



Guide d'utilisation de l'appareil Streamvault™

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

Dernière mise à jour du document : 10 novembre 2023

Mentions légales

©2023 Genetec Inc. Tous droits réservés.

Genetec Inc. distribue ce document avec du logiciel qui comprend un contrat de licence, qui est fourni sous licence, et ne pouvant 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, 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}, Community Connect, Curb Sense^{MC}, Federation^{MC}, Flexreader^{MC}, Genetec Airport Sense^{MC}, Genetec Citigraf^{MC}, Genetec Clearance^{MC}, Genetec ClearID^{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}, Synergis^{MC}, Valcri^{MC}, leurs logos respectifs ainsi que le logo Mobius Strip sont des marques de Genetec Inc. Elles peuvent être déposées ou en attente d'enregistrement dans plusieurs juridictions.

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

Brevet en instance. Genetec Security Center, Omnicast, AutoVu, Stratocast, Citigraf, Clearance et d'autres produits Genetec sont en instance de brevet ou font l'objet de brevets émis aux États-Unis ainsi que dans d'autres pays.

Toutes les spécifications sont sujettes à modification sans avis préalable.

Informations sur le document

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 : 10 novembre 2023

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 cas 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

Préface

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 des mises à jour du logiciel SV	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
Se connecter à un appareil Streamvault	12
Comptes utilisateur par défaut sur un appareil Streamvault	12

Chapitre 2 : Prise en main de SV Control Panel

À propos du SV Control Panel	15
Configurer votre appareil dans SV Control Panel	15
Activer votre licence Security Center sur un appareil	19
Activer manuellement une licence à partir de Server Admin	21
Activer System Availability Monitor	23
Activer les fonctionnalités vidéo et de contrôle d'accès Security Center	24
À propos de l'outil Inscription d'unités	27
Ouvrir l'Outil d'inscription d'unités	27
Configurer les réglages d'inscription des unités	27
Ajouter des unités	28
Effacer les unités ajoutées	29
Ignorer des unités	29
Supprimer des unités de la liste des unités ignorées	29
Configurer les réglages par défaut des caméras	30
Créer des horaires d'enregistrement personnalisés	32
À propos de la sauvegarde et de la restauration	33
Sauvegarder la base de données du Répertoire	34
Restaurer la base de données du Répertoire	35
Choisir la méthode de création des rôles Archiveur et des partitions	36
Ajouter des rôles Archiveur dans SV Control Panel	37
Ajout manuel de rôles et de partitions Archiveur	38

Chapitre 3 : Prise en main du module externe Streamvault Maintenance

À propos du module externe Streamvault Maintenance	42
Téléchargement et installation du module externe	43
Privilèges Genetec Streamvault	44
Création du rôle de module externe	46
Configuration de l'entité de surveillance Matériel Streamvault	47
Configurer une entité Gestionnaire Streamvault	49

Analyser l'état de fonctionnement d'un appareil Streamvault	52
Colonnes du volet de rapport de la tâche Matériel Streamvault.	53

Chapitre 4 : Référence SV Control Panel

Page d'accueil du SV Control Panel	55
Raccourcis Config Tool dans SV Control Panel	55
Raccourcis Security Desk dans SV Control Panel	56
Server Admin dans SV Control Panel	56
Genetec Update Service dans SV Control Panel	56
Page Configuration du SV Control Panel	57
Informations générales	57
Paramètres réseau	58
Réglages System Availability Monitor	58
Informations sur les fonctionnalités	58
Sécurité	59
Paramètres réseau	59
Sauvegarde et restauration	60
Partitions et rôles Archiveur	60
Page CylancePROTECT du SV Control Panel	62
Page À propos du SV Control Panel	63
Informations de licence	63
Informations de contrat de maintenance applicative	63
Informations système	63
Informations d'aide	64

Chapitre 5 : Ressources complémentaires

Créer une clé USB de réinitialisation d'usine	66
Garantie de votre appareil Streamvault	68
Réappliquer une image à un appareil Streamvault	69
ID système et numéro de version logicielle d'un appareil Streamvault	70
Autoriser le partage de fichiers sur un appareil Streamvault	71
Autoriser les connexions Bureau à distance à un appareil Streamvault	72

Chapitre 6 : Dépannage

Rétablissement des réglages d'usine sur un appareil SV-100E, SV-300E ou SV-350E	74
Réinitialisation de l'image logicielle sur un appareil SV-100E, SV-300E ou SV-350E à l'aide d'une clé USB de démarrage	74
Rétablir les réglages d'usine sur un appareil Streamvault poste de travail ou serveur	78
Réinitialiser l'image logicielle sur un appareil de type poste de travail ou serveur Streamvault	79
Les contrôleurs Mercury EP restent hors ligne lorsque TLS 1.1 est désactivé	81
Activer Transport Layer Security (TLS)	82
Le Bureau à distance ne peut pas se connecter à un appareil Streamvault	83
Impossible d'installer CylancePROTECT depuis SV Control Panel pour certains appareils Streamvault	88

Chapitre 7 : Assistance technique

Contacteur l'assistance Genetec	90
Contacter l'assistance Genetec par le portail GTAP	91
Contacter l'assistance Genetec par le chat en direct	91
Assistance logicielle	93
Assistance matérielle	94

Spécifications pour Streamvault ^{MC}	96
Conditions générales de l'assistance Streamvault	97
Glossaire	102
Où trouver les informations sur les produits	104

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 des mises à jour du logiciel SV"](#), page 7
- ["Connexion des composants d'un appareil Streamvault"](#), page 8
- ["Se connecter à un appareil Streamvault"](#), page 12

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, lisez les notes de version pour découvrir les nouvelles fonctionnalités, les problèmes connus et les limitations.	<p>Dans les Notes de version Streamvault de la version d'image installée sur votre appareil, consultez :</p> <ul style="list-style-type: none"> • Nouveautés • Problèmes connus • Limitations
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 12.
Suivez les assistants de configuration		
4	Terminez l' <i>Assistant de configuration Streamvault Control Panel</i> . REMARQUE : Le bureau distant est désactivé par défaut. Pour activer le bureau distant, désactivez le paramètre Bloquer le bureau distant sur la page <i>Sécurité</i> de l'assistant.	<ul style="list-style-type: none"> • Configurer votre appareil dans SV Control Panel, page 15. • Autoriser les connexions Bureau à distance à un appareil Streamvault, page 72.
5	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>. • Si l'appareil n'est pas connecté à Internet, activez votre licence manuellement depuis Server Admin. 	<ul style="list-style-type: none"> • Activer votre licence Security Center sur un appareil, page 19. • Activer manuellement une licence à partir de Server Admin, page 21.
6	Activez le System Availability Monitor.	<ul style="list-style-type: none"> • Activer System Availability Monitor, page 23.

Étape Tâche	Informations complémentaires
7 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"> • Dans le <i>Guide de l'utilisateur Genetec^{MC} Update Service</i>, consultez la section « Configuration de Genetec Update Service ».
8 Si SV Control Panel indique que d'autres mises à jour sont disponibles, installez-les maintenant.	<ul style="list-style-type: none"> • À propos des mises à jour du logiciel SV, page 7.
9 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 37. • Pour la série SV-7000E et pour un appareil tout-en-un : Ajout manuel de rôles et de partitions Archiveur, page 38.
10 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 24. • Configurer les réglages d'inscription des unités, page 27.
11 Sauvegarder la configuration de Security Center.	<ul style="list-style-type: none"> • Sauvegarder la base de données du Répertoire, page 34.

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 tableau suivant répertorie les ports qui doivent être ouverts pour le trafic entrant afin que le module externe Streamvault^{MC} Maintenance puisse communiquer avec le matériel Streamvault.

Module	Port entrant	Utilisation du port
Surveillance de matériel Streamvault ^{MC}	65115	Utilisé pour communiquer entre Security Center et le contrôleur de gestion de la carte de base iDRAC du matériel Streamvault via le réseau.

Ports requis du tableau de bord Streamvault^{MC}

Le tableau suivant répertorie les ports qui doivent être ouverts pour le trafic sortant afin que les composants du tableau de bord Streamvault^{MC} puissent se connecter aux services Cloud de Genetec.

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

Le tableau suivant répertorie les ports qui doivent être ouverts pour le trafic sortant afin que l'agent de bureau CylancePROTECT puisse communiquer 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

Port sortant	Utilisation du port	URL de destination
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 venueapi.us.cylance.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).

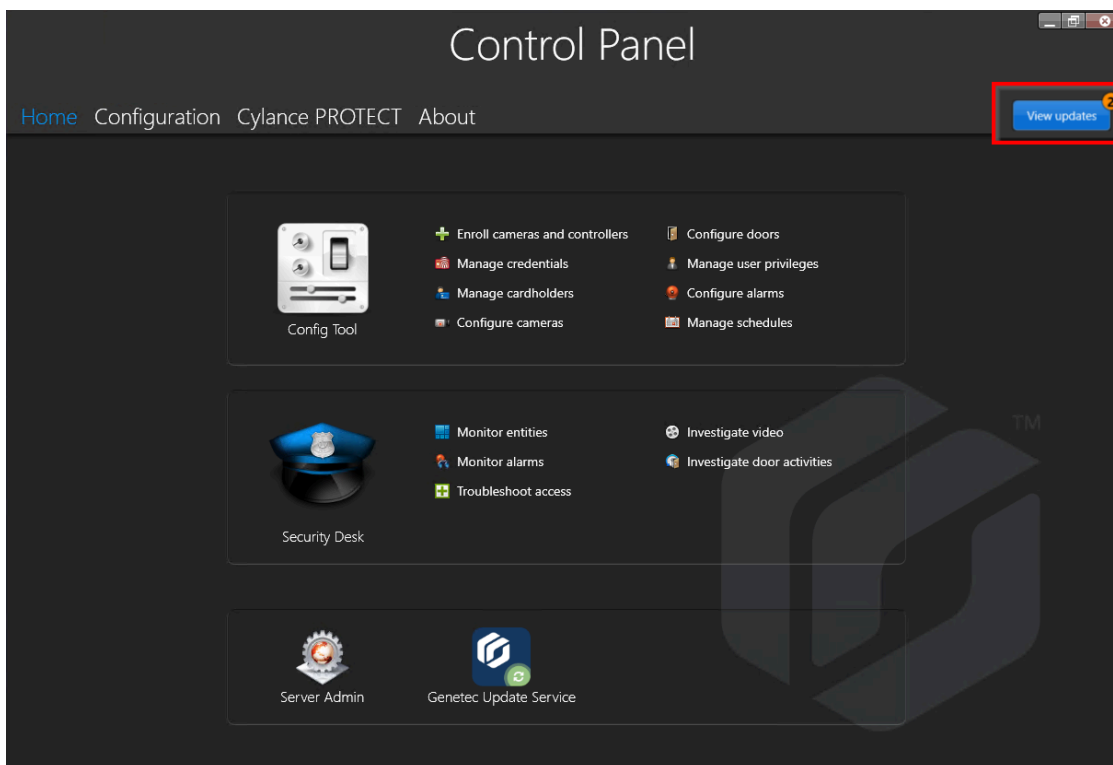
Pour plus d'informations sur les modes de communication de l'apppliance Streamvault avec les services de gestion de Genetec, voir [Page CylancePROTECT du SV Control Panel](#), page 62.

À propos des mises à jour du logiciel SV

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*.

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.

Pour connecter les périphériques et alimenter l'appareil :

- 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, puis branchez l'autre extrémité du câble dans une prise RJ-45 du réseau IP.
- 6 Pour les appareils 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, puis branchez le cordon de ce bloc dans une prise de courant.
- 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

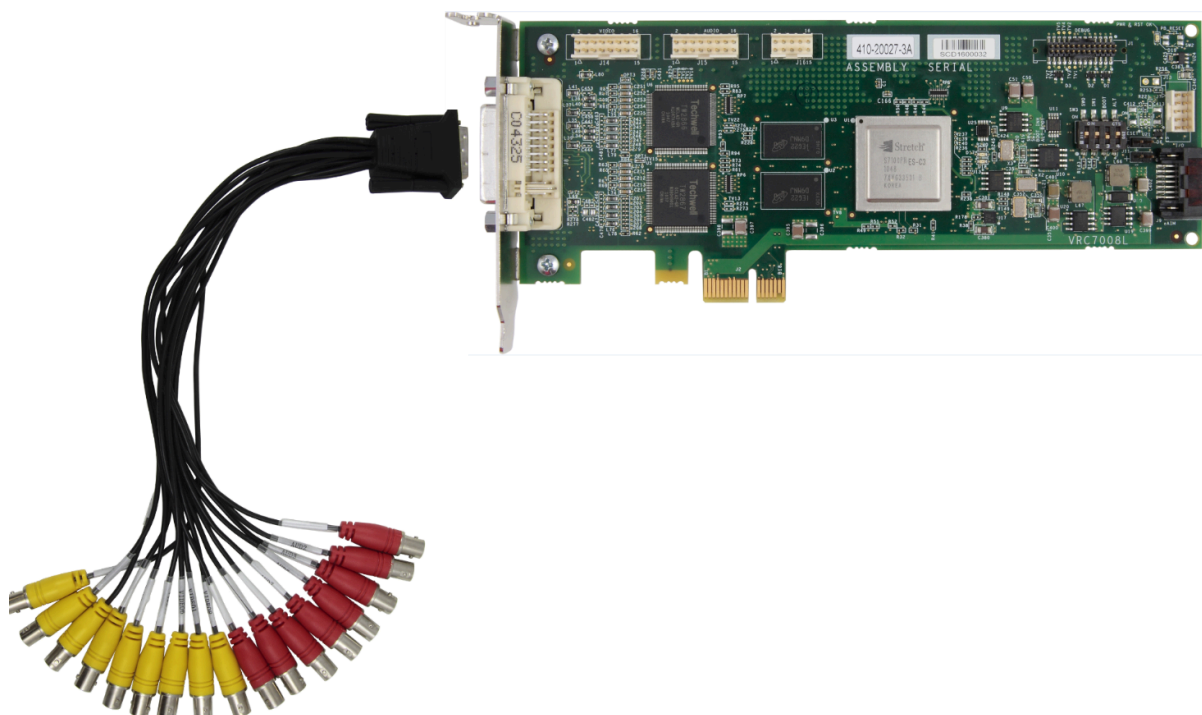
Si vous utilisez un appareil Streamvault pour déployer un système de vidéosurveillance avec des caméras analogiques, vous devez connecter les caméras à la carte de codage analogique Genetec^{MC} de l'appareil.

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 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 sur l'Outil d'inscription d'unités, reportez-vous au *Guide de l'administrateur Security Center*.

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*. Vous devez utiliser 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.

Pour désactiver les entrées de caméra sur les cartes de codage :

- 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 et vous permet de visionner la vidéo depuis cette caméra.

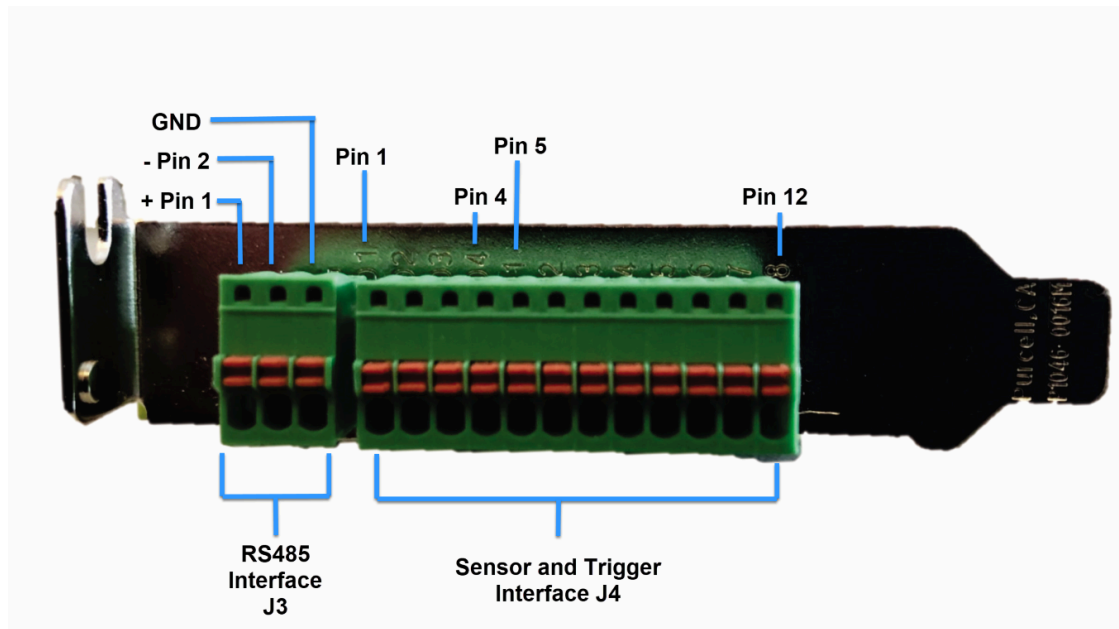
Entrées et sorties d'alarme d'un appareil Streamvault

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

Si vous commandez un appareil Streamvault avec la carte d'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. 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 les entrées et les sorties d'un appareil Streamvault, voir le *Guide de l'administrateur de Security Center*.

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. Changez 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

Vous devez être connecté en tant qu'utilisateur Admin pour configurer votre appareil dans SV Control Panel.

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

- 10 caractères minimum
- Au moins trois caractères issus des quatre catégories suivantes :
 - Lettres majuscules
 - lettres minuscules
 - Chiffres en base 10 (0-9)
 - Caractères non alphanumériques (tels que \$,%,!)

Pour vous connecter à votre appareil Streamvault pour la première fois :

- 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.](#)

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 Serveur SV Control Panel 	Non applicable
Opérateur	opérateur	<ul style="list-style-type: none"> Corbeille Bibliothèques Mon ordinateur C: lecteur Page d'accueil SV Control Panel, page de configuration, paramètres régionaux seulement, page À propos Server Admin : nécessite un mot de passe administrateur pour tous les droits 	<ul style="list-style-type: none"> Windows: arrêter et redémarrer Paramètres système Partition vidéo
Non applicable	genetecfactory	Server Admin	<p>Non applicable jusqu'à ce que SV Control Panel soit achevé.</p> <p>REMARQUE : Cette option n'est pas disponible pour les appareils de type poste de travail.</p>

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. Vous pouvez gérer tous vos mots de passe sur la page *Configuration*, dans la section *Réglages de comptes utilisateur*.

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 depuis une machine à distance, vous devez connaître le nom DNS ou l'adresse IP du serveur, le port du serveur Web et le 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.

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 15
- ["Activer votre licence Security Center sur un appareil"](#), page 19
- ["Activer manuellement une licence à partir de Server Admin"](#), page 21
- ["Activer System Availability Monitor"](#), page 23
- ["Activer les fonctionnalités vidéo et de contrôle d'accès Security Center"](#), page 24
- ["À propos de l'outil Inscription d'unités"](#), page 27
- ["Configurer les réglages par défaut des caméras"](#), page 30
- ["Créer des horaires d'enregistrement personnalisés"](#), page 32
- ["À propos de la sauvegarde et de la restauration"](#), page 33
- ["Choisir la méthode de création des rôles Archiveur et des partitions"](#), page 36

À propos du 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.

ATTENTION : Les changements de configuration effectués dans SV Control Panel remplacent les changements de configuration apportés en dehors de SV Control Panel, y compris les réglages 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 s'exécutant sur le serveur principal.

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.
- Option pour activer et désactiver Genetec^{MC} Mobile et Synergis^{MC} Softwire depuis la section *Fonctionnalités* de la page *Configuration*, s'ils sont installés sur l'appareil.
- Liens vers GTAP et la documentation produit.
- Page de configuration de la communication de CylancePROTECT pour choisir le mode de communication de l'appareil Streamvault^{MC} avec la console dans le cloud.
- La capacité de créer des partitions et rôles Archiveur supplémentaires pour les configurations sur les serveurs d'extension.

REMARQUE : Guide applicable pour le tableau de bord Streamvault 2.8 et versions antérieures.

Configurer 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.

Pour configurer votre appareil :

- 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) Sur les appareils équipés de deux cartes réseau, sélectionnez la carte que vous souhaitez configurer dans la liste **Interface réseau**.
La liste **Interface réseau** est masquée lorsqu'une seule carte réseau est connectée.
 - b) 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, puis cliquez sur **Réessayer**.
 - c) Si vous souhaitez spécifier les réglages IP, cliquez sur **Utiliser la configuration statique**, et entrez une adresse IP unique pour cet appareil.
 - d) Si le champ **État** affiche autre chose que « Connecté à Internet », cliquez sur **Réessayer**.
 - e) 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 *Sécurité*, modifiez le mot de passe utilisé par l'utilisateur administrateur pour se connecter à Windows.
Par défaut, ce mot de passe sert également à se connecter à toutes les applications Genetec^{MC}. Vous n'êtes pas invité à modifier les mots de passe sur un appareil configuré en tant que serveur d'extension Security Center.
- 7 Dans la section **Sécurité**, configurez les mots de passe en cliquant sur **Modifier le mot de passe** pour les applications suivantes :
 - **Administrateur Windows** : Le mot de passe Windows de l'utilisateur administrateur.
 - **Applications client** : 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.
- 8 Configurez les réglages de sécurité suivants, puis cliquez sur **Suivant** :
 - **Déconnexion automatique** : Activez cette option pour configurer Windows afin de déconnecter l'utilisateur après 15 minutes d'inactivité.
 - **Complexité du mot de passe** : Activez cette option pour exiger un mot de passe complexe d'au moins 10 caractères pour les utilisateurs Windows.
 - **Fonctions de gestion de serveur** : Sélectionnez cette option pour permettre aux fonctions telles que l'ajout de rôles et d'autres tâches d'utiliser les applications telles que *Windows Admin Center*, *Server Manager* ou *Windows PowerShell*.
 - **Accès au stockage amovible** : Sélectionnez cette option pour 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.

- **Activer la prise en charge des cartes à puce** : Activez cette option pour créer ou utiliser un lecteur de carte à puce avec l'application Security Desk. Pour éviter toute infection par des logiciels malveillants, cette option doit être désactivée par défaut.
 - **Connexions à distance entrantes** : Activez cette option pour accorder l'accès aux connexions *Bureau à distance* et permettre le partage de fichiers entre l'appareil et votre réseau informatique. Pour éviter toute infection de votre appareil par des logiciels malveillants, cette option a été désactivée par défaut.
 - **Bureau à distance** : Activez cette option pour autoriser les utilisateurs de votre réseau à se connecter à l'appareil à l'aide d'une application *Bureau à distance*. L'option **Connexions à distance entrantes** doit également être activée pour autoriser l'accès via une application *Bureau à distance*. Pour éviter toute infection de votre appareil par des logiciels malveillants, cette option a été désactivée par défaut.
 - **Partage de fichiers** : Activez cette option pour partager des fichiers et des dossiers situés sur l'appareil avec d'autres utilisateurs sur votre réseau. L'option **Connexions à distance entrantes** doit également être activée pour autoriser le partage de fichiers. Pour éviter toute infection de votre appareil par des logiciels malveillants, cette option a été désactivée par défaut.
- 9 Lisez les informations sur la page *À propos de CylancePROTECT*, puis cliquez sur **Suivant**.
- 10 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.
- IMPORTANT** : Lorsque CylancePROTECT est désactivé, vous ne pouvez pas basculer entre **Déconnecté** et **En ligne**. Pour modifier ces réglages, vous devez réinitialiser l'image logicielle sur l'appareil.
- 11 Pour accéder aux journaux et fonctionnalités avancées de votre système, sélectionnez **Exécuter CylancePROTECT en mode Interface avancée**.
- 12 Cliquez sur **Suivant**.
- 13 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.
- 14 Lisez l'accord de confidentialité, cochez la case **J'accepte les termes de cet accord de confidentialité**, puis cliquez sur **Appliquer**.
- 15 Sur la page *Conclusion*, cliquez sur **Fermer**.
- L'option **Lancer l'assistant d'activation après l'installation** est cochée par défaut. Si vous la décochez, un message vous rappelle d'activer le produit à une date ultérieure.
- REMARQUE** : Votre appareil doit être activé avant utilisation.

Lorsque vous avez terminé

Activez votre appareil.

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.

Pour activer votre licence Security Center à l'aide d'un ID système :

- 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.
- 7 Sur la page *Fonctionnalités complémentaires*, activez ou désactivez Synergis^{MC} Software 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 à partir de Server Admin](#), page 21

[Page À propos du SV Control Panel](#), page 63

[Informations de licence](#), page 63

Activer manuellement une licence à partir de Server Admin

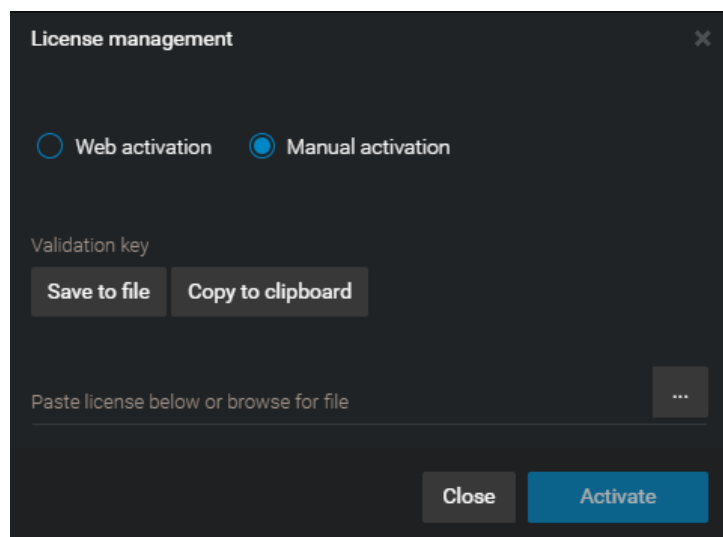
Si votre appareil Streamvault^{MC} n'a pas accès à Internet, vous pouvez activer votre licence Security Center manuellement depuis Server Admin.

Pour activer une licence manuellement à partir de Server Admin :

- 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 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) Sur la page *Informations système*, dans la section *Information sur la licence*, cliquez sur **Activer la 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 19

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](#), comme indiqué dans le *Guide de l'utilisateur de System Availability Monitor*.

Pour activer System Availability Monitor Agent :

- 1 Ouvrez SV Control Panel.
- 2 Sur la page *Configuration* dans la section *System Availability Monitor*, cliquez sur **Configurer**.
- 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 vidéosurveillance 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

Pour activer les fonctionnalités vidéo et de contrôle d'accès Security Center :

- 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.
- Lorsque vous avez lu la page de *présentation*, cliquez sur **Suivant**.
- 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 : Les fonctionnalités qui ne sont pas prises en charge par votre licence ne sont pas disponibles dans la liste.
- 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**.
- 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.
- Sur la page *Réglages d'enregistrement*, sélectionnez les réglages d'enregistrement par défaut que vous souhaitez appliquer à toutes les caméras.
 - Off :** 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.
 - **Provisionnement** : 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*.
 - 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 *d'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 30

[Créer des horaires d'enregistrement personnalisés](#), page 32

[Page d'accueil du SV Control Panel](#), page 55

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}*.

Rubriques connexes

[Raccourcis Config Tool dans SV Control Panel](#), page 55

Ouvrir l'Outil d'inscription d'unités

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

Pour ouvrir l'Outil d'inscription d'unités :

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

Pour configurer les réglages de découverte :

- 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 Configurez les options suivantes :
 - **Toujours lancer une recherche exhaustive**. Activez cette option si vous souhaitez détecter toutes les unités du système.
REMARQUE : Les unités d'autres fabricants seront parfois découvertes, car les protocoles UPnP et *Zero config* sont également utilisés durant le processus de découverte.
 - **Refuser l'authentification de base** (unités vidéo seulement). Utilisez ce commutateur pour activer ou désactiver l'authentification de base. 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 n'est disponible que pour les utilisateurs dotés des privilèges d'administrateur.

- 4 Cliquez sur **Ajouter un fabricant** (+) pour ajouter un fabricant à la liste des unités qui seront découvertes.
Pour supprimer un fabricant de la liste, sélectionnez-le et cliquez sur ✕.
- 5 Configurez les réglages individuels des 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 29).
- 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.

Pour ajouter une unité :

- 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.

Pour effacer les unités effacées :

- 1 Ajoutez les unités découvertes de votre choix au système. Voir [Ajouter des unités](#), page 28.
- 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.

Pour ignorer une unité :

- 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 29.

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.

Pour supprimer une unité de la liste des unités ignorées :

- 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*.

Pour configurer les réglages par défaut des caméras :

- 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 sont ceux qui ont été créés dans la vue **Horaires** de la tâche *Système*, ou un horaire personnalisé si vous en avez créé un dans l'assistant d'installation Security Center.
- 5 Dans la liste déroulante **Mode**, sélectionnez un mode pour l'horaire d'enregistrement :
 - **Off** : 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'enregistrement ne peut pas être interrompu par l'utilisateur durant ce laps de temps.
- **Durée par défaut de l'enregistrement manuel** : Spécifiez le nombre de minutes que vous souhaitez enregistrer lorsque l'enregistrement est déclenché par un utilisateur. 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 24

Créer des horaires d'enregistrement personnalisés

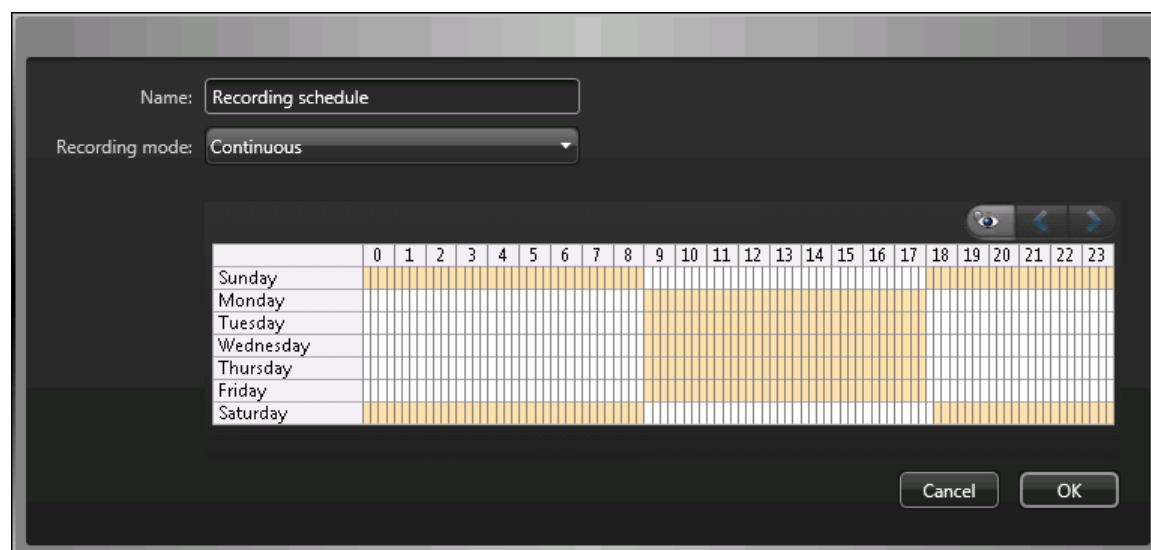
Créez des horaires d'enregistrement personnalisés dans l'assistant d'installation du Security Center pour que vos caméras utilisent différents modes d'enregistrement selon les plages horaires.

Pour configurer un horaire :

- 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 :
 - **Off** : 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.

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

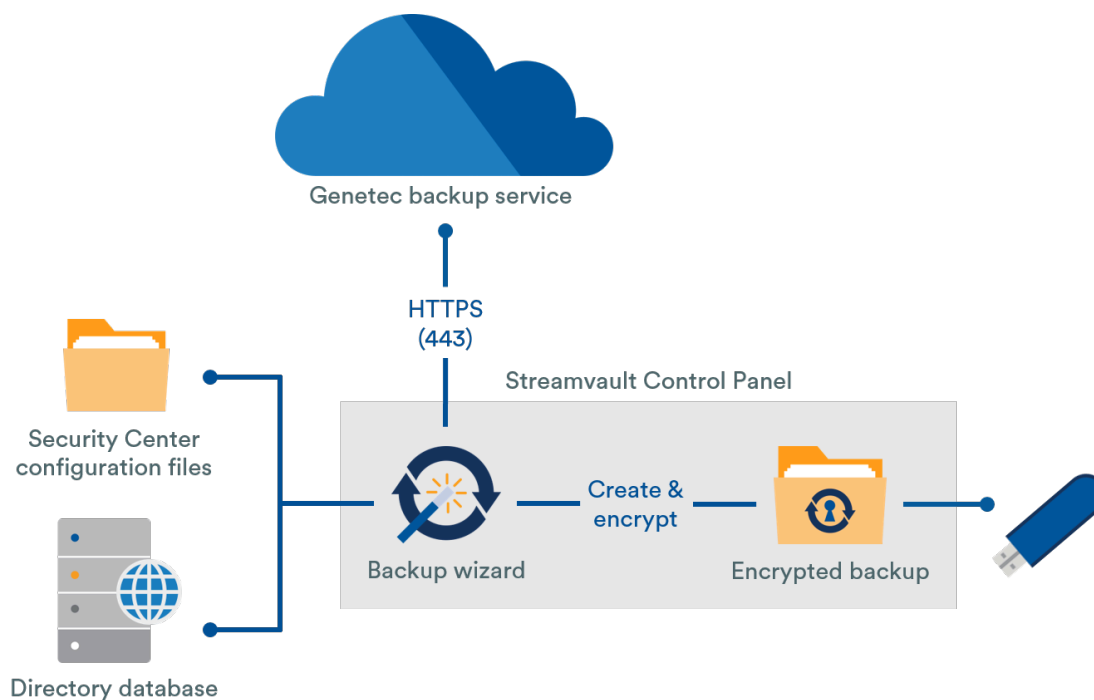
[Activer les fonctionnalités vidéo et de contrôle d'accès Security Center](#), page 24

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 sauvegarder vos fichiers dans le cloud ou en local à l'aide de l'assistant *Sauvegarde*. Lorsque vous sauvegardez dans le cloud, les cinq dernières sauvegardes sont conservées.
- 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 *Restauration*.
- 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 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 5.6 vers un système Security Center 5.5.
- 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 5.5 vers un système Security Center 5.6.

Rubriques connexes

[Sauvegarder la base de données du Répertoire](#), page 34

[Restaurer la base de données du Répertoire](#), page 35

Sauvegarder la base de données du Répertoire

Pour simplifier la configuration de votre système après une mise à niveau matérielle, ou pour restaurer vos configurations après une panne système, vous pouvez sauvegarder en toute sécurité la base de données du Répertoire et vos fichiers de configuration à l'aide des fonctions de sauvegarde et restauration.

Avant de commencer

Les conditions suivantes sont requises :

- Security Center 5.5 ou une version ultérieure est installé.
- Genetec Server est en cours d'exécution.
- Votre licence est valable et activée.

À savoir

- Vous pouvez facilement sauvegarder vos fichiers dans le cloud ou en local à l'aide de l'assistant *Sauvegarde*. Lorsque vous sauvegardez dans le cloud, les cinq dernières sauvegardes sont conservées.
- Seuls les administrateurs peuvent effectuer une sauvegarde, et toutes les sauvegardes dans le cloud doivent être authentifiées.

Pour sauvegarder la base de données du Répertoire et vos fichiers de configuration :

- 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**.
 - **Dans le cloud** Si vous avez sélectionné dans le 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 :** Vous devez créer et mémoriser 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.
 - **En local.** Si vous avez sélectionné en 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 33

[Restaurer la base de données du Répertoire](#), page 35

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 facilement restaurer vos fichiers de sauvegarde vers le même ID système en cas de défaillance du système ou de mise à niveau du matériel.

Avant de commencer

Les conditions suivantes sont requises :

- Security Center 5.5 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.

Pour restaurer la base de données du Répertoire et vos fichiers de configuration :

- 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 *Authentication*, 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 34

[À propos de la sauvegarde et de la restauration](#), page 33

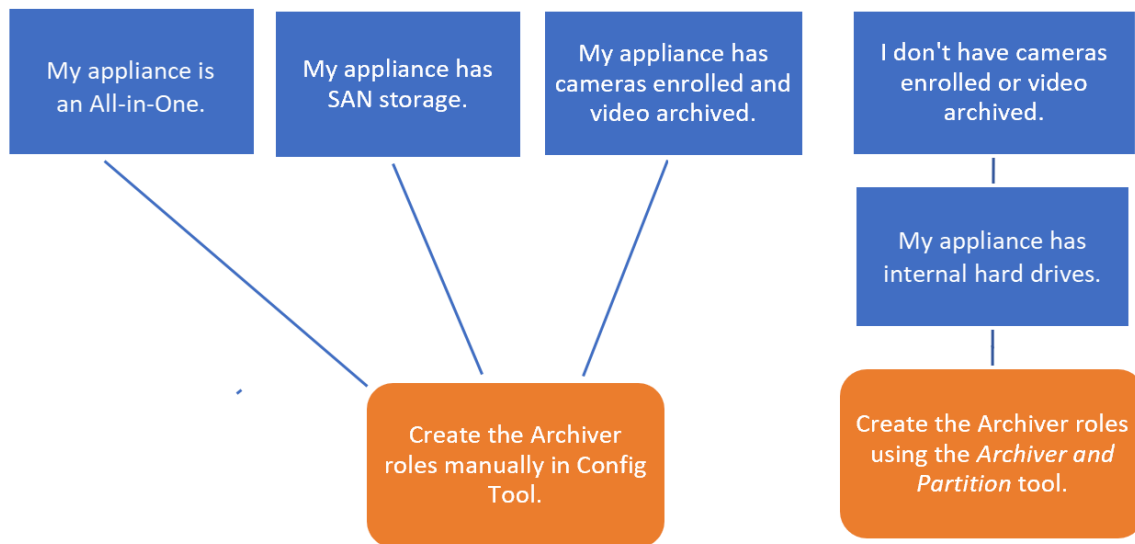
Choisir la méthode de création des rôles Archiveur et des partitions

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* dans SV Control Panel

L'outil *Rôles Archiveur et partitions* 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 SV-7000E, suivez les étapes à la section [Ajout manuel de rôles et de partitions Archiveur](#), page 38.

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

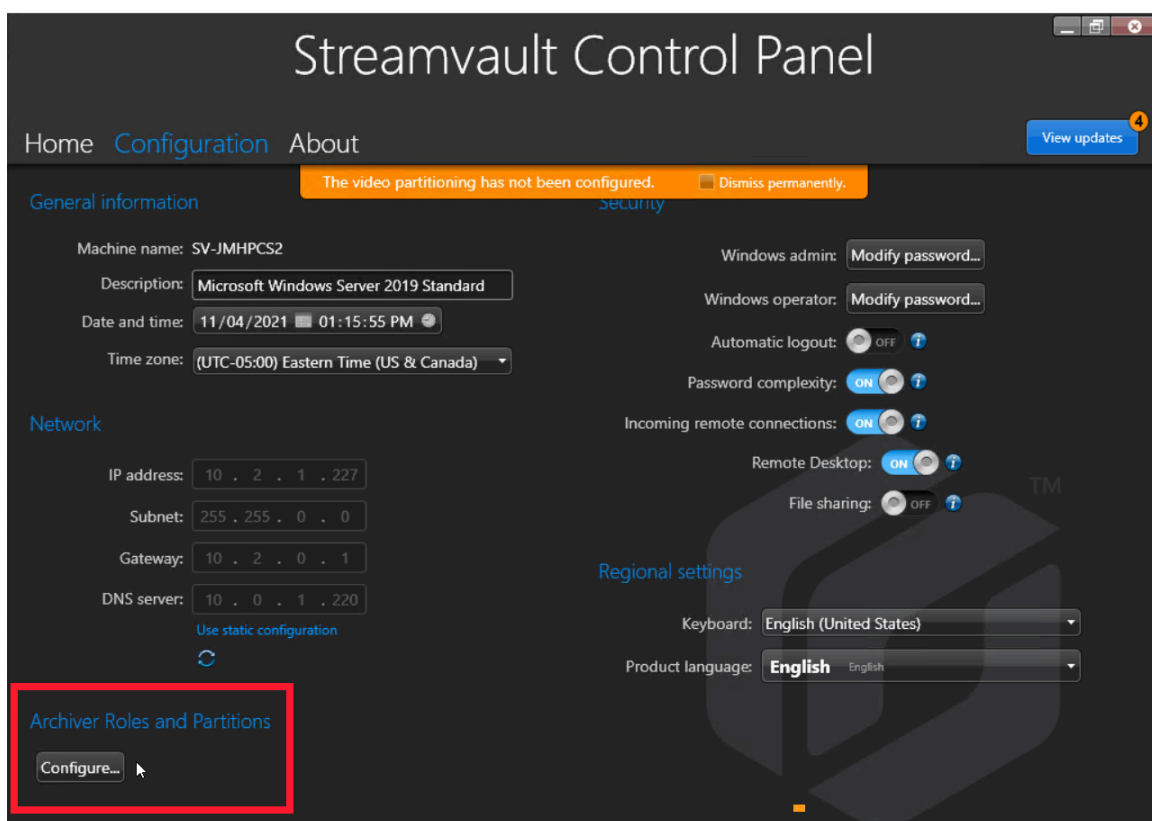
Utilisez l'outil Rôles Archiveur et partitions pour ajouter suffisamment de rôles Archiveur pour gérer le trafic vidéo escompté. Cet outil est disponible sur les appareils Archiveur séries Streamvault^{MC} 1000, 2000 et 4000.

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:.

Pour créer des rôles Archiveur et partitions supplémentaires :

- 1 Dans SV Control Panel, cliquez sur l'onglet **Configuration**.
- 2 Sous *Partitions et rôles Archiveur*, cliquez sur **Configurer**.

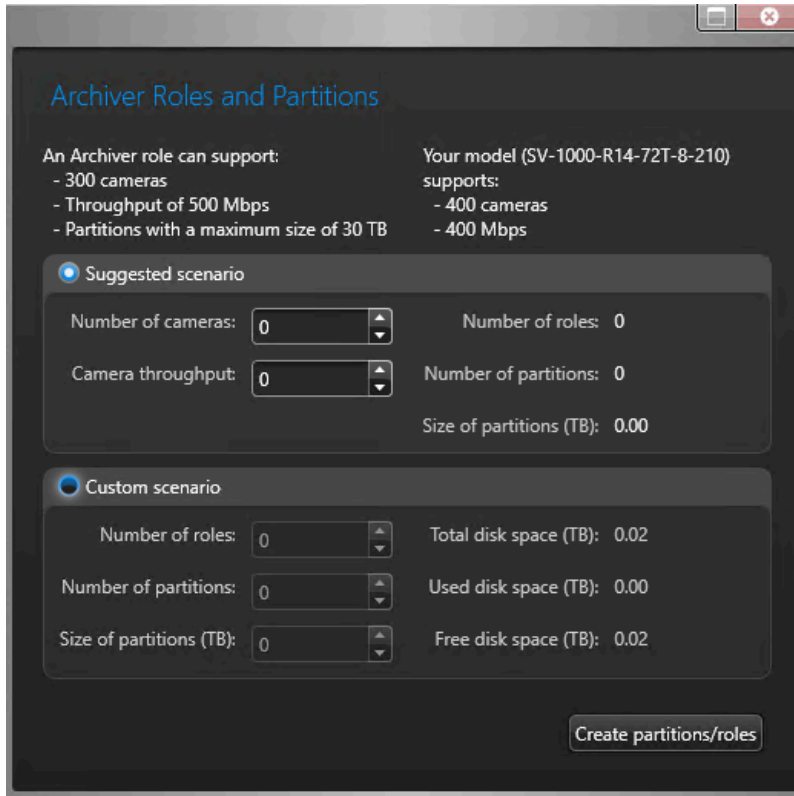


La boîte de dialogue *Rôles Archiveur et partitions* apparaît.

- 3 Sélectionnez l'une des options suivantes pour configurer le nombre de rôles Archiveur et de partitions :
 - 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 Archiveur et de partitions à créer, sélectionnez **Scénario personnalisé**, entrez 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**.

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-7000E ou SV-300E, 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.

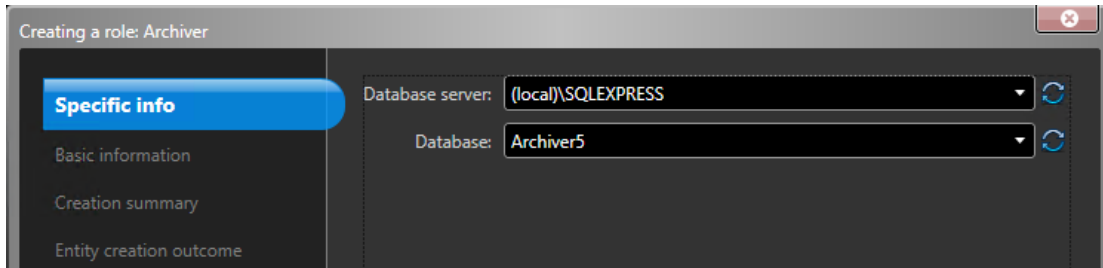
À savoir

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

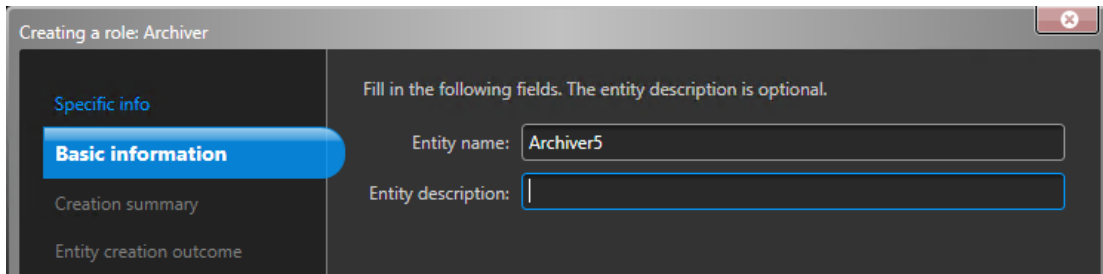
Pour distribuer des caméras sur plusieurs rôles Archiveur :

- 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. Voir « Afficher les réglages de caméras » dans le *Guide de l'utilisateur de Security Desk*.


- 2 Créez les volumes nécessaires pour les rôles Archiveur que vous prévoyez de créer sur l'appareil.
 - Sur les appareils dotés d'un stockage SAN, tels que les appareils série SV-7000E, créez un numéro d'unité logique (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.



- 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.




- 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*, puis sélectionnez une carte 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 une 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**.

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 42
- ["Téléchargement et installation du module externe"](#), page 43
- ["Privilèges Genetec Streamvault"](#), page 44
- ["Création du rôle de module externe "](#), page 46
- ["Configuration de l'entité de surveillance Matériel Streamvault"](#), page 47
- ["Configurer une entité Gestionnaire Streamvault"](#), page 49
- ["Analyser l'état de fonctionnement d'un appareil Streamvault"](#), page 52
- ["Colonnes du volet de rapport de la tâche Matériel Streamvault."](#), page 53

À propos du module externe Streamvault Maintenance

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

Le module externe Streamvault Maintenance inclut les composants suivants :

- **Rôle Streamvault** : rôle module externe qui sert à exécuter l'entité Matériel ou Gestionnaire. Il vous faut un rôle par appareil Streamvault que vous souhaitez 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**, le niveau 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 iDRAC** : permet de contrôler plus finement la gestion des identifiants. Cette fonctionnalité est disponible dans l'onglet **Gestion** du module externe.

IMPORTANT :

- Vous devez disposer de la version 6.0 ou ultérieure du micrologiciel iDRAC.
- Le module externe Streamvault Maintenance accède aux données de fonctionnement via des communications hors bande avec iDRAC. Cela signifie qu'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>.
- La majorité des utilisateurs ne sont pas concernés par la configuration via iDRAC. Pour en savoir plus, contactez l'équipe produit Streamvault.
- Guide applicable pour le module externe Streamvault Maintenance 1.0.

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 que vous souhaitez surveiller et sur tous les postes sur lesquels vous voulez configurer le module externe.

Avant de commencer

Les conditions suivantes sont requises :

- Une [version compatible](#) de Security Center est installée.

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.

Pour installer le module externe :

- 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 décompacté dans C:\Genetec.
- 5 Ouvrez le dossier décompacté, 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 tout de suite. Toutefois, vous devez redémarrer Genetec^{MC} 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 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*.

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 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 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 Matériel et l'affecter à un serveur Streamvault
	Supprimer des surveillances Matériel	Supprimer une entité de surveillance Matériel existante
	Afficher les surveillances Matériel	Afficher la configuration d'une surveillance 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** : 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** : L'entité Gestionnaire Streamvault^{MC} sert à contrôler les configurations d'alerte pour un groupe d'entités de surveillance Matériel 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, vous ne devez créer un rôle pour ces serveurs que si vous souhaitez utiliser l'entité Gestionnaire.

Pour créer un rôle module externe :

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

Configuration de l'entité de surveillance Matériel Streamvault

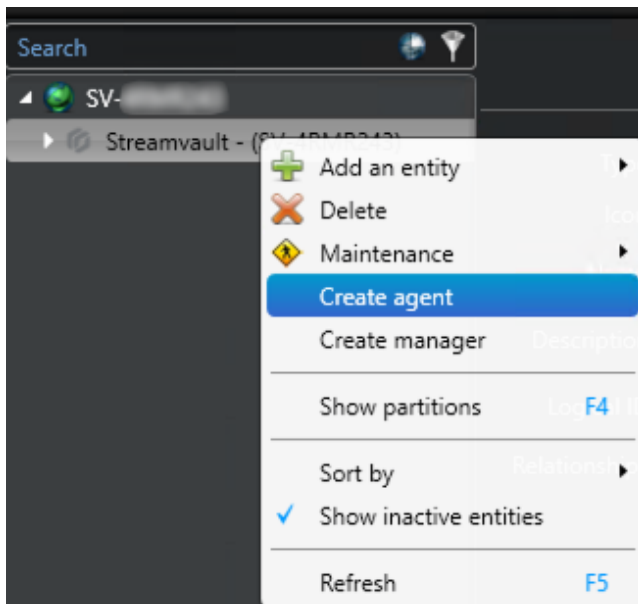
Vous pouvez configurer une entité de surveillance Matériel Streamvault^{MC} pour surveiller le fonctionnement d'un appareil Streamvault et configurer l'envoi de notifications en cas de problème.

Avant de commencer

- Inscrivez vos appareils Streamvault.
- [Créez le rôle de module externe Streamvault.](#)
- **IMPORTANT** : Un agent est créé automatiquement sur chaque serveur Streamvault qui héberge un rôle Streamvault. Si l'agent n'a pas été créé avec le rôle, vous devez créer l'agent manuellement.

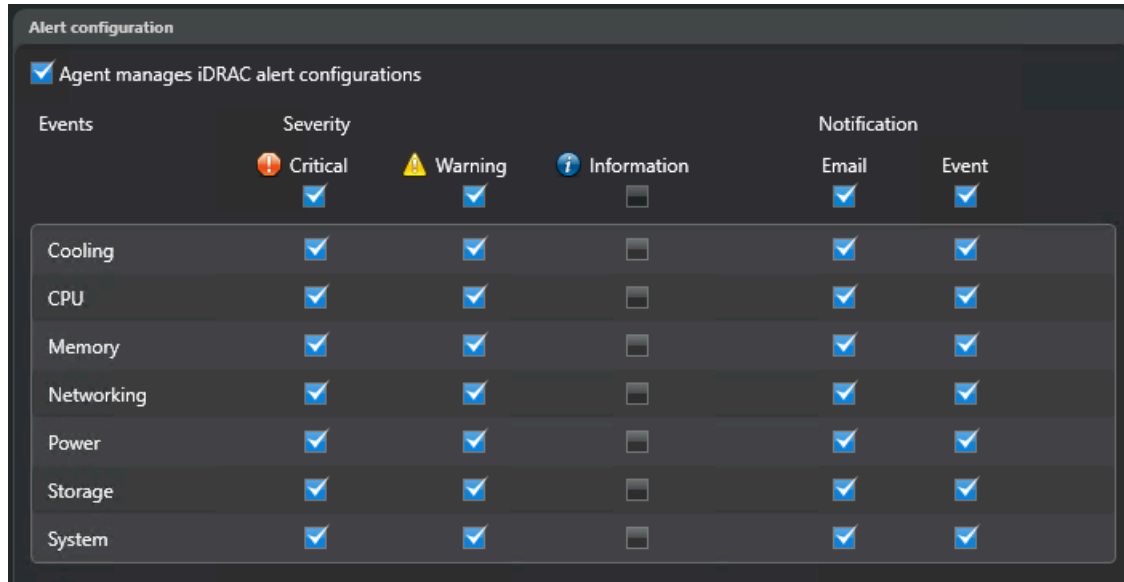
Configuration de l'entité de surveillance Matériel Streamvault :

- 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 Matériel**.



- 3 Dans l'onglet **Identité**, donnez un nom à la surveillance Matériel Streamvault dans le champ **Nom**.

- 4 Dans l'onglet **Général**, configurez les options suivantes :
- Pour gérer les configurations d'alerte via les configurations du rôle de surveillance Matériel Streamvault, cochez la case **L'agent gère les configurations d'alerte iDRAC**.
 - Dans la section **Notification d'alerte**, cochez les cases qui correspondent aux types d'**Événements**, au niveau de **Gravité** et aux types de **Notifications** que vous souhaitez inclure pour cette surveillance Matériel Streamvault.



- 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 **Configuration d'alerte** sont réunies.
- (Facultatif) Dans la section **Identifiants de gestion à distance**, cochez la case **L'agent gère le compte iDRAC** pour gérer les identifiants directement dans le module externe.
- (Facultatif) Dans la section **Identifiants de gestion à distance**, décochez la case **L'agent gère le compte iDRAC** pour utiliser iDRAC pour contrôler la création des utilisateurs et des mots de passe.
- (Facultatif) Si vous décochez la case **L'agent gère le compte iDRAC**, allez dans l'onglet **Gestion** et configurez les identifiants directement dans iDRAC.
- (Facultatif) Dans la section **Port entrant**, vous pouvez définir le port par défaut (65115) sur la valeur de votre choix. Pour en savoir plus, voir [Ports par défaut utilisés par Streamvault](#), page 4.

Configurer une entité Gestionnaire Streamvault

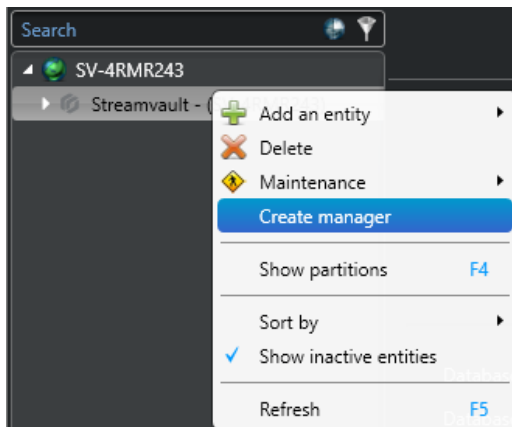
Vous pouvez configurer une entité Gestionnaire Streamvault^{MC} pour contrôler les configurations d'alerte d'un groupe de surveillances Matériel Streamvault de manière centralisée, et configurer les notifications qui doivent être envoyées en cas de survenue d'un problème. L'entité Gestionnaire Streamvault, qui ne sert qu'à ça, est facultative.

Avant de commencer

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

Pour configurer une entité Gestionnaire Streamvault :




- 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 Dans l'onglet **Général**, configurez les options suivantes :
- Pour gérer les configurations d'alerte via les configurations du Gestionnaire Streamvault, cochez la case **L'agent gère les configurations d'alerte iDRAC**.
 - Dans la section **Notification d'alerte**, cochez les cases qui correspondent aux types d'**Événements**, au niveau de **Gravité** et aux types de **Notifications** que vous souhaitez inclure pour les instances du module externe Streamvault Maintenance contrôlées par ce Gestionnaire Streamvault.

Alert configuration

Agent 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"/>

Email recipients

Admin

Administrators

Agents using custom configuration

Streamvault - (SV-2)

Agents using Streamvault Manager configuration

Streamvault - (SV-1)

REMARQUE : Les instances de Streamvault dont les configurations sont définies par le Gestionnaire Streamvault sont visibles dans la section **Agents qui utilisent la configuration Gestionnaire Streamvault**.

- 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 **Configuration d'alerte** sont réunies.
- (Facultatif) Dans la section **Identifiants de gestion à distance**, cochez la case **L'agent gère le compte iDRAC** pour gérer les identifiants directement dans le module externe.
- (Facultatif) Dans la section **Identifiants de gestion à distance**, décochez la case **L'agent gère le compte iDRAC** pour utiliser iDRAC pour contrôler la création des utilisateurs et des mots de passe.

- 7 (Facultatif) Si vous décochez la case **L'agent gère le compte iDRAC**, allez dans l'onglet **Gestion** et configurez les identifiants directement dans iDRAC.

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.

Pour afficher l'état de fonctionnement de vos appareils Streamvault :

- 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}.

- **listes d'images de** : 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 la [Présentation de l'espace de travail des tâches de rapport](#).

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 du SV Control Panel"](#), page 55
- ["Page Configuration du SV Control Panel"](#), page 57
- ["Page CylancePROTECT du SV Control Panel"](#), page 62
- ["Page À propos du SV Control Panel"](#), page 63

Page d'accueil du SV Control Panel

Utilisez la page d'*accueil* 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.

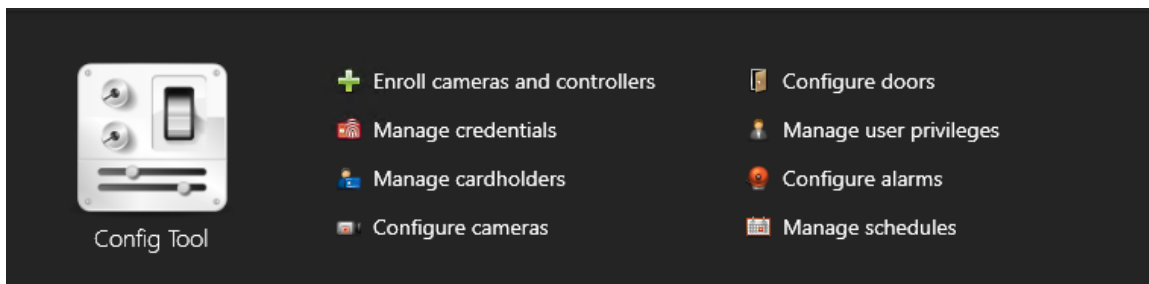
Pour les systèmes s'exécutant en mode Client, le raccourci Server Admin n'est pas disponible. De la même manière, les raccourcis Config Tool et Security Desk sont limités.

REMARQUE : Une bannière rouge est affichée si votre système n'est pas activé. Cliquez sur **Le système n'est pas activé. Cliquez ici pour activer** pour ouvrir l'assistant d'activation du tableau de bord Streamvault.

Raccourcis Config Tool dans SV Control Panel

Utilisez les raccourcis pour ouvrir les tâches principales dans l'application Config Tool.

Les raccourcis disponibles dépendent de vos options de licence.



- **Config Tool** : Cliquez sur l'icône pour ouvrir Config Tool.

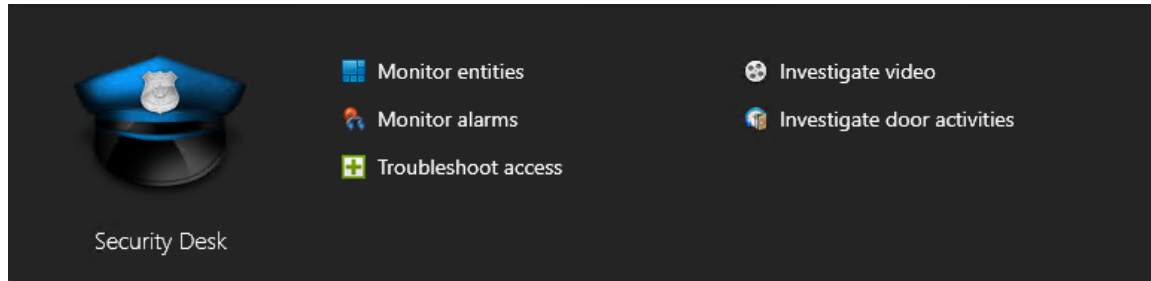
Rubriques connexes

[À propos de l'outil Inscription d'unités](#), page 27

Raccourcis Security Desk dans SV Control Panel

Utilisez les raccourcis pour ouvrir les tâches principales dans l'application Security Desk.

Les raccourcis disponibles dépendent de vos options de licence.



- **Security Desk** : Cliquez sur l'icône pour ouvrir Security Desk.
- **Surveiller des entités** : Cliquez sur la tâche *Surveillance* pour surveiller les événements système en temps réel.
- **Surveiller les alarmes** : Cliquez sur la tâche *Surveillance d'alarmes* pour surveiller et répondre aux alarmes actives et consulter les alarmes passées.
- **Dépanner les accès** : Cliquez sur l'Outil de diagnostic d'accès pour diagnostiquer les problèmes de configuration de contrôle d'accès.
REMARQUE : Ce raccourci n'est pas disponible sur les systèmes exécutés en Mode client.
- **Analyser de la vidéo** : Cliquez sur la tâche *Archives* pour rechercher des archives vidéo.
REMARQUE : Ce raccourci n'est pas disponible sur les systèmes exécutés en Mode client.
- **Analyser les activités de portes** : Cliquez sur la tâche *Activités de portes* pour analyser les événements de certaines portes.
REMARQUE : Ce raccourci n'est pas disponible sur les systèmes exécutés en Mode client.

Server Admin dans SV Control Panel

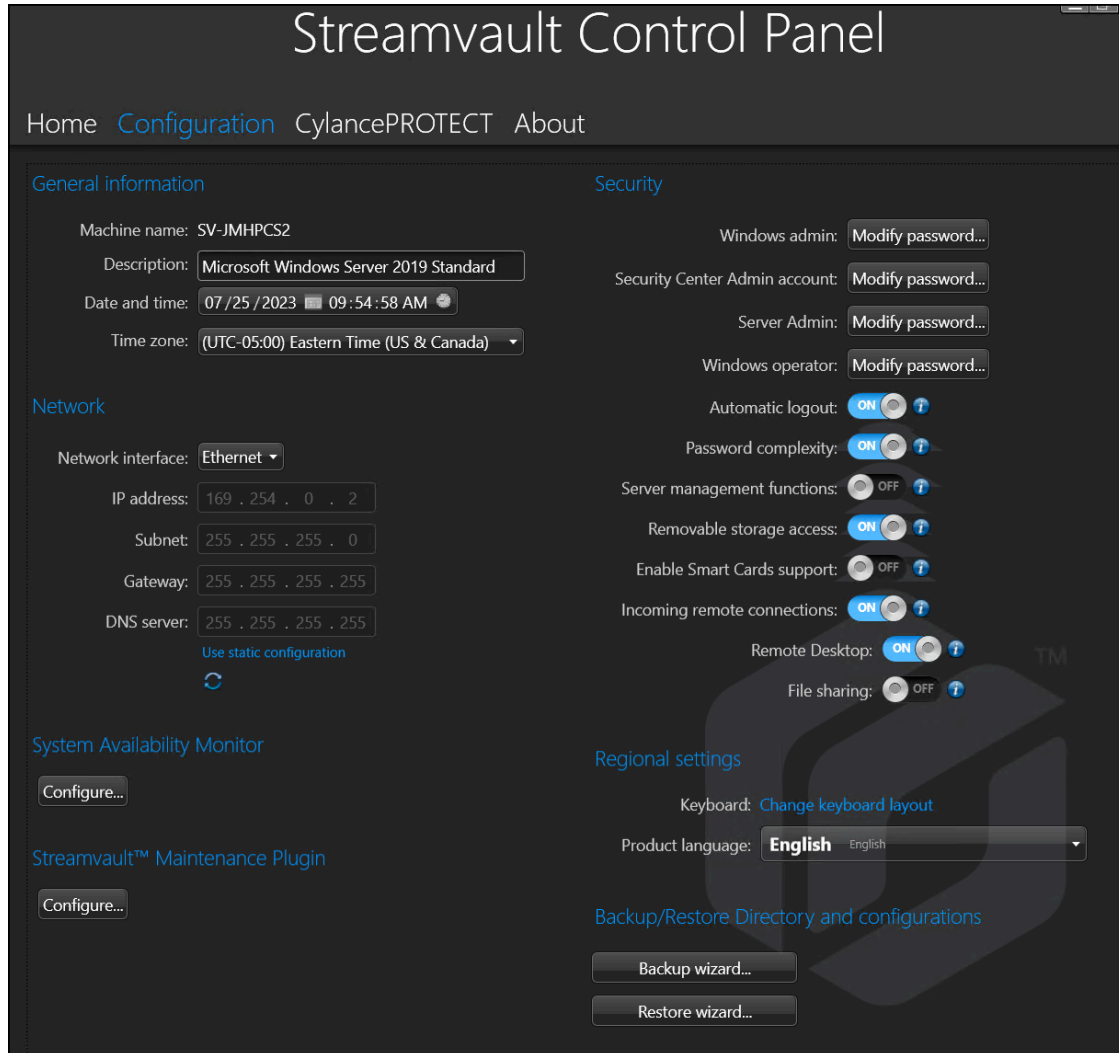
Utilisez l'application Server Admin pour appliquer manuellement une licence ou pour afficher et modifier la configuration du serveur.

Genetec Update Service dans SV Control Panel

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

Page Configuration du SV Control Panel

Utilisez la page *Configuration* de SV Control Panel pour modifier les paramètres généraux, tels que les *paramètres réseau*, les *paramètres System Availability Monitor*, les *comptes utilisateur* et les *paramètres régionaux*.



Pour les systèmes s'exécutant sur un serveur d'extension ou en mode Client, les sections *System Availability Monitor*, *Fonctionnalités* et *Répertoire de sauvegarde/restauration et configurations* ne sont pas disponibles. De la même manière, dans la section *Sécurité*, seuls les mots de passe de l'**administrateur Windows** et des **opérateurs Windows** peuvent être modifiés.

Informations générales


Utilisez la section *Informations générales* de la page *Configuration* pour modifier les réglages généraux comme le nom de votre appareil Streamvault^{MC}.

- **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 réseau

Utilisez la section *Réseau* de la page *Configuration* pour modifier les paramètres réseau comme l'adresse IP de votre appareil Streamvault^{MC}.

- **Interface réseau** : Sélectionnez la carte réseau que vous souhaitez configurer.
REMARQUE : Cette option n'est pas disponible lorsqu'une seule carte réseau est connectée.
- **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.
- **Utiliser la configuration statique** : Cliquez si vous ne voulez pas utiliser l'adresse IP affectée dynamiquement par votre serveur DHCP (Dynamic Host Configuration Protocol). 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.
-  **Actualiser (DHCP seulement)** : Cliquez pour actualiser vos réglages DHCP et obtenir une nouvelle adresse IP.

Réglages System Availability Monitor

Utilisez la section *System Availability Monitor* de la page *Configuration* pour modifier les réglages de System Availability Monitor Agent sur votre appareil Streamvault^{MC}. 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.

Informations sur les fonctionnalités

Utilisez la section *Fonctionnalités* de la page *Configuration* pour afficher et activer les fonctionnalités complémentaires que vous avez souscrites.

Les fonctionnalités suivantes peuvent être activées :

- Security Center Mobile
- Synergis^{MC} Software

REMARQUE : Si Security Center Mobile ou Synergis Software n'est pas installé, les options correspondantes ne sont pas affichées dans la section *Fonctionnalités*. Security Center Mobile est uniquement disponible pour Security Center 5.7 et versions antérieures. Pour les systèmes exécutant Security Center 5.8 GA et versions ultérieures, Security Center Mobile est activé dans Config Tool.

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

Sécurité

Utilisez la section *Sécurité* de la page *Configuration* pour modifier certains réglages du compte utilisateur et de sécurité de votre appareil Streamvault^{MC}.

REMARQUE : Différentes options de mot de passe sont disponibles pour l'utilisateur actuel sur un serveur principal ou un 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.

Spécifiez un mot de passe pour chaque produit :

- **Administrateur Windows :** Le mot de passe Windows de l'utilisateur administrateur.
- **Applications client :** 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.
- **Déconnexion automatique :** Activez cette option pour configurer Windows afin de déconnecter l'utilisateur après 15 minutes d'inactivité.
- **Complexité du mot de passe :** Activez cette option pour exiger un mot de passe complexe d'au moins 10 caractères pour les utilisateurs Windows.
- **Fonctions de gestion de serveur :** Sélectionnez cette option pour permettre aux fonctions telles que l'ajout de rôles et d'autres tâches d'utiliser les applications telles que *Windows Admin Center*, *Server Manager* ou *Windows PowerShell*.
- **Accès au stockage amovible :** Sélectionnez cette option pour 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.
- **Activer la prise en charge des cartes à puce :** Activez cette option pour créer ou utiliser un lecteur de carte à puce avec l'application Security Desk. Pour éviter toute infection par des logiciels malveillants, cette option doit être désactivée par défaut.
- **Connexions à distance entrantes :** Activez cette option pour accorder l'accès aux connexions *Bureau à distance* et permettre le partage de fichiers entre l'appareil et votre réseau informatique. Pour éviter toute infection de votre appareil par des logiciels malveillants, cette option a été désactivée par défaut.
- **Bureau à distance :** Activez cette option pour autoriser les utilisateurs de votre réseau à se connecter à l'appareil à l'aide d'une application *Bureau à distance*. L'option **Connexions à distance entrantes** doit également être activée pour autoriser l'accès via une application *Bureau à distance*. Pour éviter toute infection de votre appareil par des logiciels malveillants, cette option a été désactivée par défaut.
- **Partage de fichiers :** Activez cette option pour partager des fichiers et des dossiers situés sur l'appareil avec d'autres utilisateurs sur votre réseau. L'option **Connexions à distance entrantes** doit également être activée pour autoriser le partage de fichiers. Pour éviter toute infection de votre appareil par des logiciels malveillants, cette option a été désactivée par défaut.

Paramètres réseau

Utilisez la section *Paramètres régionaux* de la page *Configuration* pour modifier les réglages de langue de la disposition du clavier de votre appareil.

- **Modifier la disposition du clavier :** Cliquez pour ouvrir le *Panneau de configuration Windows* afin de modifier la disposition de votre clavier.
IMPORTANT : Vous devez redémarrer votre ordinateur pour que les modifications soient prises en compte.
- **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.

REMARQUE : SV Control Panel est uniquement disponible en anglais.

Sauvegarde et restauration

Utilisez la section *Sauvegarder/restaurer le Répertoire et les configurations* de la page *Configuration* pour accéder à l'assistant de *sauvegarde* et l'assistant de *restauration*.

La sauvegarde et la restauration sont des fonctionnalités du SV Control Panel dont vous pouvez vous servir pour sauvegarder la base de données et les fichiers de configuration du Répertoire en toute sécurité, puis les restaurer vers le même ID système en cas de panne système ou de mise à jour matérielle. 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.

Rubriques connexes

[À propos de la sauvegarde et de la restauration](#), page 33

[Sauvegarder la base de données du Répertoire](#), page 34

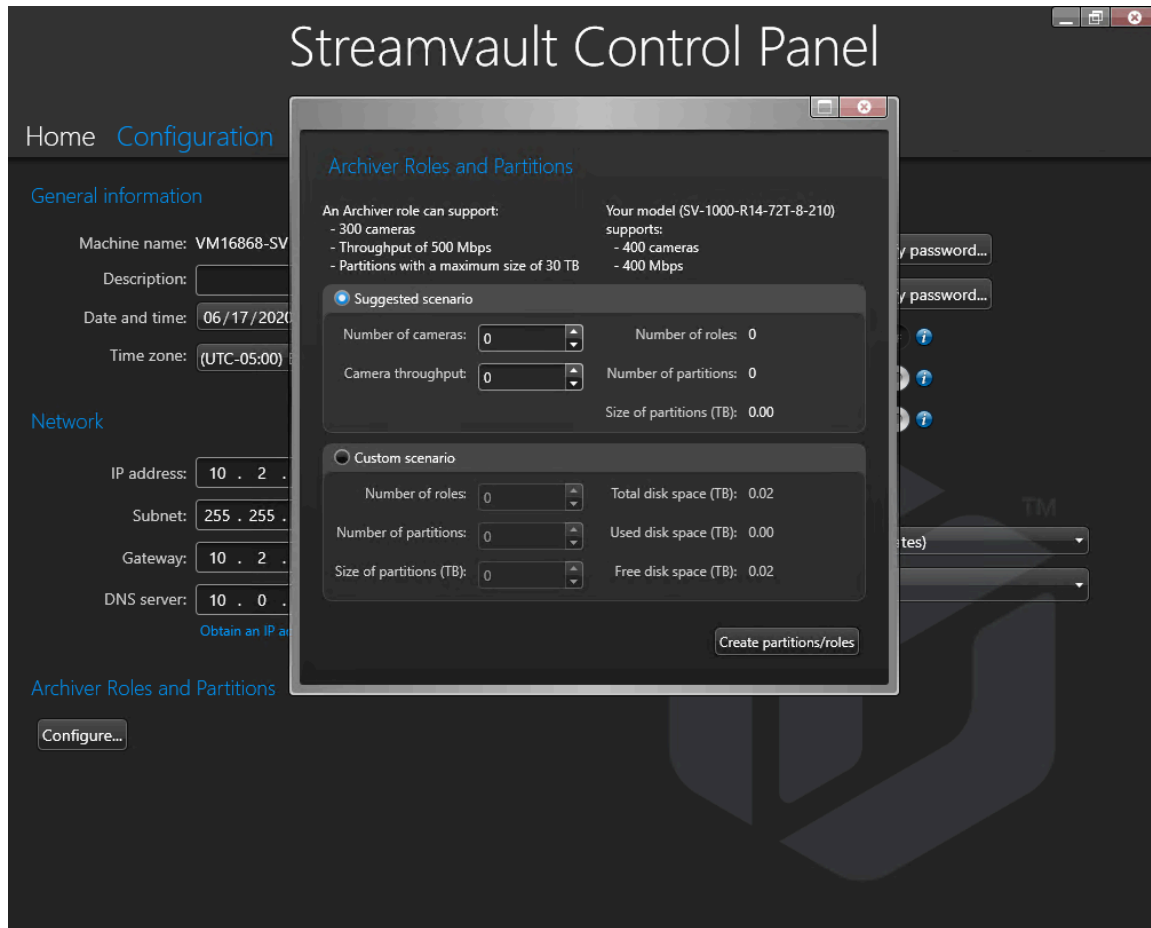
[Restaurer la base de données du Répertoire](#), page 35

Partitions et rôles Archiveur

Utilisez la section *Partitions et rôles Archiveur* de la page *Configuration* pour étendre le nombre maximum de caméras prises en charge par votre système.

Partitions et rôles Archiveur est une fonctionnalité de SV Control Panel permettant de configurer les systèmes nécessitant la prise en charge d'un nombre de caméras et d'un débit supérieurs par un même Archiveur.

Cette section est uniquement disponible pour les systèmes s'exécutant sur un serveur d'extension avec Security Center 5.8 et versions ultérieures.



- **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 37.

Page CylancePROTECT du SV Control Panel

Utilisez la page CylancePROTECT pour consulter des informations sur Cylance et choisir le mode de communication entre l'appareil Streamvault^{MC} et la console Cylance dans le cloud.

Sélectionnez l'une des options suivantes :

- **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.

IMPORTANT : Lorsque CylancePROTECT est désactivé, vous ne pouvez pas basculer entre **Déconnecté** et **En ligne**. Pour modifier ces réglages, vous devez réinitialiser l'image logicielle sur l'appareil.

ATTENTION : Basculer entre les options peut nécessiter le redémarrage de votre ordinateur entraînant une indisponibilité du système.

Pour accéder aux journaux et fonctionnalités avancées de votre système, sélectionnez **Exécuter CylancePROTECT en mode Interface avancée**.

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* contient des informations de licence, des informations sur le contrat de maintenance applicative (CMA), des liens vers le portail d'assistance technique de Genetec^{MC} (GTAP) et des liens vers la documentation produit.

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

Informations de licence

Utilisez la section *Licence* de la page *À propos* 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 des informations de licence complémentaires.

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

Rubriques connexes

[Activer votre licence Security Center sur un appareil](#), page 19

Informations de contrat de maintenance applicative

Utilisez la section *CMA* de la page *À propos* pour afficher les informations sur le contrat de maintenance applicative.

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

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

Informations système

Utilisez la section *Système* de la page *À propos* pour afficher des informations sur le système.

- **Fabricant** : Affiche le fabricant du matériel.
- **Modèle matériel** : Affiche le modèle matériel.
- **Révision logicielle** : Affiche la version ou 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* de la page *À propos* pour accéder à des liens utiles vers le portail d'assistance technique Genetec^{MC} (GTAP) et la documentation produit.

- **GTAP** : Cliquez sur le lien pour ouvrir [GTAP](#) et les forums d'assistance.
REMARQUE : Vous devez disposer d'un nom d'utilisateur et d'un mot de passe valables 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 de l'utilisateur de SV Control Panel*, qui contient également les notes de mise à jour de SV Control Panel.
- **Security Desk** : Cliquez sur le lien pour ouvrir le *Guide de l'utilisateur de Security Center*.

Ressources complémentaires

Cette section aborde les sujets suivants:

- ["Créer une clé USB de réinitialisation d'usine"](#), page 66
- ["Garantie de votre appareil Streamvault"](#), page 68
- ["Réappliquer une image à un appareil Streamvault"](#), page 69
- ["ID système et numéro de version logicielle d'un appareil Streamvault"](#), page 70
- ["Autoriser le partage de fichiers sur un appareil Streamvault"](#), page 71
- ["Autoriser les connexions Bureau à distance à un appareil Streamvault"](#), page 72

Créer une clé USB de réinitialisation d'usine

Pour réinitialiser l'image d'un appareil Streamvault^{MC} SV-100E, SV-300E, SV-350E ou de type serveur/poste de travail Streamvault^{MC}, vous devez préparer une clé USB de démarrage contenant l'image logicielle Streamvault requise.

Avant de commencer

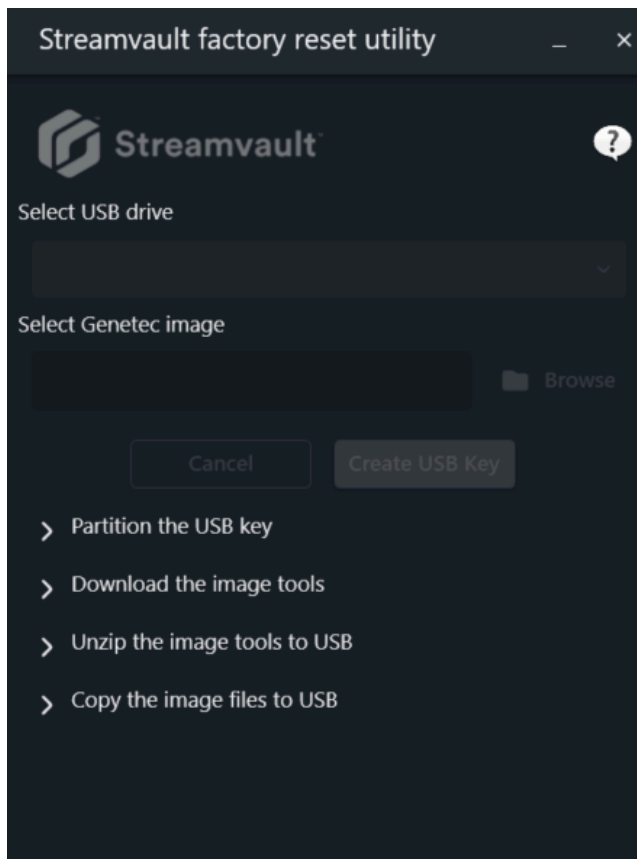
- Téléchargez *Streamvault Factory Reset Utility* à partir de la section [Téléchargements](#) du *Guide de l'utilisateur de l'appareil Streamvault^{MC}* sur le [TechDoc Hub](#).
- Avant d'ouvrir l'outil *Streamvault Factory Reset Utility*, décompressez les images de sauvegarde dans un dossier Windows.
- Assurez-vous de disposer d'une clé USB comprenant au moins 32 Go d'espace disponible.

Regardez cette vidéo pour savoir comment créer une clé USB de réinitialisation d'usine.



Pour créer une clé USB amorçable contenant l'image logicielle requise sur l'outil *Streamvault Factory Reset Utility* :

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



- 2 Dans la section *Sélectionner une image Genetec*, cliquez sur **Parcourir** et sélectionnez le fichier *.swm* requis.
 - Pour les appareils tout-en-un, sélectionnez l'un des fichiers décompressés dans le dossier *wim*.
 - Pour les postes de travail et les serveurs, sélectionnez l'image requise dans le dossier *<numéro de balise de service>*.

- 3 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, un message s'affiche dans l'outil *Streamvault Factory Reset Utility* pour vous indiquer que la clé USB a été créée avec succès.

Lorsque vous avez terminé

- Pour un appareil SV-100E, SV-300E ou SV-350E, [réinitialisez le logiciel sur l'appareil](#).
- Pour un appareil de type poste de travail ou serveur, [réinitialisez l'image de l'appareil Streamvault à l'aide de la clé USB amorçable](#).

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}](#).

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 sur les produits qui utilisent une version embarquée du logiciel de Microsoft.



REMARQUE : Chaque image de Streamvault est conçue pour fonctionner avec sa version respective de Security Center, comme indiqué dans les *Notes de version Streamvault*. La rétrogradation de Security Center vers une version antérieure peut nécessiter une réduction du niveau de renforcement 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](#).

ID système et numéro de version logicielle d'un appareil Streamvault

Lorsque vous contactez le support technique de Genetec^{MC}, vous avez besoin de l'ID système et du numéro de révision du logiciel (version de l'image) du logiciel Genetec installé sur l'appareil

Avant de commencer

Connectez-vous à Windows en tant qu'administrateur.

À savoir

Outre l'ID système et le numéro de révision du logiciel, le support technique Genetec peut également demander le numéro de certification et le numéro de série. Pour trouver ces informations, consultez l'étiquette apposée sur l'appareil Streamvault.

Pour trouver l'ID système et la version d'image de votre appareil :

- 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 le numéro de **Révision logicielle**.

Rubriques connexes

[Rétablissement des réglages d'usine sur un appareil SV-100E, SV-300E ou SV-350E, page 74](#)

[Rétablir les réglages d'usine sur un appareil Streamvault poste de travail ou serveur, page 78](#)

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 le Tableau de bord SV.

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.

Pour activer le partage de fichiers sur votre appareil :

- 1 Sur la page *Configuration* de SV Control Panel :
 - Activez l'option **Connexions à distance entrantes**.
 - Activez l'option **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.

Pour autoriser les connexions Bureau à distance à votre appareil Streamvault^{MC} :

- 1 Sur la page *Configuration* de SV Control Panel :
 - Activez l'option **Connexions à distance entrantes**.
 - Activez l'option **Bureau à distance**.
- 2 Cliquez sur **Appliquer**.

Rubriques connexes

[Le Bureau à distance ne peut pas se connecter à un appareil Streamvault](#), page 83

Dépannage

Cette section aborde les sujets suivants:

- ["Rétablissement des réglages d'usine sur un appareil SV-100E, SV-300E ou SV-350E"](#), page 74
- ["Rétablir les réglages d'usine sur un appareil Streamvault poste de travail ou serveur"](#), page 78
- ["Les contrôleurs Mercury EP restent hors ligne lorsque TLS 1.1 est désactivé"](#), page 81
- ["Activer Transport Layer Security \(TLS\)"](#), page 82
- ["Le Bureau à distance ne peut pas se connecter à un appareil Streamvault"](#), page 83
- ["Impossible d'installer CylancePROTECT depuis SV Control Panel pour certains appareils Streamvault"](#), page 88

Rétablissement des réglages d'usine sur un appareil SV-100E, SV-300E ou SV-350E

Si le logiciel sur un appareil SV-100E, SV-300E ou SV-350E ne parvient pas à démarrer ou cesse de fonctionner comme prévu, 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 34.
- 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.
- (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

- Pour les appareils avec des numéros de modèle différents de SV-100E, SV-300E et SV-350E, consultez [Rétablir les réglages d'usine sur un appareil Streamvault poste de travail ou serveur](#), page 78.
- 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.

Pour rétablir les réglages d'usine sur un appareil série SV-100E, SV-300E ou SV-350E :

- 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

[Configurez votre appareil.](#)

Rubriques connexes

[ID système et numéro de version logicielle d'un appareil Streamvault](#), page 70

Réinitialisation de l'image logicielle sur un appareil SV-100E, SV-300E ou SV-350E à l'aide d'une clé USB de démarrage

Vous pouvez réinitialiser l'image logicielle à l'aide d'un lecteur de récupération USB.

Avant de commencer

- [Munissez-vous de la clé USB contenant l'image logicielle de récupération pour votre appareil.](#)
- 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

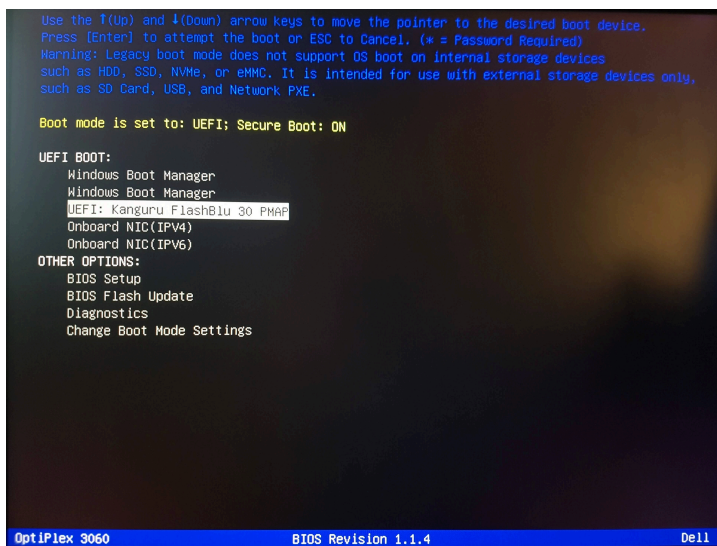
- Le rétablissement des réglages d'usine supprime et remplace toutes les données actuellement présentes sur le lecteur Windows (C:), y compris les bases de données et les journaux.
ATTENTION : Seuls les fichiers sur le disque C: sont supprimés, mais nous vous conseillons malgré tout de sauvegarder les fichiers vidéo sur tous vos disques.
- La réinitialisation prend environ 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.

Regardez cette vidéo pour savoir comment réinitialiser l'image logicielle sur un appareil SV-100E, SV-300E ou SV-350E à l'aide d'une clé USB de démarrage.

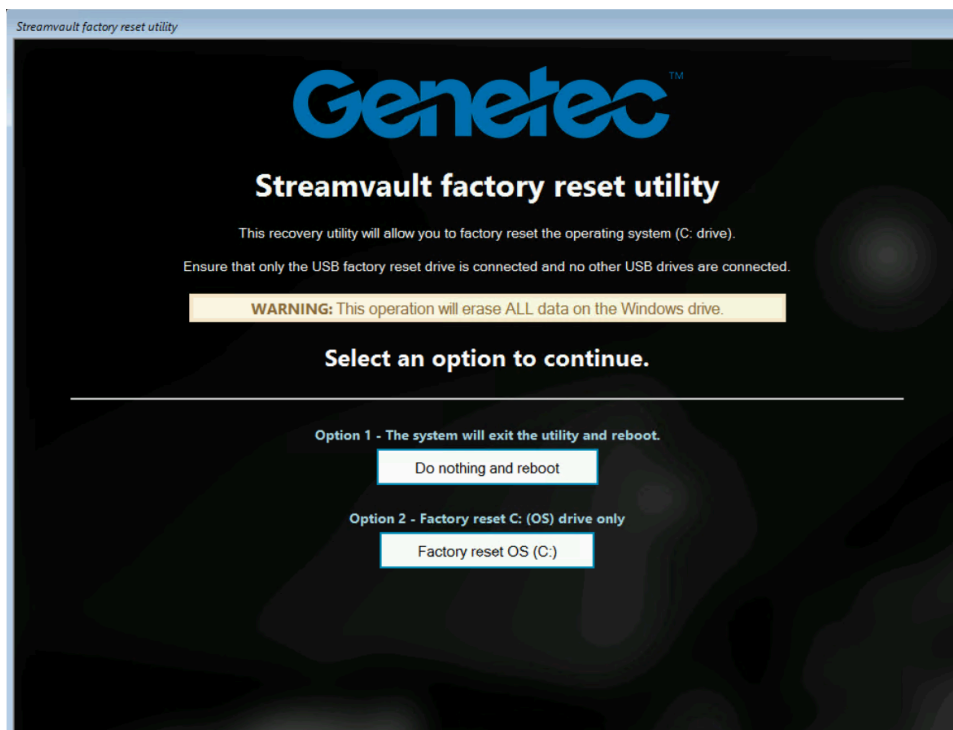


Pour réinitialiser l'image d'un appareil série SV-100E, SV-300E ou SV-350E :

- 1 Arrêtez l'appareil.
- 2 Insérez la clé USB que vous avez créée dans un port USB.
- 3 Sélectionnez le lecteur USB et appuyez sur Entrée.



- 4 Lorsque le périphérique USB démarre en mode récupération, sélectionnez l'une des options suivantes :
- **Ne rien faire et redémarrer** : Sélectionnez cette option pour quitter le programme de récupération et redémarrer l'appareil.
 - **Rétablir les réglages d'usine du SE (C:)** : Sélectionnez cette option pour formater et réinstaller le disque système de l'appareil, en conservant les fichiers vidéo sur les autres disques. Toutes les données du disque C: seront perdues : bases de données, journaux, etc.



- 5 À l'invite, tapez Yes et appuyez sur Entrée pour rétablir les réglages d'usine. Patientez ensuite jusqu'à la fin du processus.
- 6 Une fois le rétablissement des réglages d'usine terminé, retirez la clé USB de l'appareil et appuyez sur Entrée pour redémarrer.
- 7 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.
- 8 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 été validé comme étant réussi. Cependant, aucune connexion Internet n'était disponible à cet instant. Passez à l'étape suivante.
 - **ÉCHEC** : Le processus a échoué. Contactez l'assistance technique Genetec.
- 9 Si vous recevez un message **PASS** ou **PASS - Aucune transmission**, fermez la fenêtre *Genetec^{MC} Product Validator*.
- 10 Attendez que le script en arrière-plan se ferme, puis redémarrez l'appareil.

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.](#)

- Si vous avez sauvegardé la configuration de Security Center avant de rétablir les réglages d'usine, [restaurez-la avec SV Control Panel](#).

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

Si le logiciel sur votre appareil Streamvault poste de travail ou serveur 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 34.
- 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 [Rétablissement des réglages d'usine sur un appareil SV-100E, SV-300E ou SV-350E](#), page 74.
- 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. Si c'est le cas, contactez le [centre d'assistance technique de Genetec^{MC} \(GTAC\)](#).

Pour effectuer une réinitialisation d'usine sur un appareil de type poste de travail ou serveur Streamvault :

- 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

[ID système et numéro de version logicielle d'un appareil Streamvault](#), page 70

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

Vous pouvez rétablir l'état par défaut de l'image logicielle de votre appareil Streamvault en utilisant une clé USB de récupération.

Avant de commencer

- [Assurez-vous de disposer de la clé USB contenant le logiciel de récupération pour votre appareil.](#)

À savoir

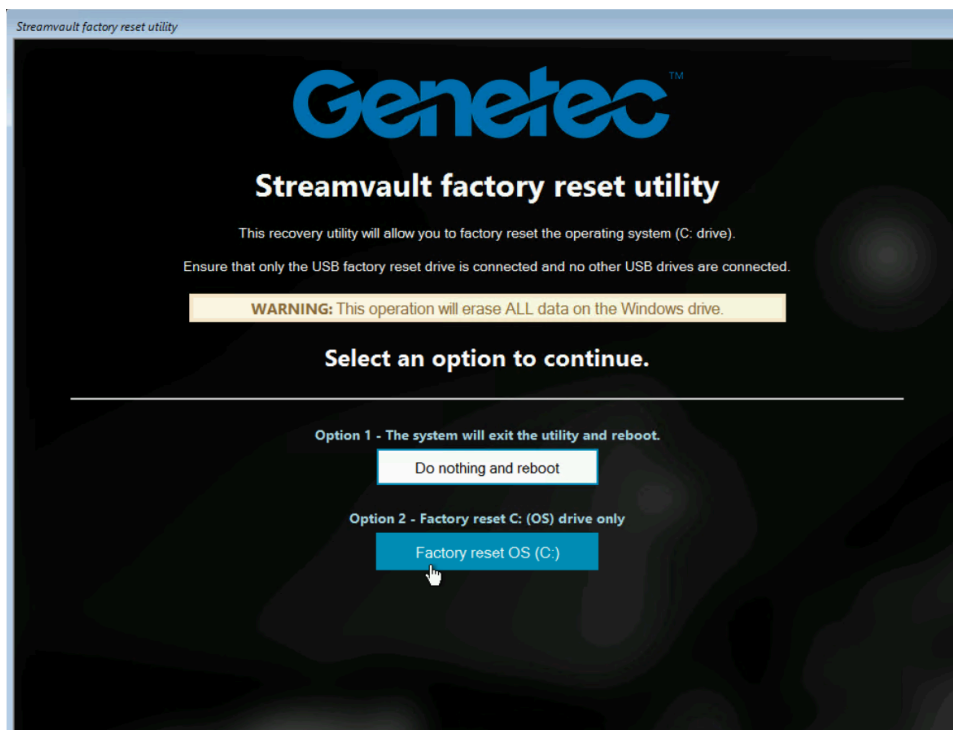
- La réinitialisation supprime toutes les données actuellement sur le disque système.
- La réinitialisation n'affecte pas les réglages d'usine RAID par défaut du disque.
- La réinitialisation peut échouer si les paramètres par défaut des disques durs, volumes RAID ou partitions de l'appareil ont été modifiés. Si c'est le cas, contactez le centre d'assistance technique de Genetec^{MC} (GTAC).

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



Pour réinitialiser l'image logicielle sur l'appareil Streamvault :

- 1 Arrêtez l'appareil.
- 2 Insérez la clé USB amorçable que vous avez créée dans un port USB.
- 3 Mettez l'appareil Streamvault sous tension.
- 4 À l'invite, appuyez sur F12.
Le *Boot Manager* s'ouvre. Cliquez sur **One-shot UEFI Boot Menu**.
- 5 Sélectionnez votre clé USB, puis appuyez sur Entrée.
Streamvault Factory Reset Utility s'ouvre.

6 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.

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.](#)
- Si vous avez sauvegardé la configuration de Security Center avant de rétablir les réglages d'usine, [restaurez-la avec SV Control Panel.](#)

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 :

- SV-100E 16.3 et versions ultérieures
- SV-300E 16.3 et versions ultérieures
- 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 dans l'Éditeur du Registre Windows.](#)

Activer Transport Layer Security (TLS)

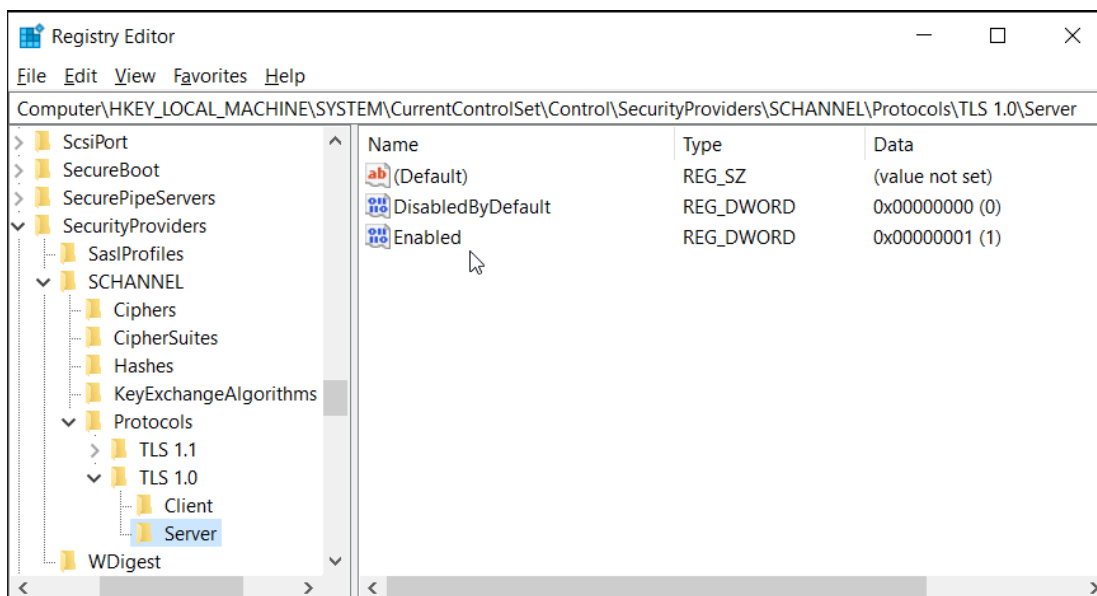
Les protocoles Transport Layer Security (TLS) 1.0 et 1.1 présentent plusieurs vulnérabilités majeures et sont donc désactivées sur les appareils Streamvault^{MC}. Si un appareil inscrit dans Security Center nécessite l'un de ces protocoles pour communiquer, vous devez activer le protocole sur votre appareil.

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.
- N'activez que la version de TLS exigée par votre appareil.
- Vous devez activer TLS sur les nœuds serveur (entrants) et client (sortants).
- Par souci de sécurité, les options de Propriétés Internet sont désactivées sur les appareils. C'est pourquoi vous ne pouvez activer TLS que depuis l'Éditeur du Registre Windows.

Pour activer TLS sur un appareil :

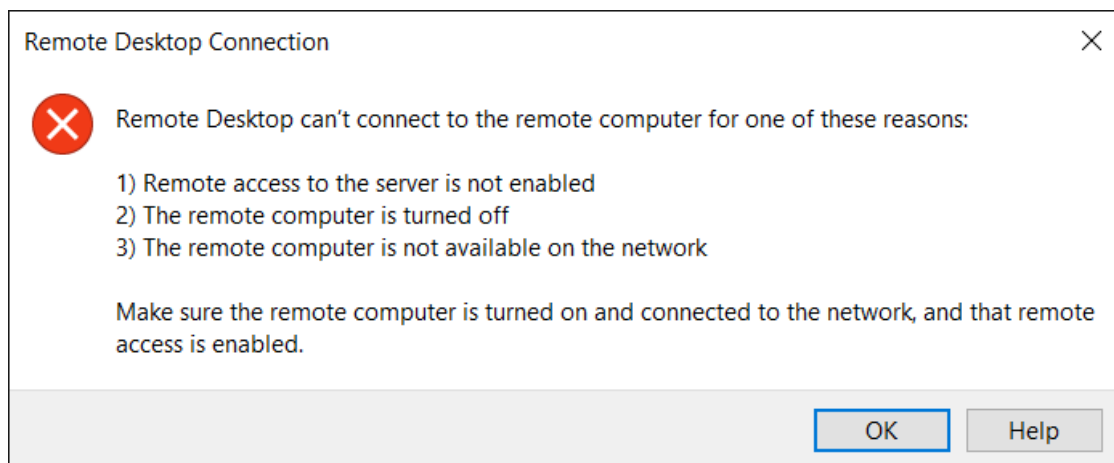
- 1 Ouvrez l'Éditeur du Registre Windows.
- 2 Activez TLS 1.*n*, où *n* représente le numéro de version mineure :
 - a) Naviguez jusqu'à `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.n`.
 - b) Sélectionnez le nœud **Serveur**, réglez **DisabledByDefault** 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

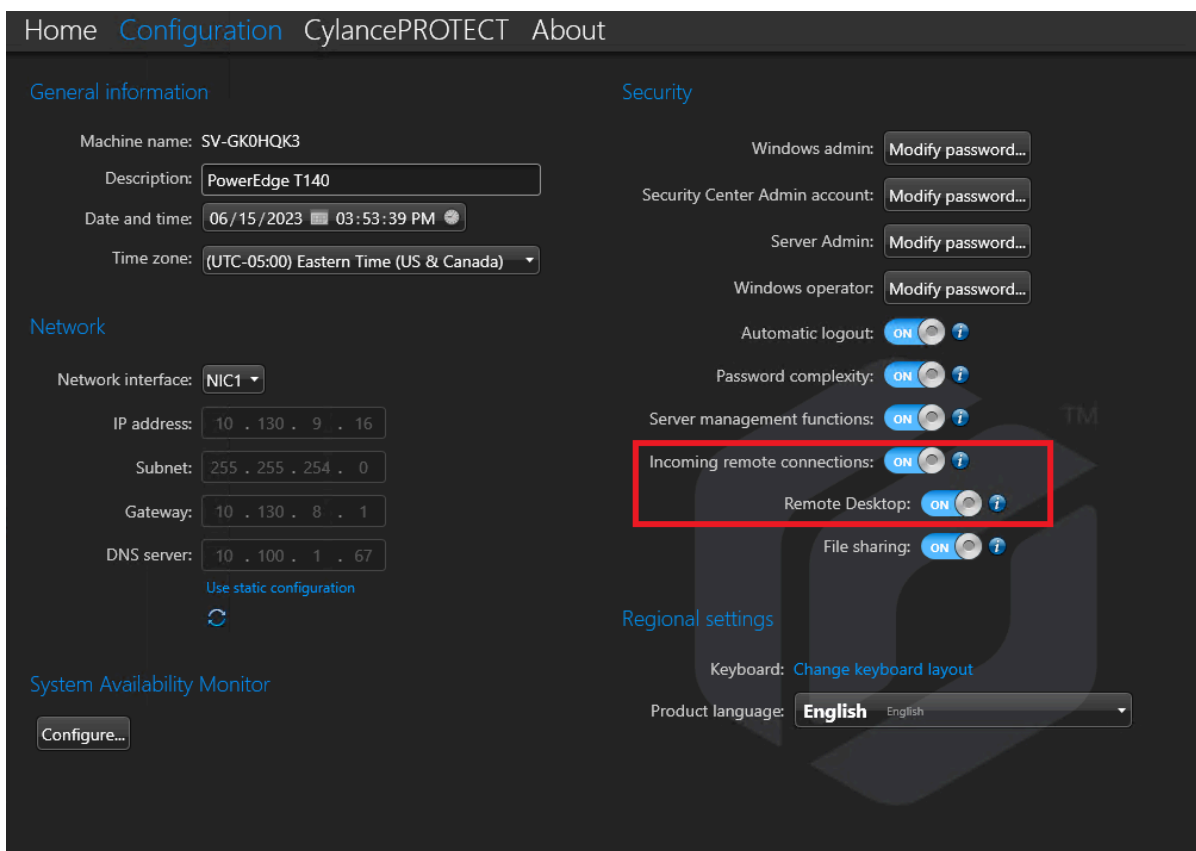
Lorsque vous tentez d'accéder à un appareil SV avec le Bureau à distance, vous recevez un message indiquant que le Bureau à distance ne peut pas se connecter à l'ordinateur distant.



Les connexions à distance et le Bureau à distance sont désactivés 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 *Configuration* de SV Control Panel, activez les options **Connexions à distance entrantes** et **Bureau à distance**.



Les connexions à distance ou le Bureau à distance ne sont pas autorisés dans Windows

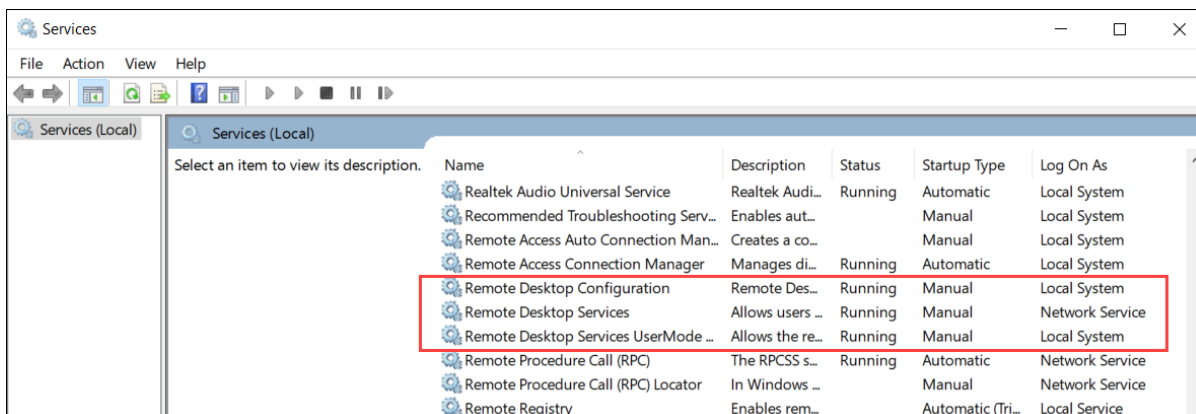
Description : Bien que les options **Connexions à distance entrantes** et **Bureau à distance** soient activées dans SV Control Panel, ces réglages ne sont pas actuellement autorisés dans Windows.

Solution : Remplacez les réglages Windows en désactivant puis en **réactivant les options Connexions à distance entrantes et Bureau à distance** dans SV Control Panel.

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.

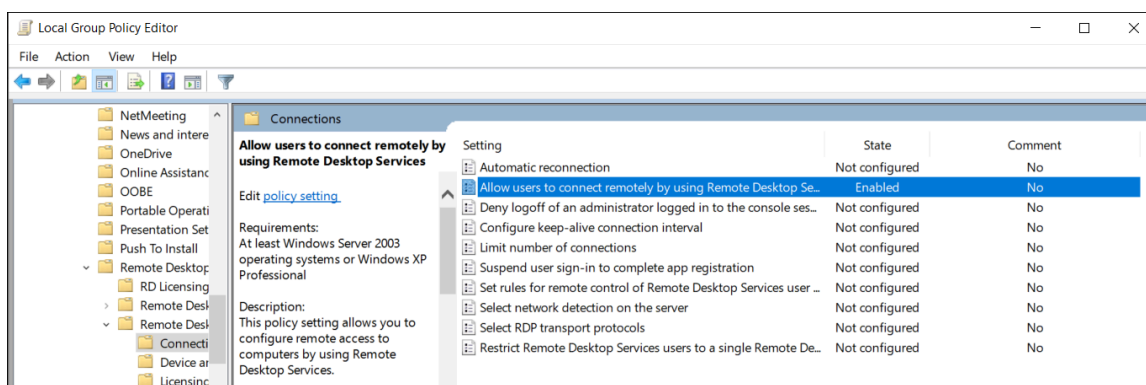


Les Services Bureau à distance sont refusés

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

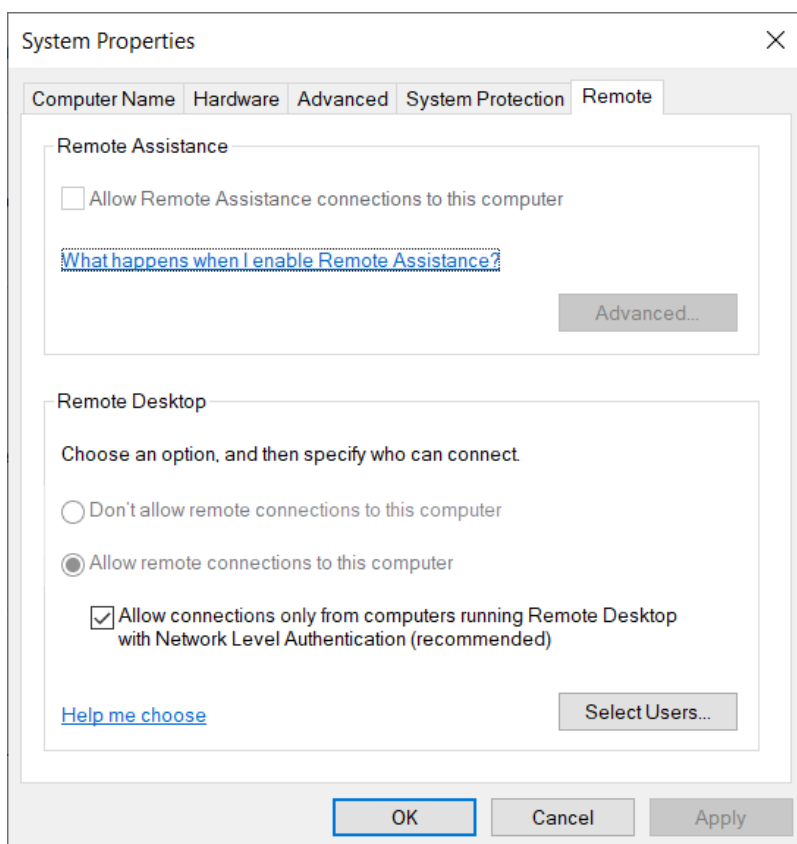
Solution : Autorisez les accès à distance à l'appareil à l'aide des Services Bureau à distance :

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



4. Dans l'invite de commande, exécutez `gpupdate /force`.
5. Dans le Panneau de configuration Windows, accédez à **Système > Paramètres d'utilisation à distance**. La fenêtre *Propriétés système* apparaît.

6. Dans l'onglet *Utilisation à distance*, dans la section *Bureau à distance*, assurez-vous que l'option **Autoriser les connexions à distance à cet ordinateur** est sélectionnée.



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 NTLM2 si négociée**.

Nous contacter

Solution : Si la connexion Bureau à distance est toujours impossible, contactez l'assistance technique.

Rubriques connexes

[Autoriser les connexions Bureau à distance à un appareil Streamvault](#), page 72

Impossible d'installer CylancePROTECT depuis SV Control Panel pour certains appareils Streamvault

Vous avez désactivé l'option **CylancePROTECT** de SV Control Panel, mais CylancePROTECT ne se désinstalle pas de votre appareil Streamvault^{MC}.

Versions affectées

Les versions d'image Streamvault suivantes sont concernées par ce problème :

- 0011.2.X.27.G (publication le 18 janvier 2021) et ultérieures
- 16.8.0 (publication le 10 mars 2021) et ultérieures
- 2019.1.C.14.G (publication le 14 janvier 2021) et ultérieures
- 2016.1.C.19.G (publication le 8 février 2021) et ultérieures

Cause

Un problème de code.

Contournement

1. Ouvrez la console *Services* de Windows.
2. Faites un clic droit sur le service **Serveur** et cliquez sur **Propriétés**.
3. Modifiez l'option **Type de démarrage** sur **Manuel**, puis démarrez le service.
4. Ouvrez SV Control Panel, cliquez sur l'onglet **CylancePROTECT** et sélectionnez l'option **Désactiver**.
Veuillez patienter 2 minutes jusqu'à la fin du processus.
5. Dans la console *Services* de Windows, modifiez le **Type de démarrage** du service **Serveur** sur **Désactivé**.
6. Redémarrez l'appareil Streamvault.

Assistance technique

Cette section aborde les sujets suivants:

- ["Contacter l'assistance Genetec"](#), page 90
- ["Assistance logicielle"](#), page 93
- ["Assistance matérielle"](#), page 94
- ["Spécifications pour Streamvault^{MC}"](#), page 96
- ["Conditions générales de l'assistance Streamvault"](#), page 97

Contactez l'assistance 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^{MC} 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 avez perdu 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 les clients en Amérique du Nord, en Europe, au Moyen-Orient et en Afrique :

1. Consultez la page [Nous contacter](#) du *centre d'assistance technique de Genetec* pour obtenir le numéro de téléphone et les horaires du GTAC dans votre région.
2. Appelez le numéro de téléphone du centre d'assistance technique de Genetec 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 nous contacter en dehors des heures de bureau, en utilisant l'assistance d'urgence 24 h/24 et 7 j/7 :

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 l'assistance Genetec par le portail GTAP

Tous les clients ont accès à une assistance 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 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 l'assistance Genetec par le chat en direct

Les clients ayant souscrit la couverture Genetec Advantage ont accès à une assistance technique en direct durant les heures de bureau dans leur région par l'intermédiaire du chat en direct sur le [portail d'assistance technique de Genetec \(GTAP\)](#).

Pour les clients qui n'ont pas souscrit une couverture 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**.

GTAC - Live Chat

Support hours for your territory:
Monday to Friday: 08:00 to 20:00 Eastern Standard Time
Status: Online

Genetec

Welcome

Please select your preferred language

English French

Please enter the System ID *

CHECK SYSTEM ID

The transcript of your chat session will be retained for quality assurance purposes

START CHAT

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^{MC}

- L'image Windows Streamvault^{MC} est couverte dans le cadre de votre garantie Streamvault^{MC} 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^{MC} est couverte dans le cadre de votre garantie Streamvault^{MC}, 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 les documents relatifs à la gestion du cycle de vie Genetec : [Description de Genetec Advantage](#) et [Description de Genetec Assurance](#).

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 (GTAC) est votre point de contact pour le diagnostic et pour la coordination avec HP et DellProSupport.

Gamme de produits	Durée de la garantie ¹		Remplacement anticipé ou réparation sur site	Retour et réparation de produit sous garantie ²
	Standard	Étendu		
SV-100E SV-300E SV-350E	3 ans	2 ans	1 an de remplacement anticipé	Intégré
SVW-300 SVW-500 SV-1000	3 ans	Non applicable	Garantie de réparation sur site HP ³	Intégrée
SV-2000E SV-4000E SV-7000E	5 ans	2 ans	Garantie Dell ProSupport de réparation sur site le jour ouvré suivant ⁴ avec conservation de votre disque dur ³	Intégrée
SVW-300E SVW-500E SV-1000E	5 ans	Non applicable	Garantie Dell ProSupport de réparation sur site le jour ouvré suivant ⁴ avec conservation de votre disque dur ³	Intégrée
SV-2000 SV-4000 SV-7000	5 ans	2 ans	Garantie de réparation sur site HP ³	Intégrée
Storage Area Network (SAN)	5 ans	Extension possible sur demande et au cas par cas.	Garantie Dell ProSupport de réparation sur site le jour ouvré suivant ⁴ avec conservation de votre disque dur ³	Intégrée

¹Vous pouvez acheter une extension de garantie de deux ans supplémentaires (pour un total de 7 ans de garantie). Cet achat doit intervenir dans les 5 ans.

² Vous pouvez choisir de renvoyer l'unité pour réparation ou de bénéficier d'un service de réparation sur site.

³Pour en savoir plus sur les conditions définies par ces fournisseurs, veuillez consulter la documentation sur l'assistance [Dell ProSupport](#) et [HP](#).

⁴La garantie de réparation sur site le jour ouvré suivant démarre à l'issue du diagnostic, lorsque le problème matériel a été identifié, que le dossier a été ouvert auprès de Dell et que Dell a déterminé qu'il s'agissait d'une défaillance matérielle. L'ouverture d'un dossier d'assistance auprès de Genetec Inc. ne compte pas pour le calcul du jour ouvré suivant.

Spécifications pour Streamvault^{MC}

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

Spécifications techniques, mécaniques et environnementales

Appareils tout-en-un :

- [Fiche technique SV-100E](#)
- [Fiche technique SV-300E](#)
- [Fiche technique SV-350E](#)

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](#)
- [Fiche technique gamme SVS-7000E NAS](#)
- [Fiche technique gamme SVS-7000E SAN](#)

Postes de travail :

- [Fiche technique gamme SVW-300E](#)
- [Fiche technique gamme SVW-500E](#)

Appareils prêts pour l'analytique :

- [Fiche technique gamme SVA-100E](#)
- [Fiche technique gamme SVA-1000E](#)

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 standard et étendue de Genetec^{MC} sont régies par les conditions générales suivantes concernant les réparations, remplacements, recours ou exclusions de la garantie.

Conditions générales

Garantie sur les réparations et les pièces de rechange

Tous les produits Genetec bénéficiant d'une maintenance de Genetec Inc. pour les réparations et pièces de rechange sont garantis contre les défauts de fabrication et de matériaux pendant 90 jours, ou pendant le restant de la garantie d'origine, selon ce qui est le plus long. Des frais supplémentaires peuvent s'appliquer si le dommage résulte d'une utilisation non prévue du produit.

Pour Streamvault^{MC}, tout ou partie des équipements remplacés deviennent la propriété de Genetec Inc. dès réception du matériel de remplacement correspondant par le client, et le client doit renvoyer dans les meilleurs délais tout ou partie de ces équipements remplacés à la demande de Genetec Inc. Si ces équipements remplacés ne sont pas renvoyés sous 30 jours à compter de la réception des nouvelles pièces, le client devra payer à Genetec Inc. la valeur des pièces de remplacement. Le service **Conserver votre disque dur** n'est pas concerné.

Recours exclusif de la garantie

Durant la période de garantie applicable et si Genetec Inc. détermine qu'un produit présente des défauts de fabrication ou d'assemblage, Genetec Inc. choisira à sa seule discrétion l'une des options suivantes :

- Rembourser le client du montant payé pour le produit défectueux.
- Réparer le produit défectueux.
- Remplacer le produit défectueux par un produit neuf ou reconditionné.
- Remplacer le produit défectueux par un produit différent doté de spécifications au moins équivalentes.

Exclusions de la garantie

Les éléments suivants ne sont pas couverts par la garantie matérielle standard de Genetec :

- Équipement non acheté auprès de Genetec Inc.
- Produits utilisés avec un matériel ou un logiciel annexe non pris en charge.
- Défauts ou dommages résultant d'une mauvaise utilisation (notamment une utilisation non conforme à la documentation et aux manuels du produit), de modifications inappropriées, d'accidents ou de négligence.
- Défauts ou dommages résultant du perçage de trous, d'ajouts d'autocollants ou autres adhésifs, ou de la peinture du produit.
- Défauts ou dommages dus à l'humidité, à la foudre, à une explosion ou à toute autre décharge électrique.
- Produits démontés ou réparés de telle manière que cela nuit aux performances ou empêche l'inspection et les tests afin de vérifier toute réclamation au titre de la garantie.
- Modification, abus ou altération du produit.
- Cas de force majeure (crue éclair, tremblement de terre, foudre, incendie, fuite de gaz, etc.).
- Usure normale.

Conditions générales des autorisations de retour RMA de Genetec

Autorisation de retour RMA

Avant de renvoyer un article, le client doit obtenir un formulaire d'autorisation de retour (Return Merchandise Authorization ou RMA) auprès de Genetec Inc. Le numéro de RMA doit être clairement indiqué sur chaque colis retourné et sur le formulaire RMA inclus dans le colis. Le client doit s'assurer de retourner le matériel précis, dans la bonne quantité et avec les numéros de série exacts (le cas échéant), tel qu'approuvé par

Genetec Inc. et inscrit sur le formulaire de RMA fourni. Tout inventaire non approuvé, mal étiqueté ou excédentaire renvoyé à Genetec Inc. sera refusé et retourné à l'expéditeur.

Conditionnement

Le client est responsable du bon emballage des produits retournés. Tout dommage subi pendant le transport en raison d'un emballage inadéquat ne sera pas couvert par la garantie matérielle de Genetec. Le client est responsable de tout dommage subi pendant le transport. En cas de manquement à ces obligations, Genetec Inc. annulera l'autorisation de retour RMA et pourra facturer les frais de réparation ou de remplacement.

Expédition

Tous les frais encourus pour le retour de l'unité incombent au client. À moins que l'autorisation de retour RMA soit annulée, tous les frais encourus pour renvoyer les produits réparés ou les unités de remplacement au client sont pris en charge par Genetec Inc.

Si Genetec Inc. expédie par erreur des produits non achetés ou en surnombre au client, Genetec Inc. couvrira les frais de retour des produits en fournissant au client des étiquettes d'expédition et des documents d'exportation, si nécessaire. Dans le cas contraire, une facture sera envoyée au client pour les produits.

Dans certaines conditions, Genetec Inc. acceptera le retour d'articles non endommagés et émettra un avoir. Pour être éligible pour un retour avec avoir, l'article doit être inutilisé et dans l'état d'origine. Il doit également être dans son emballage d'origine. L'article doit être renvoyé sous 30 jours à compter de la date d'expédition de l'article au client ou au cours de la période autorisée par le revendeur Genetec Inc., selon ce qui est le plus court.

Pour tout retour avec avoir, Genetec Inc. émettra un avoir une fois que les produits auront été reçus et inspectés et jugés comme étant dans leur état d'origine. L'avoir sera émis pour le montant d'origine, moins les frais de réapprovisionnement applicables conformément à l'Annexe A. Genetec Inc. se réserve le droit de refuser tout retour avec avoir. En outre, Genetec Inc. se réserve le droit de modifier les frais de réapprovisionnement dans des circonstances inhabituelles, à sa seule discrétion.

Les articles vendus en vertu d'une politique NCNR (non résiliable et non remboursable) ne sont pas éligibles pour un retour avec avoir.

Dommmages durant le transport

Les produits doivent être inspectés à réception. Tout dommage résultant de l'expédition doit être signalé à Genetec Inc. sous 14 jours suivant la réception du produit. En cas de non-signallement des dommages sous 14 jours suivant la réception, Genetec Inc. se réserve le droit de refuser un retour avec avoir ou le remplacement des produits endommagés. En cas de produits endommagés lors de l'expédition, contactez CustomerService@genetec.com par e-mail. Décrivez les dommages, et joignez si possible des photos.

Responsabilités et attentes

- Un RMA est valable 30 jours. Les articles doivent être renvoyés durant cette période et être identifiés avec les numéros de RMA correspondants.
- Pour les retours pour lesquels le client a choisi de contourner le centre d'assistance technique de Genetec (GTAC), des frais d'inspection seront appliqués si aucun défaut n'est constaté sur les unités retournées, conformément à l'Annexe A.
- Les unités expédiées au client dans le cadre de la garantie de remplacement anticipé seront facturées au client immédiatement et le montant sera crédité si les unités endommagées sont retournées sous 30 jours à compter de la date de création du numéro de RMA.
- Il incombe au client de retourner les unités en bon état, et conformément aux instructions fournies dans ce document. Le manquement à ces obligations par le client pourra entraîner des frais supplémentaires pour le client ou l'annulation de la demande de RMA par Genetec Inc.
- S'il est estimé qu'une unité de remplacement anticipé a été malmenée, mal utilisée ou utilisée à des fins non prévues, le client pourra se voir facturer le prix total de l'unité de remplacement dans le cadre de la garantie de remplacement anticipé.
- Les retours et réparations hors garantie sont facturés conformément à l'Annexe A.

Instructions de retour

1. Réunissez les informations suivantes avant de contacter Genetec Inc. pour une demande de RMA :
 - Nom de la société (intégrateur) ayant passé la commande.
 - Numéro de commande du client pour l'unité concernée par la demande de RMA.
 - Coordonnées valables (nom, adresse e-mail, numéro de téléphone) pour toute correspondance future.
 - La référence de l'unité qui nécessite une réparation, un remplacement ou un avoir.
 - Le numéro de série de l'unité concernée par le numéro de RMA, le cas échéant.
 - L'ID système, si disponible.
 - Motif du retour
 - Description la plus détaillée possible du problème matériel, le cas échéant.
2. Contactez Genetec Inc. pour demander un numéro de RMA.

Demandes de RMA pour retour et réparation

1. Contactez le centre d'assistance technique de Genetec (GTAC) pour nous informer du problème et demander un numéro de RMA.

Pour les clients ayant opté pour la couverture Genetec Advantage, une assistance technique en direct est disponible durant les heures de bureau par téléphone et par chat sur le [portail d'assistance technique de Genetec \(GTAP\)](#). Pour les clients qui n'ont pas souscrit une couverture Advantage, un dossier doit être ouvert sur le GTAP. Lorsque vous ouvrez un dossier, indiquez **Demande de RMA** dans l'objet afin que notre équipe puisse facilement identifier la nature de votre demande. 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*.

2. Le service clientèle Genetec fournit un formulaire RMA au client.

Ce formulaire est obligatoire pour pouvoir retourner l'unité. Le client reçoit le formulaire par e-mail sous 24 heures après notification du GTAC et traitement par le service clientèle. Ce formulaire RMA fournit au client l'adresse de retour complète de Genetec Inc. ou du revendeur, ainsi que le numéro de RMA de Genetec Inc. ou du revendeur.

Demandes de retour avec avoir

1. Contactez le service clientèle Genetec pour nous informer du motif du retour. La demande peut être envoyée par e-mail à l'adresse customerservice@genetec.com ou effectuée par téléphone. Pour obtenir le numéro de téléphone et les horaires du service clientèle dans votre région, consultez la page *Nous contacter* du [site Web de Genetec Inc.](#)
2. Le service clientèle Genetec fournit un formulaire RMA au client.

Ce formulaire est obligatoire pour pouvoir retourner l'unité. Le client reçoit le formulaire par e-mail sous 24 heures après notification du service clientèle Genetec. Ce formulaire RMA fournit au client l'adresse de retour complète ainsi que le numéro de RMA de Genetec Inc. ou du revendeur.

3. Le client retourne l'unité à Genetec Inc. ou au revendeur.
 - a. Le client prend à sa charge tous les frais d'expédition liés au retour du produit à Genetec Inc. ou au revendeur concerné.
 - b. Le client doit imprimer le formulaire RMA (envoyé par e-mail par Genetec Inc. au client) et l'inclure dans le colis avec l'unité, afin que Genetec Inc. ou ses revendeurs puissent identifier le colis.
 - c. Le numéro de RMA doit être visible sur le colis. Genetec Inc. fournit ce numéro au client sur le formulaire RMA.
 - d. Le client ne doit expédier que les produits pour lesquels le RMA a été demandé. Expédiez le colis à l'adresse complète indiquée sur le formulaire RMA.
 - e. Genetec Inc. ou le revendeur doit recevoir l'unité retournée sous 30 jours à compter de l'émission du numéro de RMA. Passé ce délai de 30 jours, tout RMA pour les services « Retour avec avoir » ou « Retour et réparation » sera annulé.
 - f. Pour les services « Remplacement anticipé », Genetec Inc. envoie l'unité de remplacement à la création du numéro de RMA ou lorsque la pièce est disponible.
REMARQUE : Si l'unité endommagée est retournée sous 30 jours à compter de la création du numéro de RMA, les unités expédiées au client dans le cadre de la garantie de remplacement anticipé sont facturées au client immédiatement et le montant est crédité.
 - g. Le client doit envoyer le numéro de suivi du colis au Service clientèle de Genetec Inc.
4. Genetec Inc. reçoit et inspecte les articles retournés.
 - a. La référence et le numéro de série (le cas échéant) de l'unité retournée doivent correspondre aux informations fournies à Genetec Inc. par le client lors de la création de la demande de RMA. En cas de différence, le service clientèle Genetec contacte le client. La demande de RMA n'est pas traitée tant que le client n'a pas été contacté, car la garantie peut varier en fonction du numéro de série et de la référence.
 - b. **Retour avec avoir :** Si elle n'est pas endommagée, l'unité est traitée comme un « retour avec avoir ». Un avoir n'est accordé qu'une fois que l'unité a été reçue et inspectée. Si l'emballage est endommagé ou altéré de quelque façon que ce soit, Genetec Inc. se réserve le droit de refuser l'avoir. Des frais de réapprovisionnement sont facturés pour un « retour avec avoir » conformément à l'Annexe A.
 - c. **Retour pour réparation :** Si l'unité est sous garantie et que les dommages ne sont pas considérés comme étant le résultat d'une mauvaise utilisation ou manipulation par le client, Genetec Inc. ou le revendeur procède à la réparation. L'unité réparée est ensuite réexpédiée au client. Dans les situations où la réparation n'est pas possible, le produit peut être remplacé par un produit entièrement fonctionnel (reconditionné ou neuf, selon la disponibilité). Les délais de réparation varient en fonction de la gamme de produits, du type de produit ou du fabricant. Si le produit n'est pas sous garantie ou en cas d'annulation du RMA, Genetec Inc. détermine si l'article est réparable. Si c'est le cas, des frais de réparation s'appliquent conformément à l'Annexe A.
 - d. **Remplacement anticipé :** Si l'unité retournée est couverte par une garantie de remplacement anticipé et que les dommages ne sont pas considérés comme étant le résultat d'une mauvaise utilisation ou manipulation par le client, aucuns frais ne sont imputés au client pour l'unité de remplacement fournie par Genetec Inc.
5. Genetec Inc. traite le RMA et renvoie l'unité, le cas échéant.
 Genetec Inc. s'acquitte de tous les frais d'expédition et droits de douane (le cas échéant) pour renvoyer l'unité au client.
 Le numéro de suivi est communiqué au client par e-mail dès que l'article est expédié.

Annexe A

Gamme de produits	Frais de réapprovisionnement	Frais de réparation ³	Frais d'inspection
Streamvault	Les frais sont déterminés au cas par cas et communiqués au client.	Les frais sont déterminés au cas par cas et communiqués au client.	Non applicable

³Si l'unité n'est pas réparable, le client est invité à décider s'il souhaite remplacer l'unité.

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 de surveillance Matériel Streamvault^{MC}. Un seul Gestionnaire Streamvault^{MC} est autorisé par système.

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}.

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. Pour accéder au TechDoc Hub, connectez-vous au [Portail Genetec](#) et cliquez sur [TechDoc Hub](#). Vous ne trouvez pas ce que vous cherchez ? Contactez 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.