ouvrir l'outil d'inscription d'unités à la fermeture de l'assistant** est sélectionnée par défaut. Vous pouvez décocher cette option et lancer l'outil d'inscription d'unités plus tard en cliquant sur le raccourci **Inscrire des caméras et contrôleurs** sur la page *Accueil* du SV Control Panel.

Lorsque vous avez terminé

[Ajoutez des unités à votre système](#) à l'aide de l'outil d'inscription d'unités.

Rubriques connexes

[Configurer les réglages par défaut des caméras](#), page 33

[Créer des horaires d'enregistrement personnalisés](#), page 35

[Page d'accueil de SV Control Panel](#), page 69

À propos de l'outil Inscription d'unités

L'Outil d'inscription d'unités vous permet de découvrir les unités IP (vidéo et contrôle d'accès) connectées à votre réseau selon leur fabricant et propriétés réseau (port de découverte, plage d'adresses IP, mot de passe, et ainsi de suite). Après avoir découvert une unité, vous pouvez l'ajouter à votre système.

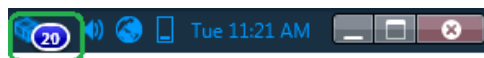
- L'outil Inscription d'unités est automatiquement lancé après l'*Assistant d'installation Security Center* si vous n'avez pas décoché l'option **Ouvrez l'outil d'inscription d'unités après la fermeture de l'assistant**.
- Lorsque vous ajoutez des unités de contrôle d'accès, seules les unités HID et Synergis^{MC} peuvent être inscrites avec l'outil d'inscription d'unités. Pour une description détaillée de l'inscription des unités Synergis, voir le *Guide de configuration de l'appareil Synergis^{MC}*.

Ouvrir l'Outil d'inscription d'unités

Vous disposez de trois façons d'ouvrir l'Outil d'inscription d'unités.

Procédure

- Procédez de l'une des manières suivantes :
 - Sur la page d'accueil de SV Control Panel, cliquez sur **+ Inscrire des caméras et contrôleurs**.
 - Sur la page d'accueil de SV Control Panel, cliquez sur l'icône **Config Tool**, puis cliquez sur **Tâches > Inscription d'unités**.
 - Sur la page d'accueil de SV Control Panel, cliquez sur l'icône **Config Tool**, puis cliquez sur l'icône **État de l'ajout d'unité** dans la zone de notification de Config Tool.




Configurer les réglages d'inscription des unités

Utilisez le bouton **Réglages et fabricants** de l'outil Inscription d'unités pour spécifier les fabricants à inclure lors de la recherche d'unités. Vous pouvez également configurer les réglages de découverte des unités, et spécifier le nom d'utilisateur et mot de passe des unités pour simplifier leur inscription.

Procédure

- 1 Sur la page d'accueil, cliquez sur **Outils > Inscription d'unités**.
- 2 Dans la boîte de dialogue *Inscription d'unités*, cliquez sur **Réglages et fabricants** ().
- 3 Utilisez l'option **Refuser l'authentification de base** pour activer ou désactiver l'authentification de base (unités vidéo uniquement). Cette option est utile si vous avez désactivé l'authentification de base dans le programme d'installation de Security Center, mais que vous devez l'activer pour effectuer la mise à jour du micrologiciel, ou pour inscrire une caméra qui ne prend en charge que l'authentification de base. Pour réactiver l'authentification de base, vous devez **désactiver** l'option **Refuser l'authentification de base**.
REMARQUE : Cette option est disponible uniquement pour les utilisateurs disposant de privilèges d'administrateur.
- 4 Cliquez sur **Ajouter un fabricant** () pour ajouter un fabricant à la liste des unités à découvrir.
 Pour supprimer un fabricant de la liste, sélectionnez-le et cliquez sur .

- 5 Configurez les paramètres individuels pour tous les fabricants que vous avez ajoutés. Pour ce faire, sélectionnez un fabricant et cliquez sur .


IMPORTANT : Vous devez saisir le bon nom d'utilisateur et mot de passe pour que l'unité soit correctement inscrite.

- 6 (Facultatif) Supprimez des unités de la liste des unités ignorées (voir [Supprimer des unités de la liste des unités ignorées](#), page 32).
- 7 Cliquez sur **Enregistrer**.

Ajouter des unités

Une fois que de nouvelles unités ont été découvertes, vous pouvez utiliser l'outil Inscription d'unités pour les ajouter à votre système.

Procédure

- 1 Sur la page d'accueil, cliquez sur **Outils > Inscription d'unités**.
- 2 Vous disposez de trois manières d'ajouter les unités nouvellement découvertes :
 - Ajoutez toutes les unités découvertes en même temps en cliquant sur le bouton **Ajouter tout**  en bas à droite de la boîte de dialogue.
 - Cliquez sur une seule unité dans la liste, puis cliquez sur **Ajouter** dans la colonne **État**.
 - Faites un clic droit sur une unité dans la liste, et cliquez sur **Ajouter ou Ajouter une unité**.

Lorsqu'une unité vidéo n'a pas le bon nom d'utilisateur et mot de passe, l'**État** de l'unité indique **Connexion incorrecte** et vous serez invité à saisir les bons identifiants lorsque vous ajouterez l'unité. Si vous souhaitez utiliser le même nom d'utilisateur et mot de passe pour toutes les caméras du système sélectionnez l'option **Enregistrer comme authentification par défaut pour tous les fabricants**.

Vous pouvez également ajouter une unité manuellement en cliquant sur le bouton **Ajout manuel** au bas de la boîte de dialogue *Outil inscription d'unités*.

REMARQUE :

- Pour les unités vidéo, si la caméra ajoutée est un codeur capable de gérer plusieurs flux, chaque flux ajouté apparaît avec *Caméra - n* ajouté au nom de la caméra, où *n* représente le numéro de flux. Pour une caméra IP qui ne fournit qu'un seul flux, le nom de la caméra n'est pas modifié.
- Si vous ajoutez une unité SharpV, par défaut, les unités de caméra incluent un certificat auto-signé qui utilise le nom commun SharpV (par exemple, SharpV12345). Pour ajouter la SharpV à l'Archiveur, vous devez générer un nouveau certificat (signé ou auto-signé) qui utilise l'adresse IP de la caméra au lieu du nom commun.

Effacer les unités ajoutées

Vous pouvez effacer les unités qui ont déjà été ajoutées au système afin qu'elles ne soient pas affichées à chaque fois que vous utilisez l'Outil d'inscription d'unités pour découvrir des unités.

À savoir

L'option **Effacement terminé** dans l'Outil d'inscription d'unités est permanente et ne peut pas être annulée.

Procédure

- 1 Ajoutez les unités découvertes de votre choix au système. Voir [Ajouter des unités](#), page 31.

- 2 Une fois que les unités ont été ajoutées, cliquez sur **Effacement terminé**.
Toute unité avec la mention **Ajouté** dans la colonne **État** est supprimée de la liste des unités découvertes.

Ignorer des unités

Vous pouvez choisir d'ignorer des unités afin qu'elles n'apparaissent pas dans la liste des unités découvertes de l'Outil d'inscription d'unités.

Procédure

- 1 Sur la page d'accueil, cliquez sur **Outils > Inscription d'unités**.
L'outil Inscription d'unités apparaît et dresse la liste des unités découvertes par le système.
- 2 Faites un clic droit sur une unité et sélectionnez **Ignorer**.
L'unité est supprimée de la liste et sera ignorée lorsque l'outil Inscription d'unités découvrira de nouvelles unités. Pour en savoir plus sur la suppression d'une unité de la liste des unités ignorées, voir [Supprimer des unités de la liste des unités ignorées](#), page 32.

Supprimer des unités de la liste des unités ignorées

Vous pouvez supprimer une unité de la liste des unités ignorées pour qu'elle ne soit plus ignorée lorsque l'Outil d'inscription d'unités lance la découverte.

Procédure

- 1 Sur la page d'accueil, cliquez sur **Outils > Inscription d'unités**.
- 2 Dans le coin supérieur droit de la boîte de dialogue *Inscription d'unités*, cliquez sur **Réglages et fabricants** (⚙️).
- 3 Cliquez sur **Unités ignorées** puis cliquez sur **Supprimer toutes les unités ignorées**, ou sélectionnez une seule unité et cliquez sur le bouton **Supprimer l'unité ignorée** (✖️).

Configurer les réglages par défaut des caméras

Dans *Réglages par défaut des caméras*, vous pouvez modifier les réglages d'enregistrement et de qualité vidéo par défaut appliqués à toutes les caméras contrôlées par l'Archiveur. Ces réglages sont définis initialement sur la page *Réglages de qualité des caméras* de l'assistant d'installation Security Center.

À savoir


Vous pouvez également appliquer des réglages vidéo et d'enregistrement à une caméra dans Config Tool en passant par l'onglet **Vidéo et enregistrement** de l'unité. Les réglages appliqués à une caméra individuelle prennent le pas sur les réglages appliqués dans l'assistant d'installation Security Center ou sur la page *Réglages par défaut des caméras*.

Procédure

- 1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Vidéo*.
- 2 Sélectionnez l'Archiveur à configurer, puis cliquez sur l'onglet **Réglages par défaut des caméras**.
- 3 Sous **Qualité vidéo (sur tous les Archiveurs)**, configurez les options suivantes :

- **Résolution :**
 - **Élevée :** 1280x720 ou plus
 - **Standard :** Supérieur à 320x240 et inférieur à 1280x720
 - **Faible :** 320x240 ou moins
 - **Par défaut :** Réglages par défaut du fabricant

La caméra utilise toujours la résolution la plus élevée qu'elle prend en charge dans la catégorie sélectionnée. Si la caméra ne prend pas en charge une résolution de la catégorie sélectionnée, elle utilise la résolution la plus élevée de la catégorie précédente. Par exemple, si la caméra ne prend pas en charge une résolution élevée, elle utilise la résolution la plus élevée de la catégorie Standard.

- 4 Sous **Enregistrement**, cliquez sur  pour ajouter un horaire.
Les horaires disponibles incluent :
 - Les horaires qui ont été créés à l'aide de la vue **Horaires** dans la tâche *Système*.
 - Un programme personnalisé, s'il a été créé dans l'assistant d'installation de Security Center.
- 5 Dans la liste déroulante **Mode**, sélectionnez un mode pour l'horaire d'enregistrement :
 - **Désactivé :** L'enregistrement est arrêté.
 - **Continu :** Les caméras enregistrent en continu. Ce sont les paramètres par défaut.
 - **Sur mouvement / manuel :** Les caméras enregistrent en cas de déclenchement par une action (comme Démarrer l'enregistrement, Ajouter un signet ou Déclencher l'alarme), de détection de mouvement ou d'intervention manuelle d'un utilisateur.
 - **Manuel :** Les caméras enregistrent en cas de déclenchement par une action (comme Démarrer l'enregistrement, Ajouter un signet ou Déclencher l'alarme) ou d'intervention manuelle d'un utilisateur.

REMARQUE : Lorsque le réglage **Manuel** est utilisé, le mouvement ne déclenche pas d'enregistrement.

 - **Personnalisé :** Vous pouvez définir un horaire pour le déclenchement de l'enregistrement.

6 Configurez les options suivantes :

- **Enregistrer l'audio** : Activez cette option si vous souhaitez enregistrer les données audio avec la vidéo. Une entité microphone doit être associée à vos caméras pour pouvoir utiliser cette option.
- **Archivage redondant** : Activez cette option si vous souhaitez autoriser le serveur principal et le serveur secondaire à enregistrer la vidéo en même temps. Ce réglage n'est effectif que si le basculement est configuré.
- **Nettoyage automatique** : Désactivez cette option si vous souhaitez supprimer la vidéo au bout d'un certain nombre de jours. La vidéo est supprimée que le stockage de l'Archiveur soit saturé ou non.
- **Durée d'enregistrement avant un événement** : Utilisez le curseur pour définir le nombre de secondes que vous souhaitez enregistrer avant un événement. Ce tampon est enregistré lorsque l'enregistrement démarre, assurant la capture de ce qui a déclenché l'enregistrement.
- **Durée d'enregistrement après mouvement** : Spécifiez le nombre de secondes que vous souhaitez enregistrer après un événement de mouvement. L'utilisateur ne peut pas arrêter l'enregistrement durant ce laps de temps.
- **Durée par défaut de l'enregistrement manuel** : Spécifiez le nombre de minutes que vous souhaitez enregistrer lorsqu'un utilisateur déclenche l'enregistrement. L'utilisateur peut interrompre l'enregistrement à tout instant durant ce laps de temps. Cette valeur est également utilisée par l'action Démarrer l'enregistrement lorsque la durée d'enregistrement par défaut est sélectionnée.

7 Cliquez sur **Appliquer**.

8 Si vous souhaitez appliquer les nouveaux réglages à toutes les caméras existantes, cliquez sur **Oui**.


Rubriques connexes

[Activer les fonctionnalités vidéo et de contrôle d'accès Security Center](#), page 27

Créer des horaires d'enregistrement personnalisés


Créez des horaires d'enregistrement personnalisés dans l'assistant d'installation du Security Center pour que vos caméras utilisent différents modes d'enregistrement selon les plages horaires.

Procédure

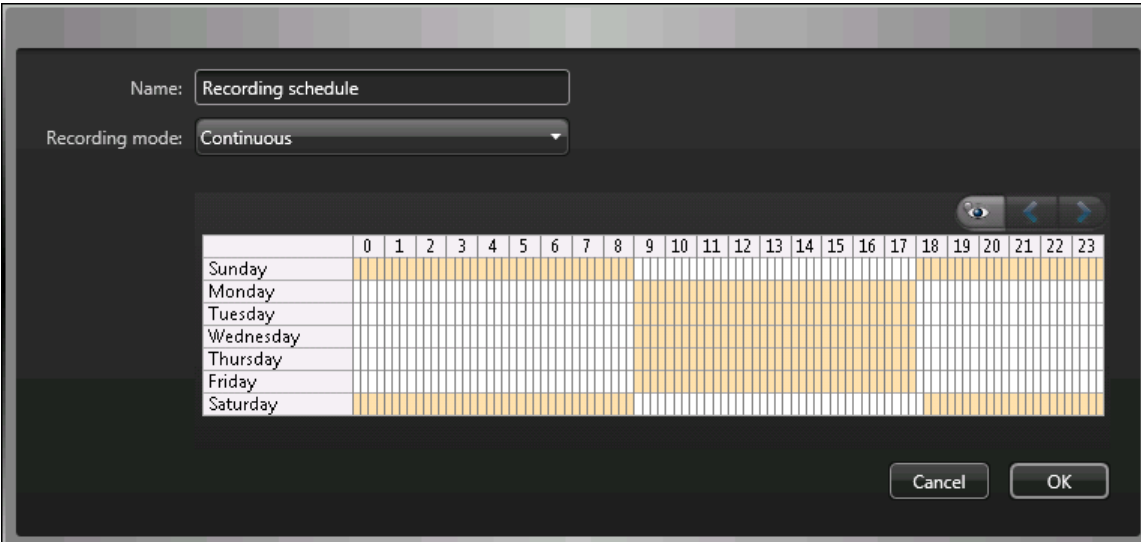
- 1 Sur la page *Réglages d'enregistrement*, cliquez sur  sous **Horaire d'enregistrement**.
- 2 Nommez le nouvel horaire.
- 3 Dans la liste **Modes d'enregistrement**, sélectionnez l'une des options suivantes :
 - **Désactivé** : L'enregistrement est arrêté.
 - **Continu** : Les caméras enregistrent en continu. Ce sont les paramètres par défaut.
 - **Sur mouvement / manuel** : Les caméras enregistrent en cas de déclenchement par une action (comme Démarrer l'enregistrement, Ajouter un signet ou Déclencher l'alarme), de détection de mouvement ou d'intervention manuelle d'un utilisateur.
 - **Manuel** : Les caméras enregistrent en cas de déclenchement par une action (comme Démarrer l'enregistrement, Ajouter un signet ou Déclencher l'alarme) ou d'intervention manuelle d'un utilisateur.
- 4 Pour chaque jour de la semaine, spécifiez une plage horaire pour l'enregistrement :
 - Cliquez et glissez pour sélectionner une plage horaire.
 - Faites un clic droit et faites glisser pour effacer une plage horaire.
 - Utilisez les touches fléchées pour parcourir la frise chronologique de 24 heures.

REMARQUE : Lorsque le réglage **Manuel** est utilisé, le mouvement ne déclenche pas d'enregistrement.

- **Personnalisé** : Vous pouvez définir un horaire pour le déclenchement de l'enregistrement.

CONSEIL : Pour basculer en mode haute résolution où chaque bloc représente 1 minute, cliquez sur .

L'exemple suivant montre un horaire d'enregistrement en continu de 18:00 à 9:00 les week-ends, et de 9:00 à 17:00 les jours de la semaine.



Rubriques connexes

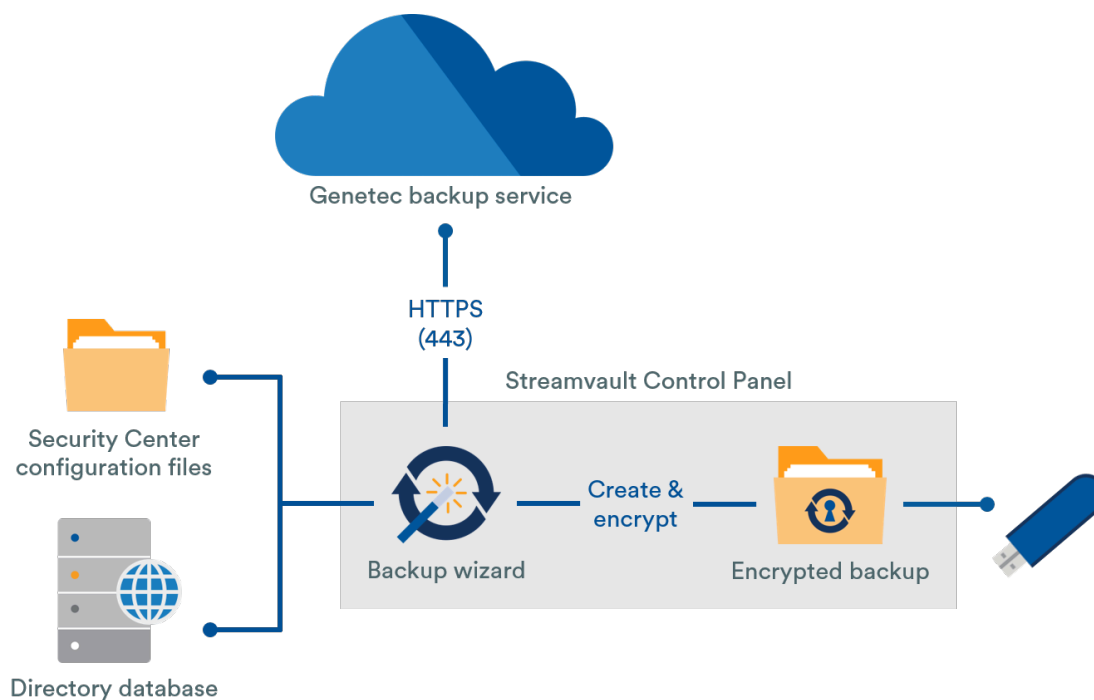
[Activer les fonctionnalités vidéo et de contrôle d'accès Security Center](#), page 27

À propos de la sauvegarde et de la restauration

Vous pouvez utiliser SV Control Panel pour sauvegarder la base de données du Répertoire et vos fichiers de configuration. Vous pouvez les restaurer plus tard vers le même ID système en cas de panne système ou de mise à niveau du matériel.

Fonctionnement de la sauvegarde et de la restauration dans SV Control Panel

Vous pouvez créer des sauvegardes de la base de données du Répertoire et des fichiers de configuration, et les stocker dans le cloud ou en local. Le diagramme d'architecture suivant illustre le fonctionnement de la sauvegarde dans SV Control Panel :



Avantages de la sauvegarde et restauration

- Vous pouvez facilement restaurer l'une des cinq sauvegardes dans le cloud ou une de vos sauvegardes en local vers le même ID système à l'aide de l'assistant *Restoration*.
- Tous les fichiers de sauvegarde peuvent être chiffrés.
- Le système se bloque après cinq tentatives de connexion infructueuses.
- Il n'est pas nécessaire d'être inscrit au programme Genetec^{MC} Advantage pour utiliser cette fonctionnalité.

Limitations de la sauvegarde et restauration

- Vos fichiers de licence, archives vidéo et autres bases de données ne sont pas inclus dans les sauvegardes.
- Vous ne pouvez pas restaurer une sauvegarde vers une version antérieure de Security Center. Par exemple, vous ne pouvez pas restaurer une sauvegarde d'un système Security Center 5.10 vers un système Security Center 5.9.
- Vous ne pouvez pas restaurer les fichiers de configuration entre versions majeures de Security Center. Par exemple, vous ne pouvez pas restaurer les fichiers de configuration d'une sauvegarde d'un système Security Center 5.9 vers un système Security Center 5.10.

Rubriques connexes

[Sauvegarder la base de données du Répertoire](#), page 37

[Restaurer la base de données du Répertoire](#), page 38

Sauvegarder la base de données du Répertoire

Vous pouvez utiliser la fonction de sauvegarde et de restauration pour sauvegarder en toute sécurité la base de données et les fichiers de configuration de Répertoire. La sauvegarde et la restauration facilitent la configuration de votre système après une mise à niveau matérielle et peuvent restaurer vos configurations après une panne du système.

Avant de commencer

Les conditions suivantes sont requises :

- Security Center 5.9 ou une version ultérieure est installé.
- Genetec Server est en cours d'exécution.
- Votre licence est valable et activée.

À savoir

-
- Seuls les administrateurs peuvent effectuer une sauvegarde, et toutes les sauvegardes dans le cloud doivent être authentifiées.

Procédure

- 1 Dans SV Control Panel, cliquez sur l'onglet **Configuration**.
- 2 Sous *Sauvegarder/restaurer le Répertoire et les configurations*, cliquez sur **Assistant de sauvegarde > Suivant**.
- 3 Sur la page *Méthode de sauvegarde*, sélectionnez **Dans le cloud** ou **En local**, puis cliquez sur **Suivant**.
 - Si vous avez sélectionné **Cloud**, procédez de la manière suivante :
 - a. Sur la page *Authentification*, entrez votre ID système ou vos identifiants GTAP pour authentifier la sauvegarde.
REMARQUE : Vos identifiants ne vous seront plus demandés pour les sauvegardes suivantes.
 - b. Sur la page *Sécurité*, sélectionnez une des options suivantes :
 - **Autoriser Genetec à gérer ma sécurité :** Il est inutile de fournir un mot de passe. Le service de sauvegarde dans le cloud de Genetec Inc. chiffre vos données.
 - **Utiliser mon propre mot de passe :** Créez et mémorisez votre propre mot de passe pour chiffrer vos fichiers de sauvegarde.
IMPORTANT : Si vous perdez ou oubliez votre mot de passe, Genetec Inc. ne pourra pas le récupérer.
 - Si vous avez sélectionné **Local**, procédez de la manière suivante :
 - a. Sur la page *Dossier de destination*, donnez un nom à la sauvegarde et naviguez jusqu'au dossier où vous souhaitez la stocker.
 - b. Sur la page *Sécurité*, créez un mot de passe pour chiffrer votre fichier de sauvegarde. Vous pouvez également sélectionner **Ne pas chiffrer ma sauvegarde**, mais cette option est déconseillée.
- 4 Suivez les étapes de l'assistant pour terminer votre sauvegarde.

Rubriques connexes

[À propos de la sauvegarde et de la restauration](#), page 36

[Restaurer la base de données du Répertoire](#), page 38

Restaurer la base de données du Répertoire

Si vous avez sauvegardé la base de données du Répertoire et vos fichiers de configuration à l'aide de la sauvegarde et restauration dans SV Control Panel, vous pouvez restaurer vos fichiers de sauvegarde vers le même ID système. Les fichiers de sauvegarde peuvent être restaurés en cas de défaillance du système ou de mise à niveau du matériel.

Avant de commencer

Les conditions suivantes sont requises :

- Security Center 5.9 ou une version ultérieure est installé.
- Genetec Server est en cours d'exécution.
- Votre licence est valable et activée.

À savoir

- Si vous sauvegardez vos fichiers dans le cloud, vous pouvez restaurer une de vos cinq dernières sauvegardes vers le même ID système.
- Si vous sauvegardez vos fichiers en local, vous pouvez restaurer la sauvegarde de votre choix vers le même ID système.
- Si vous avez créé votre propre mot de passe pour chiffrer les fichiers de sauvegarde, vous devez le saisir pour restaurer vos fichiers.

Procédure

- 1 Dans SV Control Panel, cliquez sur l'onglet **Configuration**.
- 2 Sous *Sauvegarder/restaurer le Répertoire et les configurations*, cliquez sur **Assistant de restauration** > **Suivant**.
- 3 Sur la page *Méthode de restauration*, sélectionnez **Dans le cloud** ou **En local**.
Si vous avez choisi **Dans le cloud**, entrez votre ID système ou vos identifiants GTAP sur la page *Authentification*, selon le choix que vous avez effectué pour authentifier la sauvegarde. Si vous utilisez vos identifiants GTAP, un code d'activation vous est envoyé par e-mail.
- 4 Sur la page de *Sélection de la sauvegarde*, sélectionnez le fichier que vous souhaitez restaurer sur votre système.
- 5 Si vous avez créé un mot de passe dans le cadre du processus de sauvegarde, vous devez le saisir sur la page *Restaurer*.
- 6 Suivez les étapes de l'assistant pour terminer le processus de restauration.

Rubriques connexes

[Sauvegarder la base de données du Répertoire](#), page 37

[À propos de la sauvegarde et de la restauration](#), page 36

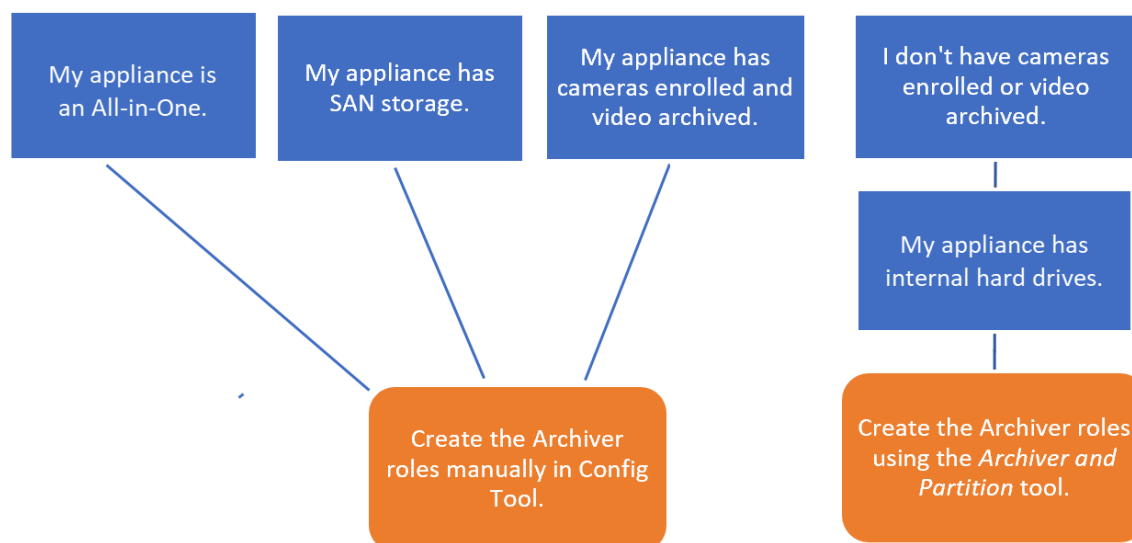
Choisir la méthode de création des rôles Archiveur et des partitions

Pour configurer votre appareil en fonction du nombre de caméras prévu et de la bande passante disponible, vous devez créer un nombre suffisant de rôles Archiveur. Selon le type et l'état de votre appareil, deux méthodes sont disponibles :

- [Utiliser l'outil Rôles Archiveur et partitions.](#)
- [Créer manuellement des partitions et des rôles Archiveur.](#)

Sélection de la méthode adaptée à votre situation

Aidez-vous de l'ordinogramme suivant pour choisir la méthode à utiliser :



À propos de l'outil Rôles Archiveur et partitions

Vous pouvez accéder à l'outil Rôles Archiveur et partitions dans SV Control Panel. L'outil calcule le nombre de rôles Archiveur dont vous aurez besoin en fonction du nombre de caméras que vous comptez déployer et de l'estimation de la bande passante qu'elles utiliseront.

Cet outil n'est disponible que sur les modèles Streamvault^{MC} qui embarquent un disque dur. Si vous configurez un dispositif de stockage externe tel qu'un SAN sur un appareil série Streamvault^{MC} SV-7000EX, suivez les étapes à la section [Ajout manuel de rôles et de partitions Archiveur](#), page 41.

Lorsque l'outil crée les partitions, tous les volumes en local à l'exception du disque C: sont effacés, et les rôles Archiveur et les caméras inscrites existants sont supprimés de Security Center. Par conséquent, si votre appareil a des caméras et des enregistrements vidéo que vous souhaitez conserver, [ajoutez manuellement les partitions et les rôles Archiveur](#).

Ajouter des rôles Archiveur dans SV Control Panel

Utilisez l'outil Rôles Archiveur et partitions pour ajouter suffisamment de rôles Archiveur pour gérer le trafic vidéo escompté. Cet outil est disponible sur les appareils Archiveur séries Streamvault^{MC} 1000, 2000 et 4000.

Avant de commencer

- Sélectionnez la méthode adaptée pour créer les rôles Archiveur et les partitions.
- Faites une sauvegarde des données importantes stockées sur le disque que vous comptez partitionner.
ATTENTION : L'outil Rôles Archiveur et partitions peut supprimer les données existantes, y compris la configuration du rôle Archiveur et tous les fichiers sur le disque D:.

Procédure

- 1 Dans SV Control Panel, cliquez sur l'onglet **Configuration**.
- 2 Sous *Partitions et rôles Archiveur*, cliquez sur **Configurer**.
La boîte de dialogue *Rôles Archiveur et partitions* apparaît.
- 3 Pour configurer le nombre de rôles Archiveur et de partitions, sélectionnez l'une des options suivantes :
 - Pour demander à l'outil de calculer le nombre de rôles, le nombre de partitions et la taille des partitions nécessaires, sélectionnez **Scénario recommandé**. Entrez le nombre de caméras que vous comptez déployer et le débit estimé de chaque caméra.
 - Pour spécifier le nombre de rôles et de partitions Archiveur à créer, sélectionnez **Scénario personnalisé**. Saisissez le nombre de rôles Archiveur, le nombre de partitions et la taille des partitions.
Le nombre de partitions doit être un multiple du nombre de rôles Archiveur.

ATTENTION : Les fichiers sur le disque que vous partitionnez sont supprimés.

4 Cliquez sur **Créer les partitions et les rôles**.

Archiver Roles and Partitions

An Archiver role can support:

- 300 cameras
- Throughput of 500 Mbps
- Partitions with a maximum size of 30 TB

Your model (SV-1000-R14-72T-8-210) supports:

- 400 cameras
- 400 Mbps

Suggested scenario

Number of cameras: 0 Number of roles: 0

Camera throughput: 0 Number of partitions: 0

Size of partitions (TB): 0.00

Custom scenario

Number of roles: 0 Total disk space (TB): 0.02

Number of partitions: 0 Used disk space (TB): 0.00

Size of partitions (TB): 0 Free disk space (TB): 0.02

Create partitions/roles

5 Dans la fenêtre *Avertissement*, cochez la case pour confirmer que vous souhaitez continuer.

6 Cliquez sur **OK**.

La fenêtre *Résultat* apparaît et affiche le nom et l'emplacement des rôles Archiveur et des partitions. Chaque rôle Archiveur est automatiquement affecté à une lettre de lecteur.

Ajout manuel de rôles et de partitions Archiveur

Pour effectuer la configuration initiale de votre appareil tout-en un SV-7000EX ou SV-300E Streamvault^{MC}, vous pouvez créer les partitions manuellement. Vous pouvez également ajouter manuellement des rôles Archiveur à un appareil qui contient déjà des données, afin de ne pas les perdre.

Avant de commencer

Choisissez une méthode de création des partitions sur votre appareil.

À savoir

Formater un volume supprime les données sur la partition. Pour conserver les données, réduisez la taille du volume, puis créez d'autres volumes.

Procédure

- 1 Si des caméras sont déjà inscrites sur l'appareil ou si ce dernier contient des archives vidéo ou des données de contrôle d'accès, procédez comme suit :
 - a) [Sauvegardez la base de données du Répertoire à l'aide de SV Control Panel.](#)
 - b) Créez un *Rapport de configuration de caméras* pour capturer un instantané de votre configuration actuelle. Pour plus d'informations, voir [Afficher les réglages de caméras](#) sur le TechDoc Hub.
- 2 Créez les volumes nécessaires pour les rôles Archiveur que vous prévoyez de créer sur l'appareil.
 - Sur les appareils qui se connectent avec un stockage SAN, tels que les appareils série SV-7000EX, créez un numéro d'unité logicielle (LUN) pour chaque rôle Archiveur.
 - Sur les appareils disposant de lecteurs de stockage internes, tels que SV-1000E, SV-2000E et SV-4000E, utilisez l'outil *Gestion des disques* de Windows pour configurer les volumes.
- 3 Dans Security Center, créez un rôle Archiveur :
 - a) Sur la page d'accueil de Config Tool, ouvrez la tâche *Système*, puis cliquez sur la vue **Rôles**.
 - b) Cliquez sur **Ajouter une entité** et sélectionnez **Archiveur**.
L'assistant de configuration de rôle Archiveur apparaît.
 - c) Sur la page *Informations spécifiques*, donnez un nom à la **base de données** du rôle Archiveur, puis cliquez sur **Suivant**.
Chaque rôle Archiveur doit avoir une base de données dédiée.


The screenshot shows the 'Creating a role: Archiver' wizard with the 'Specific info' tab selected. On the left, there is a sidebar with four tabs: 'Specific info' (active), 'Basic information', 'Creation summary', and 'Entity creation outcome'. The main area contains two dropdown menus: 'Database server' set to '(local)\SQLEXPRESS' and 'Database' set to 'Archiver5'. Both dropdowns have a refresh icon to their right.

- d) Dans la section **Informations de base**, saisissez le **Nom de l'entité** et cliquez sur **Suivant**.
Il est recommandé de nommer la base de données du rôle Archiveur d'après le nom de l'entité.

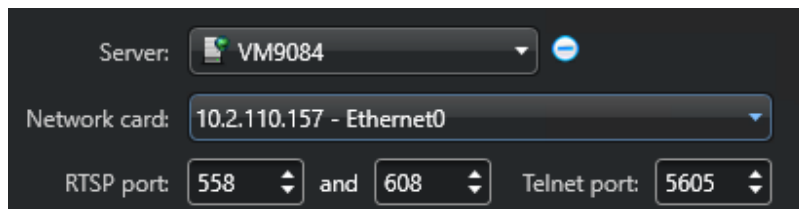
The screenshot shows the 'Creating a role: Archiver' wizard with the 'Basic information' tab selected. The sidebar now has 'Basic information' as the active tab. The main area contains the instruction 'Fill in the following fields. The entity description is optional.' followed by two input fields: 'Entity name' with the value 'Archiver5' and an empty 'Entity description' field.

- e) Vérifiez que les informations affichées sur la page *Résumé de l'opération* sont correctes, puis cliquez sur **Créer**.

4 Configurez le rôle Archiveur.

- a) Dans le navigateur d'entités, sélectionnez votre nouveau rôle Archiveur et cliquez sur **Ressources**.
- b) Cliquez sur  pour développer la section *Serveur* et sélectionnez une carte interface réseau (NIC) dans la liste **Carte réseau**.

Tous les rôles Archiveur doivent utiliser la même carte réseau.




- c) Sous *Enregistrement*, sélectionnez ou créez un **Groupe de disques** ou un **Emplacement réseau** pour le rôle Archiveur.

Chaque rôle Archiveur a besoin d'un emplacement d'enregistrement dédié. Si Archiveur A écrit sur les disques A, B et C, alors Archiveur B doit écrire sur les disques D, E et F. Un rôle peut posséder plusieurs partitions, mais deux rôles différents ne doivent jamais utiliser la même partition.

- d) Cliquez sur **Appliquer**.

5 Répétez les étapes 3 et 4 pour créer chaque rôle Archiveur.

6 Ajoutez vos caméras à leur rôle Archiveur désigné :

- a) Sur la page d'accueil de Config Tool, ouvrez la tâche *Vidéo*.
- b) Dans le navigateur d'entités, sélectionnez le rôle Archiveur auquel vous souhaitez affecter la caméra et cliquez sur **Unité vidéo** .
- c) Dans la boîte de dialogue qui s'ouvre, saisissez les informations requises concernant la caméra et cliquez sur **OK**.

REMARQUE : L'ajout des caméras peut prendre quelques secondes. Si le rôle ne parvient pas à ajouter une caméra durant ce laps de temps, un état d'échec est affiché, puis la caméra est supprimée.

- d) Cliquez sur **Appliquer**.

Chiffrer le lecteur du SE

Pour sécuriser votre appareil Streamvault^{MC} et votre mot de passe administrateur Windows, vous devez chiffrer le lecteur du système d'exploitation (C:) avec BitLocker.

Avant de commencer

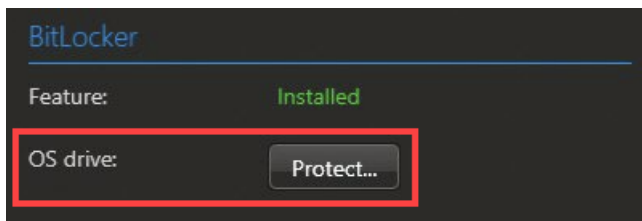
Lorsque le lecteur du SE est chiffré avec BitLocker, la clé de déchiffrement est enregistrée sur une puce TPM (Trusted Platform Module) située sur la carte système de l'appareil Streamvault. Si le lecteur du système d'exploitation devait être retiré ou si la carte système devait être remplacée, les informations sur le lecteur du SE seraient perdues. Le disque du SE ne pourrait pas accéder à la clé de déchiffrement sur le module de plateforme sécurisée. Vous pouvez créer une clé de récupération qui peut être utilisée pour déchiffrer le lecteur dans ces scénarios. Sans clé de récupération, l'appareil doit être recréé et le logiciel réinstallé.

Le disque de stockage sert principalement à stocker les archives vidéo et n'est pas chiffré avec BitLocker. Vous pouvez utiliser les fonctionnalités Security Center pour chiffrer les archives vidéo au repos.

REMARQUE : La fonctionnalité BitLocker est disponible à partir de SV Control Panel 3.2. La fonctionnalité intègre également une mise à jour du profil de renforcement pour les [appareils avec fonctions de gestion du renforcement](#). Vous pouvez obtenir cette mise à jour en téléchargeant le [Service Streamvault](#) depuis Genetec^{MC} Update Service (GUS) ou GTAP. Pour profiter pleinement de la fonctionnalité BitLocker, nous vous encourageons à chiffrer le disque du SE et à mettre à jour le profil de renforcement, le cas échéant.

Procédure

- 1 Dans le SV Control Panel, cliquez sur l'onglet **Sécurité**.
- 2 Dans la section *BitLocker*, cliquez sur **Protéger** à côté du champ **Lecteur du SE**.



REMARQUE : Si le disque du SE est déjà chiffré, le bouton **Protéger** est remplacé par un état *Protégé*.

- 3 Lorsque vous êtes invité à activer BitLocker, cliquez sur **Oui**.
Le disque du SE est chiffré, la clé de déchiffrement est enregistrée sur le module de plateforme sécurisée et une clé de récupération est créée. Par défaut, la clé de récupération est enregistrée sur un disque de données fixe. S'il n'existe aucun disque de données fixe, comme sur un poste de travail, la clé de récupération est enregistrée sur une clé USB.
IMPORTANT : Si vous enregistrez la clé de récupération sur un disque de données fixe, veillez à déplacer la clé vers un emplacement sécurisé et à la supprimer de l'appareil.
- 4 (Facultatif) S'il n'y a pas de lecteur de données fixe ou de clé USB, vous pouvez choisir de poursuivre le chiffrement sans créer de clé de récupération. Procédez de l'une des manières suivantes :
 - Cliquez sur **Oui** pour continuer sans créer de clé de récupération.
 - Cliquez sur **Non** pour annuler le chiffrement.

REMARQUE : Si vous choisissez de ne pas créer de clé de récupération, vous pouvez en créer une plus tard. Pour en savoir plus, voir [Création d'une clé de récupération](#), page 45.

Création d'une clé de récupération

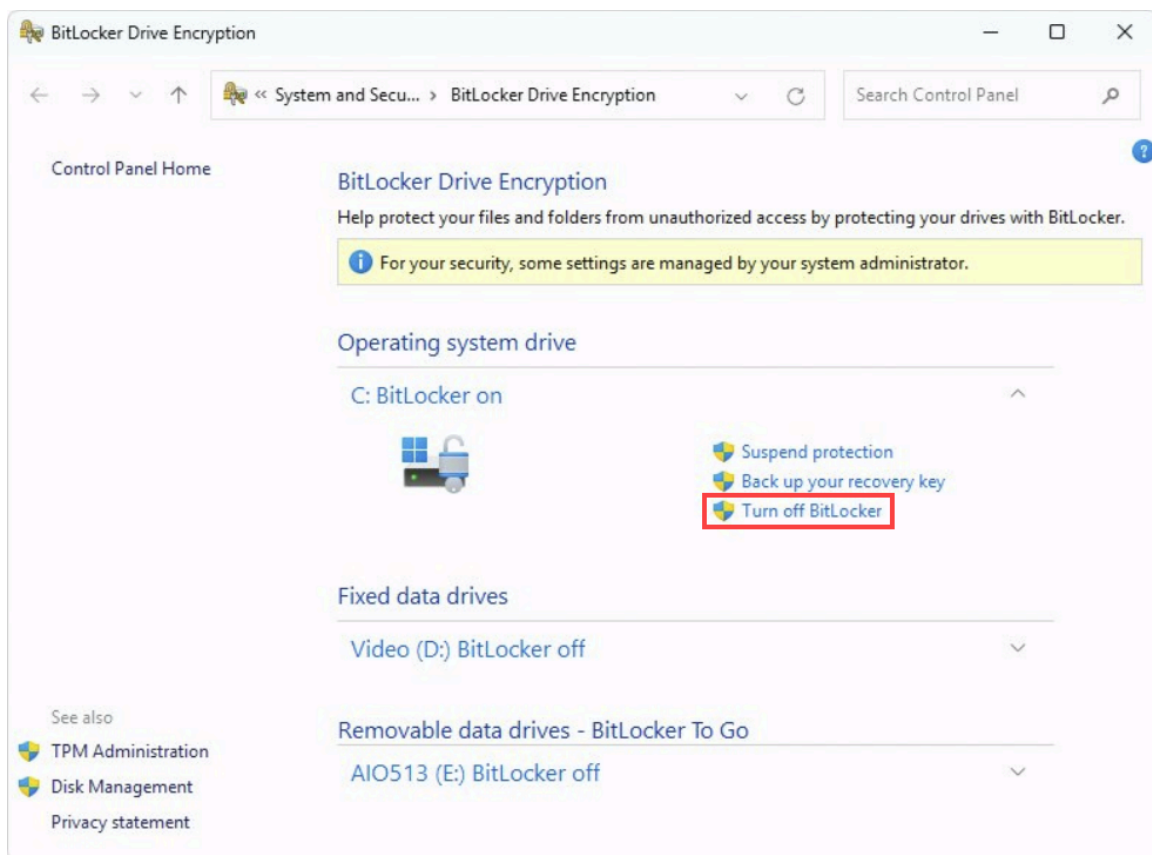
Si vous avez chiffré le lecteur du SE sur votre appareil Streamvault^{MC} avec BitLocker, mais que vous n'avez pas enregistré de clé de récupération, vous pouvez en créer une avec le chiffrement de lecteur BitLocker Windows.

À savoir

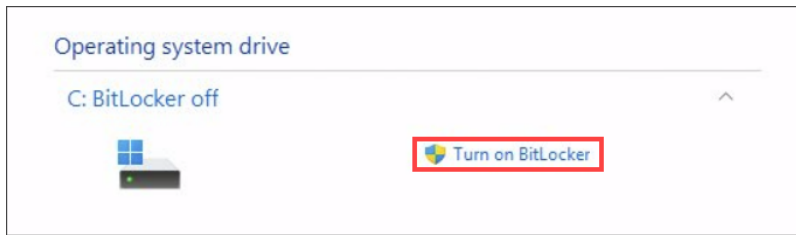
Cette procédure part du principe que vous avez chiffré le lecteur du SE via le SV Control Panel.

Procédure

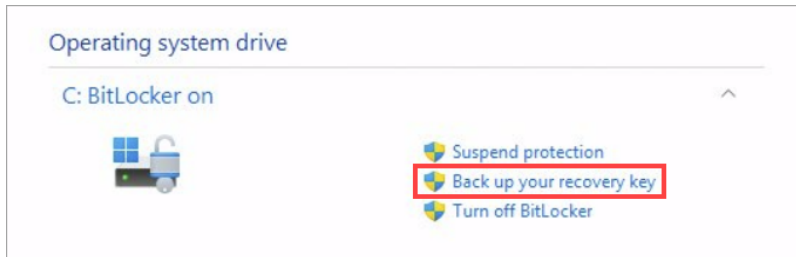
- 1 Dans le menu Démarrer de Windows, tapez **BitLocker** et sélectionnez **Gérer BitLocker** dans les résultats.
La fenêtre *Chiffrement de lecteur BitLocker*. Tous les lecteurs connectés à l'appareil sont affichés.
- 2 Dans la section *Disque du système d'exploitation*, cliquez sur **Désactiver BitLocker** et attendez que le lecteur du SE soit déchiffré. Ce processus prend plusieurs minutes.



- 3 Une fois le lecteur du SE déchiffré, cliquez sur **Activer BitLocker** et attendez que le lecteur du SE soit à nouveau chiffré avec BitLocker.



- 4 Une fois que le lecteur du SE est chiffré, cliquez sur **Sauvegarder votre clé de récupération** à côté du lecteur du SE (C:).

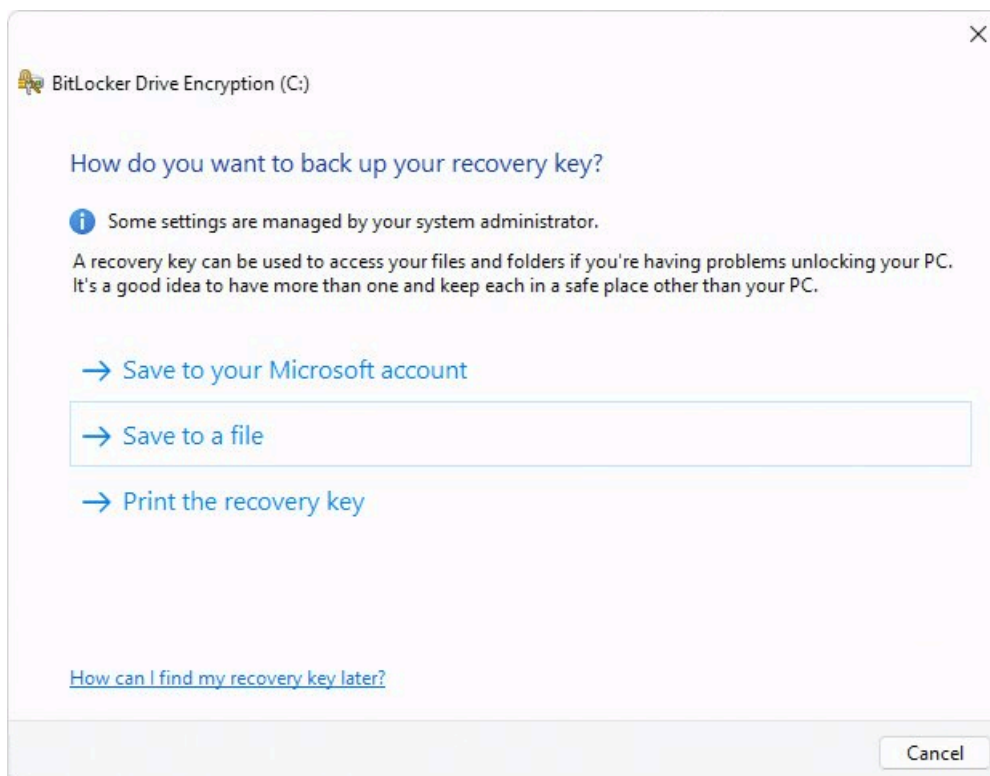


L'assistant *Chiffrement de lecteur BitLocker* s'ouvre.

5 Choisissez la manière dont vous souhaitez sauvegarder votre clé de récupération :

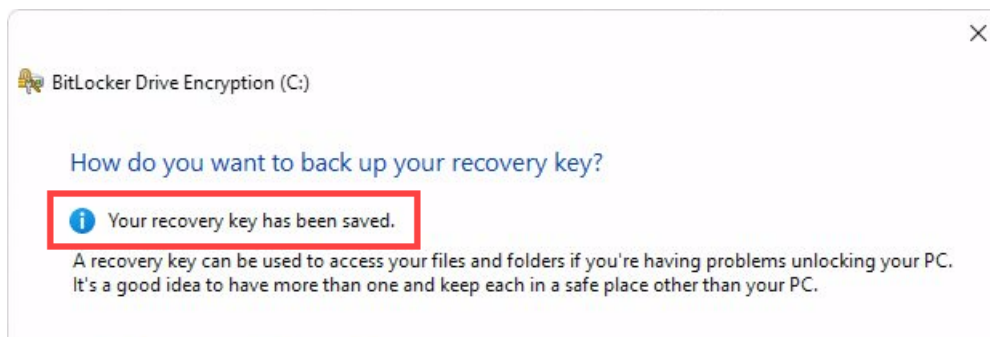
- **Sauvegarder sur votre compte Microsoft** : Sauvegardez votre clé de récupération dans la *bibliothèque de clés de récupération* de votre compte Microsoft.
- **Sauvegarder dans un fichier** : Sauvegardez votre clé de récupération sous forme de fichier texte sur un lecteur de données fixe non chiffré sur l'appareil ou sur une clé USB.
- **Imprimer la clé de récupération** : Imprimez une copie papier de votre clé de récupération.

REMARQUE : Si vous sélectionnez **Enregistrer dans un fichier**, vérifiez qu'un lecteur de données fixe ou une clé USB est disponible pour enregistrer la clé de récupération.



6 Si vous enregistrez la clé de récupération dans un fichier, sélectionnez l'emplacement où vous souhaitez sauvegarder la clé et cliquez sur **Enregistrer**.

Vous êtes notifié que la clé de récupération a bien été sauvegardée.



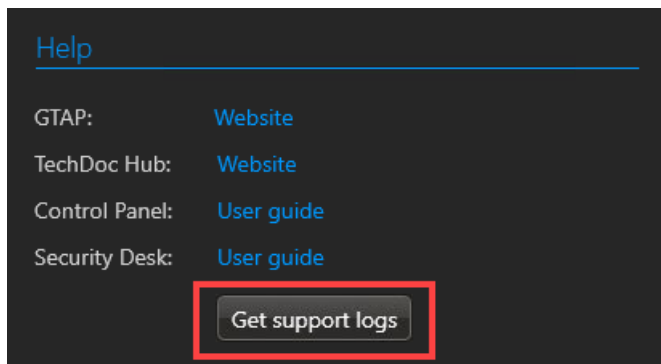
7 Cliquez sur **Terminer** pour quitter l'assistant.

Collecte des journaux d'assistance

Le centre d'assistance technique de Genetec^{MC} (GTAC) peut utiliser vos journaux Streamvault^{MC} et d'autres journaux d'application pour résoudre les problèmes sur votre appareil. Vous pouvez télécharger ces journaux d'assistance depuis le SV Control Panel.

Procédure

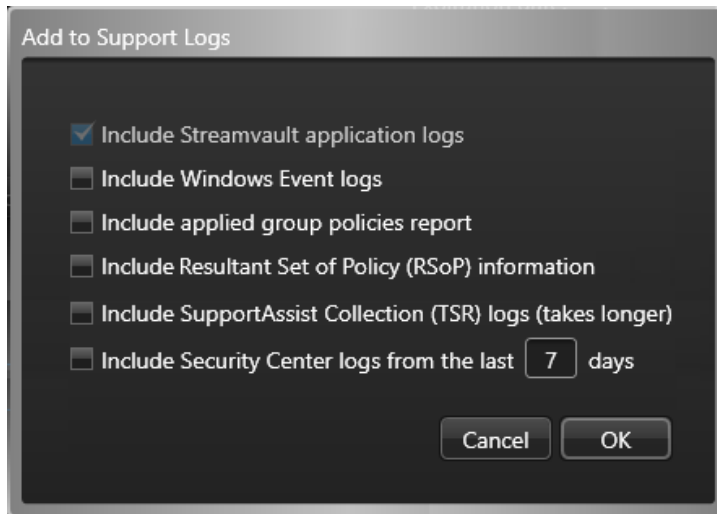
- 1 Dans le SV Control Panel, cliquez sur l'onglet **À propos**.
- 2 Dans la section *Aide*, cliquez sur **Obtenir les journaux d'assistance**.



- 3 Dans la boîte de dialogue *Ajouter aux journaux d'assistance* qui apparaît, sélectionnez les journaux que vous souhaitez télécharger :
 - **Journaux d'application Streamvault** : Ces journaux comprennent les fichiers journaux Cylance, OEM, policy, Softwire et SV Control Panel. Cette option est sélectionnée par défaut et ne peut pas être effacée.
 - **Les journaux d'événements Windows** : Ces journaux comprennent les événements d'application, de sécurité et système Windows.
 - **Rapport Stratégies de groupe appliquées** : Ce rapport concerne les systèmes qui font partie d'un domaine. Le rapport répertorie tous les objets de stratégie de groupe (GPO) actuellement appliqués, qu'ils soient appliqués au niveau local ou au niveau du domaine.
 - **Informations sur le jeu de stratégie résultant (RSOP)** : Ce rapport HTML contient tous les réglages système configurés par le biais de stratégies de groupe. Pour les systèmes non connectés à un domaine, cette option est sélectionnée par défaut. Pour les systèmes connectés à un domaine, cette option est désactivée par défaut, car le rapport contient des informations sensibles, comme le nom de domaine, le nom d'hôte de l'appareil, etc.
 - **Journaux SupportAssist collection (TSR)** : Ces journaux concernent les systèmes qui peuvent créer une collection SupportAssist, également appelée Rapport d'assistance technique (TSR). Les serveurs Dell PowerEdge, tels que les serveurs Streamvault des gammes 1000, 2000, 4000 et 7000, peuvent

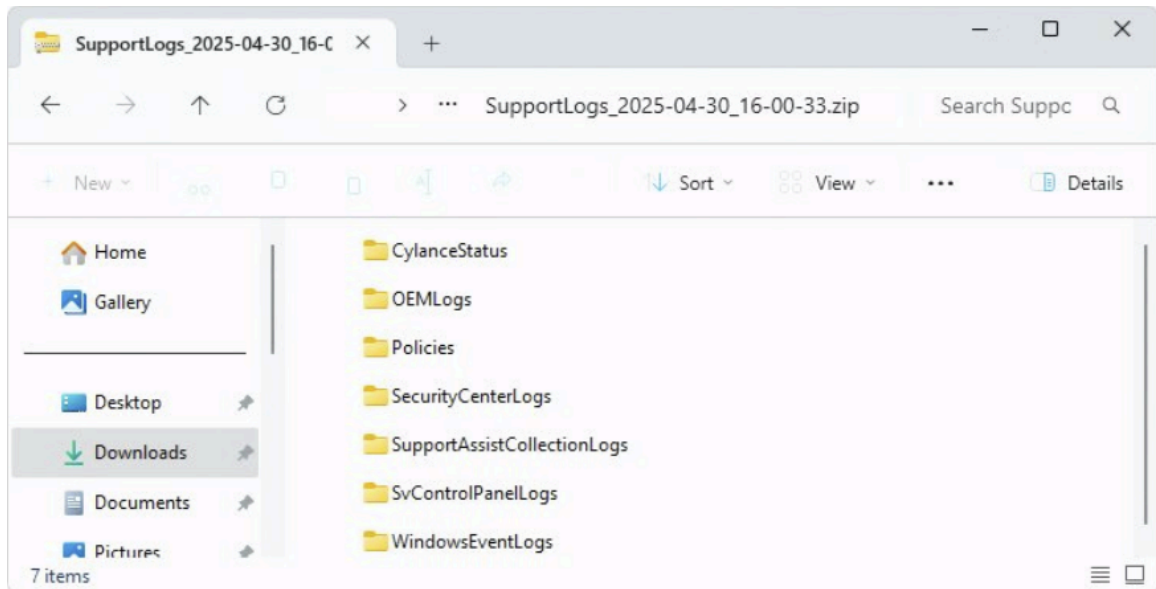
créer des collections SupportAssist. Cette option n'est disponible que pour les serveurs Streamvault qui prennent en charge iDRAC.

- **Journaux Security Center des X derniers jours** : Par défaut, les journaux Security Center des 7 derniers jours sont collectés. Entrez le nombre de jours de votre choix.



- 4 Cliquez sur **OK**.
- 5 Dans la boîte de dialogue *Rechercher un dossier*, sélectionnez le dossier dans lequel vous souhaitez enregistrer vos journaux et cliquez sur **OK**.

Vos journaux d'assistance sont enregistrés dans un dossier **.zip**.



Prise en main du module externe Streamvault Maintenance

La prise en main vous présente le module externe Streamvault Maintenance et décrit la procédure de configuration du module externe.

Cette section aborde les sujets suivants:

- ["À propos du module externe Streamvault Maintenance "](#), page 51
- ["Téléchargement et installation du module externe",](#) page 52
- ["Privilèges Genetec Streamvault",](#) page 53
- [" Création du rôle de module externe ",](#) page 55
- ["Configuration de l'entité de surveillance de matériel Streamvault",](#) page 56
- ["Configurer une entité Gestionnaire Streamvault",](#) page 60
- [" À propos de l'onglet Gestion ",](#) page 63
- ["Analyser l'état de fonctionnement d'un appareil Streamvault",](#) page 64
- ["Colonnes du volet de rapport de la tâche Matériel Streamvault.",](#) page 65
- ["Créer des mécanismes événement-action pour les dysfonctionnements de Streamvault",](#) page 66

À propos du module externe Streamvault Maintenance

Le module externe Streamvault^{MC} Maintenance sert à surveiller l'état de vos appareils Streamvault^{MC} et à veiller à ce que vous soyez notifié en cas de problème.

REMARQUE : Ce guide s'applique au le module externe Streamvault Maintenance 2.0.

Le module externe Streamvault Maintenance inclut les composants suivants :

- **Rôle Streamvault :** rôle module externe qui sert à exécuter l'entité Matériel ou Gestionnaire. Un rôle est requis pour chaque appareil Streamvault que vous devez surveiller.
- **Surveillance de Matériel Streamvault^{MC} :** entité servant à définir les configurations d'alerte pour chaque appareil Streamvault.
- **Gestionnaire Streamvault^{MC} :** entité servant à contrôler les configurations d'un groupe d'appareils Streamvault. Vous ne pouvez créer qu'une seule instance de Gestionnaire Streamvault.
- **Matériel Streamvault^{MC} :** tâche de rapport dans Security Center qui vous permet d'afficher la liste des dysfonctionnements qui affectent vos appareils Streamvault.

La configuration de l'entité module externe porte sur les réglages suivants :

- **Configurations d'alerte :** sert à spécifier les types d'**Événements**, les niveaux de **Gravité** et les types de **Notifications** qui affectent les alertes concernant l'état de fonctionnement de vos serveurs Streamvault.
- **Destinataires des e-mails :** permet de sélectionner les utilisateurs et groupes d'utilisateurs qui reçoivent les e-mails de notification.
- **Identifiants de gestion à distance :** sert à contrôler la création des profils d'utilisateurs dans iDRAC.
- **Intégration d'Integrated Dell Remote Access Controller (iDRAC) (iDRAC) :** (pour les modèles Streamvault qui prennent en charge iDRAC) : utilisé pour exercer un contrôle plus précis sur la gestion des identifiants. Cette fonctionnalité est disponible sur l'onglet **Gestion** du module externe.

Pour plus d'informations sur l'iDRAC, voir <https://www.dell.com/en-us/lp/dt/open-manage-idrac>.

IMPORTANT :

- Pour les systèmes équipés de serveurs iDRAC, le micrologiciel iDRAC doit être à la version 6.0 ou ultérieure.
- Pour les appareils prenant en charge iDRAC, le module externe Streamvault Maintenance accède aux données de fonctionnement à l'aide d'une connexion interne, à condition que le logiciel iDRAC Service Module (iSM) de Dell soit installé. iSM est installé par défaut sur les modèles prenant en charge iDRAC.

Si iSM n'est pas disponible, le module externe utilise une communication hors bande avec l'iDRAC. Dans ce cas, une connexion réseau doit exister entre le port dédié à iDRAC et au moins un port LAN si vous n'utilisez pas le partage de ports. Le port dédié à iDRAC est désactivé par défaut. Pour en savoir plus, reportez-vous au document suivant : <https://www.dell.com/support/kbdoc/en-ca/000177212/dell-poweredge-how-to-configure-the-idrac9-and-the-lifecycle-controller-network-ip>.

Téléchargement et installation du module externe

Pour intégrer le module externe Streamvault^{MC} Maintenance dans Security Center, vous devez installer le module externe sur le serveur de Répertoire, sur les serveurs Streamvault^{MC} que vous souhaitez surveiller et sur tous les postes sur lesquels vous voulez configurer le module externe.

Avant de commencer

Assurez-vous qu'une version compatible de Security Center est installée. Pour obtenir des informations, reportez-vous à la section [Modules externes pris en charge dans Security Center](#) sur TechDoc Hub.

À savoir

- **BONNE PRATIQUE** : Installez le rôle Streamvault sur chaque serveur que vous souhaitez surveiller.
- **IMPORTANT** : Vérifiez que le module iDRAC de chaque serveur est connecté à votre réseau et peut communiquer avec le système hôte. Par défaut, le module iDRAC utilise le même port LAN que le système hôte, et obtient une adresse IP par DHCP.
- **IMPORTANT** : Avant de continuer, vérifiez que le module iDRAC a été mis à jour vers la version 6.00 ou ultérieure du micrologiciel et que le BIOS du serveur a été mis à jour vers la dernière version.
- Le module externe n'est pris en charge que sur les serveurs qui exécutent le logiciel Security Center Server.
- **REMARQUE** : Le [module externe Streamvault Maintenance](#) est préinstallé sur tous les serveurs Streamvault compatibles. Il suffit donc à la plupart des utilisateurs de créer les rôles et les entités dans Security Center. Si votre serveur a été livré avant la disponibilité du module externe ou si vous avez désinstallé le module externe, procédez de la manière suivante pour l'installer.

Procédure

- 1 Ouvrez la page [Téléchargements de produits](#).
- 2 Sous **Recherche de téléchargements**, sélectionnez votre version de Security Center.
- 3 Dans la section *Modules externes Genetec*, téléchargez le pack de votre produit.
- 4 Exécutez le fichier .exe, puis décompactez le fichier.
Par défaut, le fichier est décompressé dans C:\Genetec.
- 5 Ouvrez le dossier décompressé, faites un clic droit sur le fichier *setup.exe*, et sélectionnez **Exécuter en tant qu'administrateur**.
- 6 Suivez les instructions d'installation.
- 7 Sur la dernière page de l'*Assistant d'installation*, cliquez sur **Terminer**.
IMPORTANT : L'option **Redémarrer Genetec^{MC} Server** est sélectionnée par défaut. Vous pouvez la décocher si vous ne voulez pas redémarrer Genetec^{MC} Server immédiatement. Toutefois, vous devez redémarrer Genetec Server pour terminer l'installation.
- 8 Fermez puis ouvrez toute instance de Config Tool et Security Desk.

Privilèges Genetec Streamvault

Pour utiliser les tâches *Surveillance de matériel* et *Gestionnaire* liées à l'appareil Streamvault^{MC}, les privilèges requis doivent être affectés aux comptes utilisateur.

Configuration des privilèges utilisateur pour Streamvault

Les privilèges par défaut sont affectés à certains groupes d'utilisateurs, comme les administrateurs.

Dans la tâche *Gestion des utilisateurs* de Config Tool, vous pouvez configurer ou modifier les privilèges des utilisateurs ou groupes d'utilisateurs sur la page *Privilèges* de l'utilisateur ou du groupe.

Pour en savoir plus sur la hiérarchie et l'affectation des privilèges, voir le [Guide de l'administrateur Security Center](#) et le [Guide de renforcement de Security Center](#) sur le TechDoc Hub.

REMARQUE : Pour la liste de tous les privilèges Security Center disponibles, voir la feuille de calcul [Privilèges Security Center](#). Vous pouvez trier et filtrer cette liste en fonction de vos besoins.

Privilèges du rôle de module externe Streamvault

Les privilèges du rôle de module externe Streamvault accordent l'accès aux tâches *Surveillance de matériel* et *Gestionnaire* Streamvault.

Par défaut, les administrateurs disposent de tous les privilèges. Si vous créez un compte utilisateur depuis un autre modèle de privilèges, le compte utilisateur nécessite les privilèges du rôle de module externe Streamvault suivants pour Config Tool dans Streamvault.

Sous-catégorie de privilèges	Inclut des privilèges pour	Actions pouvant être effectuées
Surveillance de matériel	Modifier les surveillances Matériel	<ul style="list-style-type: none"> • Modifier les configurations d'alertes • Modifier les destinataires d'e-mails • Modifier les identifiants de gestion à distance • Modifier les paramètres de ports
	Ajouter des surveillances Matériel	Créer une nouvelle entité de surveillance de matériel et l'affecter à un serveur Streamvault
	Supprimer des surveillances Matériel	Supprimer une entité de surveillance de matériel existante
	Afficher les surveillances Matériel	Afficher la configuration d'une surveillance de matériel
Gestionnaire	Modifier le gestionnaire	<ul style="list-style-type: none"> • Modifier les configurations d'alertes par lots • Modifier les destinataires d'e-mails par lots
	Ajouter un gestionnaire	Créer l'entité de gestionnaire et l'affecter à un serveur Streamvault

Sous-catégorie de privilèges	Inclut des privilèges pour	Actions pouvant être effectuées
	Supprimer le gestionnaire	Supprimer l'entité de gestionnaire
	Afficher le gestionnaire	Afficher la configuration du gestionnaire

Création du rôle de module externe

Avant de pouvoir configurer et utiliser le module externe, vous devez créer le rôle module externe Streamvault^{MC} Maintenance dans Config Tool.

Avant de commencer

[Téléchargez et installez le module externe.](#)

À savoir

Le module externe Streamvault Maintenance contient deux rôles module externe :

- **Surveillance de matériel Streamvault^{MC}** : L'entité de surveillance Matériel Streamvault^{MC} sert à surveiller l'état de vos appareils Streamvault^{MC} et à veiller à ce que vous soyez notifié en cas de problème. Une surveillance Matériel Streamvault^{MC} par appareil Streamvault^{MC} est requise.
- **Gestionnaire Streamvault^{MC}** : L'entité Gestionnaire Streamvault^{MC} sert à contrôler les configurations d'alerte pour un groupe d'entités Agent Streamvault^{MC}. Un seul Gestionnaire Streamvault^{MC} est autorisé par système.
- **REMARQUE** : Si les serveurs de Répertoire sont des machines virtuelles ou des serveurs non-Streamvault, créez un rôle pour ces serveurs qui si vous souhaitez utiliser l'entité Gestionnaire.

Procédure

- 1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Modules externes*.
- 2 Dans la tâche *Modules externes*, cliquez sur **Ajouter une entité** (+) et sélectionnez **Module externe**.
L'assistant création de module externe apparaît.
- 3 Sur la page *Informations spécifiques*, sélectionnez le serveur qui héberge le rôle de module externe et le type de module externe, puis cliquez sur **Suivant**.
Si votre système n'utilise pas de serveurs d'extension, l'option **Serveur** n'est pas affichée.
- 4 Sur la page *Informations de base*, spécifiez les informations sur le rôle :
 - a) Entrez le **Nom de l'entité**.
 - b) Entrez la **Description de l'entité**.
 - c) Sélectionnez la **Partition** pour le rôle module externe.
Si votre système n'utilise pas de serveur d'extension, l'option **Partition** n'est pas affichée. Les partitions sont de groupes logiques qui servent à contrôler la visibilité des entités. Seuls les utilisateurs qui sont membres de la partition peuvent afficher ou modifier le rôle.
 - d) Cliquez sur **Suivant**.
- 5 Sur la page *Résumé de l'opération*, vérifiez les informations, puis cliquez sur **Créer** ou sur **Précédent** pour apporter des modifications.
Une fois que le rôle a été créé, le message suivant est affiché : L'opération s'est déroulée avec succès.
- 6 Cliquez sur **Fermer**.

Lorsque vous avez terminé

- [Configurez l'entité de surveillance de matériel Streamvault.](#)
- [Configurez l'entité Gestionnaire Streamvault.](#)

Configuration de l'entité de surveillance de matériel Streamvault

Vous pouvez configurer une entité de surveillance de matériel Streamvault^{MC} pour surveiller le fonctionnement d'un appareil Streamvault^{MC} et configurer l'envoi de notifications en cas de problème.

Avant de commencer

- Inscrivez vos appareils Streamvault.
 - [Créez le rôle de module externe Streamvault.](#)
- IMPORTANT :** Une surveillance de matériel Streamvault est automatiquement créée sur chaque serveur Streamvault qui héberge un rôle Streamvault. Si l'entité de surveillance de matériel n'est pas présente dans votre système après la création du rôle, vous devez créer la surveillance de matériel manuellement. La surveillance de matériel ne peut être exécutée que sur un serveur Streamvault.

À savoir

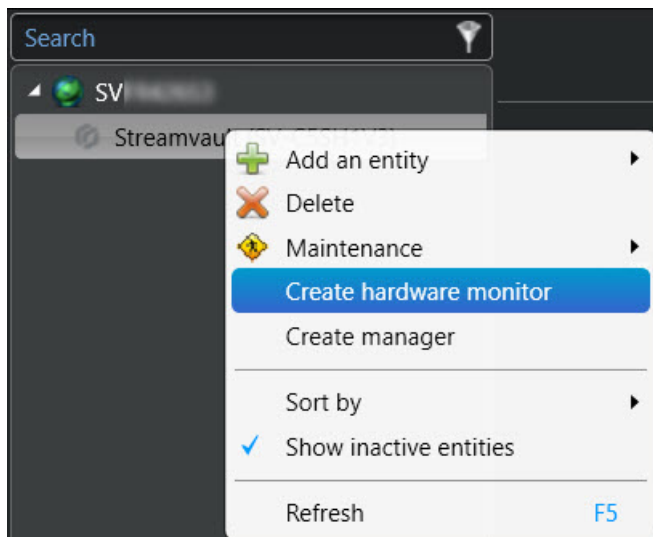
Les options de configuration sont différentes selon que vous avez des serveurs compatibles iDRAC ou d'autres serveurs non iDRAC.

- [Configuration d'un serveur compatible iDRAC.](#)
- [Configuration d'un serveur non-iDRAC.](#)

Procédure

Pour configurer un serveur compatible iDRAC :

- 1 Dans Config Tool, ouvrez la tâche *Modules externes* et cliquez sur le rôle module externe Streamvault.
- 2 Faites un clic droit sur le rôle module externe Streamvault, puis cliquez sur **Créer surveillance de matériel**.



- 3 Sur l'onglet **Identité**, donnez un nom à la surveillance de matériel Streamvault dans le champ **Nom**.
- 4 Sélectionnez l'onglet **Général**.
- 5 (Facultatif) Si vous avez créé une entité Gestionnaire Streamvault pour votre système, cochez la case **Utiliser les réglages du gestionnaire** pour utiliser les paramètres du profil de configuration d'alerte du gestionnaire Streamvault.

- 6 Dans la section *Profil de configuration d'alerte*, cochez la case **La surveillance de matériel gère les configurations d'alerte iDRAC** pour gérer les configurations d'alerte via la surveillance de matériel Streamvault.
- 7 Cochez les cases correspondant aux événements, aux niveaux **Événements**, **Gravité** et aux types **Notifications** que vous souhaitez inclure dans cette surveillance de matériel Streamvault.

Events	Severity			Notification	
	Critical	Warning	Information	Email	Event
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cooling	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CPU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Memory	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Networking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Power	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Storage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- 8 Dans la section *Destinataires des e-mails*, sélectionnez les utilisateurs et groupes d'utilisateurs qui seront notifiés par e-mail si les conditions spécifiées dans la section *Profil de configuration d'alerte* sont réunies.

Email recipients
<input type="checkbox"/> Admin
<input checked="" type="checkbox"/> Administrators No email configured for this group
<input type="checkbox"/> AutoVu
<input type="checkbox"/> AutoVu operators
<input type="checkbox"/> Patroller
<input type="checkbox"/> Patroller users

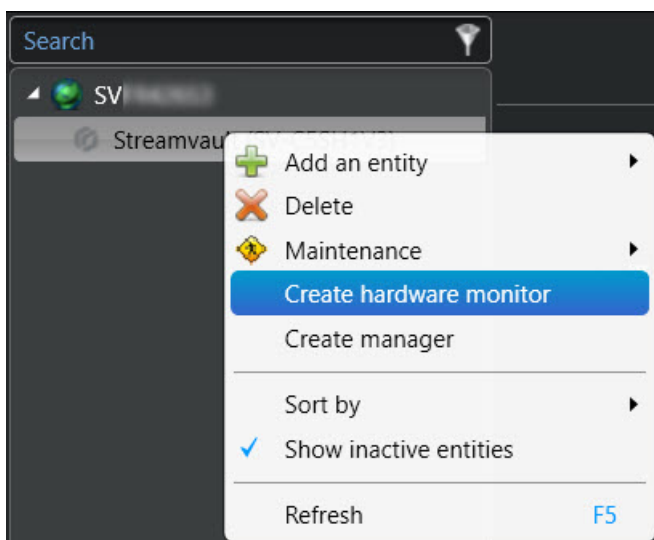
- 9 Dans la section *Identifiants de gestion à distance*, effectuez l'une des opérations suivantes :
 - Cochez la case **La surveillance de matériel gère les comptes iDRAC** pour gérer les identifiants directement via le module externe.
 - Décochez la case **La surveillance de matériel gère les comptes iDRAC** pour utiliser iDRAC afin de contrôler la création des utilisateurs et des mots de passe.
- 10 (Facultatif) Si vous décochez la case **La surveillance de matériel gère les comptes iDRAC**, allez dans l'onglet **Gestion** et configurez les identifiants directement dans iDRAC.

- 11 (Facultatif) Dans la section *Paramètres*, vous pouvez définir le **port entrant** par défaut (65115) sur la valeur de votre choix. Pour en savoir plus, voir [Ports par défaut utilisés par Streamvault](#), page 4.

- 12 Cliquez sur **Appliquer**.

Pour configurer un serveur non-iDRAC :

- 1 Dans Config Tool, ouvrez la tâche *Modules externes* et cliquez sur le rôle module externe Streamvault.
- 2 Faites un clic droit sur le rôle module externe Streamvault, puis cliquez sur **Créer surveillance de matériel**.



- 3 Sur l'onglet **Identité**, donnez un nom à la surveillance de matériel Streamvault dans le champ **Nom**.
- 4 Sélectionnez l'onglet **Général**.
- 5 (Facultatif) Si vous avez créé une entité Streamvault manager pour votre système, cochez la case **Utiliser les paramètres du gestionnaire** pour utiliser les paramètres du profil de configuration des alertes du gestionnaire Streamvault.
- 6 Dans la section *Profil de configuration d'alerte*, cochez les cases correspondant aux types **Événements** et **Notification** que vous souhaitez appliquer aux instances de module externe Streamvault Maintenance contrôlées par le Gestionnaire Streamvault.
- 7 Sous **Configuration**, définissez le **seuil d'usure** du disque SSD à partir duquel vous souhaitez recevoir une notification vous informant du remplacement prochain du SSD.

- 8 Dans la section *Destinataires des e-mails*, sélectionnez les utilisateurs et groupes d'utilisateurs qui seront notifiés par e-mail si les conditions spécifiées dans la section *Profil de configuration d'alerte* sont réunies.

☐ Use manager settings

Alert configuration profile

Events	Notification	Event	Status	Configuration
	Email	Event		
Predictive drive failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Normal	Threshold % <input type="text" value="90"/>
SSD wear	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Normal	
Offline drive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Email recipients

- ☐ Admin
- ☒ Administrators No email configured for this group
- ☐ AutoVu
- ☐ AutoVu operators
- ☐ Patroller
- ☐ Patroller users

- 9 Cliquez sur **Appliquer**.

Rubriques connexes

[À propos de l'onglet Gestion](#), page 63

Configurer une entité Gestionnaire Streamvault

Vous pouvez configurer une entité Gestionnaire Streamvault^{MC} pour contrôler les configurations d'alerte d'un groupe de surveillances Matériel Streamvault^{MC} de manière centralisée. Vous pouvez également configurer les notifications qui doivent être envoyées en cas de survenue d'un problème. L'utilisation de l'entité Gestionnaire Streamvault est facultative.

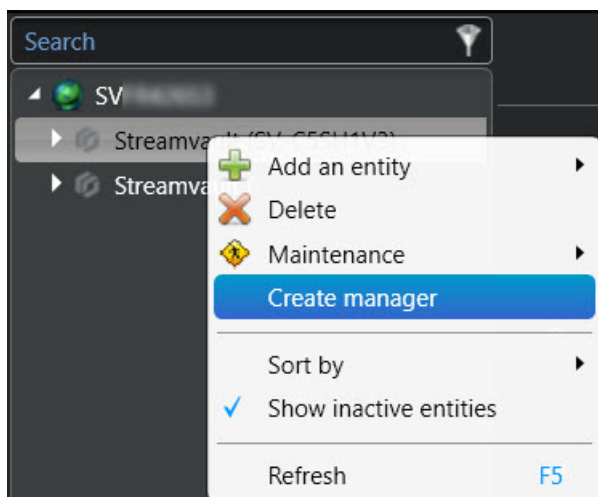
Avant de commencer

- Inscrivez vos appareils Streamvault^{MC}.
- [Créez le rôle de module externe Streamvault.](#)

REMARQUE : L'entité Gestionnaire Streamvault peut être exécutée sur n'importe quel serveur (Streamvault ou non Streamvault) ou n'importe quelle machine virtuelle de votre système Security Center. Une seule entité Gestionnaire Streamvault peut être ajoutée au système.

Procédure

- 1 Dans Config Tool, ouvrez la tâche *Modules externes* et cliquez sur le rôle module externe Streamvault.
- 2 Faites un clic droit sur le rôle module externe Streamvault, puis cliquez sur **Créer un gestionnaire**.






- 3 Sélectionnez l'entité Gestionnaire Streamvault et cliquez sur l'onglet **Général**.
Les sections suivantes sont affichées :
 - La section *Profil de configuration d'alerte iDRAC* gère les serveurs compatibles iDRAC dans votre système.
 - La section *Profil de configuration d'alerte non iDRAC* est utilisée pour gérer d'autres serveurs non-iDRAC dans le système.

Les deux sections sont toujours affichées, que vous ayez un système iDRAC ou non.

- 4 (Le cas échéant) Dans la section *Profil de configuration d'alerte iDRAC*, configurez ce qui suit :
- Pour gérer les configurations d'alerte iDRAC via la surveillance de matériel Streamvault du serveur sélectionné, cochez la case **La surveillance de matériel gère les configurations d'alerte iDRAC**.
 - Cochez les cases correspondant aux niveaux **Événements** et **Gravité** et aux types **Notifications** que vous souhaitez appliquer aux instances de module externe Streamvault Maintenance contrôlées par le Gestionnaire Streamvault.

iDRAC alert configuration profile

☒ Hardware monitor manages iDRAC alert configurations

Events	Severity			Notification	
	 Critical	 Warning	 Information	Email	Event
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cooling	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
CPU	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Memory	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Networking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Power	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Storage	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Hardware monitors using Streamvault™ manager configuration

Streamvault (SV-C5SH1V3) - Streamvault™ hardware monitor

REMARQUE : Les surveillances de matériel dont la configuration est définie par le Gestionnaire Streamvault sont répertoriées sous **Surveillances de matériel utilisant la configuration du Gestionnaire Streamvault^{MC}**. Les surveillances de matériel qui utilise ses propres configurations sont répertoriées sous **Surveillances de matériel utilisant une configuration personnalisée**.

- 5 (Le cas échéant) Dans la section *Profil de configuration d'alerte non iDRAC*, configurez ce qui suit :
- Cochez les cases correspondant aux types **Événements** et **Notification** que vous souhaitez appliquer aux instances de module externe Streamvault Maintenance contrôlées par le Gestionnaire Streamvault.
 - Sous **Configuration**, définissez le **seuil d'usure** du disque SSD à partir duquel vous souhaitez recevoir une notification vous informant du remplacement prochain du SSD.

Events	Notification		Configuration
	Email	Event	
Predictive drive failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Threshold % <input type="text" value="90"/>
SSD wear	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Offline drive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Hardware monitors using Streamvault™ manager configuration

Streamvault (SVFR426S3) - Streamvault™ hardware monitor

REMARQUE : Les surveillances de matériel dont la configuration est définie par le Gestionnaire Streamvault sont répertoriées sous **Surveillances de matériel utilisant la configuration du Gestionnaire Streamvault^{MC}**. Les surveillances de matériel qui utilise ses propres configurations sont répertoriées sous **Surveillances de matériel utilisant une configuration personnalisée**.

- 6 Dans la section *Destinataires des e-mails*, sélectionnez les utilisateurs et groupes d'utilisateurs qui seront notifiés par e-mail si les conditions spécifiées dans la section **Profil de configuration d'alerte iDRAC** ou **Profil de configuration d'alerte non iDRAC** sont réunies.

Email recipients

- ☐ Admin
- ☒ Administrators No email configured for this group
- ☐ AutoVu
- ☐ AutoVu operators
- ☐ Patroller
- ☐ Patroller users

- 7 Cliquez sur **Appliquer**.

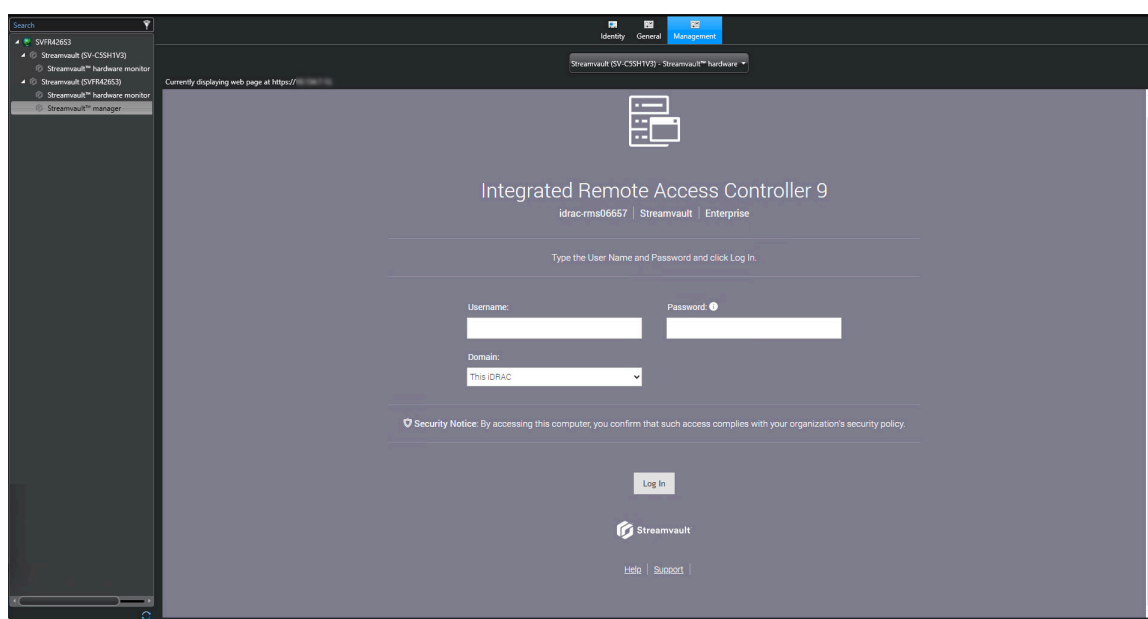
À propos de l'onglet Gestion

L'onglet **Management** affiche une page web iDRAC à travers laquelle vous pouvez configurer et gérer les informations d'identification de votre serveur iDRAC. Vous pouvez également trouver plus d'informations sur votre serveur iDRAC et configurer d'autres options qui ne sont pas disponibles via l'interface utilisateur du module externe Streamvault^{MC}.

Vous pouvez accéder à l'onglet **Gestion** via la surveillance de matériel Streamvault^{MC} de tout serveur compatible iDRAC ou via le gestionnaire Streamvault^{MC}.

Si vous accédez à l'onglet **Gestion** via le gestionnaire Streamvault, un menu déroulant apparaît en haut de la page. Vous pouvez l'utiliser pour passer d'un serveur iDRAC à un autre au lieu de devoir passer manuellement d'une surveillance de matériel à une autre. Chaque serveur iDRAC possède sa propre page web iDRAC.

Pour obtenir des informations sur la connexion, cliquez sur **Aide** au bas de la page web.



REMARQUE : Pour accéder à la page web de l'iDRAC, vous devez disposer d'une connexion réseau entre le système client qui exécute Config Tool et l'adresse IP du serveur iDRAC. Si une connexion réseau n'est pas disponible, utilisez la page Config Tool directement à partir de l'appareil Streamvault par le biais d'un bureau à distance ou d'une session de console locale.

Si votre système n'a pas de serveurs iDRAC, l'onglet **Gestion** est vide. Un message indique qu'il n'y a pas de surveillance de matériel Streamvault avec des capacités de gestion iDRAC disponibles.

REMARQUE : Si la page web de l'iDRAC ne se charge pas, cliquez sur un autre onglet, puis revenez à l'onglet **Gestion**.

Rubriques connexes

[Configuration de l'entité de surveillance de matériel Streamvault](#), page 56

[Configurer une entité Gestionnaire Streamvault](#), page 60

Analyser l'état de fonctionnement d'un appareil Streamvault

Utilisez la tâche Matériel Streamvault^{MC} pour afficher la liste des dysfonctionnements qui affectent vos appareils Streamvault.

Procédure

- 1 Sur la page d'accueil, ouvrez la tâche *Matériel Streamvault*.
- 2 Dans le filtre de recherche **Plage horaire**, spécifiez la plage horaire à utiliser pour le rapport.
- 3 Cliquez sur **Générer le rapport**.
Les propriétés d'unité sont affichées dans le volet de rapport.

Colonnes du volet de rapport de la tâche Matériel Streamvault.

Une fois le rapport généré, le résultat de votre recherche est affiché dans le volet de rapport. Cette section présente les colonnes disponibles dans la tâche Matériel Streamvault^{MC}.

- **Image** : Icône représentant le type de problème.
- **Gravité** : Niveau de gravité du problème.
- **Horodatage** : Date et heure de la survenue du problème.
- **Source** : Appareil Streamvault concerné par le problème.
- **MessageID** : Séquence alphanumérique associée au problème signalé.
- **Message** : Description du problème.
- **Description** : Description de la source du problème.

REMARQUE : Pour en savoir plus sur la création de rapports, voir [Présentation de l'espace de travail des tâches de rapport](#) sur TechDoc Hub.


Créer des mécanismes événement-action pour les dysfonctionnements de Streamvault

À l'aide d'un mécanisme événement-action, vous pouvez déclencher des actions qui se produisent lorsqu'un problème matériel Streamvault^{MC} est détecté.

Avant de commencer

- [Créez le rôle de module externe Maintenance Streamvault.](#)
- [Configurez une entité de surveillance de matériel Streamvault.](#)

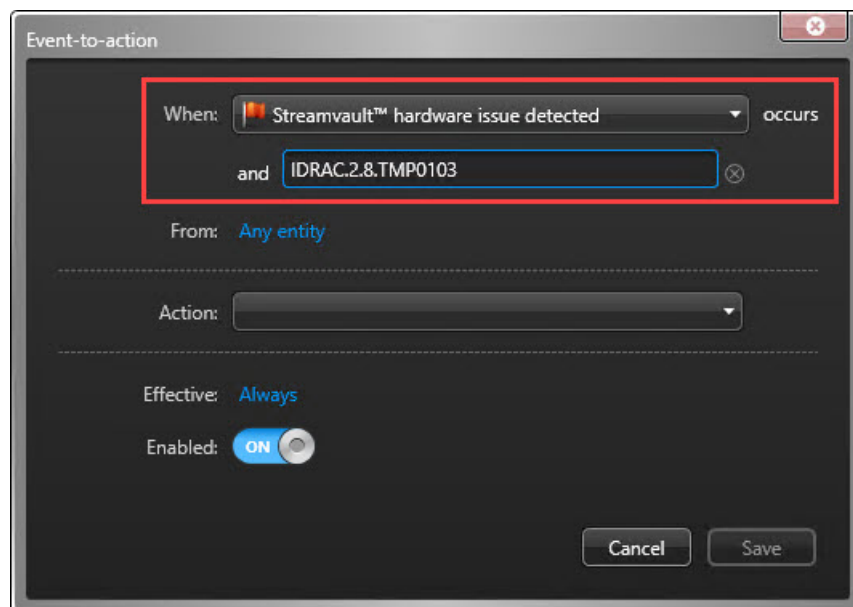
Procédure

- 1 Sur la page d'accueil de Config Tool, cliquez sur la tâche *Automatisation*, puis cliquez sur la vue **Actions**.
- 2 Cliquez sur **Ajouter un élément** .

3 Configurez votre mécanisme événement-action :

- a) Dans le menu déroulant **Quand**, sélectionnez **Problème matériel Streamvault détecté**.
- b) Cliquez sur **Indiquer une condition** et entrez le code d'erreur iDRAC. Vous pouvez également saisir l'identifiant complet pour éviter tout faux déclenchement.

Par exemple, dans la capture d'écran ci-dessous, le code d'erreur est TMP0103 et l'ID complet est IDRAC.2.8.TMP0103.



- c) (Facultatif) Dans l'option **De**, sélectionnez votre module externe Streamvault ou votre surveillance de matériel.

REMARQUE : Étant donné que le module externe Streamvault utilise des événements personnalisés qui n'ont de sens que pour lui-même, il n'est pas nécessaire d'attribuer une source.

Si vous sélectionnez le module externe Streamvault comme entité source, si le rôle module externe est supprimé, toutes les règles d'automatisation liées sont supprimées. Si aucune entité source n'est spécifiée et que le rôle est supprimé, les règles d'automatisation persistent.

- d) Dans le menu déroulant **Action**, sélectionnez un type d'action et configurez ses paramètres.
- e) (Facultatif) Sous l'option **Effectif**, cliquez sur **Toujours** et sélectionnez un horaire durant lequel cette association événement-action est active.

Si l'événement survient en dehors de la plage horaire définie, l'action n'est pas déclenchée.

4 Assurez-vous que le mécanisme événement-action est activé.

5 Cliquez sur **Enregistrer**.

REMARQUE : Pour une liste complète des codes d'erreur iDRAC, voir <https://developer.dell.com/apis/2978/versions/5.xx/docs/Error%20Codes/EEMRegistry.md>.

Référence SV Control Panel

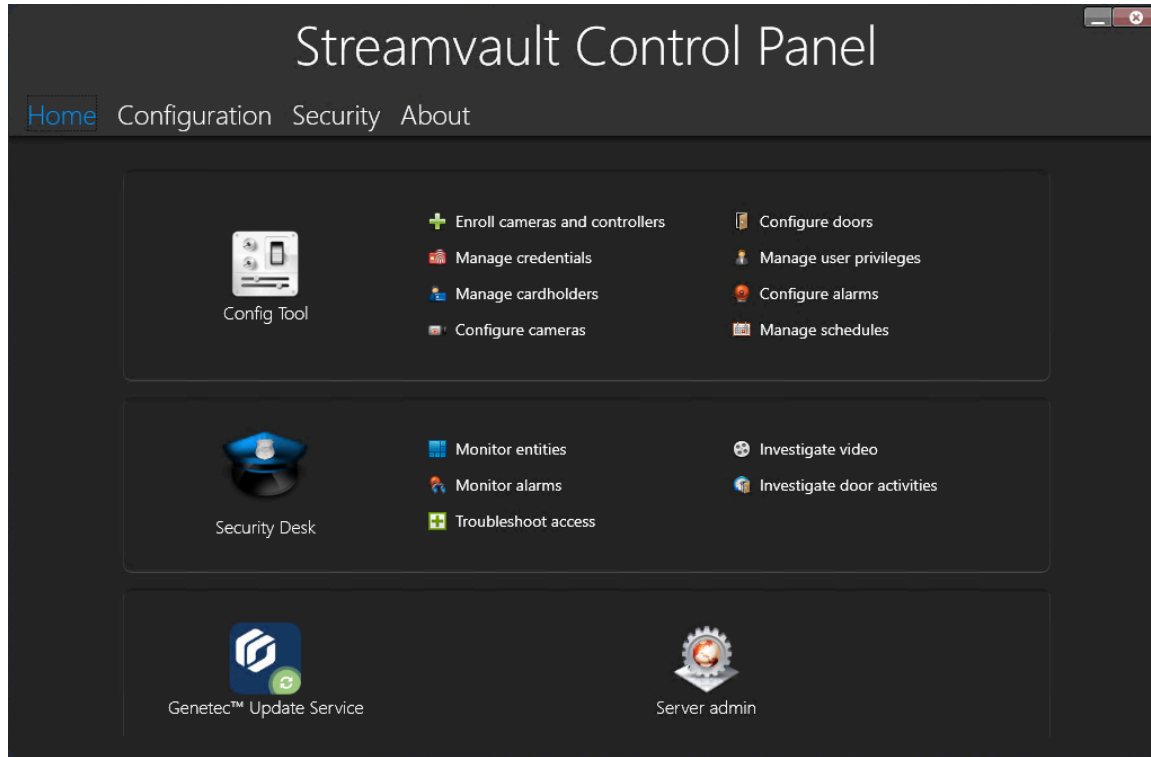
Ces pages de référence aident à comprendre le fonctionnement du SV Control Panel.

Cette section aborde les sujets suivants:

- ["Page d'accueil de SV Control Panel"](#), page 69
- ["Page Configuration de SV Control Panel"](#), page 71
- ["Page Sécurité de SV Control Panel"](#), page 74
- ["Page À propos du SV Control Panel"](#), page 78

Page d'accueil de SV Control Panel

Utilisez la page d'accueil de SV Control Panel pour accéder aux tâches de base nécessaires pour configurer et utiliser votre système. Vous pouvez cliquer sur les icônes de l'interface pour accéder aux applications Config Tool, Security Desk, Server Admin ou Genetec^{MC} Update Service.



Vous pouvez également cliquer sur les raccourcis Config Tool ou Security Desk pour ouvrir les tâches correspondantes.

Pour les systèmes s'exécutant en mode Client, le raccourci Server Admin n'est pas disponible. De la même manière, les raccourcis Config Tool et Security Desk sont limités.

REMARQUE : Remarque : si votre système n'est pas activé, une bannière rouge apparaît pour vous en informer. Cliquez sur **Le système n'est pas activé. Cliquez ici pour l'activer.** Pour ouvrir l'assistant d'activation de Streamvault^{MC} Control Panel.

Raccourcis de Config Tool

Utilisez les raccourcis pour ouvrir les tâches principales dans l'application Config Tool. Les raccourcis disponibles dépendent de vos options de licence.

Raccourci	Action
Config Tool	Ouvre Config Tool.
Inscrire des caméras et contrôleurs	Ouvre l'Outil d'inscription d'unités, où vous pouvez inscrire vos caméras et contrôleurs.
Gérer les identifiants	Ouvre la tâche <i>Gestion des identifiants</i> , dans laquelle vous pouvez gérer les informations d'identification des utilisateurs.

Raccourci	Action
Gérer les titulaires de cartes	Ouvre la tâche <i>Gestion des titulaires de cartes</i> , où vous pouvez gérer les titulaires de cartes.
Configurer des caméras	Ouvre la tâche <i>Vidéo</i> , où vous pouvez ajouter et gérer des caméras.
Configurer les portes	Ouvre la tâche <i>Vue secteur</i> , où vous pouvez ajouter et gérer des portes.
Gérer les privilèges utilisateur	Ouvre la tâche <i>Gestion des utilisateurs</i> , où vous pouvez ajouter et gérer les privilèges des utilisateurs.
Configurer des alarmes	Ouvre la tâche <i>Alarmes</i> , où vous pouvez configurer les alarmes.
Gérer les horaires	Ouvre la tâche <i>Système</i> , dans laquelle vous pouvez créer et gérer des horaires.

Raccourcis de Security Desk

Utilisez les raccourcis pour ouvrir les tâches principales dans l'application Security Desk. Les raccourcis disponibles dépendent de vos options de licence.

Raccourci	Action
Security Desk	Ouvre Security Desk.
Surveiller des entités	Ouvre la tâche <i>Surveillance</i> , où vous pouvez surveiller les événements système en temps réel.
Surveiller les alarmes	Ouvre la tâche <i>Surveillance d'alarmes</i> , dans laquelle vous pouvez surveiller et répondre aux alarmes actives et afficher les alarmes passées.
Dépanner les accès	Ouvre l'Outil de diagnostic d'accès, qui vous permet de diagnostiquer et d'accéder aux problèmes de configuration. REMARQUE : Ce raccourci n'est pas disponible sur les systèmes exécutés en Mode client.
Analyser de la vidéo	Ouvre la tâche <i>Archives</i> , où vous pouvez rechercher des archives vidéo. REMARQUE : Ce raccourci n'est pas disponible sur les systèmes exécutés en Mode client.
Analyser les activités de portes	Ouvre la tâche <i>Activités de portes</i> , où vous pouvez étudier les événements aux portes sélectionnées. REMARQUE : Ce raccourci n'est pas disponible sur les systèmes exécutés en Mode client.

Raccourci de Genetec^{MC} Update Service

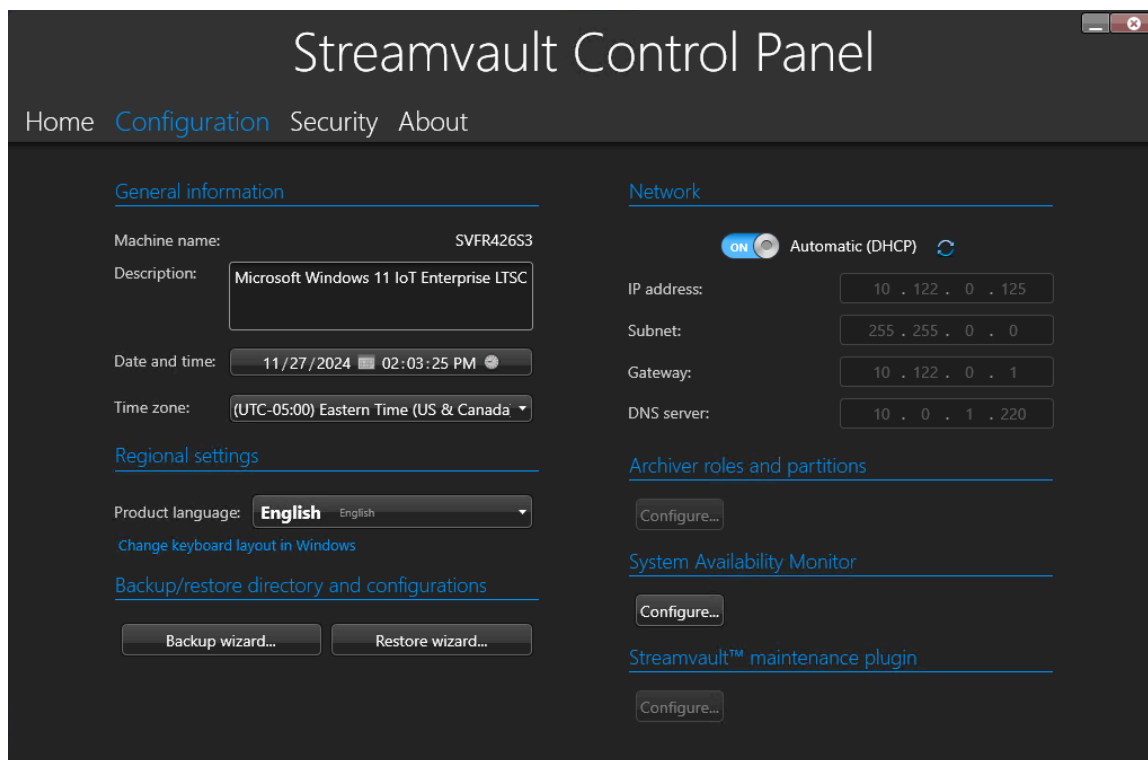
Utilisez Genetec^{MC} Update Service pour vérifier que les composants logiciels de votre appareil sont à jour.

Raccourci Server Admin

Utilisez l'application Server Admin pour appliquer manuellement une licence ou pour afficher et modifier la configuration du serveur.

Page Configuration de SV Control Panel

Utilisez la page *Configuration* du panneau de configuration Streamvault^{MC} pour modifier les paramètres généraux tels que les *paramètres régionaux*, les *paramètres réseau* et les *réglages System Availability Monitor*.



Pour les systèmes exécutés sur un serveur d'extension ou en mode Client, les sections *System Availability Monitor* et *Répertoire de sauvegarde/restauration et configurations* ne sont pas disponibles.

Paramètres d'informations générales

Utilisez la section *Informations générales* pour modifier les paramètres généraux, tels que le nom de votre appareil Streamvault.

- **Nom de la machine** : Affiche le nom de l'appareil SV.
- **Description** : Entrez une description permettant d'identifier l'appareil.
- **Date et heure** : Cliquez dans le champ pour configurer les valeurs de date et d'heure affichées sur l'appareil. Vous pouvez également cliquer sur les icônes de calendrier et d'horloge dans le champ pour configurer les réglages.
- **Fuseau horaire** : Sélectionnez un fuseau horaire dans la liste déroulante.

Paramètres régionaux

Utilisez la section *Paramètres régionaux* pour modifier les paramètres de langue de la disposition du clavier de votre système.

- **Langue du produit** : Sélectionnez une langue dans la liste pour modifier la langue de Config Tool et Security Desk.
IMPORTANT : Vous devez redémarrer les applications Security Center pour que les modifications soient prises en compte.
- **Modifier la disposition du clavier dans Windows** : Cliquez sur cette option pour ouvrir la page des *paramètres de langue et de région* de Windows afin de modifier la disposition de votre clavier.

IMPORTANT : Vous devez redémarrer votre ordinateur pour que les modifications soient prises en compte.

REMARQUE : SV Control Panel est disponible en anglais, français et espagnol.

Sauvegarde et restauration

Utilisez la section *Répertoire de sauvegarde/restauration et configurations* pour accéder à l'*assistant de sauvegarde* et à l'*assistant de restauration*.

Sauvegarde et restauration est une fonctionnalité de SV Control Panel. Il vous permet de sauvegarder en toute sécurité la base de données et les fichiers de configuration de votre Répertoire, et de les restaurer ultérieurement sur le même identifiant de système. La fonctionnalité Sauvegarde et restauration être utilisée en cas de défaillance du système ou de mise à niveau du matériel. Cette fonctionnalité ne sauvegarde pas le fichier de licence, les archives vidéo ou les autres bases de données.

Cette section n'est pas disponible pour les systèmes s'exécutant sur un serveur d'extension ou en mode Client.


- **Assistant de sauvegarde :** Cliquez sur **Assistant de sauvegarde** pour créer une sauvegarde de la base de données du Répertoire et des fichiers de configuration.
- **Assistant de restauration :** Cliquez sur **Assistant de restauration** pour restaurer une sauvegarde de la base de données du Répertoire et des fichiers de configuration sur votre système.

IMPORTANT : Vous devez ouvrir le port requis pour garantir que la fonctionnalité *Sauvegarder/restaurer le Répertoire et les configurations* peut communiquer avec SV Control Panel. Pour en savoir plus, voir [Ports par défaut utilisés par Streamvault](#), page 4.

Paramètres réseau

Utilisez la section *Réseau* pour modifier les paramètres réseau tels que l'adresse IP de votre appareil Streamvault.

- **Automatique (DHCP) :** Par défaut, le DHCP (Dynamic Host Configuration Protocol) est utilisé pour affecter automatiquement l'adresse IP, le sous-réseau, la passerelle et le serveur DNS. Désactivez cette option si vous ne souhaitez pas que l'adresse IP soit attribuée dynamiquement par votre serveur DHCP.

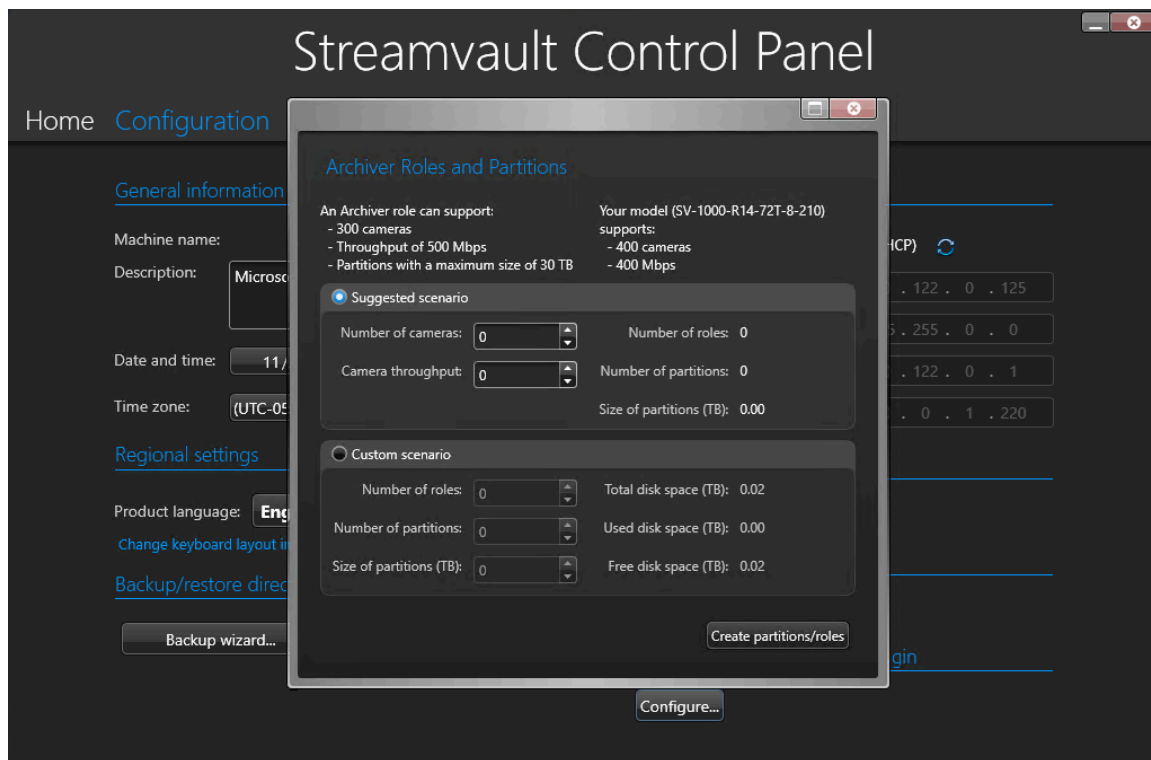
Cliquez sur **Actualiser**  pour actualiser vos paramètres DHCP et obtenir une nouvelle adresse IP.

- **Adresse IP :** L'adresse IP de l'appareil.
- **Sous-réseau :** Le masque de sous-réseau de l'appareil.
- **Passerelle :** L'adresse IP de la passerelle.
- **Serveur DNS :** L'adresse IP du serveur DNS.

Partitions et rôles Archiveur

Utilisez la section *Rôles et partitions Archiveur* pour configurer les systèmes qui nécessitent plus que le nombre maximal de caméras et le débit pris en charge par un seul Archiveur.

Cette section est disponible pour les systèmes exécutant Security Center 5.9 et versions ultérieures sur un serveur d'extension.



- **Un rôle Archiveur peut prendre en charge :** Affiche le nombre de caméras, le débit et la taille de partition pris en charge par un seul rôle Archiveur.
- **Votre modèle prend en charge :** Affiche le nombre de caméras et le débit pris en charge par votre modèle d'appareil Streamvault.
- **Scénario recommandé :** Calcule automatiquement le nombre de rôles, de partitions et la taille des partitions nécessaires pour le nombre de caméras et le débit souhaités.
- **Scénario personnalisé :** Choisissez le nombre de rôles, de partitions, et la taille des partitions souhaités pour configurer votre système.

Pour en savoir plus sur cette fonctionnalité, voir [Ajouter des rôles Archiveur dans SV Control Panel](#), page 40.

Paramètres du System Availability Monitor

Utilisez la section *System Availability Monitor* pour configurer les paramètres de System Availability Monitor Agent sur votre appareil Streamvault. Par exemple, vous pouvez spécifier la méthode de collecte de données et activer l'agent.

Vous pouvez vérifier les points suivants :

- Si l'appareil communique avec Security Center
- La date de la dernière vérification
- Les erreurs et avertissements récents signalés dans les journaux des applications et services

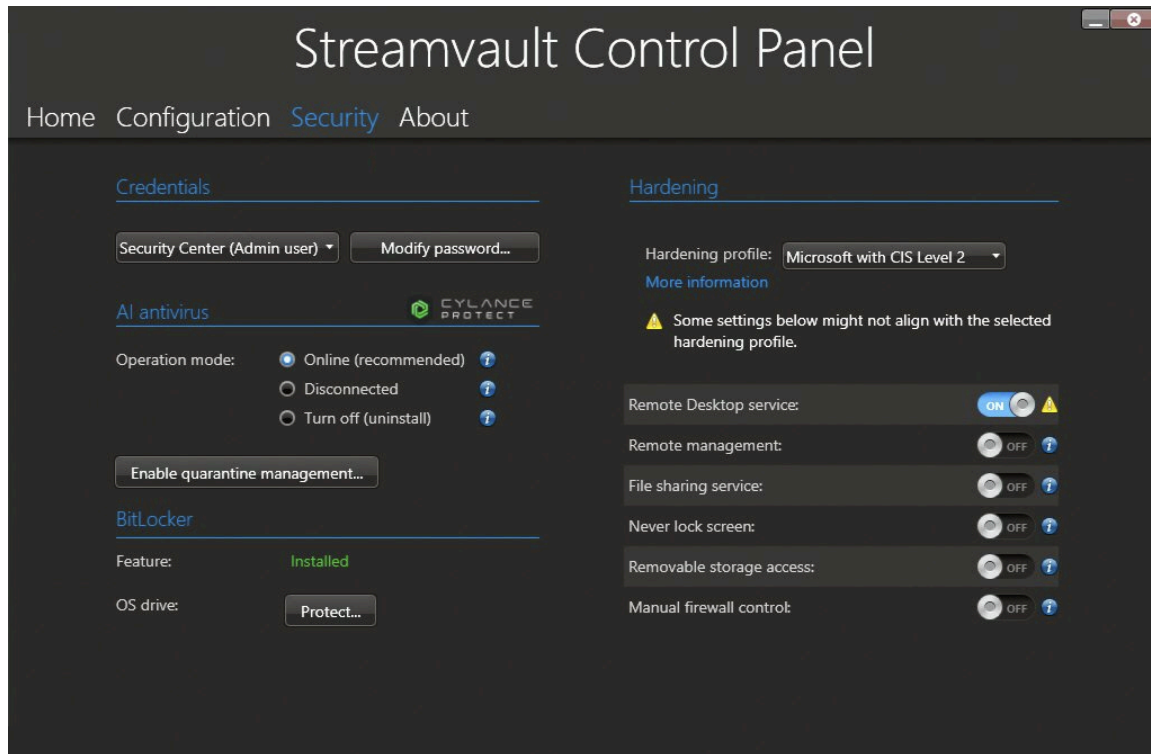
Cette section n'est pas disponible pour les systèmes s'exécutant sur un serveur d'extension ou en mode Client.

Paramètres du module externe de maintenance Streamvault

Utilisez la section du *module externe de maintenance Streamvault* pour inscrire le module externe dans Security Center, s'il n'a pas déjà été inscrit.

Page Sécurité de SV Control Panel

Utilisez la page *Sécurité* pour modifier les mots de passe des utilisateurs, choisir le mode de communication entre l'agent CylancePROTECT et Genetec^{MC} et appliquer des profils de renforcement et des paramètres de sécurité système à votre appareil Streamvault^{MC}.



Réglages de mot de passe

Utilisez la section *Informations d'identification* de la page *Sécurité* pour modifier les mots de passe des comptes utilisateurs de votre appareil Streamvault.

REMARQUE : Différentes options de mot de passe sont disponibles pour l'utilisateur actuel, tant sur le serveur principal que sur le serveur d'extension. Sur un serveur d'extension, l'administrateur ne peut que modifier les mots de passe Windows, pas ceux des applications Security Center.

Définir un mot de passe pour chaque type d'utilisateur :

- **Security Center (utilisateur Admin) :** Le mot de passe de l'utilisateur administrateur pour Security Desk, Config Tool et Genetec^{MC} Update Service.
- **Server Admin :** Le mot de passe pour l'application Genetec^{MC} Server Admin.
- **Opérateur Windows :** Cliquez sur **Modifier le mot de passe** pour modifier le mot de passe Windows de l'opérateur.

Paramètres antivirus

Utilisez la section *Antivirus AI* pour choisir le mode dans lequel l'agent CylancePROTECT communique avec Genetec.

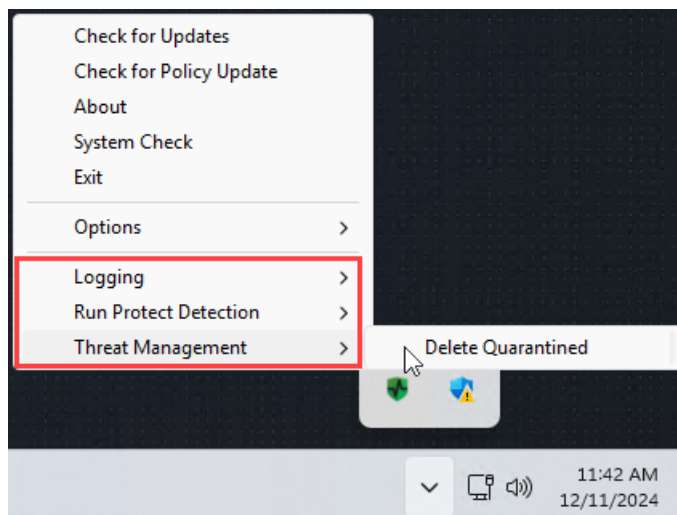
CylancePROTECT est le logiciel antivirus basé sur l'IA utilisé pour la protection et la détection des menaces.

Vous pouvez choisir parmi les modes de fonctionnement suivants :

- **En ligne (recommandé) :** L'agent CylancePROTECT communique avec Genetec pour signaler les nouvelles menaces, mettre à jour l'agent et envoyer des données qui contribuent à l'amélioration des modèles mathématiques. Cette option offre un niveau de protection maximal.
- **Déconnecté :** Le mode déconnecté est destiné aux appareils dépourvus de connexion Internet. Dans ce mode, CylancePROTECT ne peut pas se connecter ni envoyer des informations aux services de gestion de Genetec dans le cloud. Votre appareil est protégé contre la plupart des menaces. Les opérations de maintenance et les mises à jour sont disponibles à travers le service Genetec^{MC} Update Service (GUS).
- **Désactiver :** Sélectionnez ce mode pour désinstaller définitivement CylancePROTECT de votre appareil. Votre appareil utilisera les fonctions de protection et de détection des menaces de Microsoft Defender. Évitez de désactiver CylancePROTECT si l'appareil ne peut pas recevoir les mises à jour des définitions de virus pour Microsoft Defender.

ATTENTION : Le basculement entre les options peut nécessiter un redémarrage de l'ordinateur, entraînant une indisponibilité du système.

Cliquez sur **Activer la gestion de la quarantaine** pour ajouter la **gestion des menaces** au menu contextuel de l'icône Cylance dans la barre des tâches Windows. Cette option vous permet de supprimer les éléments mis en quarantaine. La **journalisation** et la **détection de protection d'exécution** sont également ajoutées au menu contextuel. Ces options vous permettent respectivement d'accéder aux journaux et de déclencher des analyses.



Réglages de chiffrement

Utilisez la section *BitLocker* pour installer la fonctionnalité BitLocker et chiffrer le lecteur du SE sur votre appareil Streamvault.

- **Fonctionnalité :** La fonctionnalité BitLocker est préinstallée sur Windows 10 et Windows 11. Si vous avez Windows Server, vous devez cliquer sur **Installer** pour installer la fonctionnalité.
- **Lecteur du SE :** Cliquez sur **Protéger** pour chiffrer le lecteur du SE (C:) avec BitLocker. La clé de déchiffrement est enregistrée sur une puce TPM (Trusted Platform Module) située sur la carte système de l'appareil Streamvault. Si le lecteur du système d'exploitation devait être retiré ou si la carte système devait être remplacée, les informations sur le lecteur du système d'exploitation seraient perdues. Le disque du SE ne pourrait pas accéder à la clé de déchiffrement sur le module de plateforme sécurisée. Vous pouvez créer une clé de récupération qui peut être utilisée pour déchiffrer le lecteur dans ces scénarios. Sans clé de récupération, l'appareil doit être recréé et le logiciel réinstallé. Le chiffrement du lecteur du SE permet également de protéger le mot de passe administrateur Windows contre les accès non autorisés.

Pour en savoir plus, voir [Chiffrer le lecteur du SE](#).

Paramètres de renforcement

Utilisez la section *Renforcement* pour choisir un profil de renforcement et définir les paramètres de sécurité système pour votre appareil Streamvault.

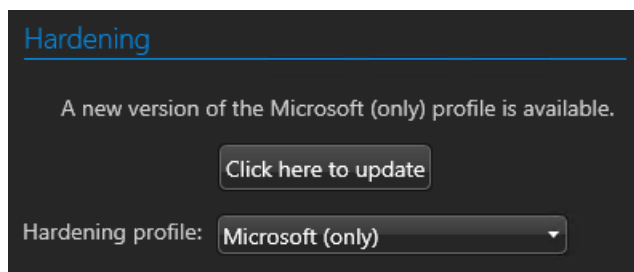
REMARQUE : Les profils de renforcement ne sont disponibles que sur les appareils dotés du [Service Streamvault](#). Pour en savoir plus, voir [À propos du service Streamvault](#), page 15.

Il existe quatre profils de renforcement prédéfinis :

- **Microsoft (uniquement) :** Ce profil de renforcement applique les lignes directrices de sécurité Microsoft à votre système. Les lignes directrices de sécurité Microsoft sont un groupe de paramètres de configuration recommandés par Microsoft qui sont basés sur les commentaires des équipes d'ingénierie de sécurité, des groupes de produits, des partenaires et des clients Microsoft.
- **Microsoft avec CIS niveau 1 :** Ce profil de renforcement applique les lignes directrices de sécurité Microsoft et le profil Center for Internet Sécurité (CIS) niveau 1 (CIS L1) à votre système. Le CIS L1 fournit des exigences de sécurité essentielles qui peuvent être mises en œuvre sur n'importe quel système avec peu ou pas d'impact sur les performances ou des fonctionnalités réduites.
- **Microsoft avec CIS niveau 2 :** Ce profil de renforcement applique les lignes directrices de sécurité Microsoft et les profils CIS L1 et niveau 2 (L2) à votre système. Le profil CIS L2 offre le plus haut niveau de sécurité et est destiné aux organisations pour lesquelles la sécurité est de la plus haute importance.
REMARQUE : La sécurité stricte apportée par ce profil de renforcement peut réduire les fonctionnalités du système et rendre la gestion du serveur à distance plus difficile.
- **Microsoft avec STIG :** Ce profil de renforcement applique les lignes directrices de sécurité Microsoft et les guides de mise en œuvre technique de Sécurité (STIG) de la Defense Information Systems Agency (DISA) à votre système. Les STIG DISA sont basés sur les normes du National Institute of Standards and Technology (NIST) et offrent une protection de sécurité avancée pour les systèmes Windows du ministère de la Défense américain.

REMARQUE : Par défaut, tous les appareils sont livrés avec le profil de renforcement Microsoft CIS de niveau 2 appliqué.

Lorsqu'une nouvelle version de votre profil de renforcement sélectionné est disponible, un bouton **Cliquer ici pour mettre à jour** apparaît. Cliquez sur le bouton pour appliquer la mise à jour.



En plus des profils de renforcement, les paramètres de sécurité système suivants peuvent être définis :

- **Service Bureau à distance :** Autorisez les utilisateurs de votre réseau à se connecter à l'appareil à l'aide d'une application *Bureau à distance*. Pour éviter toute infection de votre appareil par des logiciels malveillants, cette option a été désactivée par défaut.
- **Gestion à distance :** Activez la prise en charge à distance des outils de gestion Microsoft tels que Windows Admin Center, Microsoft Server Manager et Remote PowerShell.
- **Service Partage de fichiers :** Autorisez les utilisateurs de votre réseau à partager des fichiers et des dossiers situés sur l'appareil. Pour éviter toute infection de votre appareil par des logiciels malveillants, cette option a été désactivée par défaut.
- **Ne jamais verrouiller l'écran :** Si cette option est activée, Windows gardera l'utilisateur connecté, même après 15 minutes d'inactivité.
- **Accès au stockage amovible :** Permet d'activer l'accès à une clé USB ou à un disque dur USB connecté depuis Windows.

REMARQUE : Les utilisateurs dotés de privilèges d'administration disposent automatiquement d'un accès aux supports de stockage amovibles.

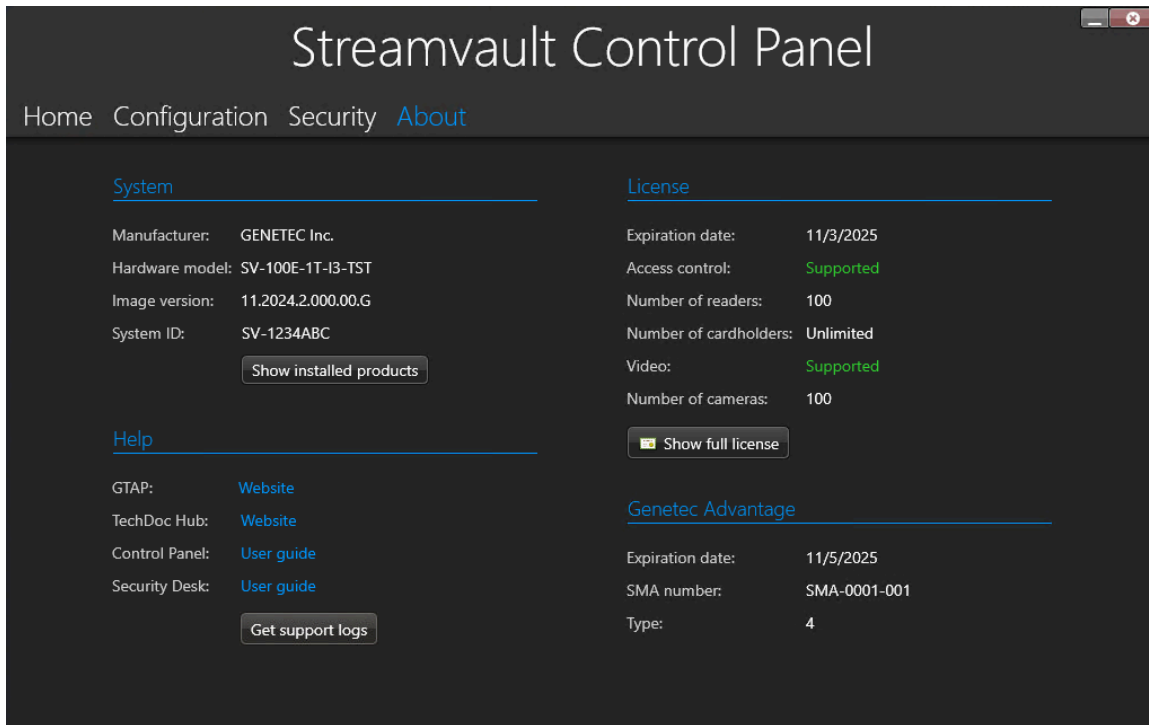
- **Contrôle manuel du pare-feu :** Par défaut, le pare-feu Windows Defender utilise les objets de stratégie de groupe (GPO) des profils de renforcement pour sécuriser le système. Activez cette option pour contrôler manuellement les stratégies de pare-feu. Tous les objets GPO seront désactivés.

Pour en savoir plus, voir [Désactiver le pare-feu Windows](#), page 125.

Page À propos du SV Control Panel

Ouvrez la page *À propos* pour afficher des informations utiles si vous avez besoin d'aide avec votre appareil Streamvault^{MC}. La page *À propos* inclut des informations système, des liens vers le portail d'assistance technique Genetec^{MC} (GTAP) et la documentation produit, des informations sur les licences et des informations sur le contrat de maintenance logicielle (CMA).

Sur les systèmes exécutés sur un serveur d'extension ou en mode Client, seules les sections *Système* et *Aide* sont disponibles.



Informations système

Utilisez la section *Système* pour afficher des informations sur le système.

- **Fabricant** : Affiche le fabricant du matériel.
- **Modèle matériel** : Affiche le modèle matériel.
- **Versión d'image** : Affiche la version de l'image du logiciel.
- **ID du système** : Affiche le numéro d'ID système.
- **Afficher les produits installés** : Cliquez pour afficher la version logicielle des composants Genetec^{MC} installés sur l'appareil.

Informations d'aide

Utilisez la section *Aide* pour accéder à des liens utiles vers GTAP et la documentation du produit.

- **GTAP** : Cliquez sur le lien pour ouvrir [GTAP](#) et les forums d'assistance.
REMARQUE : Vous devez avoir un nom d'utilisateur et un mot de passe valides pour vous connecter à GTAP.
- **TechDoc Hub** : Cliquez sur le lien pour ouvrir [Genetec TechDoc Hub](#).
- **Tableau de bord** : Cliquez sur le lien pour ouvrir le *Guide d'utilisation de l'appareil Streamvault*, qui contient des informations sur SV Control Panel.

- **Security Desk** : Cliquez sur le lien pour ouvrir le *Guide de l'utilisateur de Security Center*.
- **Obtenir les journaux d'assistance** : Cliquez pour sélectionner les journaux d'assistance que vous souhaitez télécharger à des fins de dépannage.

Informations de licence

Utilisez la section *Licence* pour afficher les informations sur la licence. Les informations affichées varient en fonction de vos options de licence.

- **Date d'expiration** : Affiche la date d'expiration de votre licence Security Center.
- **Contrôle d'accès** : Indique si les fonctionnalités de contrôle d'accès sont prises en charge.
- **Nombre de lecteurs** : Indique le nombre de lecteurs pris en charge par votre système.
- **Nombre de titulaires de cartes** : Indique le nombre de titulaires de cartes pris en charge par votre système.
- **Vidéo** : Indique si les fonctionnalités vidéo sont prises en charge.
- **Nombre de caméras** : Indique le nombre de caméras prises en charge par votre système.
- **Afficher la licence complète** : Cliquez pour afficher plus d'informations de licence.

Cette section n'est pas disponible pour les systèmes s'exécutant sur un serveur d'extension ou en mode Client.

Informations sur Genetec Advantage

Utilisez la section *Genetec Advantage* pour afficher des informations sur le CMA.

- **Date d'expiration** : Affiche la date d'expiration du contrat de maintenance applicative.
- **Numéro de CMA** : Affiche le numéro de CMA.
- **Type** : Affiche le type de CMA.

Cette section n'est pas disponible pour les systèmes exécutés sur un serveur d'extension ou en mode Client.

Ressources complémentaires

Cette section aborde les sujets suivants:

- ["Garantie de votre appareil Streamvault", page 81](#)
- [" Configurer le mot de passe du BIOS ", page 82](#)
- [" Modifier le mot de passe iDRAC par défaut ", page 85](#)
- ["Ajouter un nouvel utilisateur iDRAC avec des privilèges d'administrateur", page 86](#)
- ["Désactiver l'utilisateur root iDRAC", page 87](#)
- ["Réappliquer une image à un appareil Streamvault", page 88](#)
- ["Recherche de l'ID système et de la version d'image d'un appareil Streamvault", page 89](#)
- ["Autoriser le partage de fichiers sur un appareil Streamvault", page 90](#)
- ["Autoriser les connexions Bureau à distance à un appareil Streamvault", page 91](#)

Garantie de votre appareil Streamvault

Votre appareil Streamvault^{MC} est couvert par une garantie matérielle et logicielle standard de 3 ans, qui peut être prolongée de 2 ans.

Pour une description détaillée des conditions de la garantie du produit Genetec^{MC}, reportez-vous à la page [Présentation de la garantie produit Genetec^{MC}](#).

Configurer le mot de passe du BIOS

Pour protéger les données de votre appareil Streamvault^{MC} contre les accès non autorisés, vous devez définir un mot de passe du BIOS.

À savoir

La procédure de configuration d'un mot de passe du BIOS varie en fonction du modèle de votre appareil. Suivez la procédure applicable à votre appareil.

- Définissez le mot de passe du BIOS sur votre appareil ou poste Streamvault tout-en-un.
- Définissez le mot de passe du BIOS sur votre appareil série SV-1000, SV-2000, SV-4000 ou SV-7000 (PowerEdge).

Procédure

Pour définir le mot de passe du BIOS sur votre appareil tout-en-un ou poste Streamvault :

- 1 Allumez ou redémarrez l'appareil et appuyez plusieurs fois sur F2 jusqu'à ce que l'apparition du menu *Configuration du BIOS*.
- 2 Sélectionnez **Mots de passe** dans le menu à gauche de l'écran.
- 3 Sur la page *Mots de passe*, faites défiler la page jusqu'à *Configuration du mot de passe* et configurez les paramètres suivants :
 - Activez les options **Lettre Majuscule**, **Lettre minuscule**, **Chiffre** et **Caractère spécial**.
 - Définissez le champ **Nombre minimum de caractères** sur 14.

Genetec Inc. BIOS Setup

Streamvault

Advanced Setup ☒ ON Help Text ☒ ON Admin Password

Overview
Boot Configuration
Integrated Devices
Storage
Display
Connection
Power
Security
Passwords
Update/Recovery
System Management
Keyboard
Pre-boot Behavior
Virtualization Support
Performance
System Logs

Passwords

Password Configuration

Upper Case Letter
When enabled, this field reinforces password must contain at least one upper case letter.
☒ ON

Lower Case Letter
When enabled, this field reinforces password must contain at least one lower case letter.
☒ ON

Digit
When enabled, this field reinforces password must contain at least one digit number.
☒ ON

Special Character
When enabled, this field reinforces password must contain at least one special character.
☒ ON

Minimum Characters 14 This field controls the minimum number of characters allowed for password.

- 4 Faites défiler jusqu'en haut de la page *Mots de passe* et saisissez un nouveau mot de passe du BIOS sous **Mot de passe administrateur**.

Passwords

Admin Password

This field lets you set, change, or delete the administrator (admin) password (sometimes called the "setup" password). The admin password enables several security features. When set, it:

- * Restricts changes to the settings in Setup.
- * Restricts the Legacy boot devices listed in the F12 Boot Menu to those enabled in the "Boot Sequence" field, and restricts the UEFI boot paths listed in the F12 Boot Menu according to the configuration in General/UEFI Boot Path Security.
- * Substitutes for the system password if the system prompts for a password during power on.

Successful changes to this password take effect immediately.

NOTE: If you delete the admin password, the system password, if set, is also deleted. Also, the admin password can be used to delete the HDD password. For this reason, you cannot set an admin password if a system password or HDD password is already set. The admin password must be set first if an admin password is used with the a system password and/or HDD password.

Enter the old password:

Enter the new password and then press <Enter>. Then re-enter the new password and press <Enter> again to confirm.

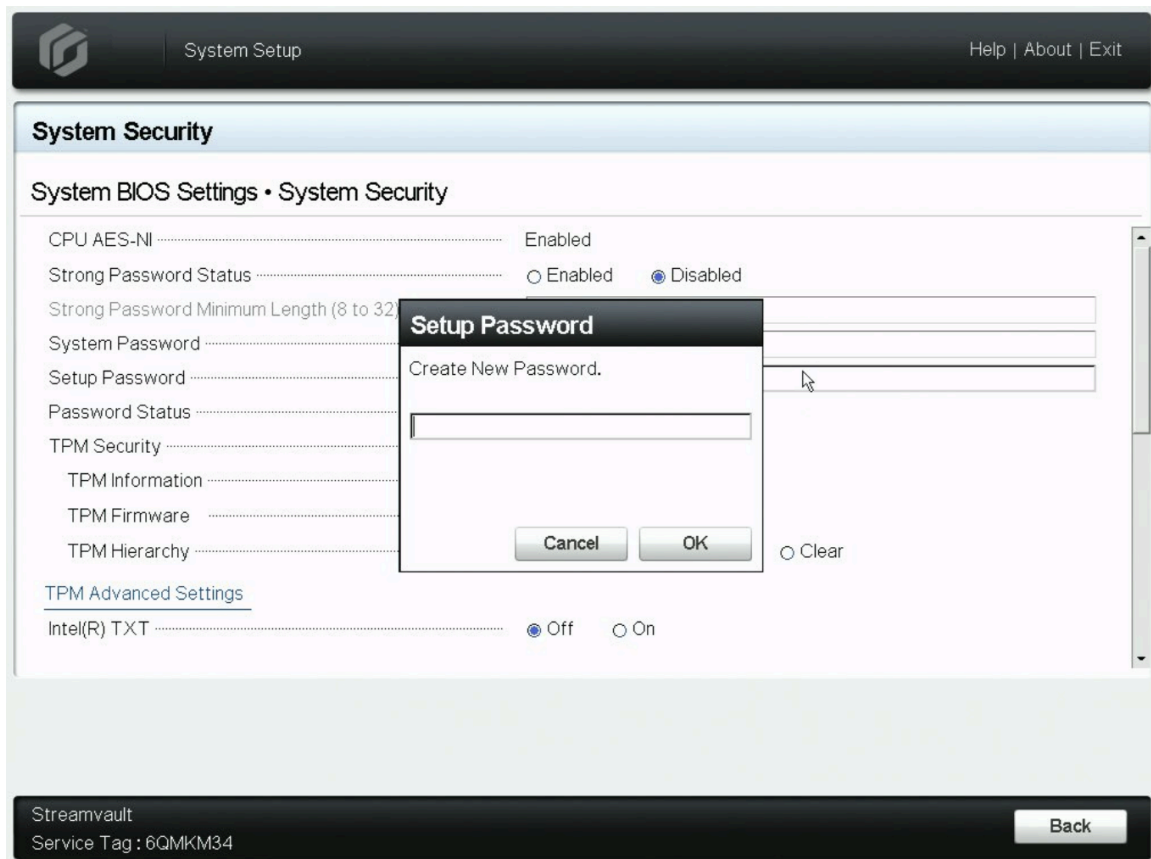
Enter the new password:

- 5 Cliquez sur **Quitter**.
Vos modifications sont enregistrées et l'appareil redémarre.

Pour définir le mot de passe du BIOS sur votre appareil série SV-1000, SV-2000, SV-4000 ou SV-7000 (PowerEdge) :

- 1 Allumez ou redémarrez l'appareil et appuyez plusieurs fois sur F2 jusqu'à ce que l'apparition du menu *Configuration du système*.
- 2 Dans le *Menu principal de la configuration du système*, cliquez sur **BIOS système**.
- 3 Dans les *Paramètres du BIOS système*, cliquez sur **Sécurité du système**.
- 4 Dans le champ **Configurer le mot de passe**, cliquez dans la zone de texte.

- 5 Dans la boîte de dialogue *Configurer le mot de passe* qui apparaît, entrez un nouveau mot de passe et cliquez sur **OK**.



- 6 Dans le champ **État du mot de passe**, sélectionnez **Verrouillé** pour exiger la saisie du mot de passe de configuration avant de modifier le mot de passe du système.
- 7 Cliquez sur **Retour > Terminer > Terminer**.
Vos modifications sont enregistrées et l'appareil redémarre.

Modifier le mot de passe iDRAC par défaut

Si votre appareil Streamvault^{MC} prend en charge iDRAC, il est recommandé de modifier immédiatement le mot de passe iDRAC par défaut de l'utilisateur root pour empêcher tout accès non autorisé à votre appareil.

Procédure

- 1 Lancez le navigateur Web Microsoft Edge et accédez à `https://idrac.local`.
- 2 Sur la page de connexion *Contrôleur d'accès à distance intégré*, utilisez le nom d'utilisateur et mot de passe par défaut pour vous connecter :
 - Sous **Nom d'utilisateur**, entrez root.
 - Sous **Mot de passe**, entrez le mot de passe situé sur le numéro de série de votre appareil.
- 3 Une fois connecté, vous êtes invité à configurer un nouveau mot de passe pour l'utilisateur root. Sélectionnez **Modifier le mot de passe par défaut**, entrez et confirmez le nouveau mot de passe, puis cliquez sur **Continuer** pour enregistrer vos modifications.

Lorsque vous avez terminé

En plus de modifier le mot de passe par défaut de l'utilisateur racine, il est recommandé de créer un autre utilisateur iDRAC avec des privilèges d'administrateur et de désactiver l'utilisateur root. Pour en savoir plus, voir [Ajouter un nouvel utilisateur iDRAC avec des privilèges d'administrateur](#).

Ajouter un nouvel utilisateur iDRAC avec des privilèges d'administrateur

L'utilisateur racine iDRAC est bien connu et son utilisation présente des risques de sécurité, même si vous avez modifié le mot de passe par défaut. Par conséquent, il est recommandé d'ajouter un nouvel utilisateur doté de privilèges d'administrateur pour accéder à iDRAC.

À savoir

Vous pouvez ajouter un utilisateur local ou utiliser Microsoft Active Directory pour créer un compte utilisateur.

Procédure

- Ajoutez un nouvel utilisateur de l'une des manières suivantes :
 - Pour ajouter un utilisateur local, voir [Configurer les utilisateurs locaux à l'aide de l'interface Web iDRAC](#) dans le *Guide de l'utilisateur iDRAC Dell*.
 - Pour utiliser Microsoft Active Directory pour créer un utilisateur, reportez-vous à [Configurer les utilisateurs Active Directory](#) dans le *Guide de l'utilisateur iDRAC Dell*.

REMARQUE : Lors de la configuration des privilèges utilisateur, vérifiez que le **Rôle d'utilisateur** est défini sur **Administrateur**.

Lorsque vous avez terminé

Pour plus de sécurité, [désactiver l'utilisateur racine iDRAC](#).

Désactiver l'utilisateur root iDRAC

Si vous avez créé un utilisateur iDRAC doté de privilèges d'administrateur, désactivez l'utilisateur root pour que personne ne puisse se connecter avec ce nom d'utilisateur.

Avant de commencer

- [Modifier le mot de passe iDRAC par défaut sur votre appareil Streamvault.](#)
- [Ajouter un nouvel utilisateur iDRAC avec des privilèges d'administrateur.](#)

À savoir

Vous pouvez désactiver l'utilisateur root en modifiant ses privilèges.

Procédure

- Pour en savoir plus sur la modification des privilèges utilisateur root iDRAC, voir [Configurer les utilisateurs locaux à l'aide de l'interface Web iDRAC](#) dans le *Guide de l'utilisateur iDRAC Dell*.

REMARQUE : Lorsque vous modifiez les privilèges de l'utilisateur root, veillez à configurer les éléments suivants :

- Définissez le **Rôle d'utilisateur** sur **Aucun**.
- Définissez **Niveau de privilège LAN** sur **Pas d'accès**.
- Définissez **Niveau de privilège du port série** sur **Pas d'accès**.
- Définissez **Série sur LAN** sur **Désactivé**.

Réappliquer une image à un appareil Streamvault

Pour réappliquer une image à un appareil Streamvault^{MC}, vous avez besoin de son [Certificat d'authenticité \(COA\)](#) Microsoft afin de déterminer quelle image peut être utilisée avec l'appareil. Chaque appareil Streamvault possède une étiquette du certificat d'authenticité qui indique l'édition de Windows exécutée sur l'appareil.

Reportez-vous aux [Notes de version de Streamvault](#) pour obtenir une liste des images qui sont compatibles avec votre appareil, en fonction de son édition Windows. N'utilisez pas l'image de votre logiciel si votre appareil exécute une édition de Windows différente de celle indiquée dans les notes de version.

Voici un exemple d'étiquette COA avec des informations sur l'édition et le certificat de Windows estampillés. Les produits qui utilisent une version embarquée du logiciel de Microsoft ont l'étiquette COA.



REMARQUE : Chaque image Streamvault est conçue pour fonctionner avec une version correspondante de Security Center, comme indiqué dans les [Notes de version Streamvault](#). Rétrograder vers une version précédente de Security Center peut entraîner une détérioration du niveau de sécurité de l'appareil.

Pour en savoir plus sur la disponibilité du produit, de l'assistance et d'autres services, voir la page [Cycle de vie des produits sur GTAP](#).

Recherche de l'ID système et de la version d'image d'un appareil Streamvault

Lorsque vous contactez le Centre d'assistance technique de Genetec^{MC} (GTAC), vous avez besoin de l'ID système et de la version d'image du logiciel Genetec^{MC} installé sur l'appareil.

Avant de commencer

Connectez-vous à Windows en tant qu'administrateur.

À savoir

En plus de l'ID système et de la version de l'image, GTAC peut demander le numéro de certification et le numéro de série. Pour trouver ces informations, consultez l'étiquette apposée sur l'appareil Streamvault^{MC}.

Procédure

- 1 Depuis le bureau Windows, ouvrez **Genetec^{MC} SV Control Panel**.
- 2 Si vous y êtes invité, entrez le mot de passe de l'utilisateur Admin.
- 3 Cliquez sur **À propos**.
- 4 Dans la section *Système*, notez l'**ID Système** et la **version de l'image**.

Rubriques connexes

[Rétablir les réglages d'usine sur un appareil tout-en-un Streamvault](#), page 93

[Rétablir les réglages d'usine sur un appareil Streamvault poste de travail ou serveur](#), page 103

Autoriser le partage de fichiers sur un appareil Streamvault

Pour partager les fichiers et dossiers situés sur votre appareil avec des gens sur votre réseau, vous devez activer le partage de fichiers dans SV Control Panel.

Avant de commencer

Sur l'appareil, connectez-vous à Windows en tant qu'utilisateur administrateur.

À savoir

- Pour une sécurité maximale, le partage de fichiers est désactivé par défaut.
- Les ordinateurs distants et votre appareil doivent être connectés au même réseau IP.

Procédure

- 1 Sur la page *Sécurité* de SV Control Panel, activez l'option **Service de partage de fichiers**.
- 2 Cliquez sur **Appliquer**.
- 3 Pour partager un dossier ou un fichier, faites un clic droit sur un dossier ou un fichier dans l'Explorateur de fichiers de Windows et cliquez sur **Partager**.

Autoriser les connexions Bureau à distance à un appareil Streamvault

Pour contrôler un appareil depuis un ordinateur ou une machine virtuelle sur votre réseau, vous devez d'abord activer l'accès à distance sur l'appareil.

Avant de commencer

Sur l'appareil, connectez-vous à Windows en tant qu'utilisateur administrateur.

À savoir

- Pour une sécurité maximale, l'accès à distance est désactivé par défaut.
- L'appareil et l'ordinateur distant doivent être connectés au même réseau.

Procédure

- 1 Sur la page *Sécurité* de SV Control Panel , activez l'option service **Bureau à distance**.
- 2 Cliquez sur **Appliquer**.

Rubriques connexes

[Le Bureau à distance ne peut pas se connecter à un appareil Streamvault](#), page 112

Dépannage

Cette section aborde les sujets suivants:

- [" Rétablir les réglages d'usine sur un appareil tout-en-un Streamvault ", page 93](#)
- ["Rétablir les réglages d'usine sur un appareil Streamvault poste de travail ou serveur", page 103](#)
- ["Les contrôleurs Mercury EP restent hors ligne lorsque TLS 1.1 est désactivé", page 108](#)
- ["Activer Transport Layer Security \(TLS\)", page 109](#)
- ["Le Bureau à distance ne peut pas se connecter à un appareil Streamvault", page 112](#)
- ["Suppression des restrictions des comptes utilisateur non administrateurs", page 116](#)
- ["Les comptes locaux ne peuvent pas accéder au Bureau à distance, au service de partage de fichier et à la gestion à distance ", page 117](#)
- ["Activer les services connexes à la carte à puce", page 118](#)
- ["Activation de la prise en charge des contrôleurs 1.x.x du micrologiciel Mercury EP ou LP", page 119](#)
- ["Activer la prise en charge de l'intégration Synergis IX", page 121](#)
- ["Modifier les objets de stratégie de groupe locaux pour les comptes utilisateur non-administrateurs", page 122](#)
- ["Désactiver le pare-feu Windows", page 125](#)

Rétablir les réglages d'usine sur un appareil tout-en-un Streamvault

Si le logiciel sur un appareil Streamvault^{MC} tout-en-un ne démarre pas ou cesse de fonctionner comme prévu, vous pouvez effectuer une réinitialisation d'usine à l'aide d'une clé USB.

Avant de commencer

- [Sauvegardez directement votre base de données dans SV Control Panel](#)
- Obtenez la licence appropriée pour la version de Security Center que vous souhaitez restaurer ou installer.
- Munissez-vous de l'ID système et du mot de passe envoyés par courrier électronique lorsque vous avez acheté l'appareil. Voir [Recherche de l'ID système et de la version d'image d'un appareil Streamvault](#), page 89.
- (Recommandé) Connectez votre appareil à Internet via une connexion Ethernet filaire afin que le système puisse valider la connectivité.
REMARQUE : La validation échoue en l'absence de connexion à Internet, mais vous pouvez continuer à utiliser votre appareil.

À savoir

Le rétablissement des réglages d'usine supprime et remplace toutes les données actuellement présentes sur le lecteur Windows (C:), y compris les bases de données et les journaux. Les fichiers vidéo sur d'autres disques ne sont pas affectés.

Procédure

- 1 [Créez une clé USB de réinitialisation d'usine contenant l'image logicielle.](#)
- 2 [À l'aide de la clé USB, réinitialisez l'image sur votre appareil.](#)

Lorsque vous avez terminé

[Reconfigurez votre appareil.](#)

Rubriques connexes

[Recherche de l'ID système et de la version d'image d'un appareil Streamvault](#), page 89

Créer une clé USB de réinitialisation d'usine pour un appareil tout-en-un Streamvault

Avant de pouvoir réinitialiser l'image d'un appareil tout-en-un Streamvault^{MC}, vous devez préparer une clé USB amorçable qui contient l'image logicielle Streamvault requise.

Avant de commencer

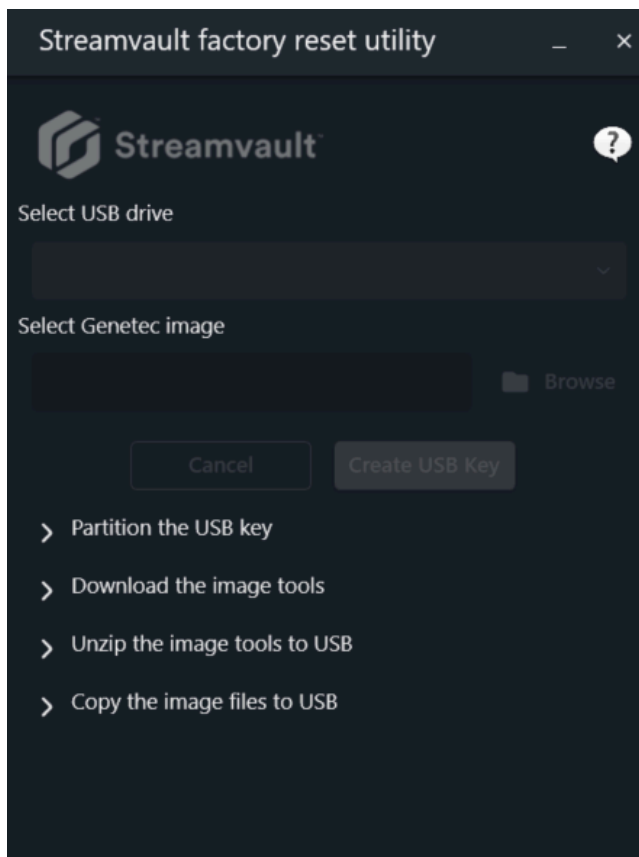
- Munissez-vous d'une clé USB avec au moins 32 Go de stockage. Certaines clés USB ne peuvent pas amorcer l'image. Si c'est le cas, essayez d'utiliser un autre modèle ou une autre marque de clé.
ATTENTION : Toutes les données sur la clé USB sont supprimées lorsque vous créez un disque amorçable.

Procédure

- 1 Contactez le [centre d'assistance technique Genetec^{MC} \(GTAC\)](#) pour récupérer l'image de récupération. L'image de récupération est fournie dans l'un des trois formats suivants :
 - Un fichier *.zip* contenant des fichiers *.swm*.
 - Un fichier *.iso* contenant les fichiers *.swm* et l'interface utilisateur de *Streamvault Factory Reset Utility*, que vous utiliserez pour réinitialiser l'image logicielle.
 - Un fichier *.iso* contenant l'assistant d'*Installation de Windows*, que vous utiliserez pour réinitialiser l'image logicielle.
- 2 Si votre image de récupération est un fichier *.zip*, décompactez le contenu dans n'importe quel dossier Windows.
- 3 Depuis la page [Téléchargement de produits](#) sur GTAP, téléchargez le créateur USB *Streamvault Factory Reset Utility*.
 - a) Dans la liste *Download Finder*, sélectionnez votre version de Security Center.
 - b) Depuis la liste *Autre*, téléchargez le pack *Streamvault Factory Reset Utility*.



- 4 Insérez la clé USB dans un port USB.
- 5 Ouvrez le Créateur USB *Streamvault Factory Reset Utility* que vous avez téléchargé depuis le TechDoc Hub.
- 6 Dans la liste **Sélectionner un lecteur USB**, sélectionnez une clé USB disposant d'au moins 32 Go d'espace disponible.



- 7 Dans la section *Sélectionner une image Genetec*, cliquez sur **Parcourir** et sélectionnez le fichier *.swm* ou *.iso* que vous avez téléchargé.

REMARQUE : Si vous avez besoin d'un fichier *.swm*, sélectionnez n'importe lequel des fichiers décompactés depuis le dossier *wim*. Tous les fichiers *.swm* de ce dossier seront copiés vers la clé USB.

- 8 Cliquez sur **Créer une clé USB**.

L'outil *Streamvault Factory Reset Utility* commence à partitionner la clé USB, à télécharger les outils d'image et à copier les fichiers d'image.

Une fois le téléchargement terminé, le message suivant s'affiche : La clé USB a été créée avec succès.

La vidéo suivante montre comment créer une clé USB de réinitialisation d'usine avec un fichier *.iso*.



Lorsque vous avez terminé

Réinitialisez l'image logicielle de votre appareil tout-en-un Streamvault .

Réinitialisation de l'image logicielle sur un appareil tout-en-un

Une fois que vous avez préparé une clé USB amorçable dotée de l'image logicielle Streamvault^{MC} requise, vous pouvez l'utiliser pour réinitialiser l'image logicielle sur un appareil Streamvault tout-en-un.

Avant de commencer

- Assurez-vous de disposer de la clé USB contenant le logiciel de récupération pour votre appareil.

À savoir

- La réinitialisation prend environ 20-30 minutes, durant lesquelles plusieurs scripts sont exécutés et l'appareil redémarre plusieurs fois.
- N'interrompez pas le processus de réinitialisation. La fermeture ou l'arrêt manuel de l'appareil peut endommager la récupération.

Procédure

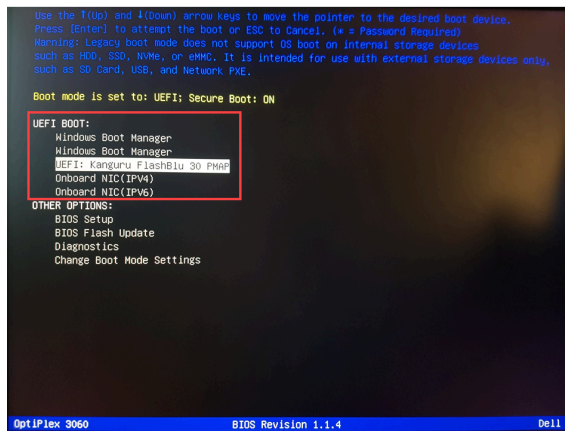
Pour réinitialiser l'image logicielle :

- Arrêtez l'appareil.
- Insérez la clé USB que vous avez créée dans un port USB.
- Mettez l'appareil sous tension et appuyez sur F12 à plusieurs reprises jusqu'à ce que le menu d'amorçage s'affiche.

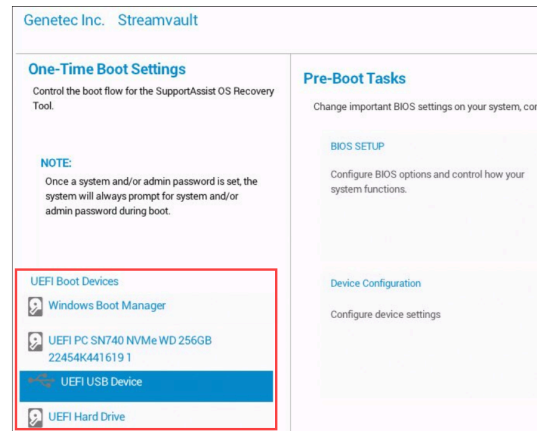
En fonction de votre appareil, le menu Démarrer de l'UEFI ou le menu Démarrer en une seule fois de Streamvault s'ouvre.

- 4 Sélectionnez le lecteur USB et appuyez sur Entrée.

REMARQUE : L'apparence de votre menu de démarrage peut être différente.



UEFI Boot menu



Streamvault One-time Boot menu

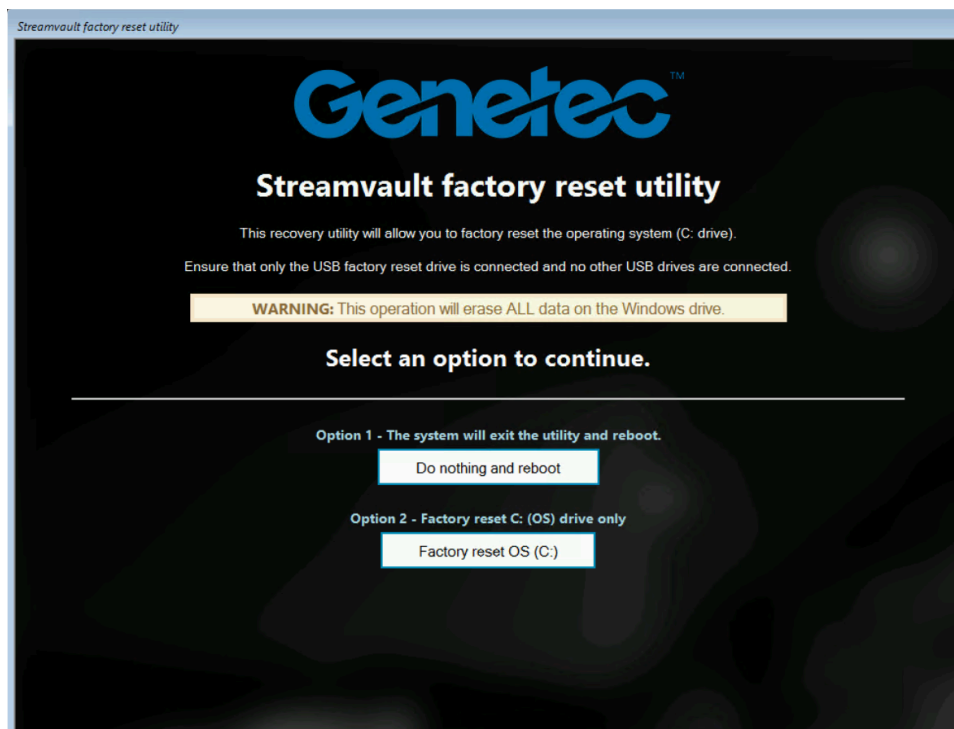
Selon l'image logicielle, soit l'assistant de *Streamvault Factory Reset Utility* ou *Installation de Windows* s'ouvre.

- 5 Réinitialisez l'image logicielle à l'aide de l'outil qui s'applique à votre appareil :

- [Streamvault Factory Reset Utility](#)
- [Assistant d'installation de Windows](#)

Pour réinitialiser l'image logicielle à l'aide de Streamvault Factory Reset Utility :

- 1 Lorsque le port USB démarre en mode récupération, sélectionnez **Rétablir les réglages d'usine du SE (C:)** pour formater et réinstaller le lecteur système de l'appareil.



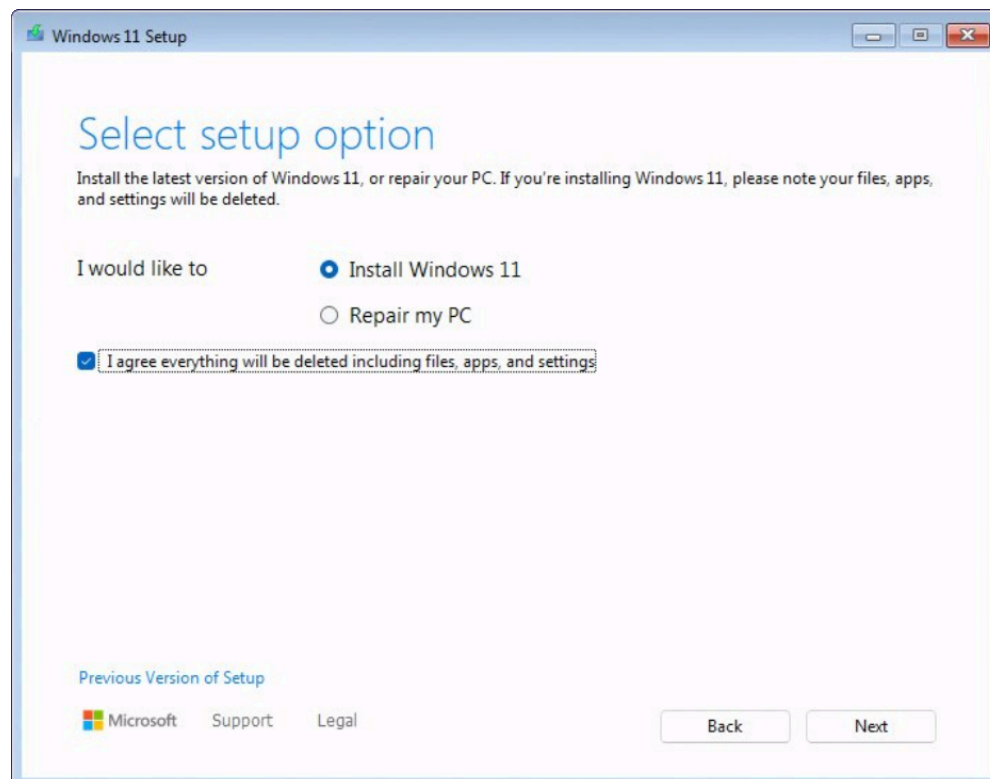
- 2 Lorsque vous y êtes invité, tapez Oui et appuyez sur Entrée. Attendez la fin de la réinitialisation des réglages d'usine.
- 3 Une fois le rétablissement des réglages d'usine terminé, retirez la clé USB de l'appareil et appuyez sur Entrée pour redémarrer.

- 4 Dans la boîte de dialogue *Genetec^{MC} Product Validator*, entrez le numéro de pièce de l'appareil (n ° de produit) et le numéro de série Genetec^{MC}.
Ces numéros se trouvent sur l'étiquette Genetec située en haut de l'appareil. S'il n'y a pas d'étiquette, vous pouvez entrer n'importe quel texte pour continuer.
Le bouton **Démarrer** apparaît.
- 5 Cliquez sur **Démarrer**.
L'un des messages d'état suivants est affiché :
 - **VALIDÉ** : Le processus a réussi. Passez à l'étape suivante.
 - **VALIDÉ - Pas de transmission** : Le processus a réussi, mais aucune connexion Internet n'était disponible à ce moment-là. Passez à l'étape suivante.
 - **ÉCHEC** : Le processus a échoué. Contactez le [centre d'assistance technique Genetec^{MC} \(GTAC\)](#).
- 6 Si vous recevez un message *PASS* ou *PASS - Aucune transmission*, fermez la fenêtre *Genetec^{MC} Product Validator*.
- 7 Attendez que le script en arrière-plan se ferme, puis redémarrez l'appareil.

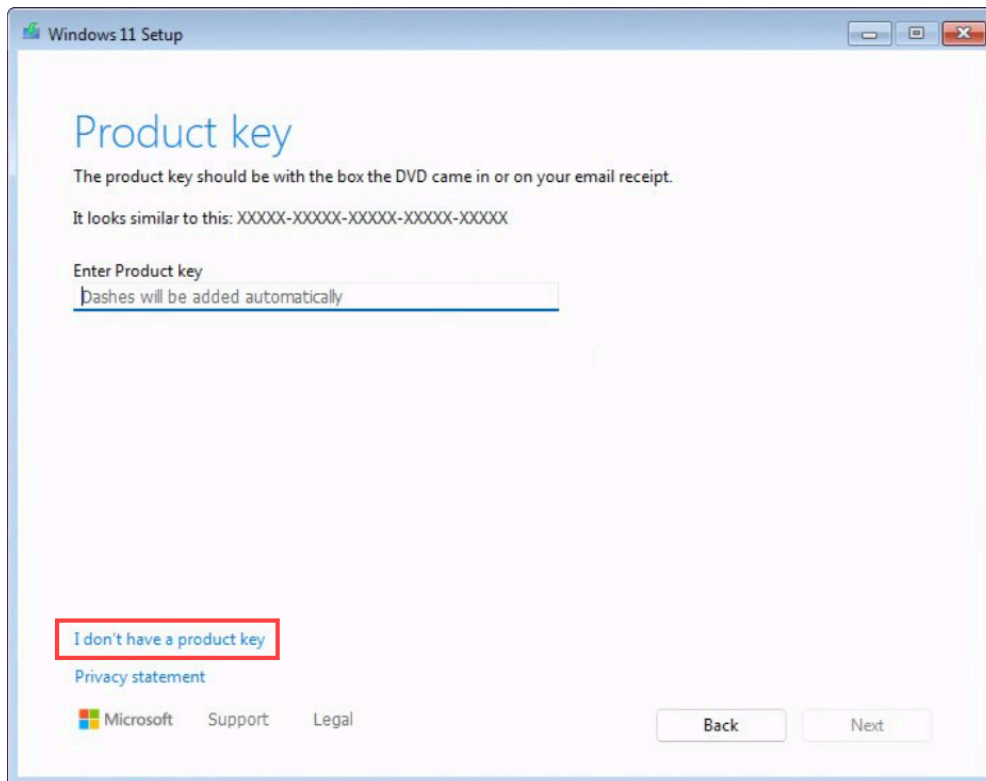
Pour réinitialiser l'image logicielle à l'aide de l'assistant d'installation de Windows :

- 1 Sur l'écran *Sélectionner les paramètres de langue*, sélectionnez les réglages de langue et d'heure de votre choix, puis cliquez sur **Suivant**.
- 2 Sur l'écran *Sélectionner les réglages du clavier*, sélectionnez votre clavier préféré et cliquez sur **Suivant**.
- 3 Sur l'écran *Sélectionner l'option de configuration*, sélectionnez **Installer Windows X**, où X correspond à la version de Windows que vous installez. Confirmez que vos fichiers, applications et paramètres seront supprimés et cliquez sur **Suivant**.

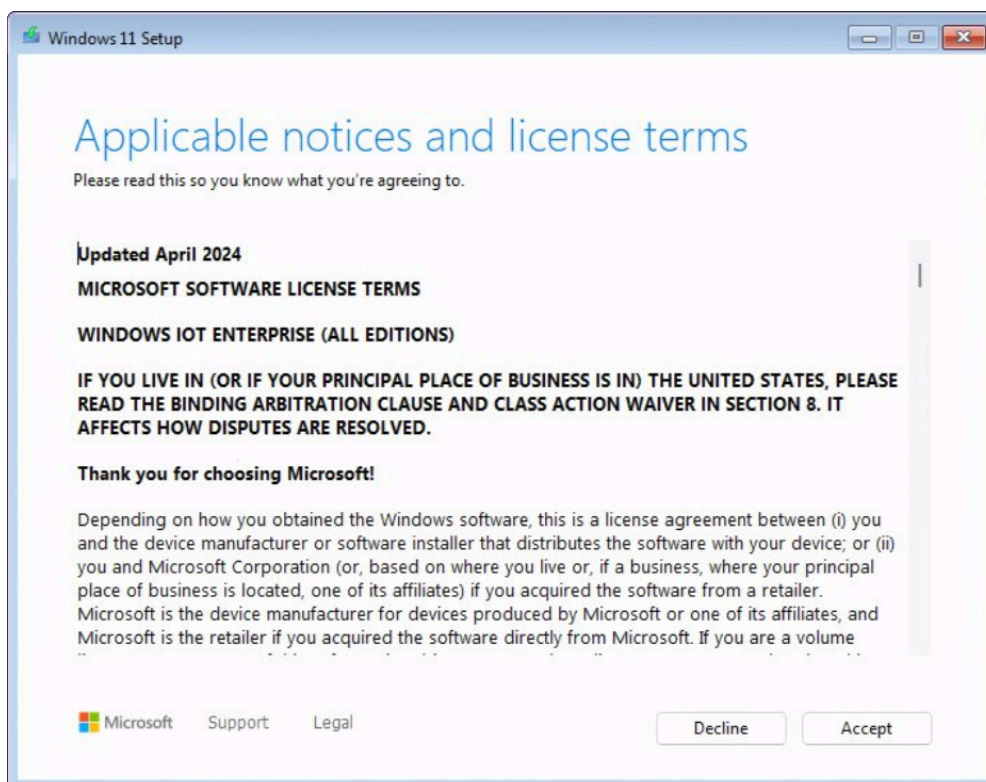
REMARQUE : Les archives vidéo stockées sur le disque vidéo secondaire ne sont pas affectées. Seuls les fichiers sur le disque du SE sont supprimés.



- 4 Sur l'écran *Clé de produit*, procédez de l'une des manières suivantes :
- Si l'appareil est connecté à Internet, cliquez sur **Je n'ai pas de clé de produit** pour continuer. L'appareil récupère automatiquement ses données d'activation auprès de Microsoft.
 - Si l'appareil n'est pas connecté à Internet, entrez la clé de licence située sur l'étiquette de [Certificat d'authenticité \(COA\)](#) apposée sur votre appareil et cliquez sur **Suivant**.



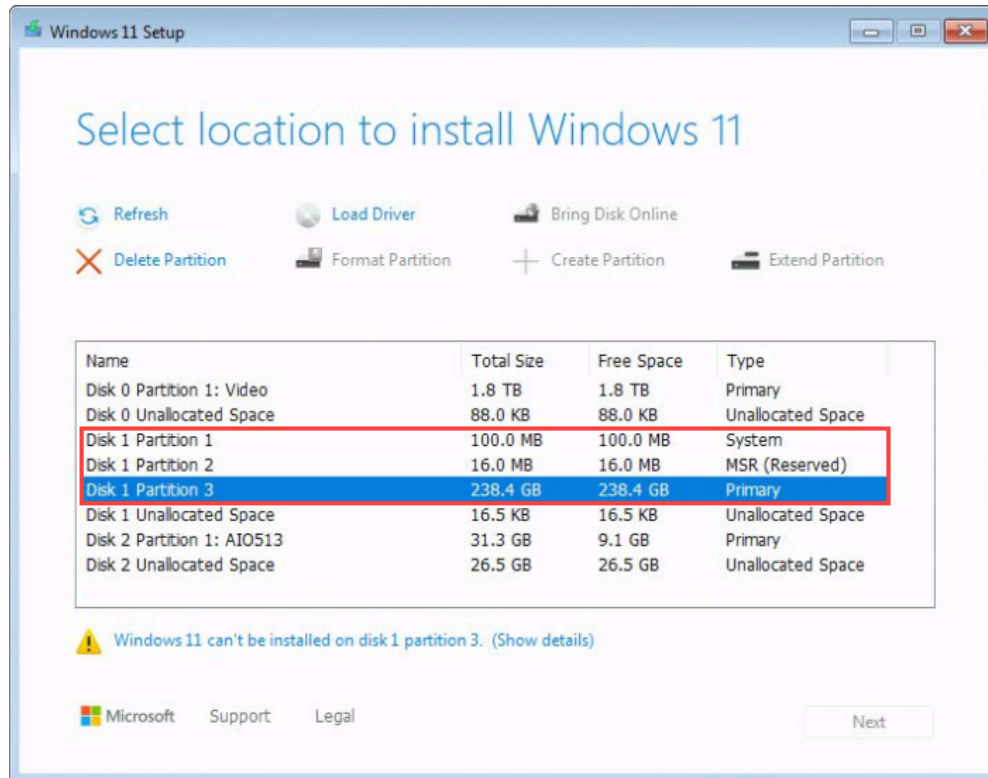
- 5 Sur l'écran *Avis et conditions de licence applicables*, lisez les termes de la licence et cliquez sur **Accepter**.



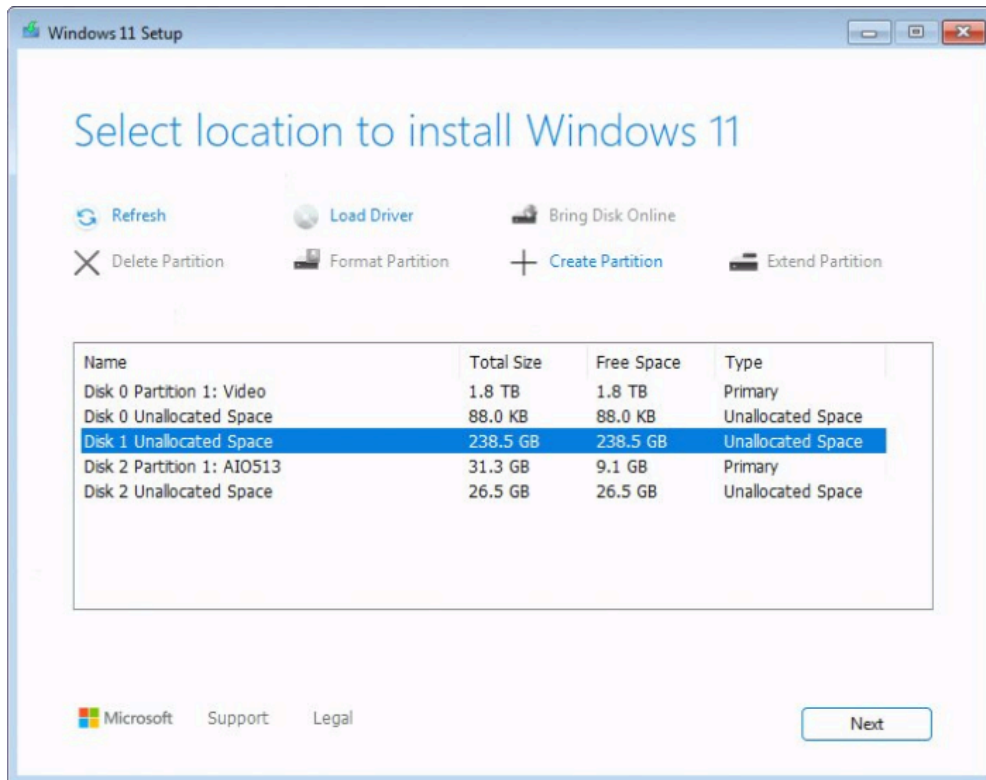
- 6 Sur l'écran *Sélectionnez l'emplacement d'installation de Windows X*, supprimez les partitions principale, système et MSR (le cas échéant) sur le disque du SE.

Seul l'espace non alloué restera sur le disque du SE, et l'assistant d'installation de Windows recréera automatiquement les partitions supprimées pendant le processus d'installation.

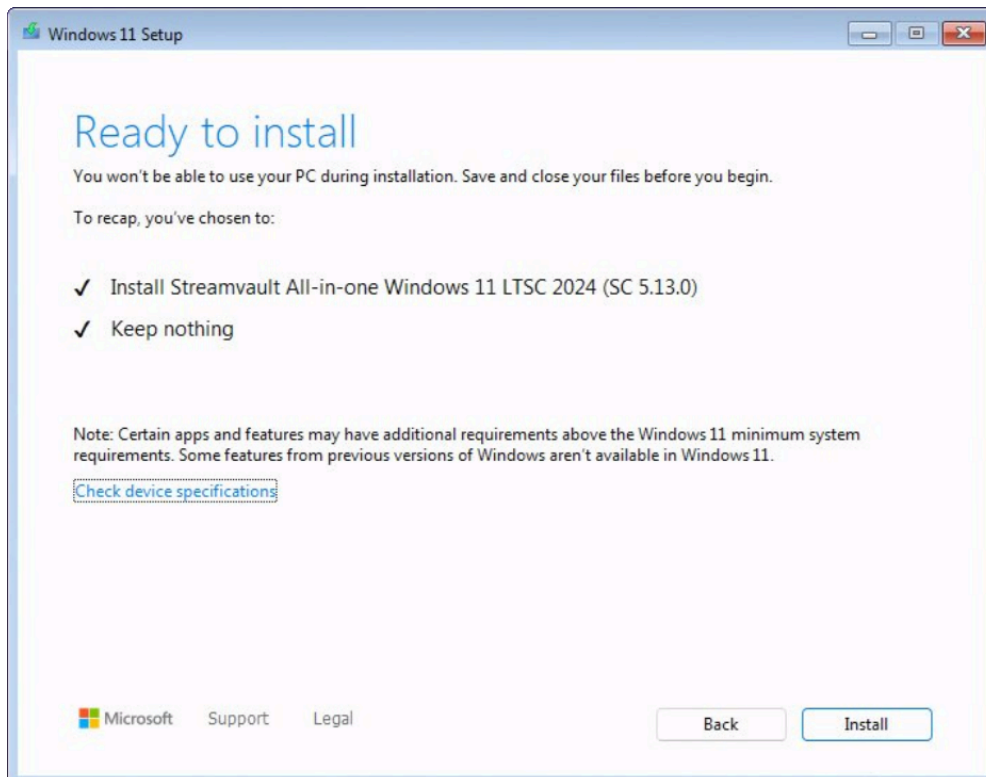
ATTENTION : La partition principale sur le disque du SE a généralement une taille inférieure à 1 To. Ne supprimez pas la partition principale sur le disque de stockage vidéo, qui stocke vos archives vidéo.



- 7 Sélectionnez l'espace non alloué sur le disque du SE et cliquez sur **Suivant**.



- 8 Sur le *Prêt à installer* écran, cliquez sur **Installer**.



- 9 Lorsque l'installation est terminée, le système redémarre Windows et un script est automatiquement exécuté pour finaliser l'installation. Lorsque l'exécution du script est terminée, redémarrez l'appareil.

Regardez cette vidéo pour savoir comment réinitialiser l'image logicielle sur un appareil tout-en-un à l'aide d'une clé USB amorçable contenant des fichiers *.swm*.



Lorsque vous avez terminé

- Ouvrez une session Windows avec le nom d'utilisateur et mot de passe par défaut indiqués sur l'autocollant apposé sur l'appareil.
- [Activez votre licence Security Center.](#)
- Si vous avez sauvegardé les configurations de Security Center avant de rétablir les réglages d'usine, [restaurez-les avec SV Control Panel.](#)
- [Reconfigurez votre appareil.](#)

Rétablir les réglages d'usine sur un appareil Streamvault poste de travail ou serveur

Si le logiciel sur votre poste de travail ou serveur Streamvault^{MC} ne démarre plus ou présente des dysfonctionnements, vous pouvez rétablir les réglages d'usine à l'aide d'une clé USB.

Avant de commencer

- Sauvegardez toute la configuration de Security Center à l'aide de SV Control Panel. Pour en savoir plus, voir [Sauvegarder la base de données du Répertoire](#), page 37.
- Munissez-vous d'une clé USB avec au moins 32 Go de stockage. Certaines clés USB ne peuvent pas amorcer l'image. Si c'est le cas, essayez d'utiliser un autre modèle ou une autre marque de clé.
ATTENTION : Toutes les données sur la clé USB sont supprimées lorsque vous créez un disque amorçable.
- Obtenez la licence appropriée pour la version de Security Center que vous souhaitez restaurer ou installer.
- Munissez-vous de l'ID système et du mot de passe envoyés par courrier électronique lorsque vous avez acheté l'appareil.

À savoir

- **S'applique à** : Tous les modèles commençant par SVW, SVR et SVA, et tous les serveurs dont le numéro de modèle est SV-1000E et au-delà.
- Pour les appareils tout-en-un, consultez [Rétablir les réglages d'usine sur un appareil tout-en-un Streamvault](#), page 93.
- Une réinitialisation d'usine supprime toutes les données actuellement présentes sur le lecteur système (OS), mais n'affecte pas les paramètres du volume RAID par défaut.
- La réinitialisation peut échouer si les paramètres par défaut des disques durs, volumes RAID ou partitions de l'appareil ont été modifiés. Dans ce cas, contactez le [centre d'assistance technique Genetec^{MC} \(GTAC\)](#).

Procédure

- 1 [Créez une clé USB de réinitialisation d'usine.](#)
- 2 [À l'aide de la clé USB, réinitialisez l'image sur votre appareil.](#)

Lorsque vous avez terminé

[Configurez votre appareil.](#)

Rubriques connexes

[Recherche de l'ID système et de la version d'image d'un appareil Streamvault](#), page 89

Créer une clé USB de réinitialisation d'usine pour un appareil de type poste de travail ou serveur Streamvault

Avant de pouvoir réinitialiser l'image d'un appareil de type poste de travail ou serveur Streamvault^{MC}, vous devez préparer une clé USB amorçable qui contient l'image logicielle Streamvault requise.

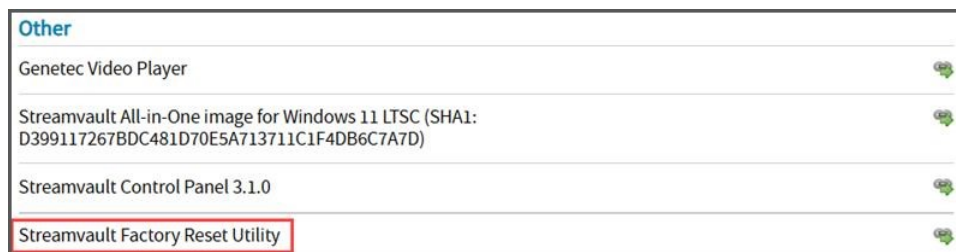
Avant de commencer

Munissez-vous d'une clé USB avec au moins 32 Go de stockage. Certaines clés USB ne peuvent pas amorcer l'image. Si c'est le cas, essayez d'utiliser un autre modèle ou une autre marque de clé.

ATTENTION : Toutes les données sur la clé USB sont supprimées lorsque vous créez un disque amorçable.

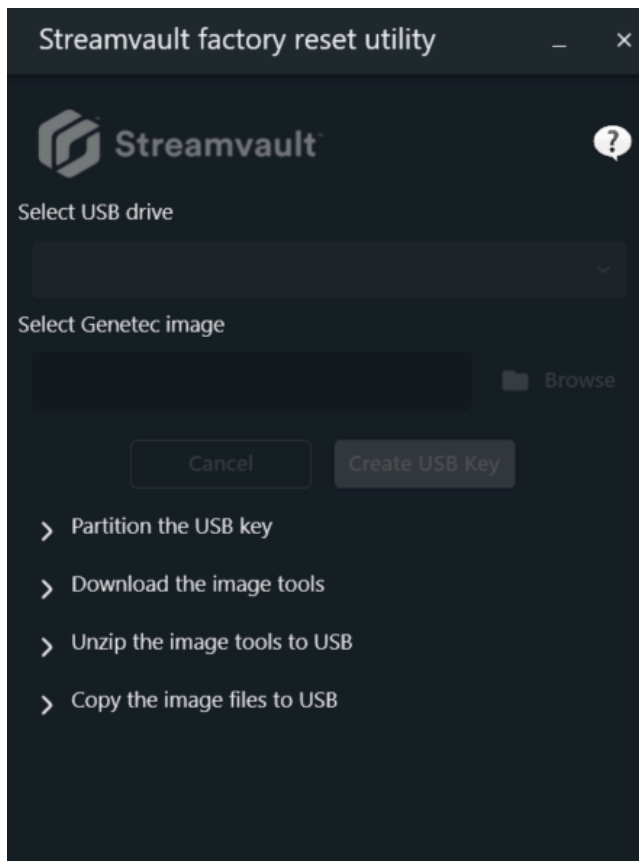
Procédure

- 1 Contactez le [centre d'assistance technique Genetec^{MC} \(GTAC\)](#) pour récupérer l'image de récupération. L'image de récupération est fournie dans l'un des trois formats suivants :
 - Un fichier *.zip* contenant des fichiers *.swm*.
 - Un fichier *.iso* contenant les fichiers *.swm* et l'interface utilisateur de *Streamvault Factory Reset Utility*, que vous utiliserez pour réinitialiser l'image logicielle.
 - Un fichier *.iso* contenant l'assistant d'*Installation de Windows*, que vous utiliserez pour réinitialiser l'image logicielle.
- 2 Si votre image de récupération est un fichier *.zip*, décompactly le contenu dans n'importe quel dossier Windows.
- 3 Depuis la page [Téléchargement de produits](#) sur GTAP, téléchargez le créateur USB *Streamvault Factory Reset Utility*.
 - a) Dans la liste *Download Finder*, sélectionnez votre version de Security Center.
 - b) Depuis la liste *Autre*, téléchargez le pack *Streamvault Factory Reset Utility*.



- 4 Insérez la clé USB dans un port USB.
- 5 Ouvrez le Créateur USB de *Streamvault Factory Reset Utility*.

- 6 Dans la liste **Sélectionner un lecteur USB**, sélectionnez une clé USB disposant d'au moins 32 Go d'espace disponible.



- 7 Dans la section *Sélectionner une image Genetec*, cliquez sur **Parcourir** et sélectionnez le fichier *.swm* ou *.iso* que vous avez téléchargé.
Si vous avez besoin d'un fichier *.swm*, sélectionnez l'image requise depuis le dossier *<service tag number>*.
- 8 Cliquez sur **Créer une clé USB**.
L'outil *Streamvault Factory Reset Utility* commence à partitionner la clé USB, à télécharger les outils d'image et à copier les fichiers d'image.

Une fois le téléchargement terminé, le message suivant s'affiche : La clé USB a été créée avec succès.

La vidéo suivante montre comment créer une clé USB de réinitialisation d'usine avec un fichier *.iso*.



Lorsque vous avez terminé

Réinitialisez l'image logicielle de votre appareil de type poste de travail ou serveur Streamvault .

Réinitialiser l'image logicielle sur un appareil de type poste de travail ou serveur Streamvault

Une fois que vous avez préparé une clé USB amorçable dotée de l'image logicielle Streamvault^{MC}, vous pouvez l'utiliser pour réinitialiser l'image logicielle sur un appareil de type poste de travail ou serveur.

Avant de commencer

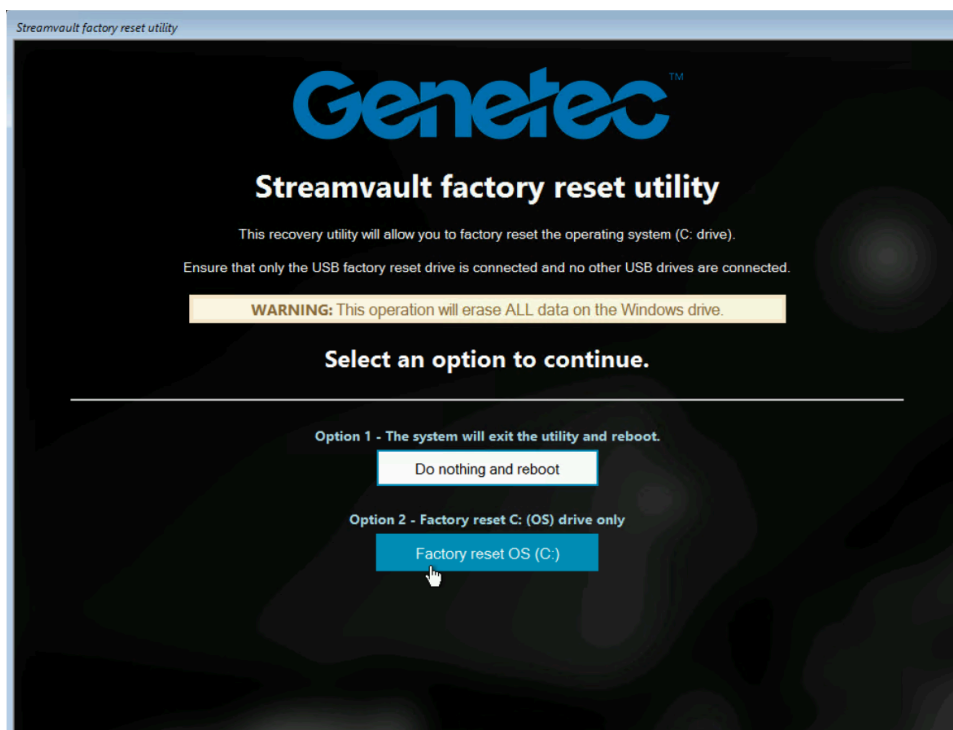
- Assurez-vous de disposer de la clé USB contenant le logiciel de récupération pour votre appareil.

À savoir

- La réinitialisation n'affecte pas les réglages d'usine RAID par défaut du disque.
- La réinitialisation peut échouer si les paramètres par défaut des disques durs, volumes RAID ou partitions de l'appareil ont été modifiés. Dans ce cas, contactez le [centre d'assistance technique Genetec^{MC} \(GTAC\)](#).

Procédure

- Arrêtez l'appareil.
- Insérez la clé USB amorçable que vous avez créée dans un port USB.
- Mettez l'appareil Streamvault sous tension.
- À l'invite, appuyez sur F12.
Le *Boot Manager* s'ouvre. Cliquez sur **One-shot UEFI Boot Menu**.
- Sélectionnez votre clé USB, puis appuyez sur Entrée.
Streamvault Factory Reset Utility s'ouvre.
- Cliquez sur **Rétablir les réglages d'usine du SE (C:)**.



Une invite de commande apparaît et *Streamvault Factory Reset Utility* analyse le système pour détecter le disque système.

- 7 À l'invite de commande, tapez Yes pour confirmer que le bon disque dur a été détecté, puis appuyez sur Entrée pour lancer le rétablissement des réglages d'usine.
IMPORTANT : N'interrompez pas, n'éteignez pas ou ne redémarrez pas le poste durant le processus de réapplication de l'image. Comptez jusqu'à une vingtaine de minutes, selon la vitesse de votre clé USB.
- 8 Une fois que le rétablissement des réglages d'usine est terminé, appuyez sur Entrée lorsque vous êtes invité à redémarrer le poste.
- 9 Retirez la clé USB de l'ordinateur.

L'état par défaut du poste est à présent rétabli.

Regardez cette vidéo pour savoir comment réinitialiser l'image logicielle sur un appareil de type poste de travail ou serveur Streamvault.



Lorsque vous avez terminé

- Ouvrez une session Windows avec le nom d'utilisateur et mot de passe par défaut indiqués sur l'autocollant apposé sur l'appareil.
- [Activez votre licence Security Center.](#)
- Si vous avez sauvegardé les configurations de Security Center avant de rétablir les réglages d'usine, [restaurez-les avec SV Control Panel.](#)
- [Reconfigurez votre appareil.](#)

Les contrôleurs Mercury EP restent hors ligne lorsque TLS 1.1 est désactivé

Après l'inscription d'un contrôleur Mercury EP dans Security Center, l'unité ne se connecte pas. Vous ne recevez aucune erreur ni aucun avertissement concernant ce problème.

S'applique à :

- Streamvault^{MC} SV-100E 16.3 et versions ultérieures
- Streamvault^{MC} SV-300E 16.3 et versions ultérieures
- Streamvault^{MC} SV-350E 16.3 et versions ultérieures

Cause

Tous les contrôleurs Mercury EP nécessitent le protocole Transport Layer Security (TLS) 1.1 pour communiquer avec Security Center. Toutefois, le protocole est désactivé sur tous les appareils tout-en-un Streamvault^{MC} 16.3 et ultérieur.

Solution

[Activez TLS 1.1.](#)

Activer Transport Layer Security (TLS)

Les protocoles Transport Layer Security (TLS) 1.0 et 1.1 présentent plusieurs vulnérabilités majeures et sont donc désactivées sur les appareils Streamvault^{MC}. Si un appareil inscrit dans Security Center nécessite l'un de ces protocoles pour communiquer, vous devez activer le protocole sur votre appareil.

À savoir

- TLS 1.1 est désactivé dans l'image logicielle Streamvault 16.3 et ultérieur.
- TLS 1.0 est désactivé dans l'image logicielle Streamvault 16.0 et ultérieur.
- Activez uniquement la version de TLS requise par votre appareil.
- Activez TLS sur les nœuds serveur (entrants) et client (sortants).
- Par souci de sécurité, les options de Propriétés Internet sont désactivées sur les appareils. Si votre appareil dispose du service Streamvault, vous pouvez activer TLS à partir de l'éditeur de stratégie de groupe locale. Si votre appareil ne dispose pas du service Streamvault, vous ne pouvez activer TLS qu'à partir de l'éditeur de registre Windows.

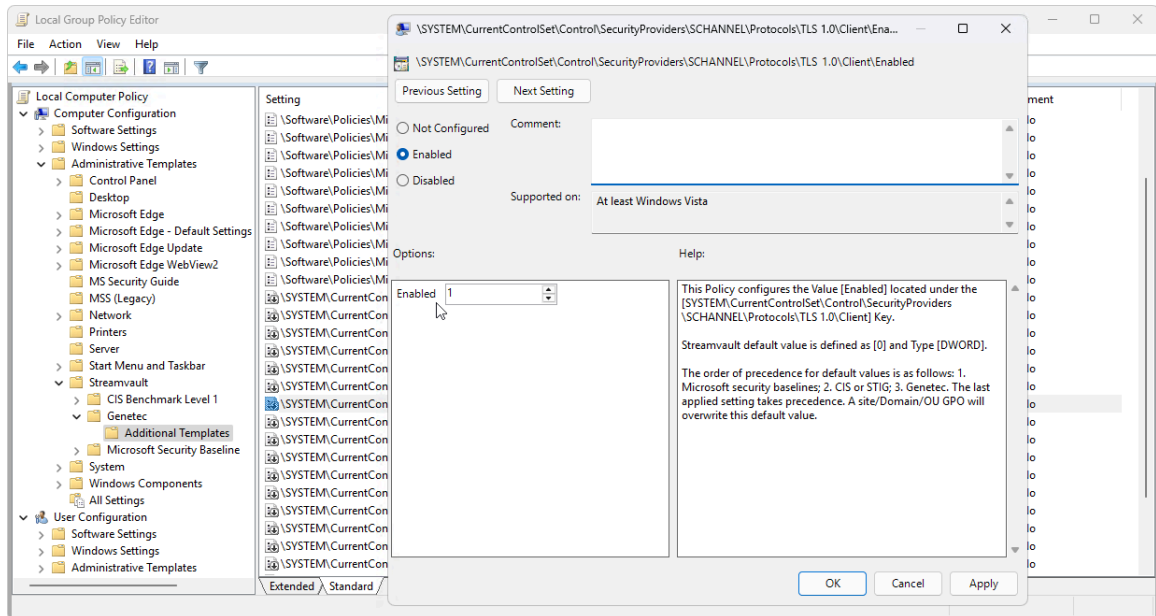
Procédure

Pour activer TLS sur un appareil avec le service Streamvault :

- 1 Ouvrez une invite de commande en tant qu'administrateur et exécutez `gpedit.msc`.
L'éditeur de stratégie de groupe locale s'ouvre.
- 2 Accédez à **Configuration ordinateur > Modèles d'administration > Streamvault > Genetec > Modèles supplémentaires**.
- 3 Activez TLS 1.*n* sur le client, où *n* représente le numéro de version mineure :
 - a) Cliquez avec le bouton droit sur `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n\Client\Enabled` et cliquez sur **Modifier**.
 - b) Définissez **Enabled** to 1 et cliquez sur **Appliquer > OK**.
 - c) Cliquez avec le bouton droit sur `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n\Client\DisabledByDefault` et cliquez sur **Modifier**.
 - d) Définissez **DisabledByDefault** sur 0 and cliquez sur **Appliquer > OK**.

4 Activer TLS 1.n sur le serveur :

- Cliquez avec le bouton droit sur `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n\Server\Enabled` et cliquez sur **Modifier**.
- Définissez **Enabled** to 1 et cliquez sur **Appliquer** > **OK**.
- Cliquez avec le bouton droit sur `\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n\Server\DisabledByDefault` et cliquez sur **Modifier**.
- Définissez **DisabledByDefault** sur 0 and cliquez sur **Appliquer** > **OK**.

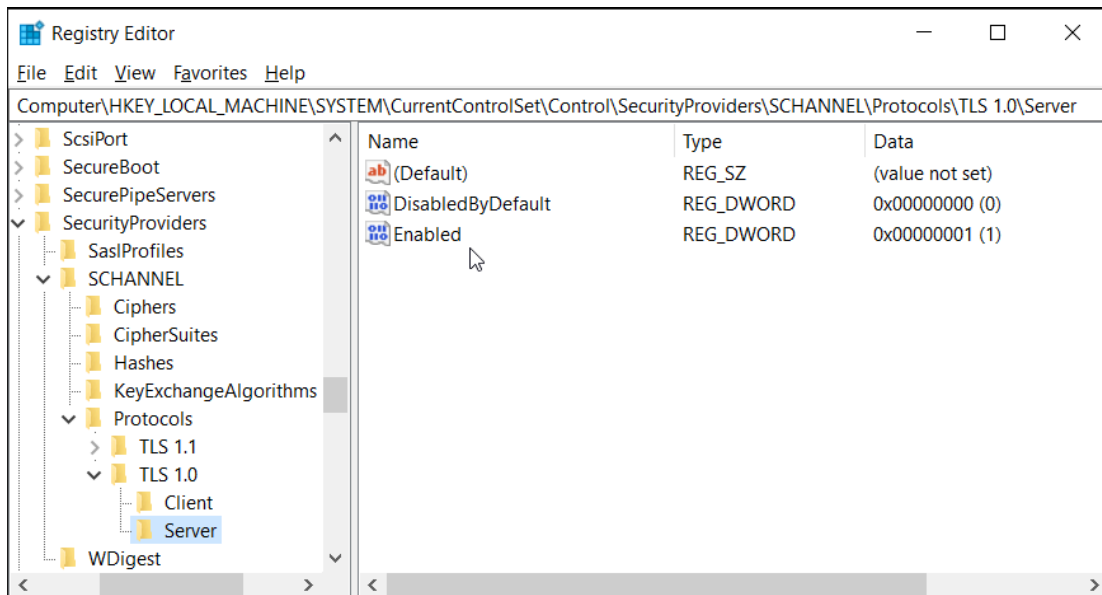


5 Redémarrez Windows.

Pour activer TLS sur un appareil sans le service Streamvault :

- Ouvrez l'Éditeur du Registre Windows.

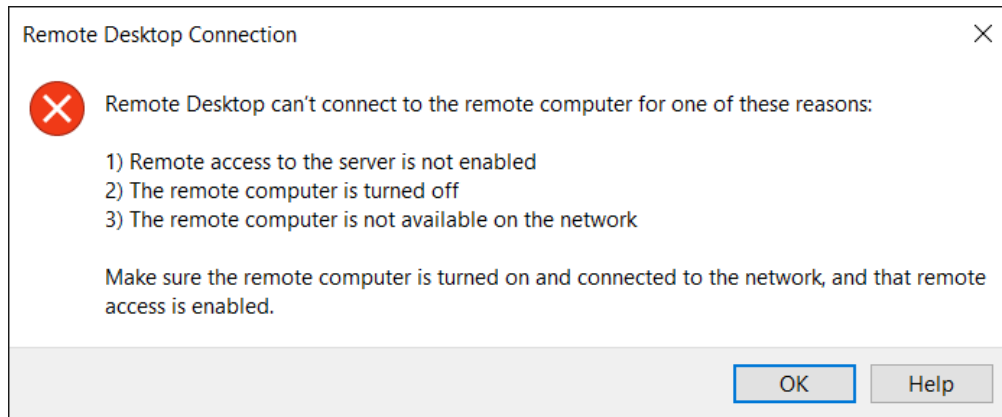
- 2 Activez TLS 1.*n*, où *n* représente le numéro de version mineure :
- a) Naviguez jusqu'à `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n`.
 - b) Sélectionnez le nœud **Serveur**, réglez **DisabledByDefault** sur 0, et réglez **Activé** sur 1.
 - c) Sélectionnez le nœud **Client**, réglez **DisabledByDefault** sur 0, et réglez **Activé** sur 1.



- 3 Redémarrez Windows.

Le Bureau à distance ne peut pas se connecter à un appareil Streamvault

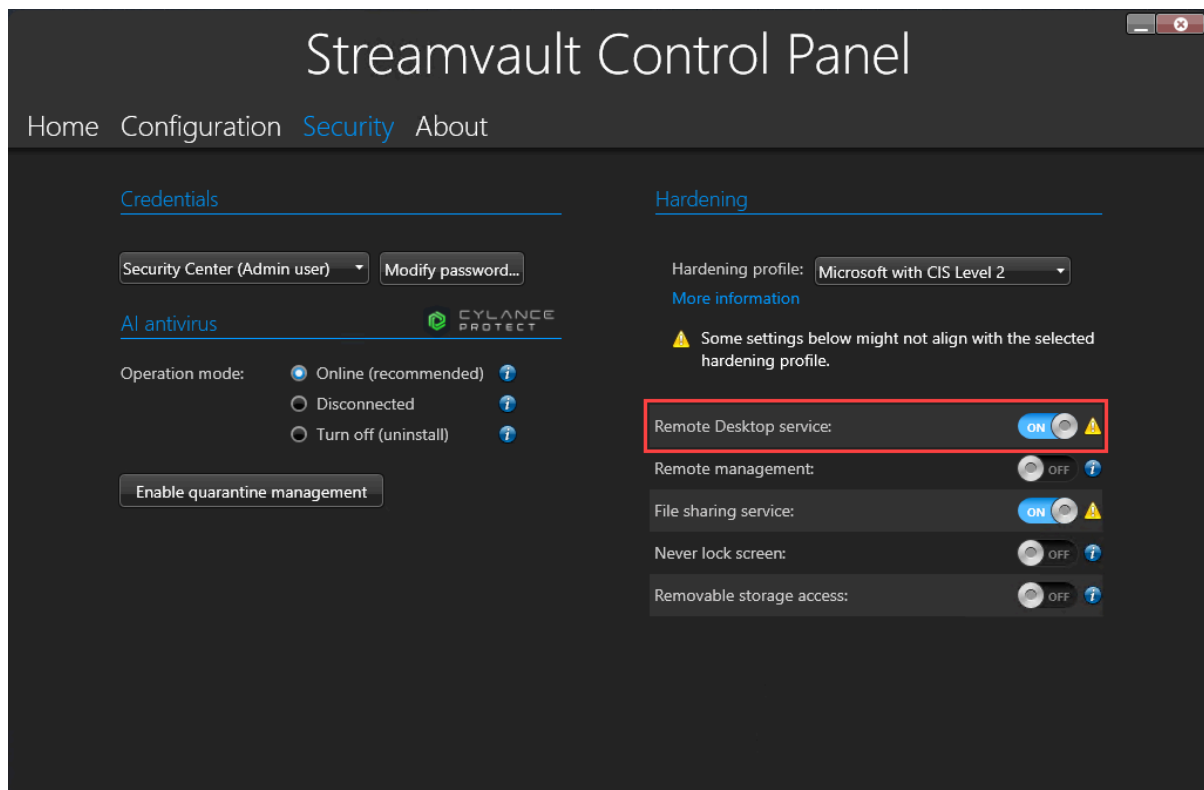
Lorsque vous tentez d'accéder à un appareil Streamvault^{MC} avec le Bureau à distance, vous recevez un message indiquant que le Bureau à distance ne peut pas se connecter à l'ordinateur distant.



Le service Bureau à distance est désactivé dans SV Control Panel

Description : Par défaut, l'accès à distance est désactivé sur les appareils pour maximiser la sécurité.

Solution : [Activez l'accès à distance sur l'appareil](#). Sur la page *Sécurité* de SV Control Panel, activez le service **Bureau à distance**.



Le bureau à distance n'est pas autorisé sous Windows

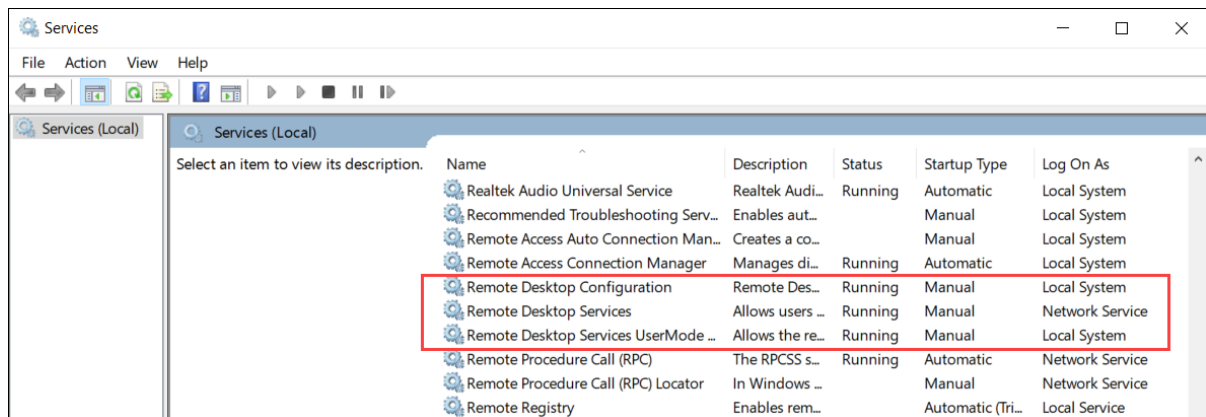
Description : bien que le **service Bureau à distance** soit activé dans SV Control Panel, ce paramètre n'est actuellement pas autorisé dans Windows.

Solution : remplacez le paramètre Windows en désactivant puis en activant l'option **Service Bureau à distance**.

Les Services Bureau à distance ne sont pas lancés

Description : Les Services Bureau à distance ont été arrêtés dans Windows.

Solution : Ouvrez la console Services Windows, vérifiez que **Services Bureau à distance** est connecté en tant qu'utilisateur de **Service réseau** et que les autres services Bureau à distance sont en cours d'exécution.

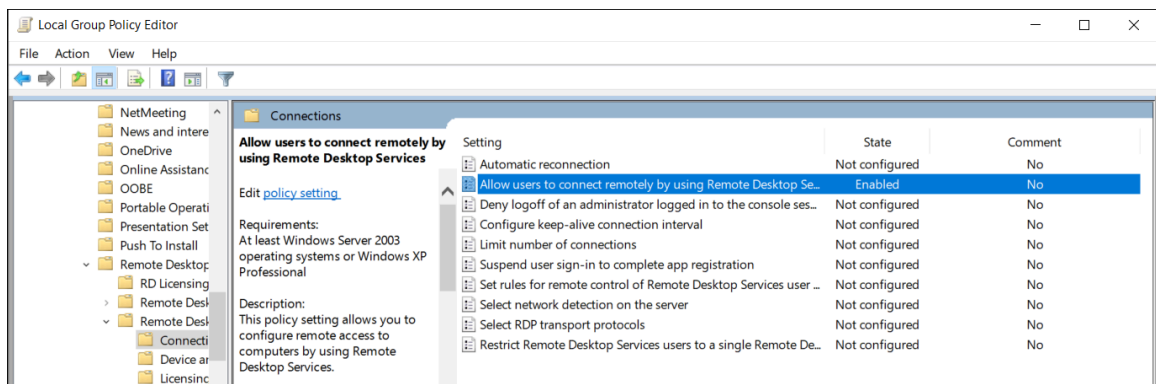


Les Services Bureau à distance sont refusés

Description : Windows est configuré pour refuser l'accès aux Services Bureau à distance aux utilisateurs distants.

Solution : Autorisez les accès à distance à l'appareil à l'aide des Services Bureau à distance :

- Ouvrez une invite de commande en tant qu'administrateur et exécutez `gpedit .msc`.
- Accédez à **Configuration ordinateur > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Connexions**.
- Activez **Autoriser les utilisateurs à se connecter à distance à l'aide des services Bureau à distance**.

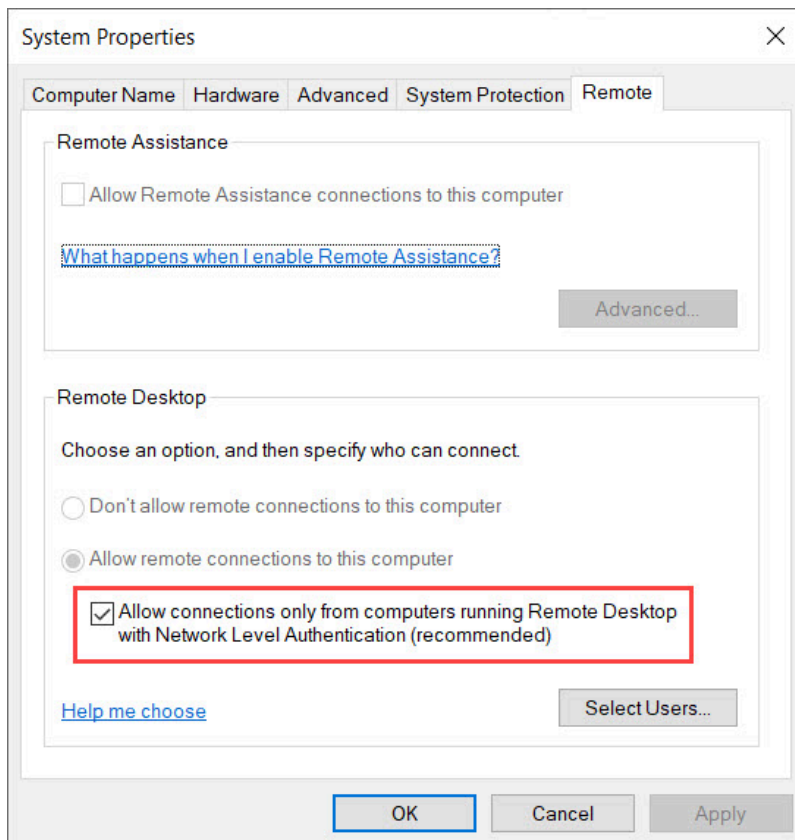


- Dans l'invite de commande, exécutez `gpupdate /force`.

5. Dans le tableau de configuration Windows, accédez à **Système et sécurité > Paramètres d'utilisation à distance Autoriser l'accès à distance**.

La fenêtre *Propriétés système* s'ouvre sur l'onglet **Utilisation à distance**.

6. Dans la section *Bureau à distance*, assurez-vous que la case **N'autoriser que la connexion des ordinateurs exécutant le Bureau à distance avec authentification NLA (recommandé)** est cochée.



Les stratégies de groupe locales refusent les accès à distance

Description : Les stratégies de groupe locales sont configurées pour bloquer les accès à distance à votre appareil.

Solution : Configurez les stratégies de groupe sur votre appareil pour autoriser l'accès à distance :

1. Ouvrez une invite de commande en tant qu'administrateur et exécutez `gpedit.msc`.
2. Accédez à **Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits d'utilisateur**.
3. Vérifiez les paramètres de stratégies de groupe suivants :
 - **Autoriser l'ouverture de session par les services Bureau à distance** est défini sur **Administrateurs**.
 - **Interdire l'accès à cet ordinateur à partir du réseau** est défini sur **Invités**.
 - **Interdire l'ouverture de session par les services Bureau à distance** est défini sur **Invités**.

L'authentification NTLMv2 n'est pas prise en charge

Description : L'appareil ou l'ordinateur distant ne prend pas en charge l'authentification NTLMv2.

REMARQUE : Si tous les ordinateurs client prennent en charge NTLMv2, Microsoft et plusieurs organismes indépendants recommandent vivement la stratégie *Envoyer uniquement des réponses NTLMv2*. Consultez les

meilleures pratiques et considérations de sécurité dans « [Sécurité réseau : niveau d'authentification LAN Manager](#) » de Microsoft avant de modifier vos réglages.

Solution : Pour faire en sorte que votre environnement autorise l'authentification NTLMv2 :

1. Ouvrez une invite de commande en tant qu'administrateur et exécutez `gpedit.msc`.
2. Accédez à **Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Sécurité réseau : niveau d'authentification LAN Manager**.
3. Définissez la stratégie sur **Envoyer LM et NTLM - utiliser la sécurité de session NTLMv2 si négociée**.

Nous contacter

Solution : si la connexion Bureau à distance est toujours impossible, [contactez le Centre d'assistance technique de Genetec \(GTAC\)](#).

Rubriques connexes

[Autoriser les connexions Bureau à distance à un appareil Streamvault](#), page 91

Suppression des restrictions des comptes utilisateur non administrateurs

Par défaut, les comptes utilisateur non administrateurs, y compris l'opérateur, ont un accès limité aux fonctionnalités de Streamvault^{MC} Control Panel. Vous pouvez supprimer les restrictions de ces comptes pour leur donner davantage d'accès aux fonctionnalités.

Avant de commencer

- Seule une personne connectée en tant qu'administrateur peut supprimer les restrictions des comptes non administrateurs.
- Les restrictions ne peuvent être supprimées que sur les systèmes dotés du service Streamvault.

Procédure

- 1 Ouvrez l'Explorateur de fichiers et accédez à *C:\Windows\System32\GroupPolicyUsers*.
- 2 Supprimez le dossier *S-1-5-32-545* et tout son contenu. Ce dossier contient les restrictions pour les non-administrateurs.
- 3 Redémarrez Windows.

Les comptes locaux ne peuvent pas accéder au Bureau à distance, au service de partage de fichier et à la gestion à distance

Lorsque les options **Service Bureau à distance**, **Gestion à distance** ou **Service de partage de fichiers** sont activées dans SV Control Panel, les comptes locaux ne peuvent toujours pas accéder aux fonctionnalités.

Ce comportement s'applique aux produits Windows Server dotés de SV Control Panel 3.0 et versions ultérieures :

- Série Streamvault^{MC} SV-1000E
- Série Streamvault^{MC} SV-2000E
- Série Streamvault^{MC} SV-4000EX
- Série Streamvault^{MC} SV-7000EX

Par défaut, le service Bureau à distance, la gestion à distance et le service de partage de fichiers sont désactivés pour l'administrateur local et les comptes locaux, tels que l'opérateur. Avec les versions précédentes de SV Control Panel, l'administrateur local et les comptes locaux avaient tous accès à ces fonctionnalités lorsqu'elles étaient activées. À partir de SV Control Panel 3.0, seul l'administrateur local y a accès lorsque les fonctionnalités sont activées.

Ce nouveau comportement est contrôlé via la stratégie de sécurité réseau **Interdire l'accès à cet ordinateur à partir du réseau** et est conforme à la ligne directrice de sécurité de Microsoft pour Windows Server.

Activer les services connexes à la carte à puce

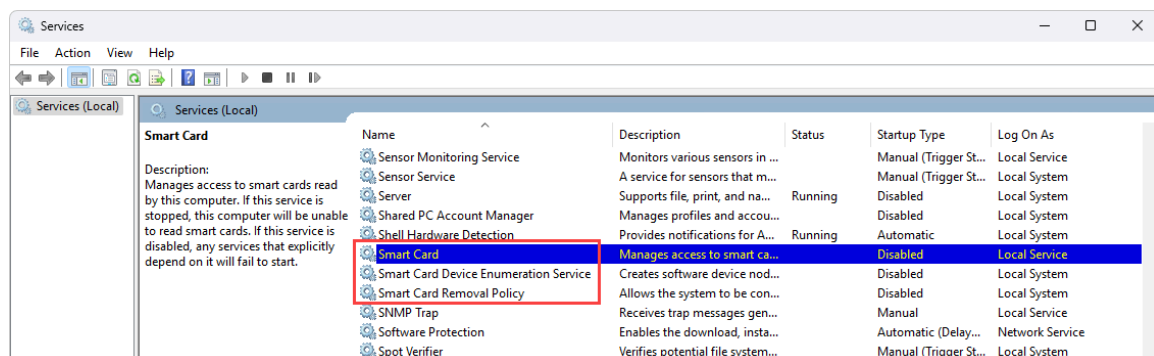
Si vous avez effectué une mise à niveau vers SV Control Panel 3.0 à partir d'une ancienne version et que vous souhaitez activer les services connexes à la carte à puce, vous pouvez le faire via l'application Services Windows.

À savoir

L'option **Activer la prise en charge des cartes à puce** n'est pas disponible dans SV Control Panel 3.0, car les services de carte à puce sont activés par défaut.

Procédure

- 1 Sous Windows, exécutez *services.msc* pour ouvrir l'application *Services*.
- 2 Activez le service **Carte à puce**.
 - a) Cliquez avec le bouton droit sur le service **Carte à puce** et sélectionnez **Propriétés**.
La boîte de dialogue *Propriétés* s'ouvre.
 - b) Dans l'onglet **Général**, recherchez le champ **Type de démarrage** et sélectionnez **Automatique**.
 - c) Cliquez sur **Appliquer** > **OK**.
- 3 Activez le **service d'énumération des appareils de carte à puce**.
 - a) Cliquez avec le bouton droit sur **Service d'énumération des appareils de carte à puce** et sélectionnez **Propriétés**.
La boîte de dialogue *Propriétés* s'ouvre.
 - b) Dans l'onglet **Général**, recherchez le champ **Type de démarrage** et sélectionnez **Manuel**.
 - c) Cliquez sur **Appliquer** > **OK**.
- 4 Activez le **service d'énumération des appareils de carte à puce**.
 - a) Cliquez avec le bouton droit sur le service **Politique de suppression de carte à puce** et sélectionnez **Propriétés**.
La boîte de dialogue *Propriétés* s'ouvre.
 - b) Dans l'onglet **Général**, recherchez le champ **Type de démarrage** et sélectionnez **Manuel**.
 - c) Cliquez sur **Appliquer** > **OK**.



Activation de la prise en charge des contrôleurs 1.x.x du micrologiciel Mercury EP ou LP

Avant de pouvoir intégrer les contrôleurs 1.x.x du micrologiciel Mercury EP ou LP à votre appareil Streamvault^{MC}, vous devez activer une ancienne suite de chiffrement SSL.

À savoir

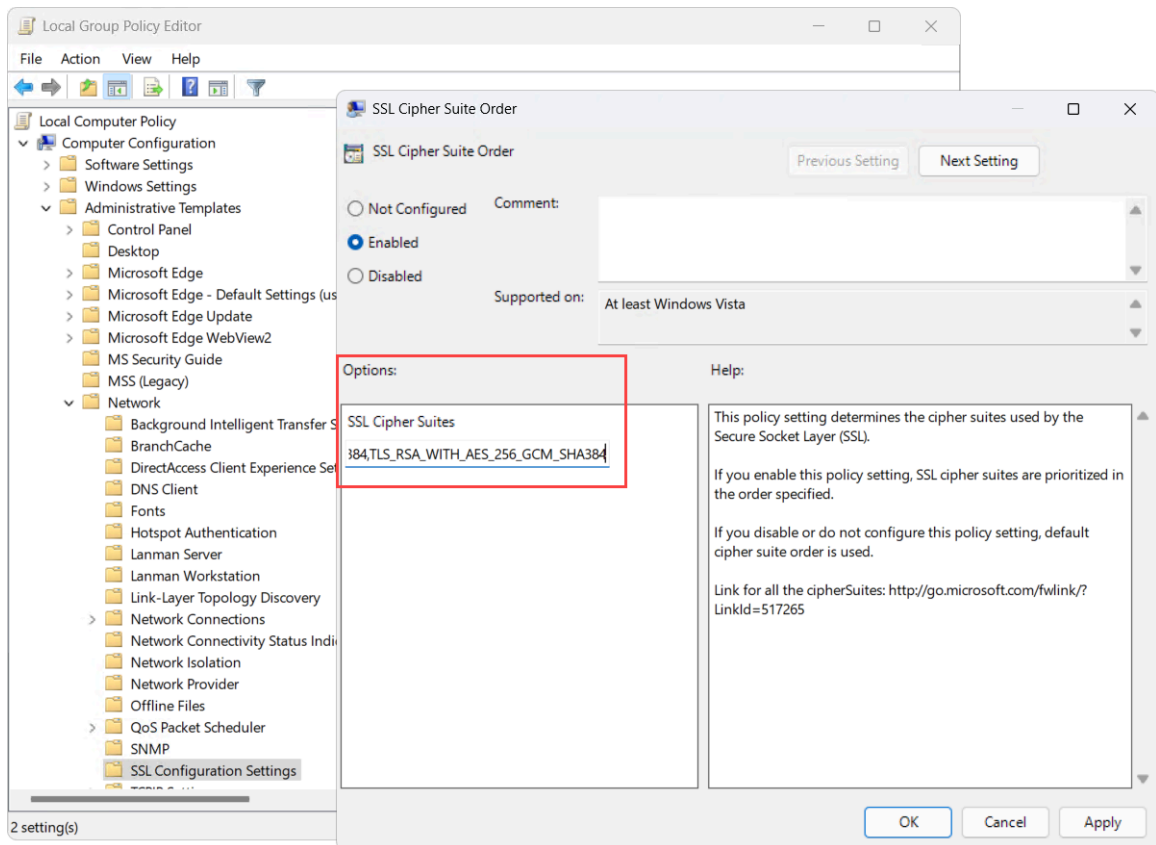
Selon votre intégration, l'une des suites de chiffrement suivantes doit être ajoutée pour permettre aux unités de communiquer avec l'appareil :

- **Intégration des contrôleurs Mercury LP avec le micrologiciel 1.31 et antérieur :**
 - TLS_RSA_WITH_AES_256_GCM_SHA384
 - TLS_RSA_WITH_AES_128_GCM_SHA256
- **Intégration des contrôleurs Mercury EP sur le micrologiciel 1.29.7 et antérieur :**
 - TLS_RSA_WITH_AES_256_CBC_SHA

Procédure

- 1 Sous Windows, exécutez `gpedit.msc` pour ouvrir *l'éditeur de stratégie de groupe locale*.
- 2 Accédez à **Configuration ordinateur > Modèles d'administration > Network > Paramètres de configuration SSL**.
- 3 Double-cliquez sur **SSL Cipher Suite Order**.
- 4 Dans le volet *Options* dans le champ **Suites de chiffrement SSL**, ajoutez une virgule à la fin de la liste, suivie de la suite de chiffrement applicable à votre intégration. N'ajoutez aucun espace.

- 5 Cliquez sur **OK** pour enregistrer l'objet de stratégie de groupe (GPO).



- 6 Redémarrez le service Softwire ou redémarrez l'appareil.

Activer la prise en charge de l'intégration Synergis IX

Avant de pouvoir inscrire des contrôleurs Synergis^{MC} IX sur votre appareil Streamvault^{MC}, vous devez ajouter une suite de chiffrement SSL supplémentaire.

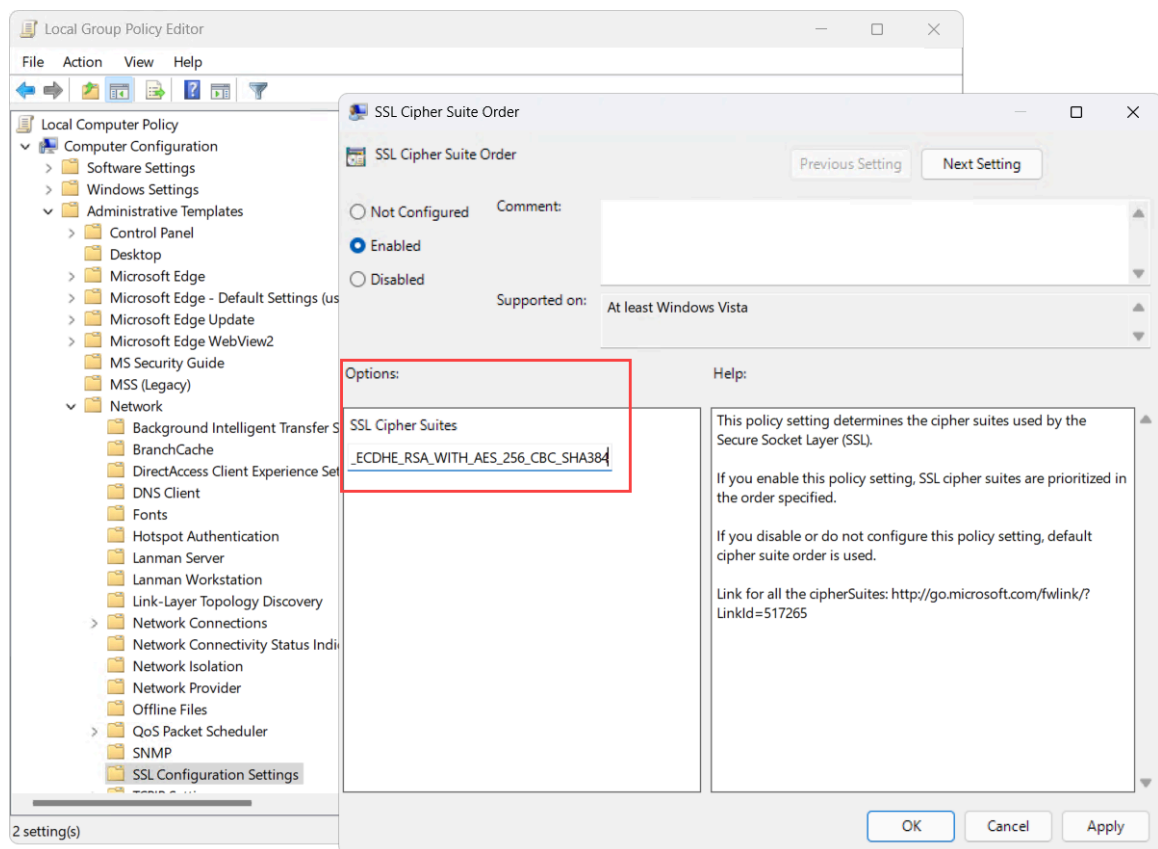
À savoir

L'une des suites de chiffrement suivantes doit être ajoutée pour inscrire les contrôleurs Synergis IX sur votre appareil Streamvault :

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Procédure

- 1 Sous Windows, exécutez `gpedit.msc` pour ouvrir l'*éditeur de stratégie de groupe locale*.
- 2 Accédez à **Configuration ordinateur** > **Modèles d'administration** > **Network** > **Paramètres de configuration SSL**.
- 3 Double-cliquez sur **SSL Cipher Suite Order**.
- 4 Dans le volet *Options*, dans le champ **Suites de chiffrement SSL**, ajoutez une virgule à la fin de la liste suivie de TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ou TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA256. N'ajoutez aucun espace.
- 5 Cliquez sur **OK** pour enregistrer l'objet de stratégie de groupe (GPO).



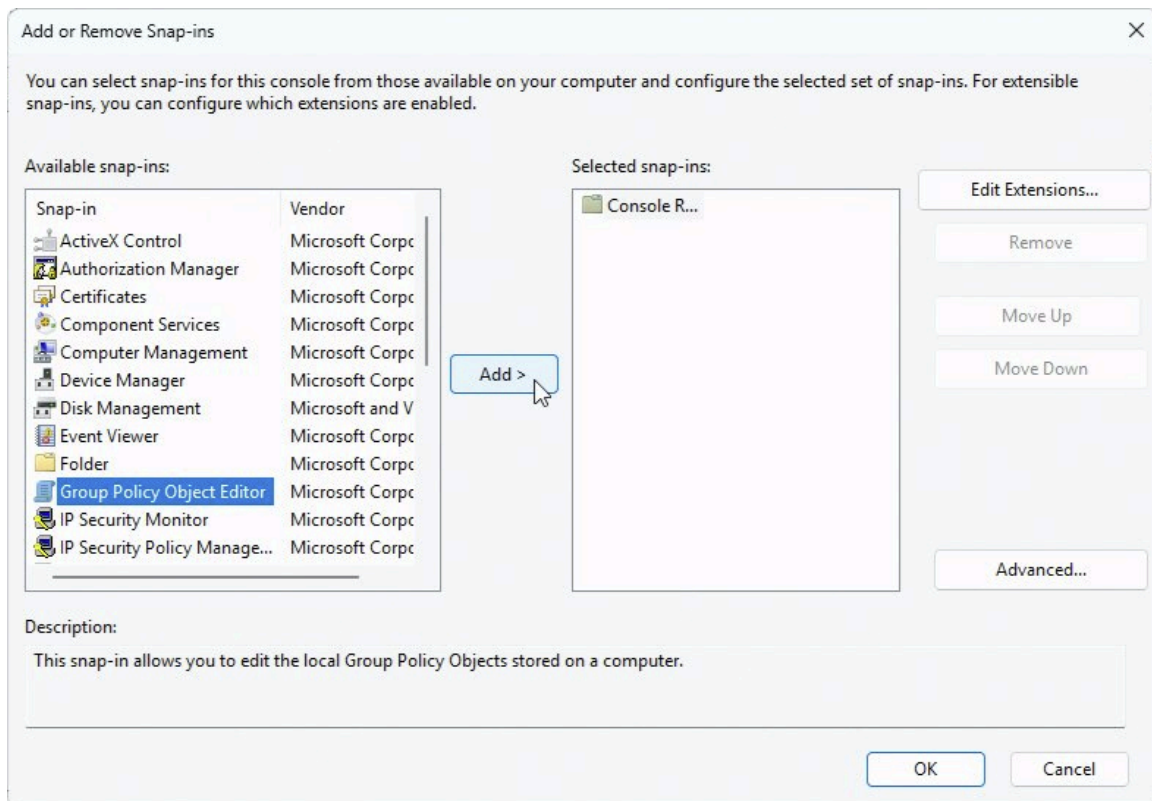
- 6 Redémarrez le service Software ou redémarrez l'appareil.

Modifier les objets de stratégie de groupe locaux pour les comptes utilisateur non-administrateurs

Par défaut, les comptes utilisateur non-administrateurs ont un accès restreint aux fonctionnalités de l'appareil Streamvault^{MC}. Pour personnaliser leurs autorisations, vous pouvez modifier les objets de stratégie de groupe (GPO) locaux pour le **Non-administrateurs** via la console de gestion Microsoft.

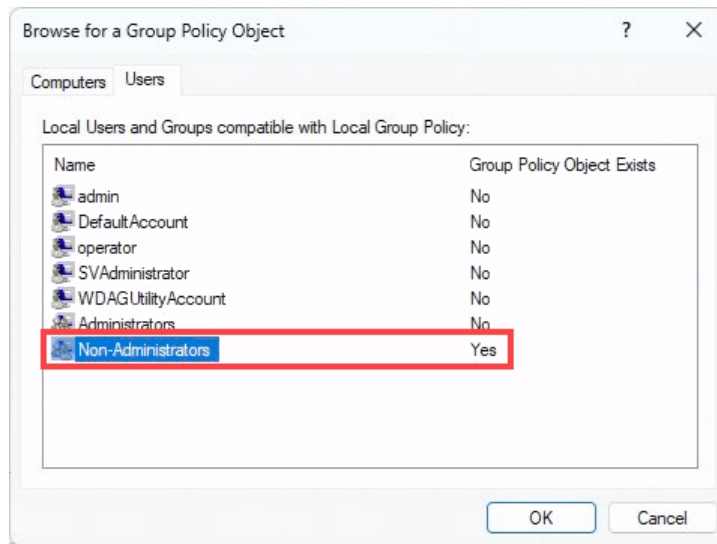
Procédure

- 1 Dans le menu Démarrer de Windows, sélectionnez **Exécuter**, puis tapez `mmc . exe` et cliquez sur **OK**. *Microsoft Management Console* s'ouvre.
- 2 Dans le volet de gauche, cliquez sur **Fichier > Ajouter/Supprimer un composant logiciel enfichable**. La boîte de dialogue *Ajouter ou supprimer des composants logiciels enfichables* apparaît.
- 3 Dans la section **Composants logiciels enfichables disponibles**, sélectionnez **Éditeur d'objets de stratégie de groupe** et cliquez sur **Ajouter**.



- 4 Dans l'assistant *Objet de stratégie de groupe*, cliquez sur **Parcourir**.

- 5 Dans la boîte de dialogue *Rechercher un objet de stratégie de groupe*, cliquez sur l'onglet **Utilisateurs** et sélectionnez le groupe **Non-administrateurs** pour lequel un objet de stratégie de groupe local existe, et cliquez sur **OK**.

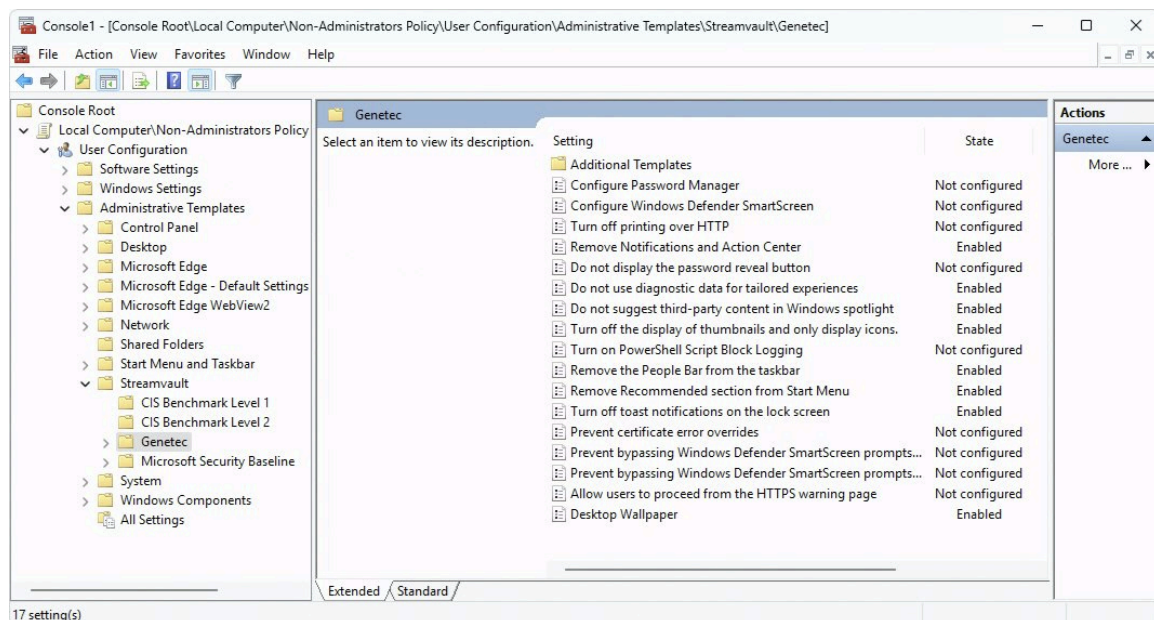


- 6 Dans la boîte de dialogue *Sélectionner un objet de stratégie de groupe*, cliquez sur **Terminer**.
- 7 La boîte de dialogue *Ajouter ou supprimer des composants logiciels enfichables*, cliquez sur **OK**.
- 8 Dans la fenêtre *Microsoft Management Console*, accédez à **Racine de la console > Stratégie Ordinateur Local\Non-Administrateurs > Configuration de l'utilisateur > Modèles d'administration > Streamvault > <renforcement de profil>**,

où <renforcement de profil> représente l'un des quatre profils de renforcement prédéfinis : CIS Benchmark Level 1, CIS Benchmark Level 2, Genetec^{MC} et Microsoft Security Baseline.

Tous les objets de stratégie de groupe configurés pour les comptes non-administrateurs sont affichés dans le profil de renforcement sélectionné.

REMARQUE : Un objet GPO est configuré si son état est *Activé* ou *Désactivé*. Un objet GPO avec un état de *Non configuré* n'est pas contrôlé par Streamvault.



- 9 Double-cliquez sur les objets de stratégie de groupe individuels pour les afficher ou les modifier.

Rubriques connexes

[Informations de connexion pour les comptes utilisateur par défaut sur un appareil Streamvault](#), page 12

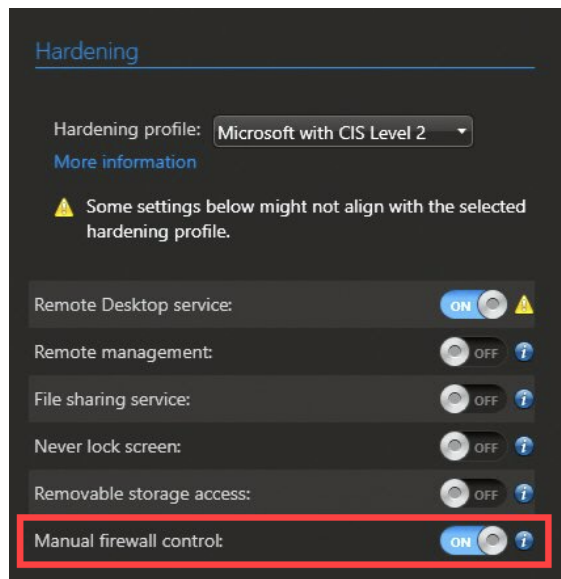
Désactiver le pare-feu Windows

Par défaut, le pare-feu Windows utilise les objets de stratégie de groupe (GPO) locaux des profils de renforcement pour sécuriser l'appareil Streamvault^{MC}. Si vous souhaitez désactiver le pare-feu Windows à des fins de dépannage, vous devez d'abord activer le contrôle manuel du pare-feu dans SV Control Panel.

Procédure

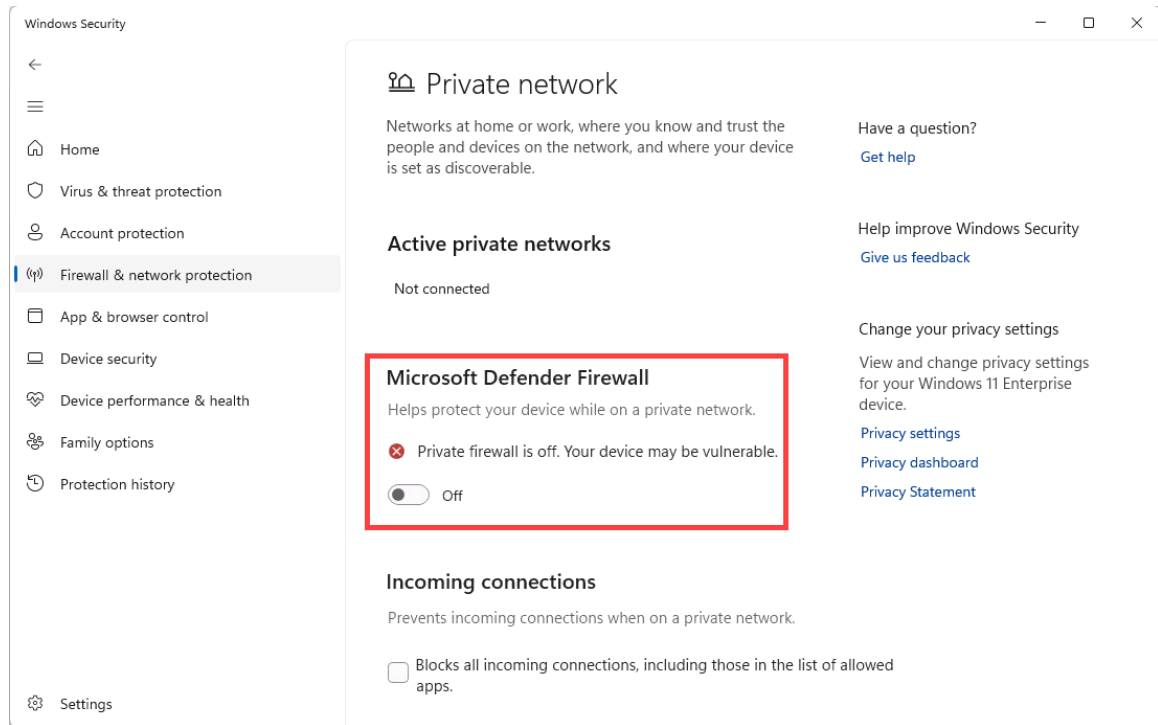
- 1 Ouvrez le SV Control Panel et accédez à la page *Sécurité*.
- 2 Dans la section *Renforcement*, activez le **Contrôle manuel du pare-feu** et cliquez sur **Appliquer**. Attendez que le paramètre soit appliqué.

REMARQUE : Lorsque cette option est activée, tous les objets GPO locaux sont désactivés. Aucune règle de pare-feu n'est affectée.



- 3 Dans le menu Démarrer de Windows, ouvrez **Pare-feu et protection du réseau**.
- 4 Sélectionnez le réseau pour lequel vous souhaitez désactiver le pare-feu.

5 Dans le *Pare-feu Microsoft Defender*, désactivez le pare-feu.



REMARQUE : Vous pouvez également désactiver le pare-feu via *Pare-feu Windows Defender avec sécurité avancée*.

Assistance technique

Cette section aborde les sujets suivants:

- [" Contacter le centre d'assistance technique de Genetec "](#), page 128
- ["Assistance logicielle"](#), page 131
- ["Assistance matérielle"](#), page 132
- ["Spécifications pour Streamvault"](#), page 133
- ["Conditions générales de l'assistance Streamvault"](#), page 134

Contacter le centre d'assistance technique de Genetec

Le centre d'assistance technique de Genetec^{MC} (GTAC) se tient à votre disposition pour vous aider à résoudre tout problème logiciel ou matériel lié à un appareil Streamvault^{MC}.

REMARQUE : Pour les demandes concernant des problèmes logiciels avec Genetec^{MC} Security Center, une assistance technique vous est offerte par l'intermédiaire de notre ligne d'assistance technique habituelle. Pour obtenir le numéro de téléphone et les horaires du GTAC dans votre région, consultez la page [Nous contacter](#) du *centre d'assistance technique de Genetec*.

Informations utiles

Lorsque vous ouvrez un dossier d'assistance, munissez-vous des informations suivantes :

- Votre ID système de la licence Security Center. Pour en savoir plus, consultez [Comment trouver mon ID système ?](#)
- Votre numéro de série Genetec ou l'étiquette d'entretien matériel.
- Votre code Genetec, qui se trouve sur le châssis (non applicable aux appareils tout-en-un). Le code est requis si vous perdez l'accès administratif au système et si vous avez besoin d'une image d'usine.



- Votre fichier journal TSR de diagnostic (le cas échéant). Pour en savoir plus, voir [Collecte des journaux d'assistance](#).

Contacter le GTAC par téléphone

L'assistance téléphonique pour les problèmes liés à Streamvault^{MC} est disponible pour tous les clients pendant les heures d'ouverture de leur région.

Pour les clients en Amérique du Nord, en Europe, au Moyen-Orient et en Afrique :

1. Consultez la page [Centre d'assistance technique de Genetec \(GTAC\)](#) *Nous contacter* pour obtenir le numéro de téléphone et les horaires du GTAC dans votre région.
2. Appelez le numéro de téléphone du GTAC et choisissez l'option #2.

Pour les clients de la région Asie-Pacifique :

Pour la région Asie-Pacifique, une assistance est fournie par le chat en direct et les dossiers d'assistance sur le [portail d'assistance technique de Genetec \(GTAP\)](#). Ce service fonctionne du lundi au vendredi, de 8:00 à 20:00 (heure locale).

Pour l'assistance d'urgence 24 h/24 et 7 j/7 en dehors des heures de bureau :

1. Appelez le numéro du GTAC dans votre région.
2. Saisissez votre numéro de certification Genetec.
3. Saisissez le numéro de contrat Genetec Advantage ou le numéro d'abonnement Genetec.
4. Sélectionnez le produit.
5. Laissez un message en indiquant votre nom, votre numéro de téléphone et une description du problème. L'ingénieur d'astreinte vous contactera dans un délai de 30 minutes.

IMPORTANT : Une assistance d'urgence 24 h/24 et 7 j/7 est proposée uniquement aux clients ayant ajouté cette option à leur contrat Genetec Advantage. Pour en savoir plus, contactez-nous à l'adresse advantage@genetec.com.

Les clients qui n'ont pas souscrit une couverture Advantage doivent ouvrir un dossier sur le [portail d'assistance technique de Genetec \(GTAP\)](#).

Contactez le GTAC par l'intermédiaire du GTAP

L'assistance pour les problèmes liés à Streamvault^{MC} est disponible pour tous les clients durant les heures de bureau dans leur région par l'intermédiaire des dossiers d'assistance en ligne sur le [portail d'assistance technique de Genetec^{MC} \(GTAP\)](#).

Pour les clients qui n'ont pas souscrit une couverture Genetec^{MC} Advantage, un dossier doit être ouvert sur le [portail d'assistance technique de Genetec \(GTAP\)](#). Pour en savoir plus sur Genetec Advantage, contactez-nous à l'adresse advantage@genetec.com.

Pour soumettre un dossier par l'intermédiaire du portail en ligne :

1. Accédez au [portail d'assistance technique de Genetec](#).
2. Connectez-vous à l'aide de votre adresse e-mail d'entreprise.
3. Cliquez sur **+ Créer un dossier**.



4. Dans la liste **ID système**, sélectionnez le système concerné.
5. Pour les retours ou les réparations de matériel, indiquez **Demande de RMA** dans l'objet afin que notre équipe puisse facilement identifier la nature de votre demande.

Description of the issue

Please Note:

- If you have more than one issue to report, please open one case for each
- If you have a problem with an order and/or its license parts, please contact customerservice@Genetec.com
- If you have any sales-related questions, please contact sales@Genetec.com
- If you are reporting a hardware issue with a StreamVault™ appliance, please type 'RMA' in the Title.

Title:

Description:

6. Indiquez le numéro de série de votre produit, le code Genetec et le fichier journal TSR de diagnostic (le cas échéant).
7. Cliquez sur **Envoyer le dossier**.
Vous recevrez un e-mail de confirmation de dossier vous indiquant le délai de réponse estimé.

Contactez le GTAC par l'intermédiaire du chat en direct

L'assistance pour les problèmes liés à Streamvault^{MC} est disponible pour les clients bénéficiant d'une couverture Genetec^{MC} Advantage par chat en direct sur le [Portail d'assistance technique de Genetec \(GTAP\)](#). Les clients peuvent bénéficier d'une assistance pendant les heures d'ouverture de leur région.

Pour les clients qui n'ont pas souscrit une couverture Genetec Advantage, un dossier doit être ouvert sur le [portail d'assistance technique de Genetec \(GTAP\)](#). Pour en savoir plus sur Genetec Advantage, contactez-nous à l'adresse advantage@genetec.com.

Pour démarrer un chat en direct :

1. Accédez au [portail d'assistance technique de Genetec](#).
2. Connectez-vous à l'aide de votre adresse e-mail d'entreprise.
3. Cliquez sur le bouton **Cliquez pour lancer le chat**.



4. Choisissez votre langue de prédilection.
5. Saisissez l'ID système complet (GSC-xxxxxx-xxxxxx), puis cliquez sur **Vérifier l'ID système**.
6. Indiquez si vous voulez discuter d'un dossier nouveau ou existant.
7. Sélectionnez le produit.
8. Cliquez sur **Démarrer le chat**.

The image shows a web interface for "GTAC - Live Chat". At the top is a red header with the text "GTAC - Live Chat" and a dropdown arrow. Below the header, there is a section for "Support hours for your territory:" stating "Monday to Friday: 08:00 to 20:00 Eastern Standard Time" and "Status: Online". The Genetec logo is displayed. A white box contains a "Welcome" message, a language selection prompt "Please select your preferred language" with radio buttons for "English" and "French", and a prompt "Please enter the System ID *". Below this is a text input field with a placeholder "Please enter the System ID" and a red "CHECK SYSTEM ID" button. At the bottom of the white box, there is a note "The transcript of your chat session will be retained for quality assurance purposes" and a red "START CHAT" button.

9. Pour demander un RMA, indiquez le numéro de série de votre produit, le code Genetec et le fichier journal TSR de diagnostic (le cas échéant).
Délai de réponse (uniquement durant les heures de bureau dans votre région) : généralement 5 minutes.

Assistance logicielle

Le logiciel de création d'image Windows Streamvault^{MC} inclut la version la plus récente du logiciel Security Center et du tableau de bord au moment de la création d'image. L'assistance est gérée séparément pour le logiciel de création d'image Windows et pour Security Center.

Logiciel Streamvault

- L'image Windows Streamvault est couverte dans le cadre de votre garantie Streamvault pendant l'intégralité du cycle de vie de l'appareil.
IMPORTANT : La mise à niveau du système d'exploitation Windows n'est pas couverte par votre garantie. La mise à niveau du système d'exploitation Windows supprime les pilotes nécessaires, le renforcement et les logiciels installés avec l'image.
- L'image de sauvegarde fournie pour la réapplication d'image d'un appareil Streamvault^{MC} inclut le système d'exploitation d'origine et l'image fournie avec l'appareil lors de l'achat.
- L'image Windows Streamvault est couverte dans le cadre de votre garantie Streamvault, quel que soit votre statut Genetec^{MC} Advantage.

Logiciel Security Center

Les problèmes rencontrés avec le logiciel Security Center sont couverts par l'accord de niveau de service et les procédures d'assistance décrites dans le document relatif à Genetec^{MC} Lifecycle Management (GLM) : [Description de Genetec Advantage](#)

Assistance matérielle

Les garanties HP et [Dell ProSupport](#) sont disponibles par l'intermédiaire de Genetec^{MC}. Pour tout problème matériel, le centre d'assistance technique de Genetec^{MC} (GTAC) est votre point de contact pour le diagnostic et pour la coordination avec HP et Dell ProSupport.

Consultez la [Présentation de la garantie matérielle Genetec](#) pour plus de détails sur les garanties matérielles Streamvault proposées par Genetec.

Spécifications pour Streamvault

Reportez-vous aux spécifications techniques, mécaniques et environnementales suivantes avant et pendant le déploiement de l'appareil Streamvault^{MC}.

Spécifications techniques, mécaniques et environnementales

Appareils tout-en-un :

- [Fiche technique SV-300E](#)

Appareils montés en rack :

- [Fiche technique gamme SV-1000E](#)
- [Fiche technique gamme SV-2000E](#)
- [Fiche technique gamme SV-4000E](#)

Stockage centralisé haute disponibilité :

- [Fiche technique gamme SV-7000EX](#)

Postes de travail :

- [Fiche technique de la série SVW-100E](#)
- [Fiche technique gamme SVW-300E](#)
- [Fiche technique gamme SVW-500E](#)

Appareils de surveillance de véhicule tout-en-un :

- [Fiche technique gamme SVR-300A](#)
- [Fiche technique gamme SVR-300AR](#)
- [Fiche technique gamme SVR-500A](#)

Conditions générales de l'assistance Streamvault

Les garanties matérielles Genetec^{MC} Standard et Extended sont régies par les conditions générales décrites dans la [Présentation de la garantie matérielle Genetec](#).

Glossaire

appareil SV

Les appareils Streamvault^{MC} sont des équipements de sécurité en réseau avec système d'exploitation embarqué et Security Center préinstallé. Les appareils Streamvault^{MC} vous permettent de déployer rapidement un système unifié ou autonome de vidéosurveillance et de contrôle d'accès.

Gestionnaire Streamvault^{MC}

L'entité Gestionnaire Streamvault^{MC} sert à contrôler les configurations d'alerte pour un groupe d'entités Agent Streamvault^{MC}. Un seul Gestionnaire Streamvault^{MC} est autorisé par système.

image de fabrication

Une image de fabrication est une image Streamvault^{MC} qui est envoyée aux clients lorsqu'ils achètent un appareil. Les versions du logiciel installées sur cette image varient en fonction de la commande du client.

image de récupération

Une image de récupération est utilisée pour la réimagerie des appareils Streamvault^{MC}. Il s'agit d'une image fixe avec des versions logicielles spécifiques préinstallées.

Matériel Streamvault^{MC}

Matériel Streamvault^{MC} est une tâche de rapport dans Security Center qui permet d'afficher la liste des dysfonctionnements qui affectent vos appareils Streamvault^{MC}.

Service Streamvault

Le service Streamvault est un service Windows qui permet aux utilisateurs de configurer un appareil Streamvault^{MC}, par exemple en appliquant des profils de renforcement.

Streamvault Factory Reset Utility

Streamvault Factory Reset Utility est un outil qui vous permet de rétablir les paramètres d'usine d'un appareil Streamvault. Il vous aide à créer une clé USB amorçable avec l'image logicielle Streamvault requise.

Surveillance de Matériel Streamvault^{MC}

L'entité de surveillance Matériel Streamvault^{MC} sert à surveiller l'état de vos appareils Streamvault^{MC} et à veiller à ce que vous soyez notifié en cas de problème. Une surveillance Matériel Streamvault^{MC} par appareil Streamvault^{MC} est requise.

SV-1000E

Le SV-1000E est un appareil de sécurité en rack économique conçu pour les systèmes de sécurité de taille moyenne. Il vous permet d'évoluer vers un système de sécurité unifié associant vidéosurveillance, contrôle d'accès, reconnaissance automatique de plaques d'immatriculation, communications, détection d'intrusions et outils d'analyse à l'aide d'un même appareil. Security Center et le SV Control Panel sont préinstallés sur le SV-1000E.

SV-100E

Le SV-100E est un appareil tout-en-un ultra-compact sur lequel Microsoft Windows, Security Center et le Tableau de bord SV sont préinstallés. Le SV-100E est conçu pour les installations à petite échelle et à un serveur, et prend en charge les caméras et les lecteurs de contrôle d'accès.

SV-2000E

Le SV-2000E est un appareil de sécurité en rack qui vous permet de déployer facilement un système unifié associant vidéosurveillance, contrôle d'accès, reconnaissance automatique de plaques d'immatriculation et communications. Security Center et le SV Control Panel sont préinstallés sur le SV-2000E.

SV-300E

Le SV-300E est un appareil tout-en-un compact prêt à l'emploi sur lequel Microsoft Windows, Security Center et le Tableau de bord SV sont préinstallés. Avec les cartes de capture à codage analogique intégrées, vous

pouvez utiliser l'appareil pour déployer rapidement un système de vidéosurveillance ou de contrôle d'accès autonome, ou un système unifié.

SV-350E

Le SV-350E est un appareil de sécurité en rack tout-en-un et prêt à l'emploi qui vous permet d'évoluer vers un système unifié associant vidéosurveillance, contrôle d'accès, détection d'intrusion et communications. Microsoft Windows, Security Center et le Tableau de bord SV sont préinstallés sur l'appareil. Il intègre RAID 5 pour un stockage vidéo critique.

SV-4000E

Le SV-4000E est un appareil de sécurité en rack qui offre des performances et une fiabilité de niveau entreprise. Ses configurations matérielles certifiées et sa protection renforcée contre les cybermenaces prête à l'emploi simplifient la conception et le déploiement d'un nouveau système de sécurité. Security Center et le SV Control Panel sont préinstallés sur le SV-4000E.

SV-7000E

Le SV-7000E est un appareil de sécurité en rack conçu pour des applications qui associent un grand nombre de caméras haute résolution, d'utilisateurs et d'événements. Security Center et le SV Control Panel sont préinstallés sur le SV-7000E.

SVA-100E

Le SVA-100E est un appareil compact qui vous permet d'enrichir facilement votre système avec KiwiVision^{MC} video analytics. Sa conception est optimisée pour que vous puissiez appliquer un plus grand nombre de flux d'analyse à votre système de vidéosurveillance, que vous utilisiez un ou plusieurs flux d'analyse par caméra.

SV Control Panel

SV Control Panel est une application qui vous permet de configurer rapidement un appareil Streamvault^{MC} pour qu'il fonctionne avec Security Center pour le contrôle d'accès et la vidéosurveillance.

SVW-300E

Le poste de travail SVW-300E est une solution clé en main conçue pour la surveillance de systèmes de sécurité de taille modeste ou moyenne, avec la prise en charge de plusieurs affichages. Security Center est préinstallé sur le SVW-300E.

SVW-500E

Le poste de travail SVW-500E est une solution hautes performances conçue pour les utilisateurs qui veulent afficher des caméras en très haute résolution sur des murs vidéo ou des moniteurs 4K. Security Center est préinstallé sur le SVW-500E.

Où trouver les informations sur les produits

Vous trouverez la documentation sur les produits aux emplacements suivants :

- **Genetec^{MC} TechDoc Hub** : La dernière documentation est disponible sur [TechDoc Hub](#).

Vous ne trouvez pas ce que vous cherchez ? Envoyez un e-mail à l'adresse documentation@genetec.com.

- **Pack d'installation** : Le guide d'installation et les notes de version sont disponibles dans le dossier Documentation du pack d'installation. Ces documents comportent également un lien de téléchargement direct vers la dernière version du document.
- **Aide** : Les applications client Security Center offrent une aide en ligne qui décrit le fonctionnement du produit et la marche à suivre pour utiliser ses fonctionnalités. Pour accéder à l'aide, cliquez sur **Aide**, appuyez sur F1, ou sélectionnez le point d'interrogation '?' dans les différentes applications client.