Guide d'installation et de mise à niveau

Security Center 5.5 SR4

Cliquez ici pour obtenir la dernière version de ce document.

Avis de copyright

Informations sur le document

Titre du document : Guide d'installation et de mise à niveau Security Center 5.5 SR4

Numéro de document original : EN.500.002-V5.5.C4(2)

Numéro de document : FR.500.002-V5.5.C4(2)

Date de mise à jour du document : 23 janvier 2017

Envoyez vos commentaires, corrections et suggestions concernant ce guide à documentation@genetec.com.

À propos de ce guide

Ce guide décrit la marche à suivre pour installer et mettre à niveau les composants de 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.
- **Remarque**. 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 : Les sujets abordés dans ce guide peuvent faire référence à des informations publiées sur des sites web de tiers qui étaient correctes au moment de leur publication, mais qui peuvent changer sans que Genetec n'en soit notifié au préalable.

Table des matières

1

Installation de Security Center

Cette section aborde les sujets suivants:

Préparer l'installation Security Center

Pour une installation de Security Center sans incident, vous devez effectuer une série de tâches de préconfiguration.

Avant d'installer Security Center :

1 Lisez les *Notes de version Security Center* pour en savoir plus sur d'éventuels problèmes connus, les chemins de mise à niveau pris en charge et d'autres informations. Cliquez ici pour obtenir la dernière version de ce document.

2 Consultez votre configuration système pour vérifier la compatibilité de la configuration matérielle (serveurs et postes de travail) et logicielle (Windows, navigateur web, etc.).

3 Installez les derniers pilotes graphiques et réseau sur les serveurs et postes de travail.

4 Vérifiez que les serveurs ne sont pas des contrôleurs de domaine.

5 Désactivez les options d'économie d'énergie sur tous les serveurs.

6 Vérifiez que Windows Update n'est pas configuré pour redémarrer automatiquement vos serveurs après l'installation de mises à jour.

7 Si vous utilisez Windows 7, Windows 8, Windows 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 ou Windows Server 2012 R2, vous devez installer Microsoft hotfix KB2999226.

8 Sur chaque serveur, dans la liste *Cartes et liaisons* qui classe les connexions dans l'ordre d'accès par les services réseau, vérifiez que les cartes réseau qui doivent être utilisées par Security Center sont situées en haut de la liste.

9 Vérifiez les connexions réseau entre vos serveurs, postes de travail et unités.

10 Vérifiez les connexions réseau et réglages de mono et multidiffusion.

11 Prenez connaissance des prérequis pour l'installation de Security Center Client et Server disponibles sur le site d'information technique Genetec[MC].

Security Center Le programme d'installation vérifie et installe automatiquement les prérequis logiciels, mais il est recommandé de savoir ce qu'il va se passer.

12 Si vous faites une mise à niveau :

a) Prenez connaissance de la Configuration requise pour la rétrocompatibilité de Security Center.

b) Vérifiez que le chemin de mise à niveau ou de migration est pris en charge.

Pour en savoir plus, voir les *Notes de version Security Center*.

c) Sauvegardez les bases de données du Répertoire et des autres rôles.

Pour en savoir plus, consultez le *Guide de l'administrateur Security Center* de la version de votre système.

13 Munissez-vous de votre ID et mot de passe système pour activer votre licence sur le serveur principal.

Votre ID système et mot de passe sont disponibles dans le document *Informations de licence Security Center*. L'assistance technique de Genetec vous envoie ce document à l'achat du produit.

14 Vérifiez que vous avez les privilèges d'administrateur. Dans le cas contraire, le fichier d'installation *setup.exe* doit être exécuté en tant qu'administrateur.

Dans certains cas, vous devez être un administrateur de domaine Microsoft Windows pour accéder aux bases de données et au stockage des ordinateurs. Contactez votre administrateur informatique.

15 (Pour le basculement du Répertoire ou le fonctionnement de VSS) Installez SQL Server sur un lecteur distinct.

16 Accordez les autorisations SQL Server nécessaires à tous les utilisateurs des services.

17 Fermez Internet Explorer.

18 (Windows 7 seulement) Activez .NET Framework 3.5.1.

Sous Windows 8 et Windows 2012, la fonctionnalité .NET Framework est automatiquement activée par l'Assistant InstallShield si vous êtes connecté à Internet.

19 (Windows 2012 seulement) Activez la fonctionnalité Media Foundation.

20 Ouvrez le pack d'installation Security Center

21 Débloquez tout fichier bloqué.

Après le téléchargement du pack d'installation Security Center, les fichiers ZIP devront parfois être débloqués avant de pouvoir extraire leur contenu.

Lorsque vous avez terminé

Installez Security Center.

Activer .NET Framework 3.5.1

Si vous souhaitez installer Security Center sur un ordinateur équipé de Windows 7, vous devez activer manuellement .NET Framework 3.5.1.

À savoir

Sous Windows 8 et Windows 2012, la fonctionnalité .NET Framework est automatiquement activée par l'Assistant InstallShield si vous êtes connecté à Internet.

Pour activer .NET Framework 3.5.1 :

1 Sélectionnez **Démarrer** > **Panneau de configuration** > **Programmes et fonctionnalités**.
2 Dans la boîte de dialogue *Programmes et fonctionnalités*, cliquez sur **Activer ou désactiver des fonctionnalités Windows**.
3 Dans la boîte de dialogue *Fonctionnalités Windows*, sélectionnez l'option **Microsoft .NET Framework 3.5.1** et cliquez sur **OK**.

Activer la fonctionnalité Media Foundation

Si vous souhaitez installer Security Center sur un ordinateur équipé de Windows 2012, vous devez activer manuellement la fonctionnalité Media Foundation.

Pour activer la fonctionnalité Media Foundation :

1 Ouvrez *Gestionnaire de serveur* et cliquez sur **Ajouter des rôles et fonctionnalités**.
2 Sur la page **Avant de commencer**, cliquez sur **Suivant**.
3 Sélectionnez le type d'installation **Installation basée sur un rôle ou une fonctionnalité**, et cliquez sur **Suivant**.
4 Sélectionnez le serveur concerné, et cliquez sur **Suivant**.
5 Sur la page *Sélectionnez des rôles de serveurs*, cliquez sur **Suivant**.
6 Sur la page *Sélectionner les fonctionnalités*, sélectionnez **Media Foundation** et cliquez sur **Suivant** > **Installer**.
7 Sélectionnez l'option **Redémarrer automatiquement le serveur de destination, si nécessaire** pour que le serveur redémarre et applique les modifications une fois l'installation terminée.

Security Center 5.5 configuration système requise

La configuration requise englobe les composants matériels et logiciels recommandés, nécessaires pour que votre produit et votre système fonctionnent de manière optimale.

Pour connaître la dernière Security Center 5.5 configuration système requise, cliquez ici.

Installer SQL Server sur un disque distinct

Selon vos exigences de déploiement, vous pouvez devoir installer SQL Server sur un lecteur qui est distinct du lecteur système (en général le lecteur C:). Vous devez effectuer cette procédure avant d'installer les composants de Security Center.

Avant de commencer

Si vous installez l'édition SQL Server Standard ou Enterprise, vous devez l'acheter auprès de Microsoft, puis télécharger le programme d'installation.

À savoir

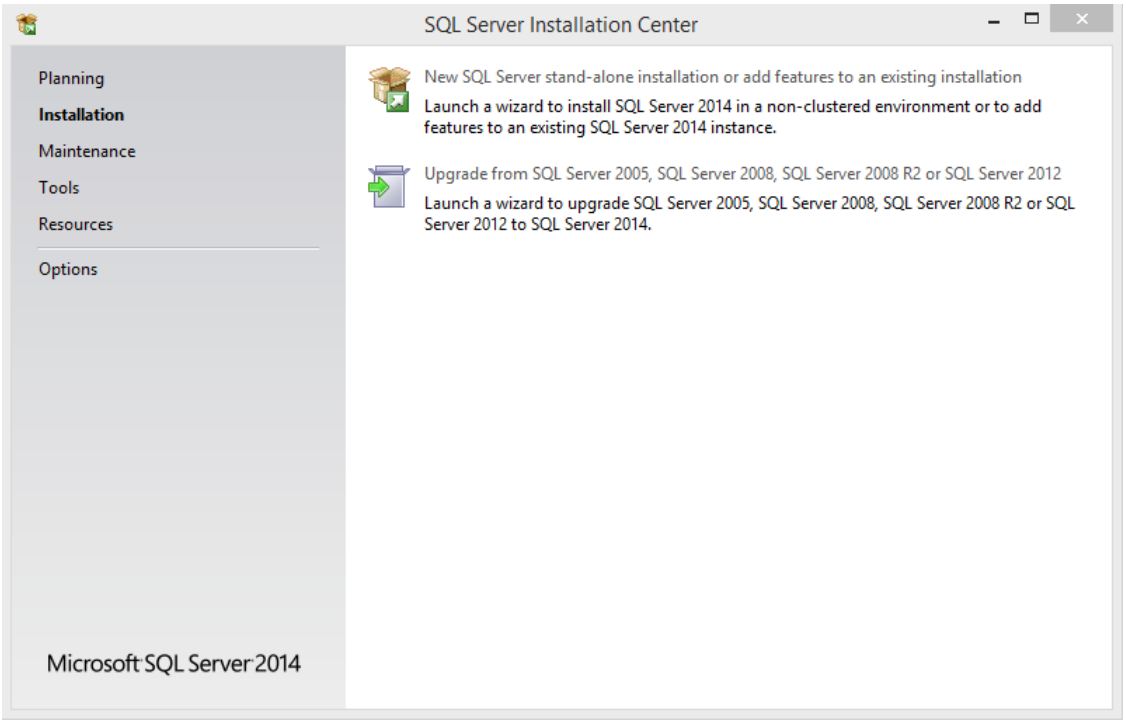
Vous devez Installer SQL Server sur un disque distinct dans les situations suivantes :

- Vous comptez configurer le basculement et l'équilibrage de charge du Répertoire. Dans ce cas, installez SQL Server sur un serveur différent de tous vos serveurs de Répertoire. Pour en savoir plus, voir le *Security Center Guide de l'administrateur*.
- Microsoft Volume Shadow Copy Service (VSS) est activé sur votre serveur. Dans ce cas, installez SQL Server sur un lecteur distinct du lecteur système et veillez à ce que VSS ne prenne que des instantanés du lecteur système.

  ATTENTION : Ne pas désactiver VSS. Le fait de désactiver VSS interfère avec le fonctionnement de la restauration du système sous Windows.

Pour installer SQL Server sur un disque distinct :

1. Procédez de l'une des manières suivantes :
   - Si vous installez SQL Server Standard ou Enterprise :
     1. Sous Windows, naviguez jusqu'au dossier du pack d'installation de SQL.
     2. Cliquez deux fois sur Setup.exe.
   - Si vous installez SQL Server Express :
     1. Sous Windows, naviguez jusqu'au dossier du pack d'installation de Security Center.
     2. Allez dans **SC Packages** > **SQLExpress**.
     3. Cliquez deux fois sur l'un des fichiers suivants :
        - Si vous utilisez un ordinateur 64 bits : *SQLEXRWT_x64_ENU.exe*.
        - Si vous utilisez un ordinateur 32 bits : *SQLEXRWT_x86_ENU.exe*.
2. Dans le *Centre d'installation de SQL Server*, cliquez sur **Nouvelle installation ou ajout de fonctionnalités à une installation existante**.
3. Sur la page *Types d'installation*, sélectionnez **Nouvelle installation ou ajout de fonctionnalités partagées**, puis cliquez sur **Suivant**.



4 Lisez le contrat de licence logicielle, sélectionnez **J'accepte les termes du contrat de licence**, puis cliquez sur **Suivant**.

5 Sur la page *Sélection de composant*, sélectionnez les fonctionnalités que vous souhaitez installer.

6 Dans le champ **Répertoire des fonctionnalités partagées**, sélectionnez l'emplacement où vous souhaitez installer les fonctionnalités partagées SQL Server.

7 Cliquez sur **Suivant**.

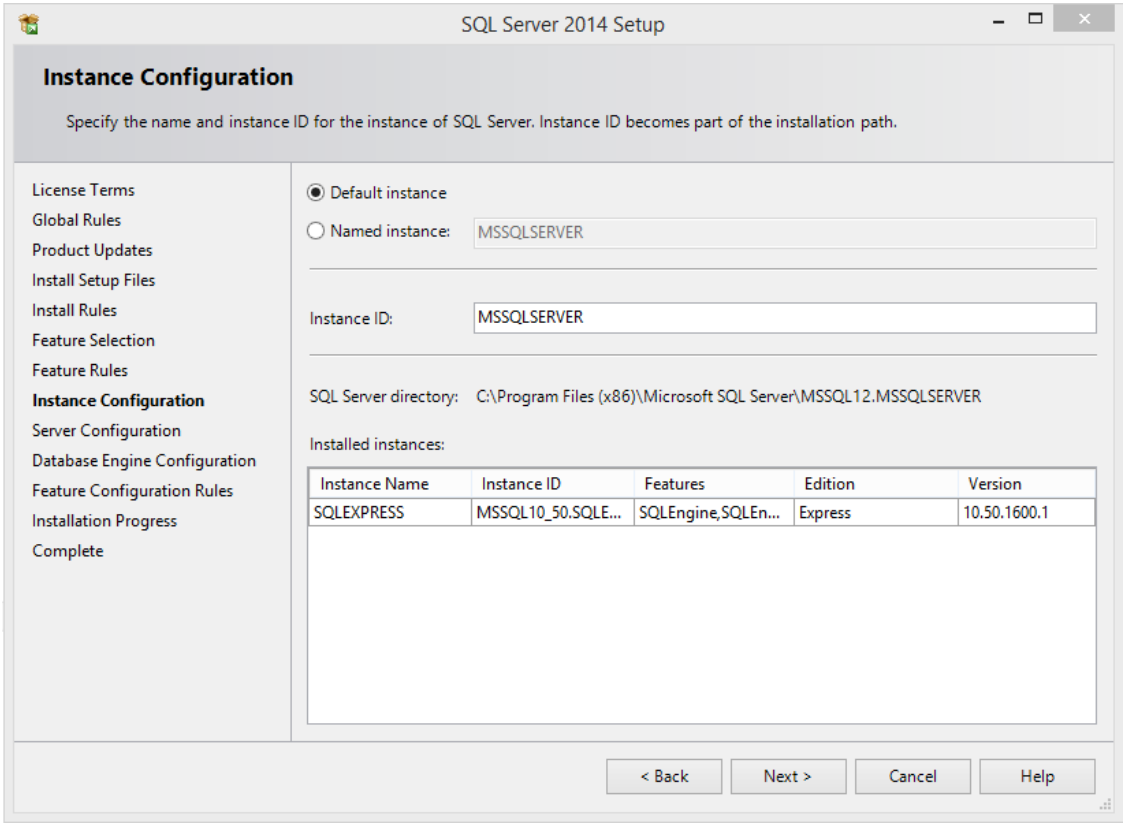
8 Sur la page *Configuration de l'instance*, donnez un nom à l'instance de SQL Server.

REMARQUE : Le nom du serveur de base de données ne distingue pas les majuscules des minuscules, mais doit suivre les règles suivantes :

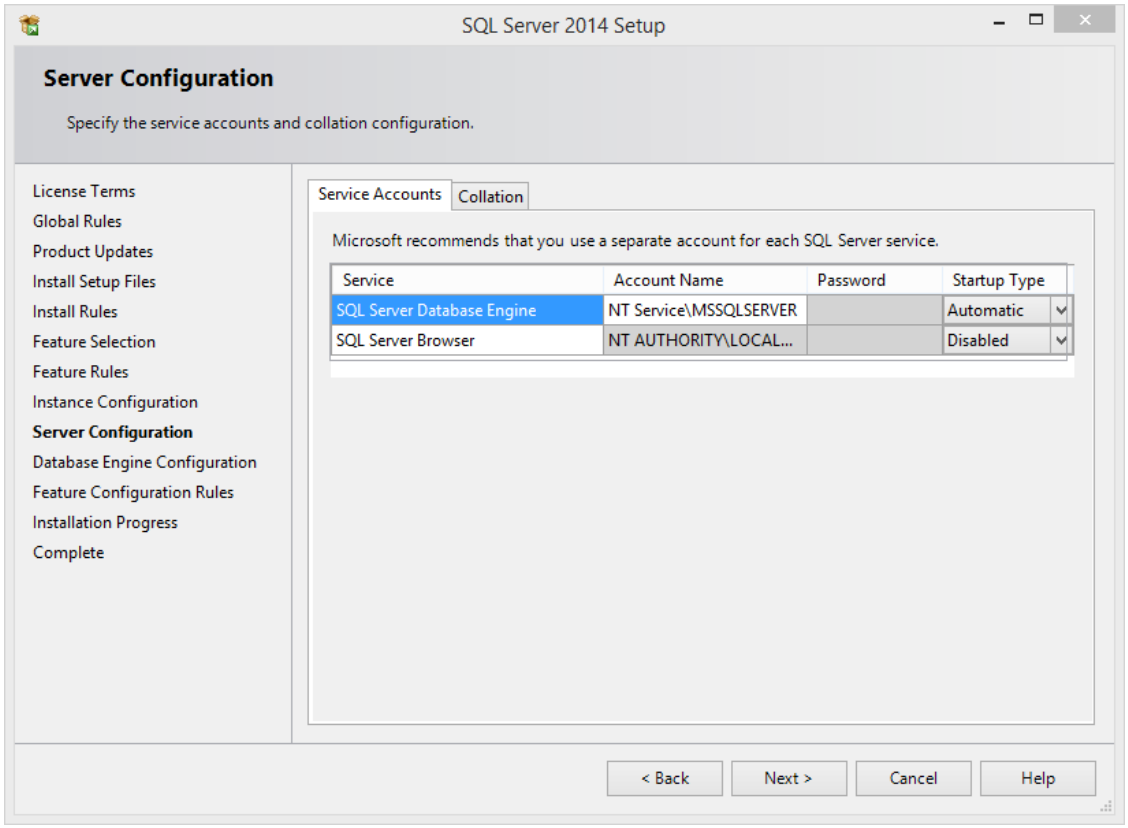
- Il ne peut pas utiliser un mot clé réservé de SQL Server, comme DEFAULT, PRIMARY, etc. Pour une liste complète des mots clés réservés, voir https://msdn.microsoft.com/en-us/library/ms189822.aspx.
- Il ne doit pas faire plus de 16 caractères.
- La première lettre du nom de l'instance doit être une lettre ou le signe souligné (_). Les lettres acceptables, définies par la norme Unicode Standard 2.0, incluent les caractères latins a-z et A-Z, et certains caractères d'autres alphabets.
- Les caractères suivants peuvent être des lettres définies par la norme Unicode Standard 2.0, des chiffres décimaux (scripts latins ou autres), le signe dollar ($) ou souligné (_).
- Les espaces et d'autres caractères spéciaux sont interdits, dont les suivants :barre oblique inverse (\), virgule (,), deux-points (:), point-virgule (;), guillemet simple ('), esperluette (&), dièse (#) et arobase (@).

9 Dans le champ **Répertoire racine de l'instance**, indiquez l'emplacement d'installation de SQL Server et de tous les fichiers de base de données du Répertoire, puis cliquez sur **Suivant**.

Vous pouvez saisir le chemin ou naviguer jusqu'au dossier.

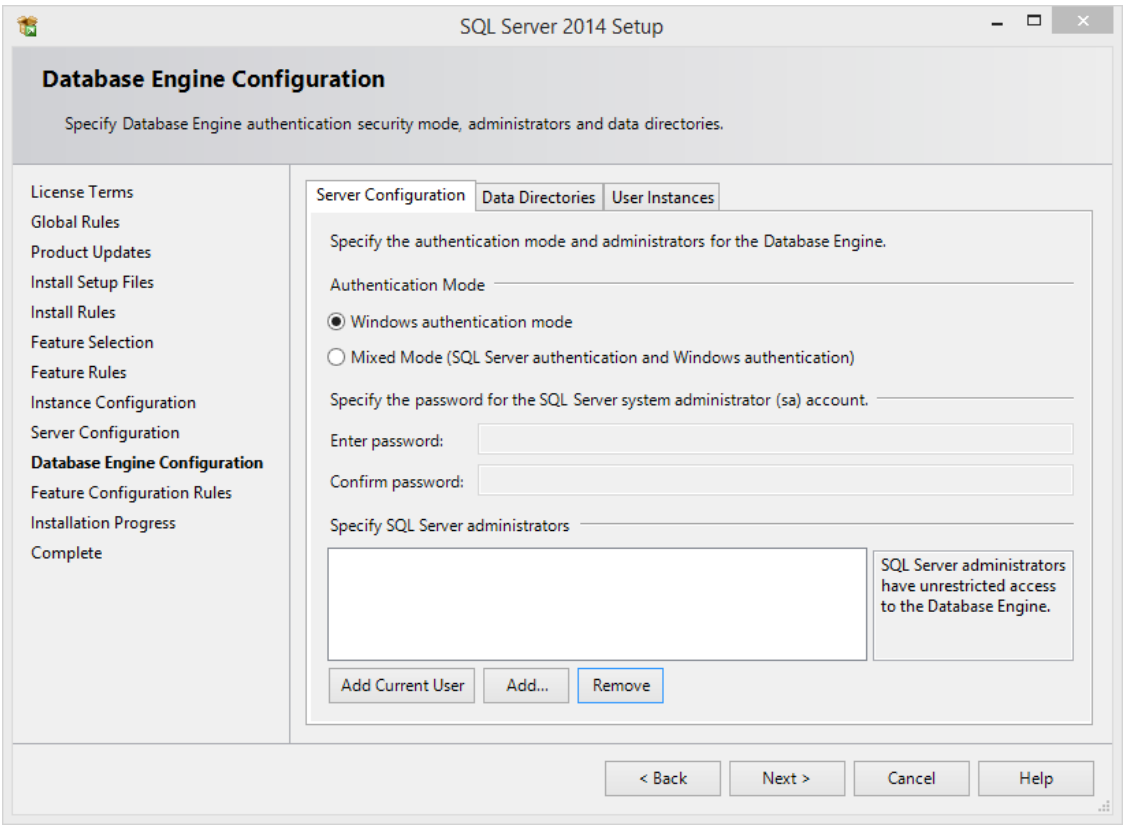


10 Sur la page *Configuration du serveur*, sélectionnez le nom de compte pour chaque service SQL Server, puis cliquez sur **Suivant**.



11 Sur la page *Configuration du moteur de base de données*, sélectionnez le mode d'authentification permettant d'accéder au moteur de base de données, puis cliquez sur **Suivant**.

- **Mode d'authentification Windows:** Nom d'utilisateur et mot de passe Windows.
- **Mixed mode:** Les administrateurs Windows peuvent accéder au moteur de base de données avec leurs identifiants Windows ou avec le mot de passe que vous spécifiez ici.



12 Sur la page *Rapport d'erreurs*, indiquez si vous voulez transmettre les erreurs éventuelles à Microsoft, puis cliquez sur **Suivant**.

13 Patientez jusqu'à la fin de l'installation. Cela peut prendre plusieurs minutes.

14 Cliquez sur **Fermer**.

L'instance de SQL Server peut désormais servir de serveur de base de données Security Center.

Lorsque vous avez terminé

Installez Security Center sur le serveur principal, et utilisez le nouveau SQL Server en tant que serveur de base de données.

Rubriques connexes

Préparer une installation silencieuse, page 97

Accorder les autorisations SQL Server

Pour que le rôle Répertoire puisse fonctionner, les utilisateurs de services qui ne sont pas administrateur Windows (nom de connexion SYSADMIN) doivent recevoir l'autorisation SQL *Afficher l'état du serveur*.

À savoir

Le rôle serveur SQL minimum pris en charge par Security Center est *dbcreator*, et le rôle base de données SQL minimum est *db_owner*. Par conséquent, vous devez vérifier que les membres du rôle serveur *dbcreator* et que les membres du rôle base de données *db_owner* disposent de l'autorisation *Afficher l'état du serveur*.

Pour en savoir plus sur les rôles serveur et leurs caractéristiques, consultez votre documentation Microsoft.

REMARQUE : La procédure suivante s'applique à SQL Server 2014 Express. Si vous utilisez une autre version de SQL Server, consultez la documentation de Microsoft pour savoir comment accorder les autorisations.

Pour accorder les autorisations SQL Server :

- Dans SQL Server Management Studio, procédez de l'une des manières suivantes :
  - Exécutez la requête suivante : `GRANT VIEW SERVER STATE TO [nom de connexion]`.
  - Modifiez les autorisations utilisateur manuellement de la manière suivante :
    1. Faites un clic droit sur l'instance de SQL server concernée et sélectionnez **Propriétés**.
    2. Cliquez sur la page *Autorisations*.
    3. Sous **Connexions ou rôles**, sélectionnez l'utilisateur ou le rôle que vous souhaitez modifier.
    4. Dans la section **Autorisations**, cliquez sur l'onglet **Explicite** et cochez la case **Accorder** en regard de l'autorisation **Afficher l'état du serveur**.
    5. Cliquez sur **OK**.

Lorsque vous avez terminé

Les utilisateurs qui disposent de cette autorisation en local sur le serveur Genetec doivent être ajoutés en tant qu'utilisateurs de SQL Server.

Security Center Packs d'installation

Les packs d'installation de Security Center contiennent le programme d'installation du produit qui permet d'installer tout le nécessaire pour qu'il soit opérationnel.

Packs téléchargeables

Les packs d'installation de Security Center sont des fichiers zip que vous pouvez télécharger depuis la page *Téléchargements de produits* de GTAP à l'adresse https://gtap.genetec.com/SystemManagement/DownloadSection/. Vous devez disposer d'un nom d'utilisateur et d'un mot de passe pour vous connecter à GTAP.

- **SecurityCenterWebSetup.exe:** Le programme d'installation web. Pendant l'installation, le programme d'installation web télécharge les composants nécessaires pour votre poste depuis Internet.
- **Pack d'installation complet:** Téléchargez le pack d'installation complet si vos ordinateurs n'ont pas accès à Internet. Il s'agit d'un pack autonome. Il ne fait pas appel à des éléments extérieurs.

  Le pack d'installation complet contient les éléments suivants :

  - **setup.exe:** Situé dans le dossier racine, il s'agit de la version du programme d'installation autonome qui s'exécute automatiquement.
  - **Security Center Setup.exe:** Situé dans le dossier *SC Packages*, il s'agit du programme d'installation autonome.
  - **SC Packages:** Ce dossier contient tous les composants (dans des sous-dossiers distincts) dont vous pouvez avoir besoin pour votre installation Security Center. Tous les prérequis pour l'installation de Security Center s'y trouvent.
  - **Documentation:** Ce dossier contient les versions PDF du *Guide d'installation et de mise à niveau de Security Center* ainsi que les *notes de version*.

Modes d'installation

Il existe deux modes d'installation de Security Center :

- **Mode assistant:** Le programme d'installation Assistant InstallShield pour Security Center offre une interface conviviale qui vous guide étape par étape par l'intermédiaire d'une série de questions, puis qui exécute le programme d'installation avec les options choisies. Il existe deux versions du programme d'installation :
  - **Version web:** Exécutez la version web du programme d'installation si votre poste est connecté à Internet. Pour lancer le programme d'installation web, téléchargez le fichier *SecurityCenterWebSetup.exe* sur GTAP, puis cliquez deux fois sur celui-ci. Le programme d'installation web se connecte au site de Genetec et ne télécharge que les modules que vous décidez d'installer.
  - **Version autonome:** Exécutez la version autonome du programme d'installation si votre poste n'est pas connecté à Internet. Pour lancer le programme d'installation autonome, téléchargez le pack d'installation complet sur GTAP, puis cliquez deux fois sur le fichier *setup.exe* situé à la racine du pack.
- **Mode silencieux:** Le mode silencieux sert à exécuter le programme d'installation à l'invite de commande, sans intervention de l'utilisateur. Pour en savoir plus, voir Installation silencieuse de Security Center, page 96.

IMPORTANT : L'installateur de Security Center ne prend pas en charge l'utilisation de lecteurs mappés dans la spécification du chemin.

Langues d'installation

Le programme d'installation de Security Center est disponible en anglais et en français, mais le logiciel Security Center installé est disponible dans de nombreuses langues. La langue est sélectionnée sur l'écran de démarrage du programme d'installation de Security Center.

Installer Security Center

Lorsque vous êtes prêt à installer Security Center, vous devez effectuer les tâches suivantes.

Avant de commencer

- Lisez les *Notes de version Security Center* pour en savoir plus sur d'éventuels problèmes connus, les chemins de mise à niveau pris en charge et d'autres informations. Cliquez ici pour obtenir la dernière version de ce document.
- Créez une liste des ordinateurs qui formeront votre nouveau système, et définir les composants logiciels à installer sur chaque ordinateur :
  - Security Center Server (serveur principal ou d'extension)
  - Security Center Client (Config Tool, Security Desk ou les deux)
  - SQL Server (serveur de base de données dédié)

  Consultez votre configuration système pour vérifier la compatibilité de la configuration matérielle (serveurs et postes de travail) et logicielle (Windows, navigateur web, etc.).
- Complétez la liste de contrôle pré-installation.

À savoir

IMPORTANT :

- Si vous installez Security Center Server sur un ordinateur après avoir installé Client, utilisez toujours le pack Security Center téléchargé. L'utilisation de l'option *Modifier* dans *Programmes et fonctionnalités* n'installera pas le composant SQL Express nécessaire.
- L'installateur de Security Center ne prend pas en charge l'utilisation de lecteurs mappés dans la spécification du chemin.

Pour installer Security Center :

1 (Facultatif) Installer SQL Server sur un disque distinct de celui du SE.

SQL Server est généralement installé automatiquement avec Security Center. L'installation distincte de SQL Server dépend des exigences particulières de votre déploiement.

2 Installez les composants Security Center sur le serveur principal qui hébergera le rôle Directory.

3 Activez la licence du produit sur le serveur principal.

4 Vérifiez que tous les ports utilisés par Security Center sont ouverts et redirigés au niveau du routeur pour le pare-feu et la traduction d'adresses réseau.

Pour la liste des ports utilisés par défaut par Security Center, voir Ports utilisés par défaut par Security Center, page 44.

5 (Facultatif) Installez les composants Security Center sur les serveurs d'extension qui se connecteront au serveur principal, afin de renforcer la capacité de traitement de votre système Security Center.

6 Installez Security Center Client (Config Tool, Security Desk ou les deux).

7 Débloquez tout fichier bloqué.

Lorsque vous avez terminé

Complétez la liste de contrôle post-installation.

Débloquer des fichiers manuellement

Après le téléchargement d'un pack d'installation Security Center, vous devrez parfois débloquer certains fichiers.

À savoir

- Seules certaines versions de Windows Server exigent le déblocage des fichiers ZIP pour pouvoir extraire leur contenu. Le bouton **Débloquer** évoqué ci-dessous ne sera pas forcément présent.
- Les packs d'installation de Security Center sont des fichiers zip que vous pouvez télécharger depuis la page *Téléchargements de produits* de GTAP à l'adresse https://gtap.genetec.com/SystemManagement/DownloadSection/. Vous devez disposer d'un nom d'utilisateur et d'un mot de passe pour vous connecter à GTAP.

Pour débloquer les fichiers d'un pack d'installation Security Center :

1 Faites un clic droit sur le fichier ZIP dans l'Explorateur Windows et sélectionnez **Propriétés**.
2 Dans l'onglet **Général**, cliquez sur **Débloquer**.
3 Cliquez sur **OK**.

Rubriques connexes

Dépannage : Des fichiers restent bloqués après un déblocage manuel, page 110

Installer Security Center sur le serveur principal

Le serveur principal est le seul serveur du système Security Center qui héberge le rôle Directory. Vous devez installer le serveur principal en premier, afin que les autres serveurs puissent s'y connecter. Vous devez également activer votre licence Security Center sur le serveur principal.

Avant de commencer

Préparez l'installation de Security Center.

IMPORTANT : Si vous n'êtes pas connecté à Windows en tant qu'administrateur, vous devez faire un clic droit sur le fichier exécutable, puis cliquer sur **Exécuter en tant qu'administrateur**.

À savoir

La procédure d'installation du serveur principal installe les éléments suivants :

- Le service Genetec Server *avec* le rôle Répertoire.

  Lorsque vous installez Genetec Server, la base de données du rôle Répertoire (facultativement SQL Express 2014), Server Admin et le service Watchdog sont également installés. Le logiciel installé s'occupe de la création ou de la mise à jour de toutes les bases de données du système. Vous ne devez que spécifier le nom de votre serveur de base de données. Si vous n'en avez pas, Microsoft SQL Server 2014 Express Edition est installé par défaut.
- (Facultatif) Applications client (Config Tool, Security Desk ou les deux).
- (Facultatif) Packs de compatibilité Omnicast pour visionner la vidéo provenant de systèmes Omnicast fédérés.

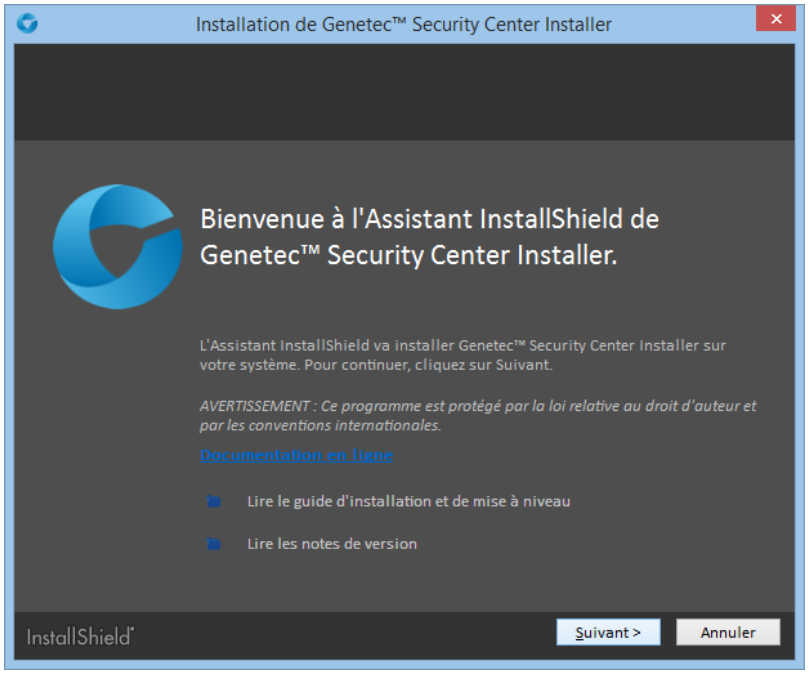
Pour installer Security Center sur le serveur principal :

1 Cliquez deux fois sur *setup.exe* (version autonome) ou sur *SecurityCenterWebSetup.exe* (version web) pour lancer le programme d'installation de Security Center.

REMARQUE : Seul l'Assistant InstallShield autonome est illustré dans cette procédure.

2 Sur la page *Setup Language* (Langue de l'installation), sélectionnez l'anglais ou le français, puis cliquez sur **Suivant**.

La fenêtre *Bienvenue à l'Assistant InstallShield* apparaît.

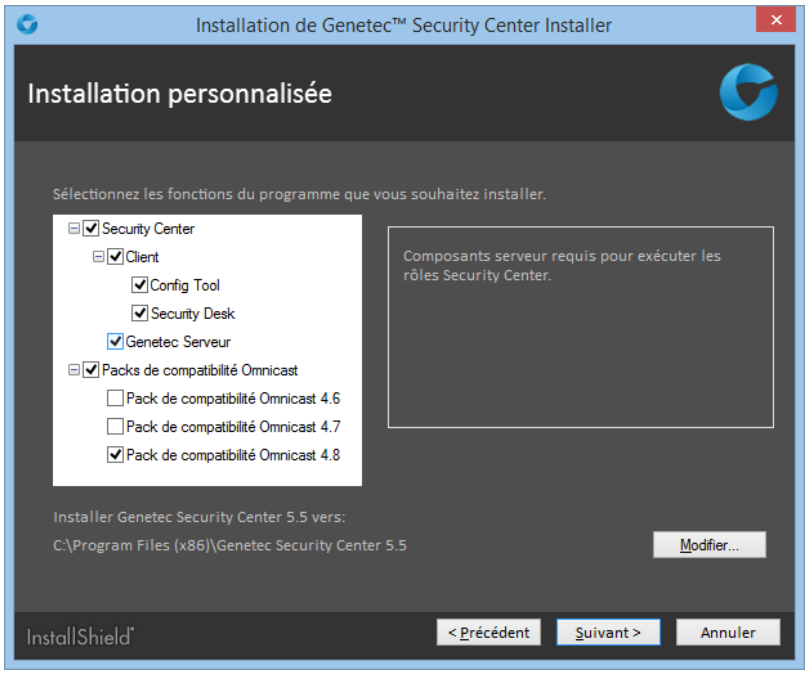


3 Sur la page de *Bienvenue*, cliquez sur **Suivant**.

Des liens sont fournis pour consulter la documentation Security Center pertinente en ligne ou au format PDF.

4 Sur la page *Contrat de licence*, lisez les conditions du *Contrat de licence logicielle Genetec*, sélectionnez **J'accepte les termes de ce contrat de licence**, et cliquez sur **Suivant**.

5 Sur la page *Installation personnalisée*, sélectionnez les applications Security Center à installer.



Vous disposez des options suivantes :

- **Serveur:** Installe le service Genetec Server, les bases de données SQL, Server Admin et le service Watchdog.
- **(Facultatif) Client:** Installe les applications Security Center client : Vous pouvez choisir Config Tool, Security Desk ou les deux.

- **(Facultatif) Packs de compatibilité Omnicast:** Si vous comptez fédérer les systèmes Omnicast, sélectionnez les packs de compatibilité Omnicast nécessaires.

6 Pour changer le dossier d'installation, cliquez sur **Modifier**, puis cliquez sur **Suivant**.

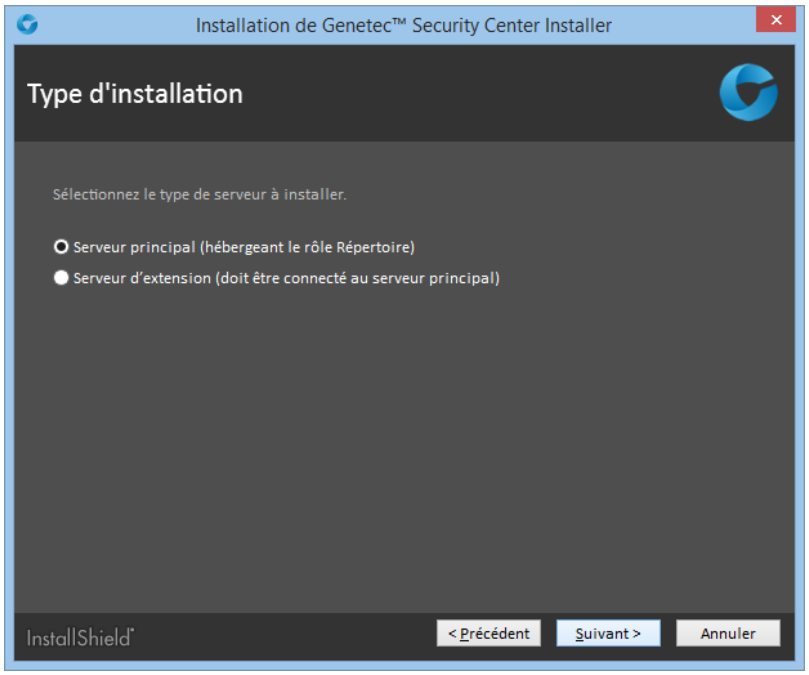
7 Sur la page *Sélection de la langue*, sélectionnez la langue de l'interface utilisateur des applications Security Center, et cliquez sur **Suivant**.

REMARQUE : L'aide en ligne des applications Security Center n'est pas disponible dans toutes les langues. Pour la liste des langues disponibles, voir les *Notes de version Security Center*.

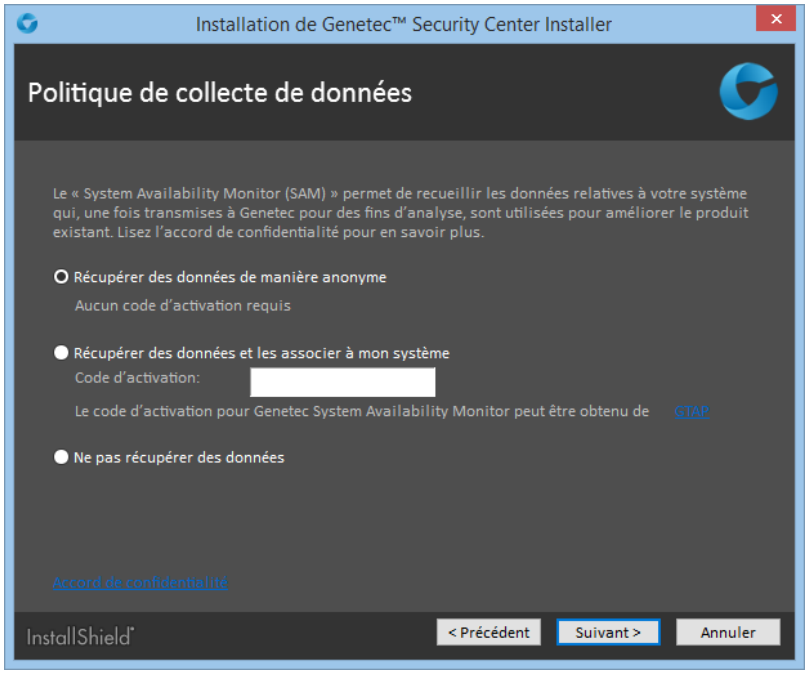
CONSEIL : Après l'installation, vous pouvez modifier la langue de l'interface à tout moment à l'aide de l'*outil langue* disponible dans le sous-dossier Outils du groupe de programmes Genetec Security Center.

8 Sur la page *Type d'installation*, sélectionnez l'option **Serveur principal**, et cliquez sur **Suivant**.

IMPORTANT : Vous ne devez utiliser le type d'installation **Serveur principal** qu'une fois par système. Si votre licence Security Center prend en charge des serveurs de Répertoire supplémentaires, tous les serveurs de Répertoire qui ne correspondent pas à votre serveur principal doivent être installés en tant que serveurs d'extension. Pour en savoir plus, voir le *Guide de l'administrateur Security Center*.



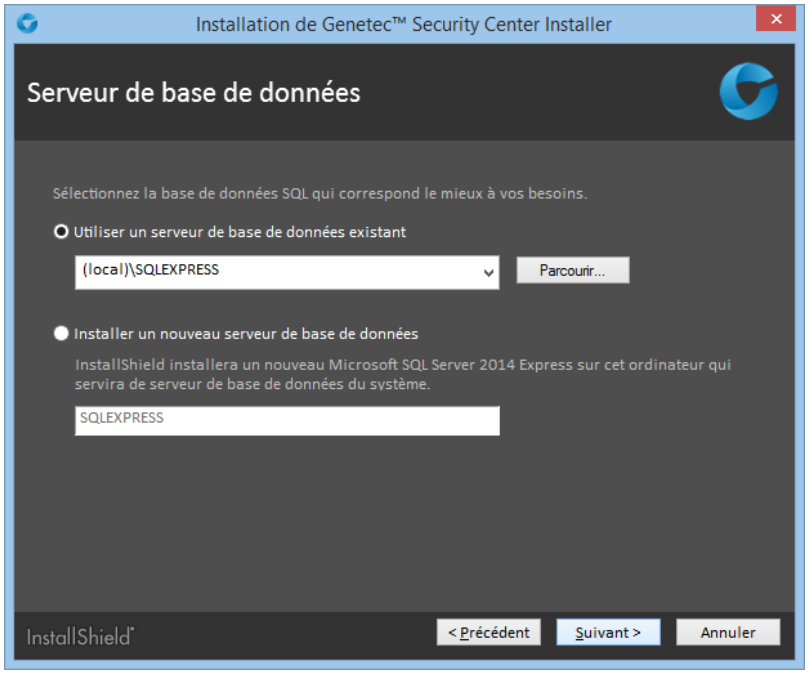
9 Sur la page *Politique de collecte de données*, sélectionnez l'une des options suivantes :



- **Récupérer des données de façon anonyme:** (Par défaut) 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 intraçables. Ces données ne sont utilisées que par Genetec à des fins statistiques, et ne sont pas accessibles via GTAP.
- **Récupérer des données et les associer à mon système:** Votre système doit être couvert par Genetec^{MC} Advantage, et un code d'activation est requis. Pour en savoir plus sur la création d'un code d'activation, voir le *Guide de l'utilisateur de System Availability Monitor*.
- **Ne pas récupérer de données:** Le System Availability Monitor Agent est installé mais ne recueillera pas de données.

a) (Facultatif) Cliquez sur **Voir l'accord de confidentialité** pour consulter la déclaration de confidentialité qui décrit les informations transmises à Genetec et la manière dont elles sont utilisées.
b) (Facultatif) Cliquez sur **Imprimer** pour imprimer l'accord de confidentialité.
c) Cliquez sur **OK**.

10 Sur la page *Serveur de base de données*, sélectionnez une des options suivantes :



- **Utiliser un serveur de base de données existant:** Sélectionnez une instance existante de Microsoft SQL Server qui hébergera la base de données.

  Une bonne pratique consiste à remplacer `(local)` par le nom de votre ordinateur. Vous devez indiquer explicitement le nom de l'ordinateur si vous configurez le Répertoire pour l'équilibrage de charge.

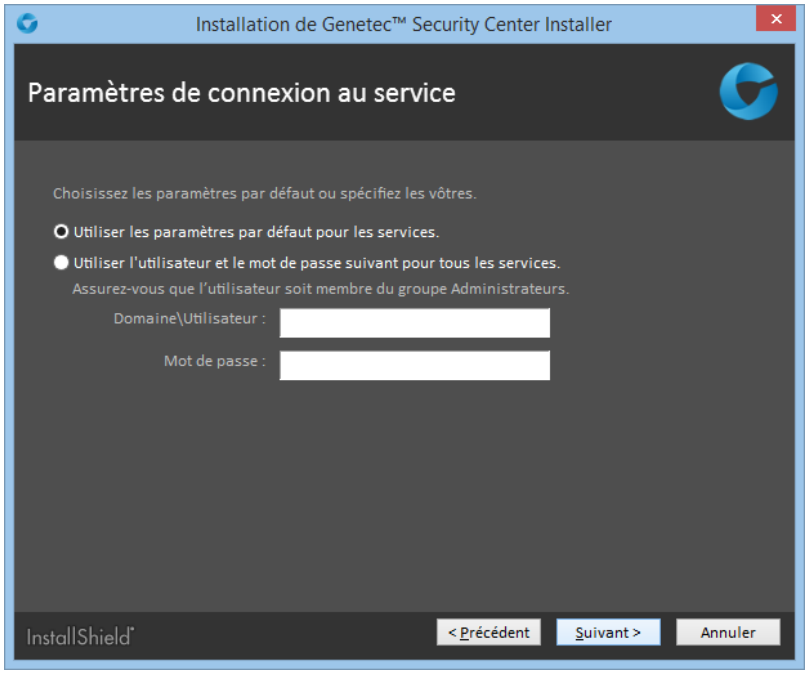
- **Installer un nouveau serveur de base de données:** Installe Microsoft SQL Server 2014 Express Edition. Vous devez choisir un nom de serveur de base de données. Le nom par défaut est SQLEXPRESS.

  REMARQUE : Le nom du serveur de base de données ne distingue pas les majuscules des minuscules, mais doit suivre les règles suivantes :

  - Il ne peut pas utiliser un mot clé réservé de SQL Server, comme DEFAULT, PRIMARY, etc. Pour une liste complète des mots clés réservés, voir https://msdn.microsoft.com/en-us/library/ms189822.aspx.
  - Il ne doit pas faire plus de 16 caractères.
  - La première lettre du nom de l'instance doit être une lettre ou le signe souligné (_). Les lettres acceptables, définies par la norme Unicode Standard 2.0, incluent les caractères latins a-z et A-Z, et certains caractères d'autres alphabets.
  - Les caractères suivants peuvent être des lettres définies par la norme Unicode Standard 2.0, des chiffres décimaux (scripts latins ou autres), le signe dollar ($) ou souligné (_).
  - Les espaces et d'autres caractères spéciaux sont interdits, dont les suivants :barre oblique inverse (\), virgule (,), deux-points (:), point-virgule (;), guillemet simple ('), esperluette (&), dièse (#) et arobase (@).

11 Cliquez sur **Suivant**.

12 Sur la page *Paramètres de connexion au service*, sélectionnez l'une des options suivantes :



- **Utiliser le nom et le mot de passe par défaut:** Utiliser le nom d'utilisateur par défaut (du système local) pour exécuter les services Security Center. Cette option fonctionne dans la plupart des cas.
- **Spécifier le nom d'utilisateur et le mot de passe pour tous les services.:** Entrez un nom d'utilisateur et mot de passe de domaine valables.

  IMPORTANT : Vérifiez que l'utilisateur du service appartient au groupe Administrateurs, dispose des droits sur la base de données locale ou distante et des droits d'utilisateur *Ouverture de session en tant que service*. Si ce serveur hébergera le rôle Active Directory, l'utilisateur concerné doit disposer d'un accès en lecture et en écriture à l'Active Directory auquel vous souhaitez connecter le serveur.

13 Cliquez sur **Suivant**.

14 Sur la page *Paramètres du serveur*, renseignez les champs suivants :

- **Port du serveur Web:** Le port HTTP utilisé pour l'administration sur le Web avec Server Admin. Si vous modifiez le port par défaut, vous devez inclure le port dans l'adresse de Server Admin (par

exemple *http://ordinateur:port/Genetec* au lieu de *http://ordinateur/Genetec*). Le lien vers Server Admin (disponible dans le menu Démarrer) utilise automatiquement ce port.

ATTENTION : Méfiez-vous de conflits potentiels avec d'autres logiciels exécutés sur le serveur qui utilisent également le port 80 (comme n'importe quel serveur web).

- **Port du serveur:** Le port TCP utilisé par les serveurs pour communiquer.
- **Mot de passe du serveur/Confirmer le mot de passe:** Entrez et confirmez un nouveau mot de passe (8 caractères minimum) pour ouvrir l'app web Server Admin.

  IMPORTANT : Si vous perdez le mot de passe serveur, contactez l'assistance technique Genetec[MC] pour le réinitialiser.

15 Cliquez sur **Suivant**.

16 Sur la page *Règles de pare-feu*, sélectionnez l'option **Autoriser Genetec Security Center 5.5 à créer les règles de pare-feu nécessaires pour ses applications**, puis cliquez sur **Suivant**.

Cette option permet de configurer correctement les règles de sécurité du pare-feu Windows.

REMARQUE : Vous devez également configurer les ports Security Center sur le pare-feu de votre société après l'installation.

17 Sur la page *Installation de WinPcap*, sélectionnez l'option **Installer WinPcap**, et cliquez sur **Suivant**.

Cette boîte de dialogue n'apparaît pas si WinPcap 4.1.3 est déjà installé. Cette option permet de capturer des données de diagnostic sur les unités et d'autres services Security Center. Ces données sont utilisées par l'équipe technique de Genetec[MC] si vous avez besoin d'une assistance. L'installation de WinPcap ne démarre pas immédiatement. Vous serez invité à l'installer plus tard.

18 Sur la page *Réglages de sécurité*, configurez les options suivantes :

- **Activer l'authentification du Répertoire:** Sélectionnez cette option pour forcer toutes les applications client et serveur sur le poste actuel à valider le certificat d'identité du Répertoire avant de s'y connecter (désactivé par défaut).

  BONNE PRATIQUE : Si vous décidez d'activer l'authentification du Répertoire, il est recommandé d'utiliser un certificat émis par une autorité de certification (AC) de confiance. Sinon, l'utilisateur sera invité à confirmer l'identité du serveur de Répertoire lors de la première connexion au Répertoire.

  Pour en savoir plus sur l'authentification du Répertoire, voir le *Guide de l'administrateur Security Center*.

- **Désactiver l'authentification de base:** L'authentification de base des caméras est désactivée par défaut pour empêcher l'interception des identifiants des caméras lorsque l'Archiveur se connecte à une unité vidéo.

  IMPORTANT : Lorsque cette option est sélectionnée, les caméras qui ne prennent en charge que le mode authentification de base ne peuvent pas être utilisées avec Security Center.

  REMARQUE : Le cas échéant, vous pouvez configurer cette option individuellement pour chaque extension de fabricant de caméras dans Config Tool, dans l'onglet **Extensions** de l'Archiveur.

19 Sélectionnez **Je confirme que j'ai lu et compris les implications de l'activation de ces réglages de sécurité**, puis cliquez sur **Suivant**.

Le **Programme d'installation de Genetec Security Center 5.4** est lancé et démarre l'installation.

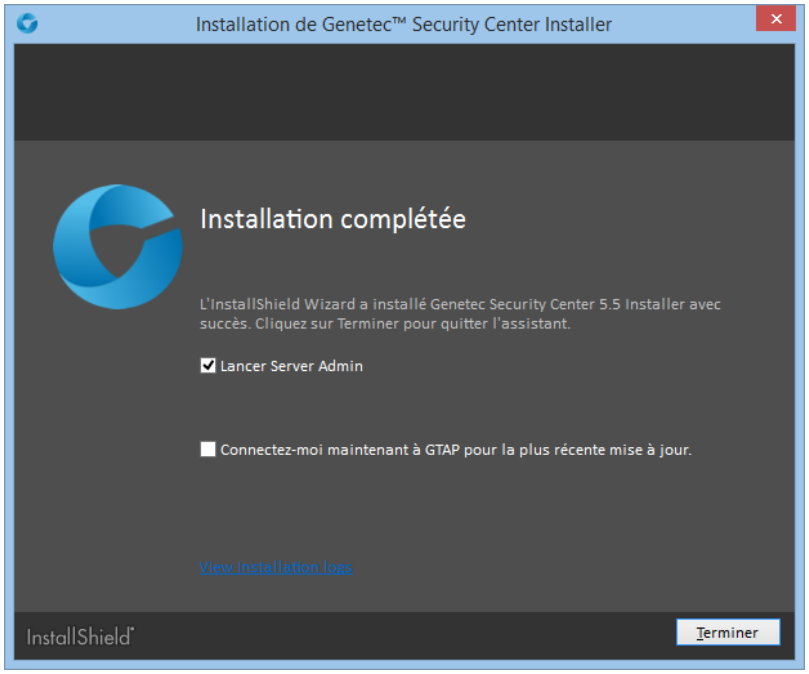
20 Si vous avez choisi d'installer WinPcap 4.1.3, l'*Assistant d'installation WinPcap 4.1.3* apparaît :

a) Suivez les instructions de l'*Assistant d'installation WinPcap 4.1.3*.

b) Sur la page *Options d'installation*, sélectionnez l'option **Lancer automatiquement le pilote WinPcap au démarrage** et cliquez sur **Installer**.

c) Cliquez sur **Terminer**, et poursuivez l'installation de Security Center.

21 (Facultatif) Lorsque la page *Installation complétée* apparaît, cliquez sur **Consulter les journaux d'installation** pour ouvrir le dossier qui contient les journaux, que vous pouvez consulter avec Bloc-notes.



22 Cliquez sur **Terminer**.

Si vous avez sélectionné l'option **Lancer Server Admin** à la fin de l'installation, Server Admin est lancé dans votre navigateur.

Si vous avez sélectionné l'option **Se connecter à GTAP pour obtenir la dernière mise à jour**, votre navigateur web ouvre la page Téléchargement de produits Genetec sur GTAP. Vous devez disposer d'un nom d'utilisateur et d'un mot de passe pour vous connecter à GTAP.

Security Center est désormais installé sur le serveur principal.

Lorsque vous avez terminé

Procédez de la manière suivante :

- Activez la licence du produit dans Server Admin.

- Installez Security Center sur les serveurs d'extension.

Rubriques connexes

Activer la licence Security Center sur le Web, page 23
Activer la licence Security Center sans accès à Internet, page 26
Installer Security Center sur un serveur d'extension., page 31

Activer la licence Security Center sur le Web

La Security Center licence est activée sur le serveur principal. Vous devez activer votre licence Security Center après l'installation de Security Center sur le serveur principal, et lorsque vous transformez un serveur d'extension en serveur principal. Si vous êtes connecté à Internet, vous pouvez activer votre licence Security Center sur le Web via Server Admin.

Avant de commencer

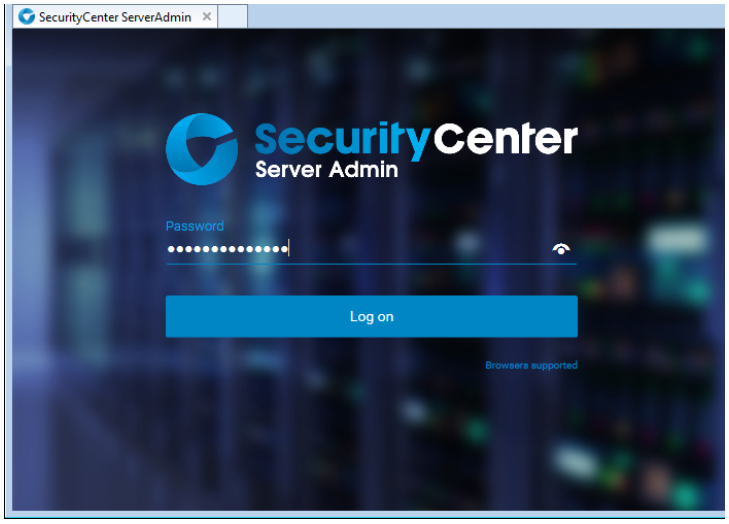
Pour activer votre licence en vous servant du Web, vous devez disposer des éléments suivants :

- **Connexion à Internet:** Si votre serveur ne dispose pas d'un accès à Internet, alors consultez Activer la licence Security Center sans accès à Internet, page 26.
- **ID système et mot de passe:** L'ID système et mot de passe sont disponibles dans le document *Informations de licence Security Center*. Le service client de Genetec vous envoie ce document à l'achat du produit.
- **Mot de passe du serveur:** Le mot de passe serveur sert à vous connecter à Server Admin. Le mot de passe du serveur est défini à l'installation.

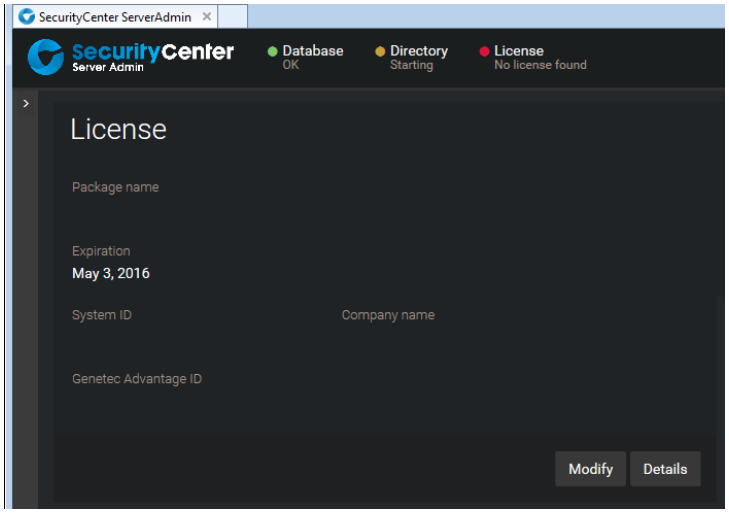
Pour activer la licence Security Center en passant par le Web :

1 Ouvrez la page web Server Admin de l'une des manières suivantes :
   - Dans la barre d'adresse de votre navigateur web, entrez `http://ordinateur:port/Genetec`, où `ordinateur` est le nom DNS ou l'adresse IP de votre serveur et `port` est le numéro de port du serveur web spécifié à l'installation de Security Center.

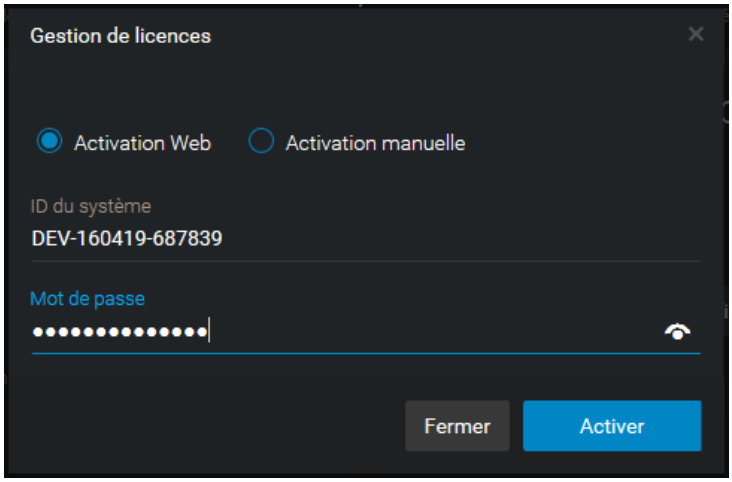
     Vous pouvez omettre le numéro de port si vous utilisez la valeur 80 par défaut.
   - Si vous vous connectez à Server Admin depuis l'hôte local, vous pouvez cliquer deux fois sur le raccourci **Genetec Server Admin** ( ) disponible dans le dossier *Genetec Security Center 5.5* du menu Démarrer de Windows.
2 Entrez le mot de passe serveur spécifié à l'installation du serveur, puis cliquez sur **Connexion**.



   La page *Présentation* de Server Admin apparaît.
3 Procédez de l'une des manières suivantes :
   - Cliquez sur **Licence** en haut de la page de Server Admin.
   - Cliquez sur **Modifier** dans la section *Licence* de la page *Présentation* de Server Admin.

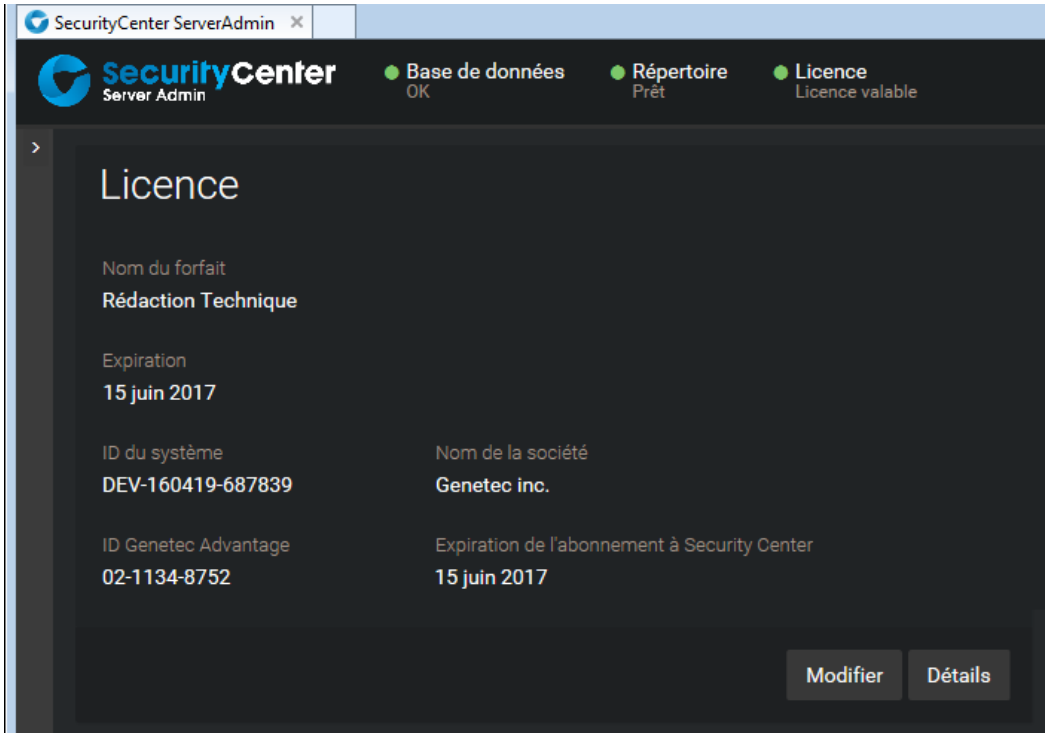


4 Dans la boîte de dialogue *Gestion de licences*, cliquez sur **Activation Web**, puis entrez votre **ID du système** et **Mot de passe** tels qu'indiqués dans le document *Information sur la licence Security Center* reçu à l'achat de votre licence.

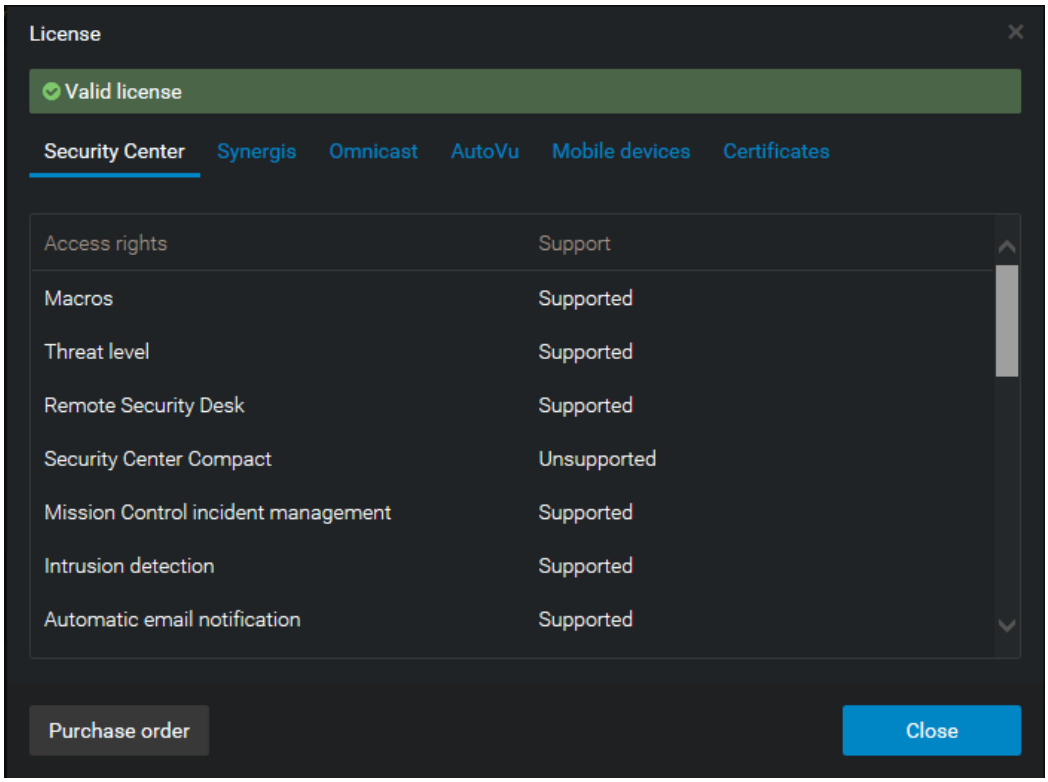


5 Cliquez sur **Activer**.

Les informations de licence apparaissent dans la section *Licence* de la page *Présentation* de Server Admin.



6 Cliquez sur **Détails** pour afficher les options de votre licence dans une boîte de dialogue.



Les options de licence sont réparties dans six onglets. Pour en savoir plus, voir le *Guide de l'administrateur Security Center*.

7 Cliquez sur **Fermer**, puis fermez la fenêtre du navigateur.

Activer la licence Security Center sans accès à Internet

La Security Center licence est activée sur le serveur principal. Vous devez activer votre licence Security Center après l'installation de Security Center sur le serveur principal, et lorsque vous transformez un serveur d'extension en serveur principal. Si vous n'avez pas accès à Internet, vous pouvez activer votre licence Security Center manuellement avec Server Admin et GTAP.

Avant de commencer

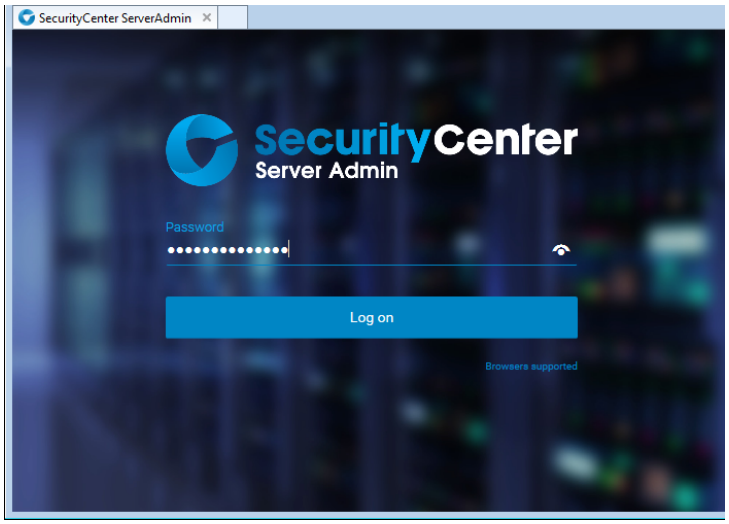
Pour activer votre licence, vous devez disposer des éléments suivants :

- **ID système et mot de passe:** L'ID système et mot de passe sont disponibles dans le document *Informations de licence Security Center*. Le service client de Genetec vous envoie ce document à l'achat du produit.
- **Mot de passe du serveur:** Le mot de passe serveur sert à vous connecter à Server Admin. Le mot de passe du serveur est défini à l'installation.

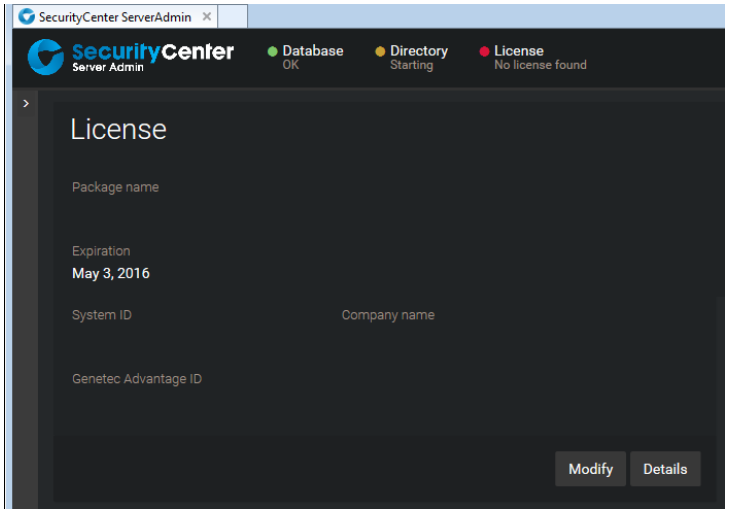
Pour activer votre licence Security Center sans accès à Internet :

1 Ouvrez la page web Server Admin de l'une des manières suivantes :
   - Dans la barre d'adresse de votre navigateur web, entrez `http://ordinateur:port/Genetec`, où `ordinateur` est le nom DNS ou l'adresse IP de votre serveur et `port` est le numéro de port du serveur web spécifié à l'installation de Security Center.

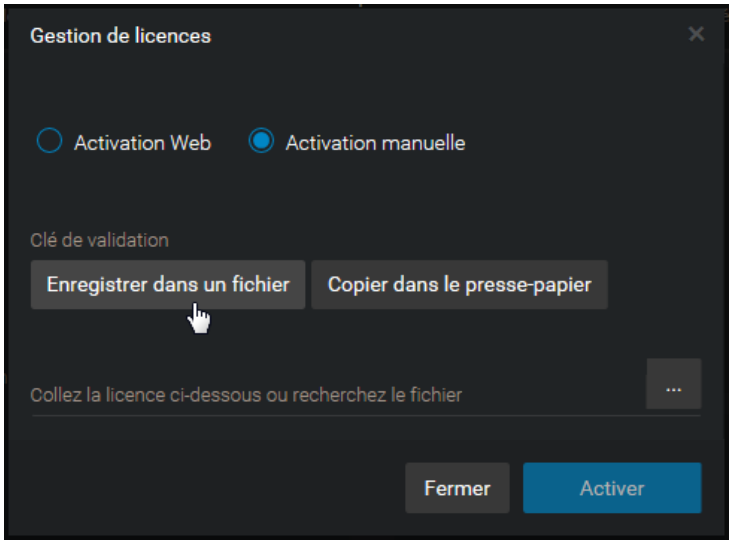
     Vous pouvez omettre le numéro de port si vous utilisez la valeur 80 par défaut.
   - Si vous vous connectez à Server Admin depuis l'hôte local, vous pouvez cliquer deux fois sur le raccourci **Genetec Server Admin** () disponible dans le dossier *Genetec Security Center 5.5* du menu Démarrer de Windows.
2 Entrez le mot de passe serveur spécifié à l'installation du serveur, puis cliquez sur **Connexion**.



   La page *Présentation* de Server Admin apparaît.
3 Procédez de l'une des manières suivantes :
   - Cliquez sur **Licence** en haut de la page de Server Admin.
   - Cliquez sur **Modifier** dans la section *Licence* de la page *Présentation* de Server Admin.



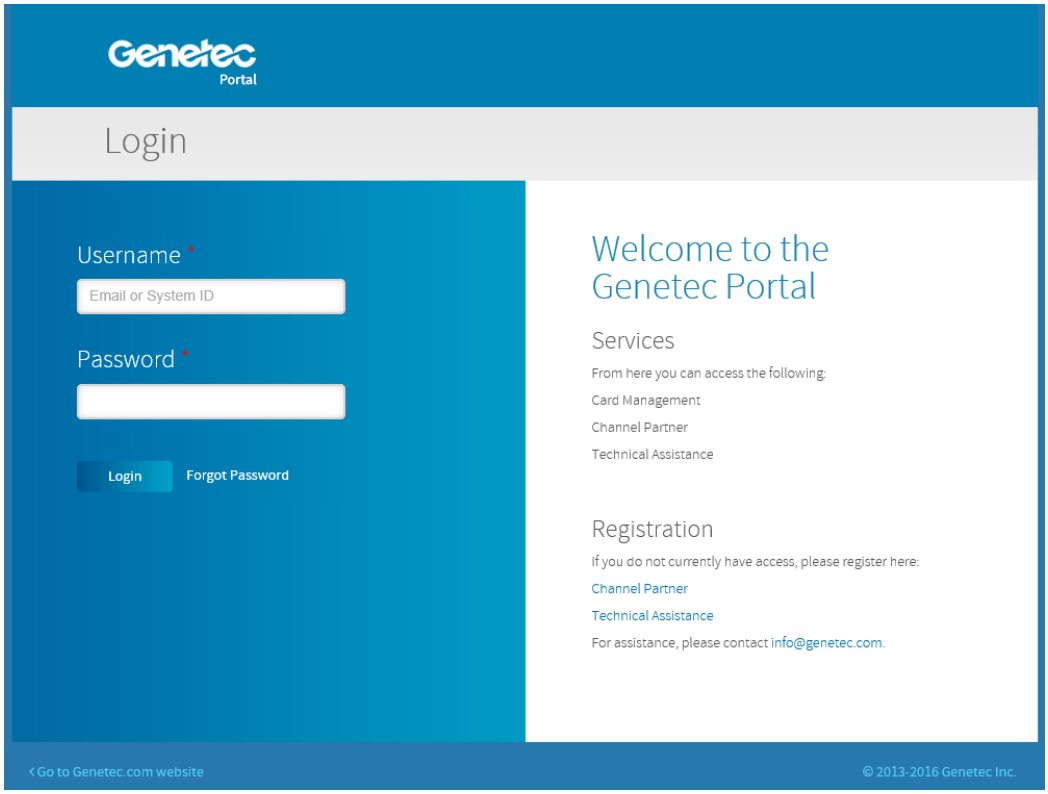
4 Dans la boîte de dialogue *Gestion de licences*, cliquez sur **Activation manuelle**, puis sous *Clé de validation*, cliquez sur **Enregistrer dans un fichier**.



La clé de validation est une séquence de chiffres (en hexadécimal au format texte) unique générée par Security Center qui identifie votre serveur. Elle sert à générer la clé de licence qui déverrouille votre logiciel Security Center. La clé de licence générée ne peut être appliquée qu'au serveur identifié par la clé de validation.

Un fichier texte nommé *validation.vk* est enregistré dans votre dossier *Téléchargements* par défaut. Veillez à copier ce fichier dans un emplacement (il peut s'agir d'une clé USB) auquel vous pouvez accéder depuis un autre poste connecté à Internet.

5 Sur un autre ordinateur connecté à Internet, connectez-vous sur GTAP à l'adresse : https://gtap.genetec.com

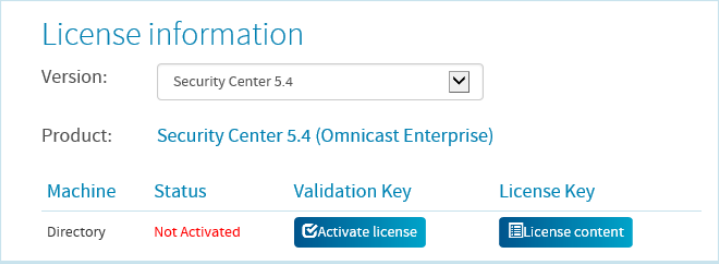


6 Sur la page de connexion GTAP, procédez de l'une des manières suivantes :

- Entrez l'ID système et le mot de passe spécifiés dans le document *Informations de licence Security Center*, et cliquez sur **Connexion**.
- Entrez votre compte utilisateur GTAP (votre adresse de messagerie électronique) et votre mot de passe, puis cliquez sur **Connexion**.
  1 Sur la page *Portail Genetec - Accueil*, cliquez sur **Activer le nouveau système**.
  2 Dans la liste déroulante **ID du système**, sélectionnez votre système et cliquez sur **Envoyer**.

Le navigateur s'ouvre à la page *Informations système*.

7 Défilez jusqu'à la section *Informations de licence* et cliquez sur **Activer la licence**.



8 Dans la boîte de dialogue qui s'ouvre, parcourrez jusqu'à votre clé de validation (.vk file), et cliquez sur **Envoyer**.

Le message **License activation successful** (Activation de licence réussie) s'affiche.

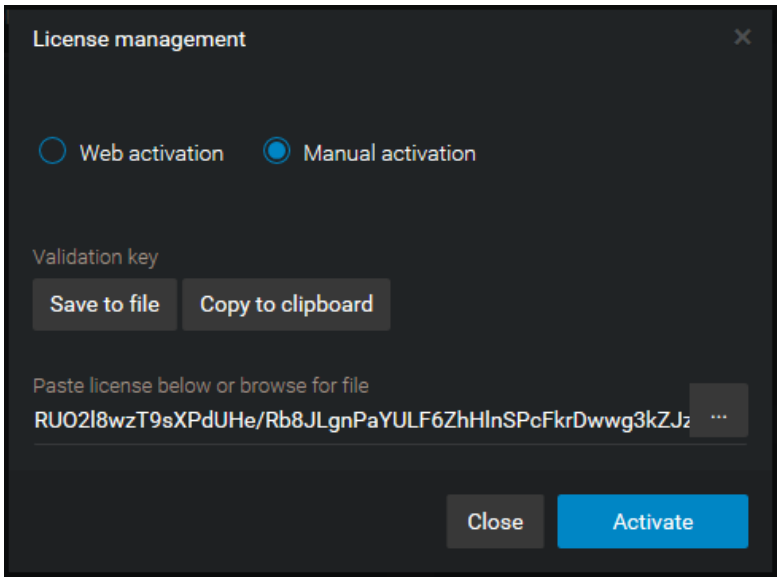
9 Cliquez sur **Télécharger la licence**, et enregistrez la clé de licence dans un fichier.

Le nom par défaut est votre ID système suivi de *_Directory_License.lic*.

10 Revenez à Server Admin qui est connecté à votre serveur principal Security Center.

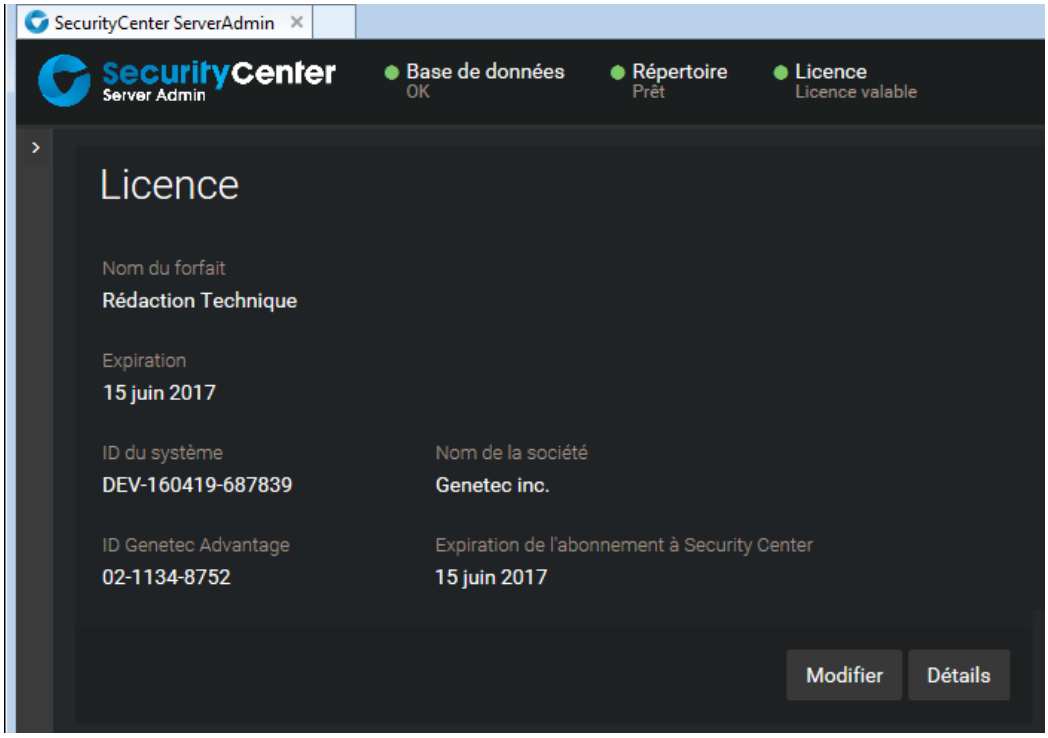
11 Dans la boîte de dialogue *Gestion de licences*, procédez de l'une des manières suivantes :

- Collez vos informations de licence à partir du fichier de clé de licence (que vous ouvrez dans un éditeur de texte).
- Recherchez la clé de licence (fichier .lic), et cliquez sur **Ouvrir**.

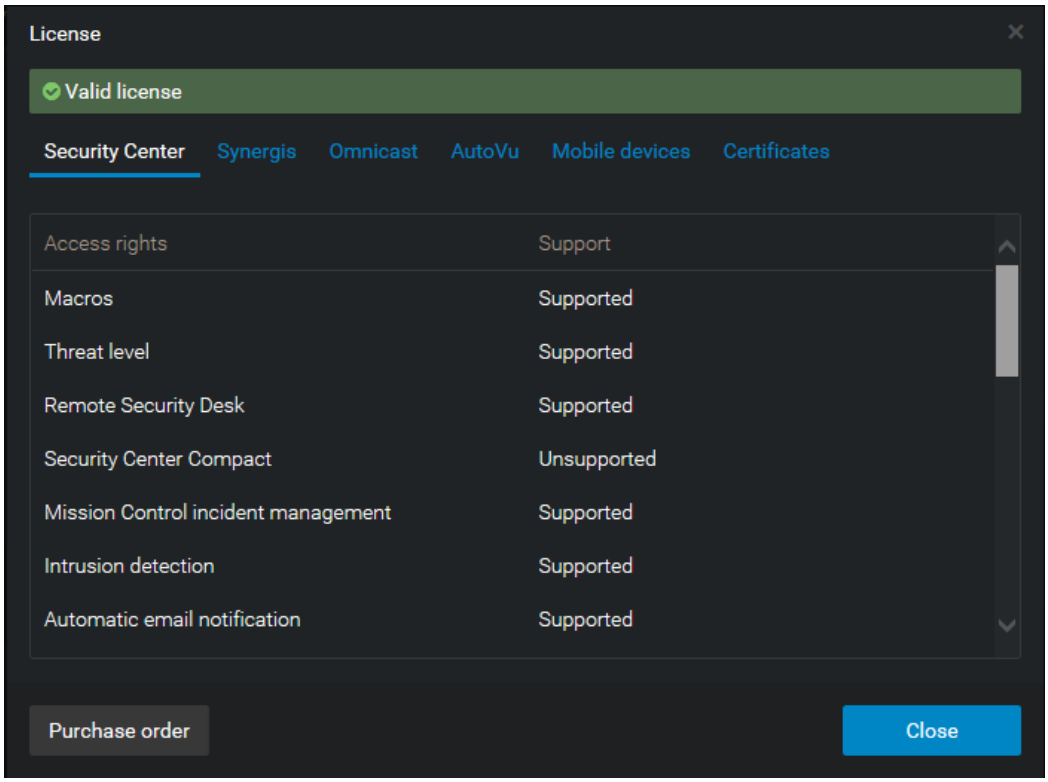


12 Cliquez sur **Activer**.

Les informations de licence apparaissent dans la section *Licence* de la page *Présentation* de Server Admin.



13 Cliquez sur **Détails** pour afficher les options de votre licence dans une boîte de dialogue.



Les options de licence sont réparties dans six onglets. Pour en savoir plus, voir le *Guide de l'administrateur Security Center*.

14 Cliquez sur **Fermer**, puis fermez la fenêtre du navigateur.

Installer Security Center sur un serveur d'extension.

Pour renforcer la capacité de traitement de votre système Security Center, vous pouvez ajouter des serveurs d'extension qui se connectent au serveur principal.

Avant de commencer

- Préparez l'installation de Security Center.
- Installez Security Center sur le serveur principal, et vérifiez que le serveur fonctionne correctement.

À savoir

La procédure d'installation d'un serveur d'extension installe les éléments suivants :

- Le service Genetec Server *sans* le rôle Répertoire.

  Lorsque vous installez Genetec Server, la base de données du rôle Répertoire (facultativement SQL Express 2014), Server Admin et le service Watchdog sont également installés.
- (Facultatif) Applications client (Config Tool, Security Desk ou les deux).

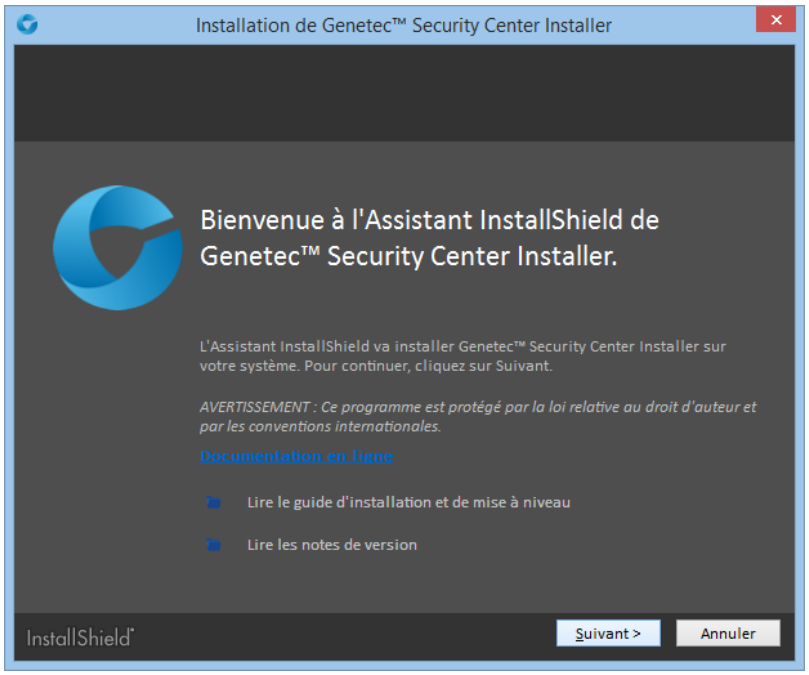
Pour installer Security Center sur un serveur d'extension :

1 Cliquez deux fois sur *setup.exe* (version autonome) ou sur *SecurityCenterWebSetup.exe* (version web) pour lancer le programme d'installation de Security Center.

REMARQUE : Seul l'Assistant InstallShield autonome est illustré dans cette procédure.

2 Sur la page *Setup Language* (Langue de l'installation), sélectionnez l'anglais ou le français, puis cliquez sur **Suivant**.

La fenêtre *Bienvenue à l'Assistant InstallShield* apparaît.

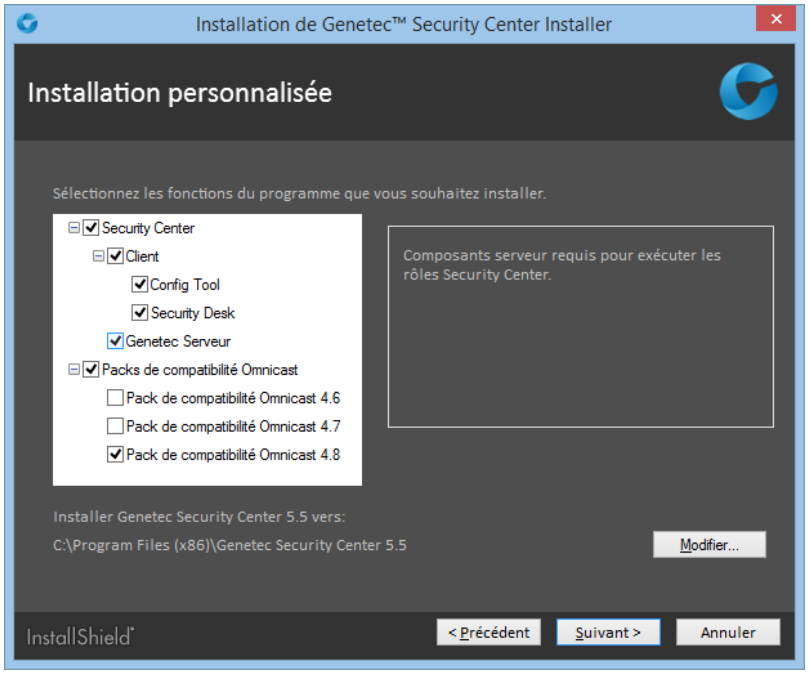


3 Sur la page de *Bienvenue*, cliquez sur **Suivant**.

Des liens sont fournis pour consulter la documentation Security Center pertinente en ligne ou au format PDF.

4 Sur la page *Contrat de licence*, lisez les conditions du *Contrat de licence logicielle Genetec*, sélectionnez **J'accepte les termes de ce contrat de licence**, et cliquez sur **Suivant**.

5 Sur la page *Installation personnalisée*, sélectionnez les applications Security Center à installer.



Vous disposez des options suivantes :

- **Serveur:** Installe le service Genetec Server, les bases de données SQL, Server Admin et le service Watchdog.
- **(Facultatif) Client:** Installe les applications Security Center client : Vous pouvez choisir Config Tool, Security Desk ou les deux.
- **(Facultatif) Packs de compatibilité Omnicast:** Si vous comptez fédérer les systèmes Omnicast, sélectionnez les packs de compatibilité Omnicast nécessaires.

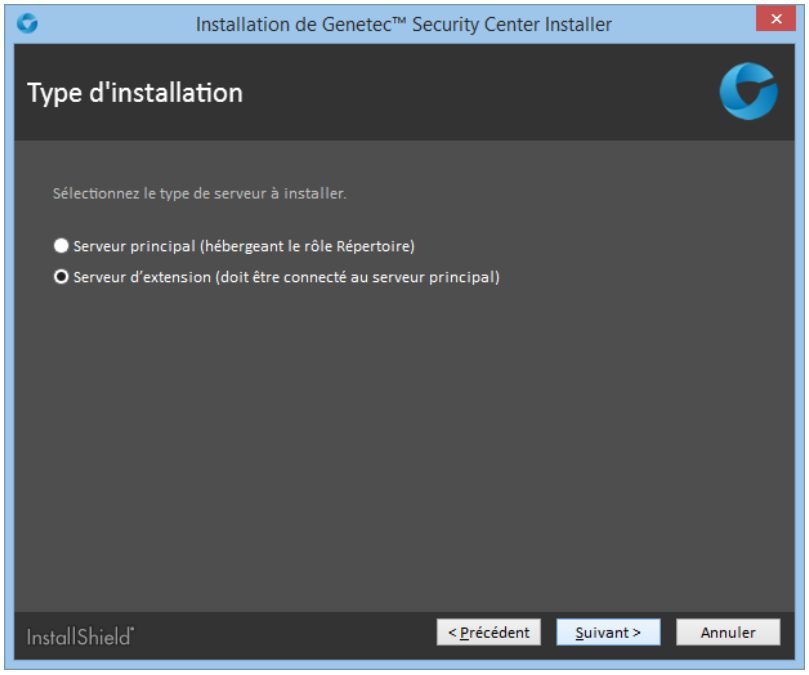
6 Pour changer le dossier d'installation, cliquez sur **Modifier**, puis cliquez sur **Suivant**.

7 Sur la page *Sélection de la langue*, sélectionnez la langue de l'interface utilisateur des applications Security Center, et cliquez sur **Suivant**.

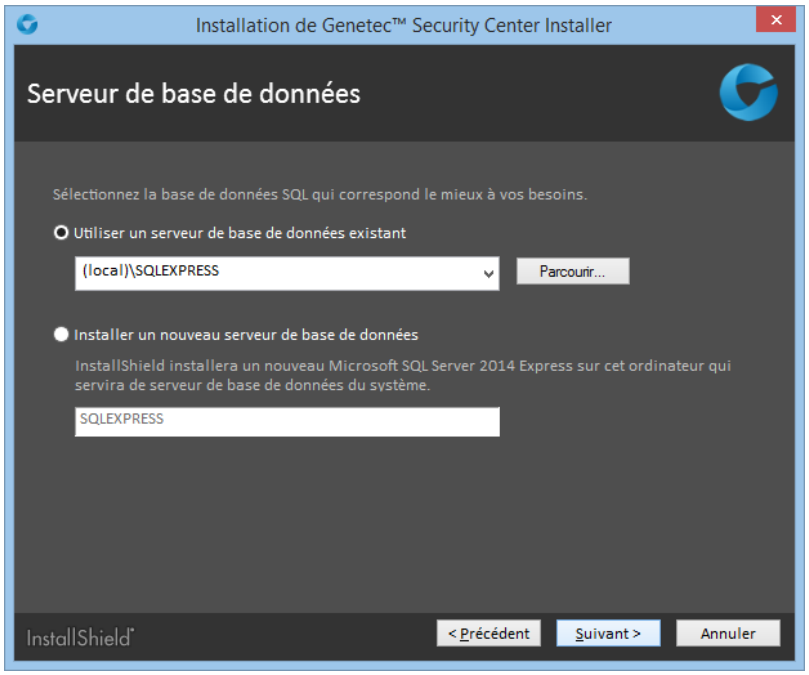
REMARQUE : L'aide en ligne des applications Security Center n'est pas disponible dans toutes les langues. Pour la liste des langues disponibles, voir les *Notes de version Security Center*.

CONSEIL : Après l'installation, vous pouvez modifier la langue de l'interface à tout moment à l'aide de l'*outil langue* disponible dans le sous-dossier Outils du groupe de programmes Genetec Security Center.

8 Sur la page *Type d'installation*, sélectionnez l'option **Serveur d'extension**, et cliquez sur **Suivant**.



9 Sur la page *Serveur de base de données*, sélectionnez une des options suivantes :



- **Utiliser un serveur de base de données existant:** Sélectionnez une instance existante de Microsoft SQL Server qui hébergera la base de données.

  Une bonne pratique consiste à remplacer `(local)` par le nom de votre ordinateur. Vous devez indiquer explicitement le nom de l'ordinateur si vous configurez le Répertoire pour l'équilibrage de charge.

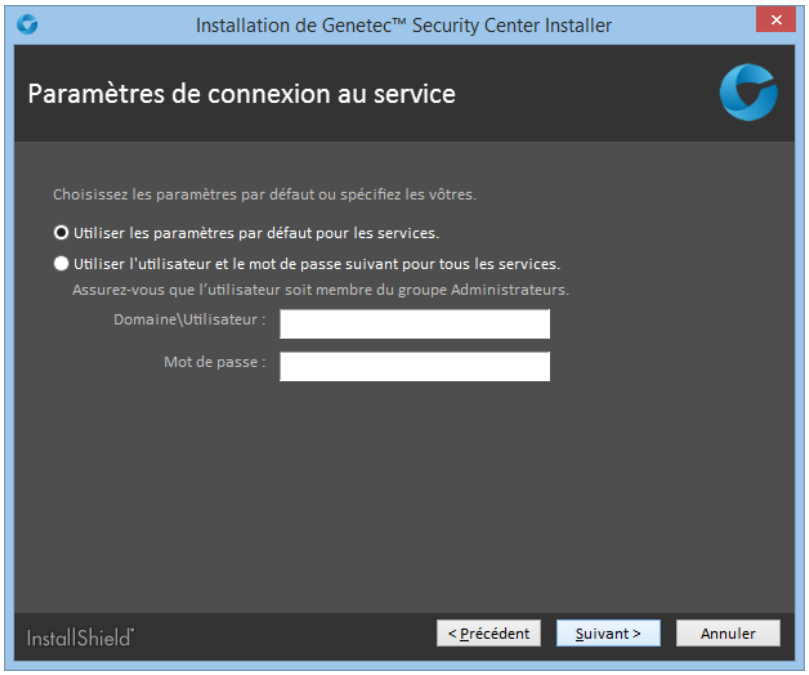
- **Installer un nouveau serveur de base de données:** Installe Microsoft SQL Server 2014 Express Edition. Vous devez choisir un nom de serveur de base de données. Le nom par défaut est SQLEXPRESS.

  REMARQUE : Le nom du serveur de base de données ne distingue pas les majuscules des minuscules, mais doit suivre les règles suivantes :

- Il ne peut pas utiliser un mot clé réservé de SQL Server, comme DEFAULT, PRIMARY, etc. Pour une liste complète des mots clés réservés, voir https://msdn.microsoft.com/en-us/library/ms189822.aspx.
- Il ne doit pas faire plus de 16 caractères.
- La première lettre du nom de l'instance doit être une lettre ou le signe souligné (_). Les lettres acceptables, définies par la norme Unicode Standard 2.0, incluent les caractères latins a-z et A-Z, et certains caractères d'autres alphabets.
- Les caractères suivants peuvent être des lettres définies par la norme Unicode Standard 2.0, des chiffres décimaux (scripts latins ou autres), le signe dollar ($) ou souligné (_).
- Les espaces et d'autres caractères spéciaux sont interdits, dont les suivants :barre oblique inverse (\), virgule (,), deux-points (:), point-virgule (;), guillemet simple ('), esperluette (&), dièse (#) et arobase (@).

10 Cliquez sur **Suivant**.

11 Sur la page *Paramètres de connexion au service*, sélectionnez l'une des options suivantes :



- **Utiliser le nom et le mot de passe par défaut:** Utiliser le nom d'utilisateur par défaut (du système local) pour exécuter les services Security Center. Cette option fonctionne dans la plupart des cas.
- **Spécifier le nom d'utilisateur et le mot de passe pour tous les services.:** Entrez un nom d'utilisateur et mot de passe de domaine valables.

  IMPORTANT : Vérifiez que l'utilisateur du service appartient au groupe Administrateurs, dispose des droits sur la base de données locale ou distante et des droits d'utilisateur *Ouverture de session en tant que service*. Si ce serveur hébergera le rôle Active Directory, l'utilisateur concerné doit disposer d'un accès en lecture et en écriture à l'Active Directory auquel vous souhaitez connecter le serveur.

12 Cliquez sur **Suivant**.

13 Sur la page *Paramètres du serveur*, renseignez les champs suivants :

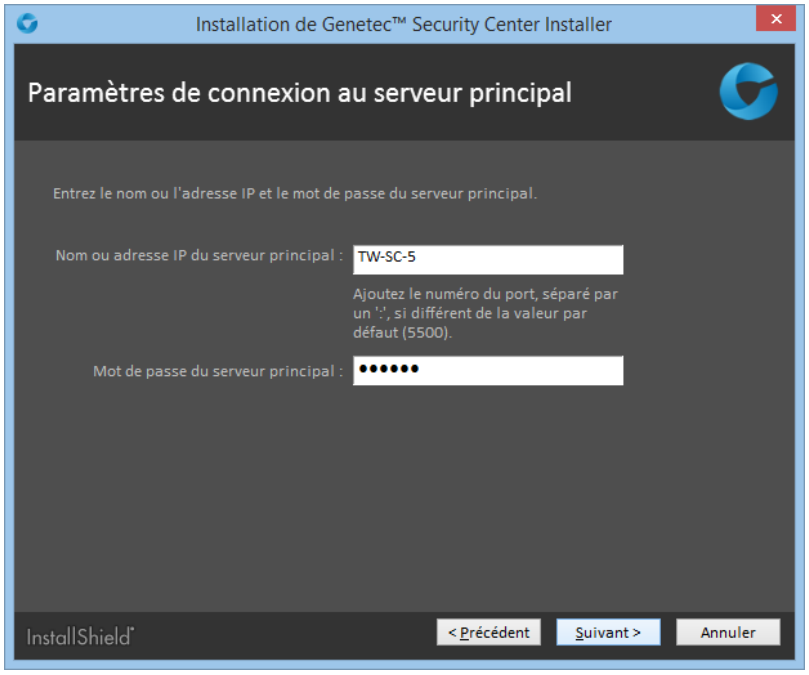
- **Port du serveur Web:** Le port HTTP utilisé pour l'administration sur le Web avec Server Admin. Si vous modifiez le port par défaut, vous devez inclure le port dans l'adresse de Server Admin (par exemple *http://ordinateur:port/Genetec* au lieu de *http://ordinateur/Genetec*). Le lien vers Server Admin (disponible dans le menu Démarrer) utilise automatiquement ce port.

  ATTENTION : Méfiez-vous de conflits potentiels avec d'autres logiciels exécutés sur le serveur qui utilisent également le port 80 (comme n'importe quel serveur web).
- **Port du serveur:** Le port TCP utilisé par les serveurs pour communiquer.
- **Mot de passe du serveur/Confirmer le mot de passe:** Entrez et confirmez un nouveau mot de passe (8 caractères minimum) pour ouvrir l'app web Server Admin.

  IMPORTANT : Si vous perdez le mot de passe serveur, contactez l'assistance technique Genetec[MC] pour le réinitialiser.

14 Cliquez sur **Suivant**.

15 Sur la page *Paramètres de connexion au serveur principal*, renseignez les champs suivants :



- **Le nom ou l'adresse IP du serveur:** Le nom DNS ou l'adresse IP du serveur principal.

  Si vous avez modifié le numéro de port (4502) sur le serveur principal, vous devez ajouter le numéro de port au nom du serveur, en les séparant avec le signe deux points (:).

- **Mot de passe du serveur principal:** Entrez le mot de passe utilisé pour configurer le serveur principal.

16 Sur la page *Règles de pare-feu*, sélectionnez l'option **Autoriser Genetec Security Center 5.5 à créer les règles de pare-feu nécessaires pour ses applications**, puis cliquez sur **Suivant**.

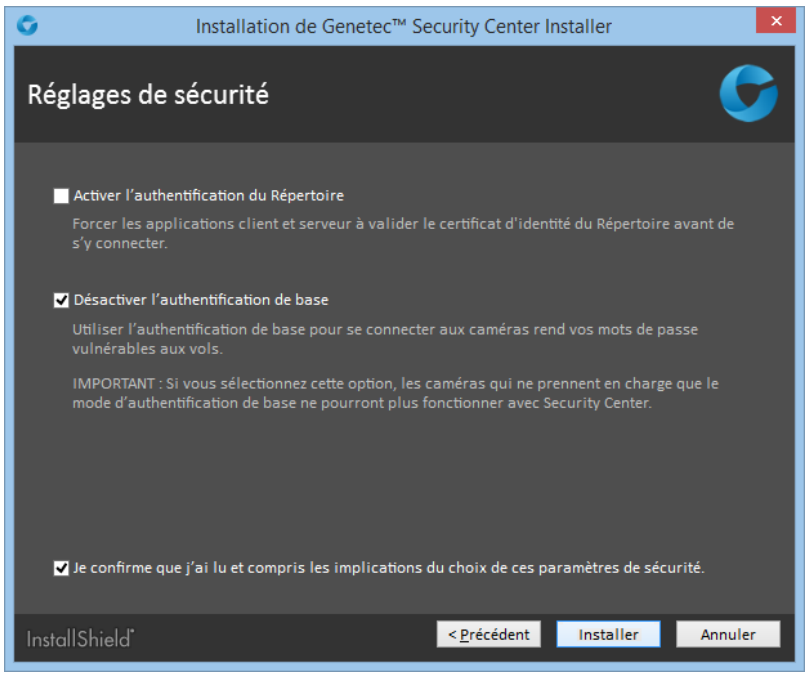
Cette option permet de configurer correctement les règles de sécurité du pare-feu Windows.

REMARQUE : Vous devez également configurer les ports Security Center sur le pare-feu de votre société après l'installation.

17 Sur la page *Installation de WinPcap*, sélectionnez l'option **Installer WinPcap**, et cliquez sur **Suivant**.

Cette boîte de dialogue n'apparaît pas si WinPcap 4.1.3 est déjà installé. Cette option permet de capturer des données de diagnostic sur les unités et d'autres services Security Center. Ces données sont utilisées par l'équipe technique de Genetec^{MC} si vous avez besoin d'une assistance. L'installation de WinPcap ne démarre pas immédiatement. Vous serez invité à l'installer plus tard.

18 Sur la page *Réglages de sécurité*, configurez les options suivantes :



- **Activer l'authentification du Répertoire:** Sélectionnez cette option pour forcer toutes les applications client et serveur sur le poste actuel à valider le certificat d'identité du Répertoire avant de s'y connecter (désactivé par défaut).

  BONNE PRATIQUE : Si vous décidez d'activer l'authentification du Répertoire, il est recommandé d'utiliser un certificat émis par une autorité de certification (AC) de confiance. Sinon, l'utilisateur sera invité à confirmer l'identité du serveur de Répertoire lors de la première connexion au Répertoire.

  Pour en savoir plus sur l'authentification du Répertoire, voir le *Guide de l'administrateur Security Center*.

- **Désactiver l'authentification de base:** L'authentification de base des caméras est désactivée par défaut pour empêcher l'interception des identifiants des caméras lorsque l'Archiveur se connecte à une unité vidéo.

  IMPORTANT : Lorsque cette option est sélectionnée, les caméras qui ne prennent en charge que le mode authentification de base ne peuvent pas être utilisées avec Security Center.

  REMARQUE : Le cas échéant, vous pouvez configurer cette option individuellement pour chaque extension de fabricant de caméras dans Config Tool, dans l'onglet **Extensions** de l'Archiveur.

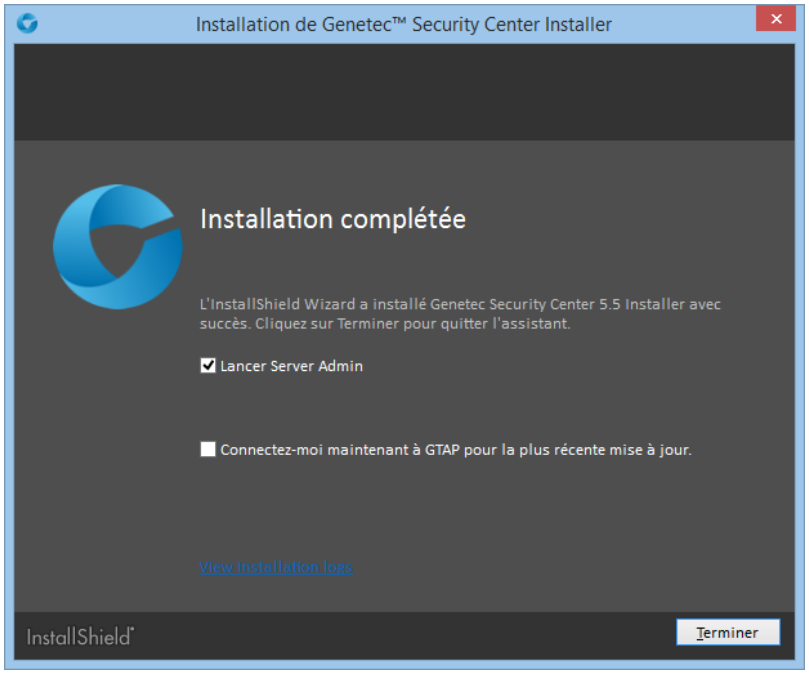
19 Sélectionnez **Je confirme que j'ai lu et compris les implications de l'activation de ces réglages de sécurité**, puis cliquez sur **Suivant**.

Le **Programme d'installation de Genetec Security Center 5.4** est lancé et démarre l'installation.

20 Si vous avez choisi d'installer WinPcap 4.1.3, l'*Assistant d'installation WinPcap 4.1.3* apparaît :

a) Suivez les instructions de l'*Assistant d'installation WinPcap 4.1.3*.
b) Sur la page *Options d'installation*, sélectionnez l'option **Lancer automatiquement le pilote WinPcap au démarrage** et cliquez sur **Installer**.
c) Cliquez sur **Terminer**, et poursuivez l'installation de Security Center.

21 (Facultatif) Lorsque la page *Installation complétée* apparaît, cliquez sur **Consulter les journaux d'installation** pour ouvrir le dossier qui contient les journaux, que vous pouvez consulter avec Bloc-notes.



22 Cliquez sur **Terminer**.

Si vous avez sélectionné l'option **Lancer Server Admin** à la fin de l'installation, Server Admin est lancé dans votre navigateur.

Si vous avez sélectionné l'option **Se connecter à GTAP pour obtenir la dernière mise à jour**, votre navigateur web ouvre la page Téléchargement de produits Genetec sur GTAP. Vous devez disposer d'un nom d'utilisateur et d'un mot de passe pour vous connecter à GTAP.

Security Center est désormais installé sur le serveur d'extension.

Lorsque vous avez terminé

Connectez le serveur d'extension au serveur principal.

Connecter les serveurs d'extension au serveur principal

Lorsque vous déplacez le serveur principal sur un nouvel ordinateur, vous devez utiliser Server Admin pour reconnecter tous les serveurs d'extension de votre système au nouvel ordinateur.

Avant de commencer

Lorsque vous installez un serveur d'extension, celui-ci se connecte automatiquement au serveur principal. Vous ne devez délibérément connecter un serveur d'extension au serveur principal que si :

- Vous avez saisi les mauvais paramètres de connexion au serveur principal durant l'installation du serveur d'extension.
- Vous avez déplacé le serveur principal vers un autre ordinateur.
- Vous avez modifié le mot de passe sur le serveur principal pendant que le serveur d'extension était hors ligne.
- Vous avez activé l'authentification du Répertoire sur le serveur d'extension, mais votre certificat de Répertoire n'est pas signé par une autorité de certification de confiance.

Pour connecter un serveur d'extension au serveur principal :

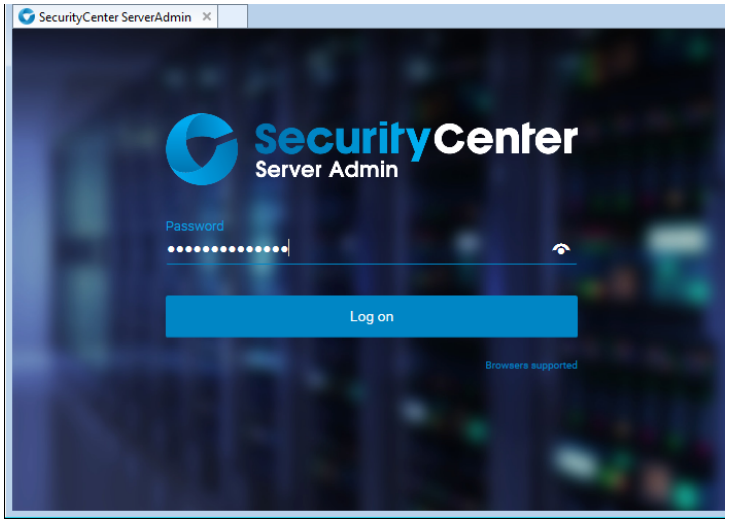
1 Ouvrez la page web Server Admin de l'une des manières suivantes :

- Dans la barre d'adresse de votre navigateur web, entrez `http://ordinateur:port/Genetec`, où `ordinateur` est le nom DNS ou l'adresse IP de votre serveur et `port` est le numéro de port du serveur web spécifié à l'installation de Security Center.

  Vous pouvez omettre le numéro de port si vous utilisez la valeur 80 par défaut.

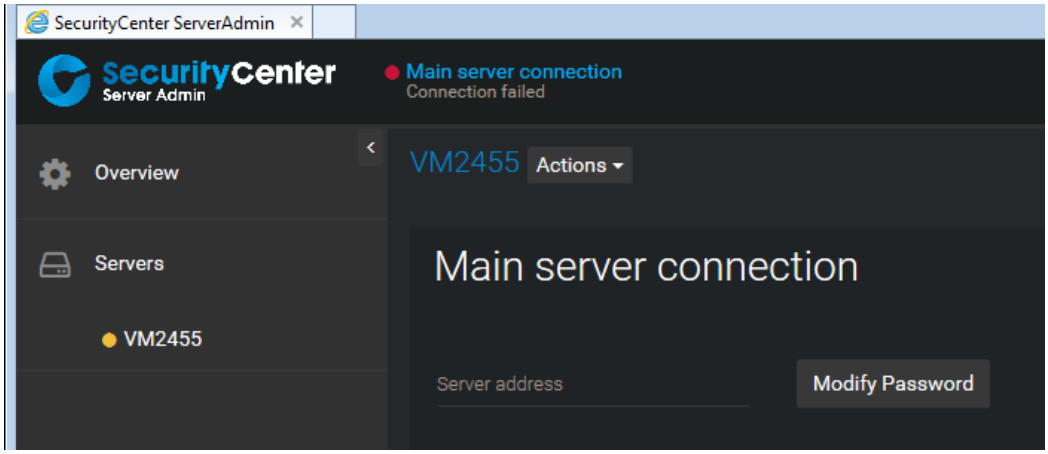
- Si vous vous connectez à Server Admin depuis l'hôte local, vous pouvez cliquer deux fois sur le raccourci **Genetec Server Admin** () disponible dans le dossier *Genetec Security Center 5.5* du menu Démarrer de Windows.

2 Entrez le mot de passe serveur spécifié à l'installation du serveur, puis cliquez sur **Connexion**.



La page *Présentation* de Server Admin apparaît.

3 Si vous n'êtes pas connecté au serveur principal, cliquez sur **Connexion au serveur principal** en haut de la fenêtre de Server Admin.

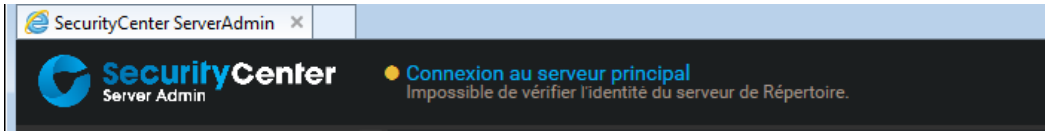


4 Entrez l'**Adresse du serveur** (nom DNS ou adresse IP du serveur principal) et le **Mot de passe**, puis cliquez sur **Enregistrer**.

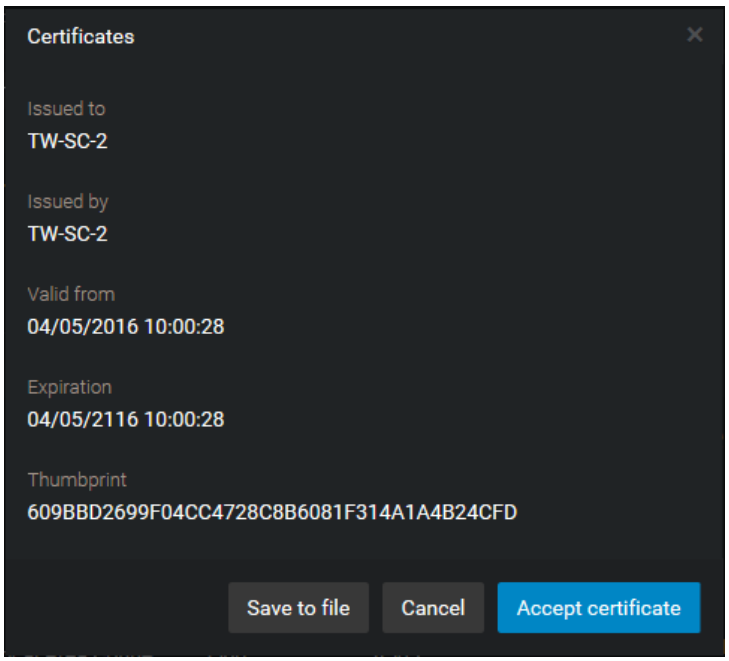
5 Lorsque vous êtes invité à redémarrer le service, cliquez sur **Oui**.

Pendant le redémarrage du service *Genetec Server*, vous êtes déconnecté de Server Admin.

6 En vous reconnectant à Server Admin, si un message vous indique que l'identité du Répertoire ne peut pas être vérifiée, cliquez sur **Connexion au serveur principal**.



7 Dans la boîte de dialogue qui apparaît, vérifiez que le certificat de votre serveur principal est conforme, puis cliquez sur **Accepter le certificat**.



IMPORTANT : Une fois qu'il est accepté, le certificat est stocké dans une liste blanche en local, et vous ne serez plus invité à l'accepter. Dans le cas contraire, notifiez immédiatement votre service informatique.

BONNE PRATIQUE : Pour éviter d'avoir à accepter le certificat de votre serveur principal à chaque fois que quelqu'un essaie de s'y connecter depuis un nouveau poste, n'utilisez que les certificats signés par une autorité de certification acceptée par le service informatique de votre société.

8 Cliquez sur **Enregistrer**

9 Lorsque vous êtes invité à redémarrer le service, cliquez sur **Oui**.

Pendant le redémarrage du service *Genetec Server*, vous êtes déconnecté de Server Admin.

Le serveur d'extension est désormais connecté au serveur principal. Les deux serveurs resteront connectés, même lorsque vous changez le certificat sur l'un ou l'autre des serveurs, dès lors que les deux serveurs sont connectés au moment du changement.

Installer Security Center Client

L'option Security Center Client installe Config Tool et Security Desk par défaut.

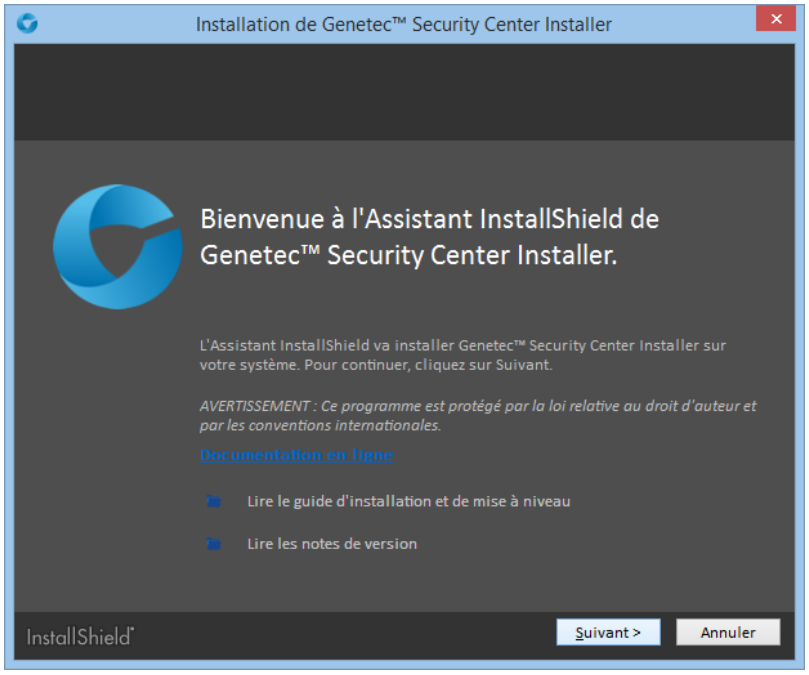
Pour installer Security Center Client :

1 Cliquez deux fois sur *setup.exe* (version autonome) ou sur *SecurityCenterWebSetup.exe* (version web) pour lancer le programme d'installation de Security Center.

REMARQUE : Seul l'Assistant InstallShield autonome est illustré dans cette procédure.

2 Sur la page *Setup Language* (Langue de l'installation), sélectionnez l'anglais ou le français, puis cliquez sur **Suivant**.

La fenêtre *Bienvenue à l'Assistant InstallShield* apparaît.



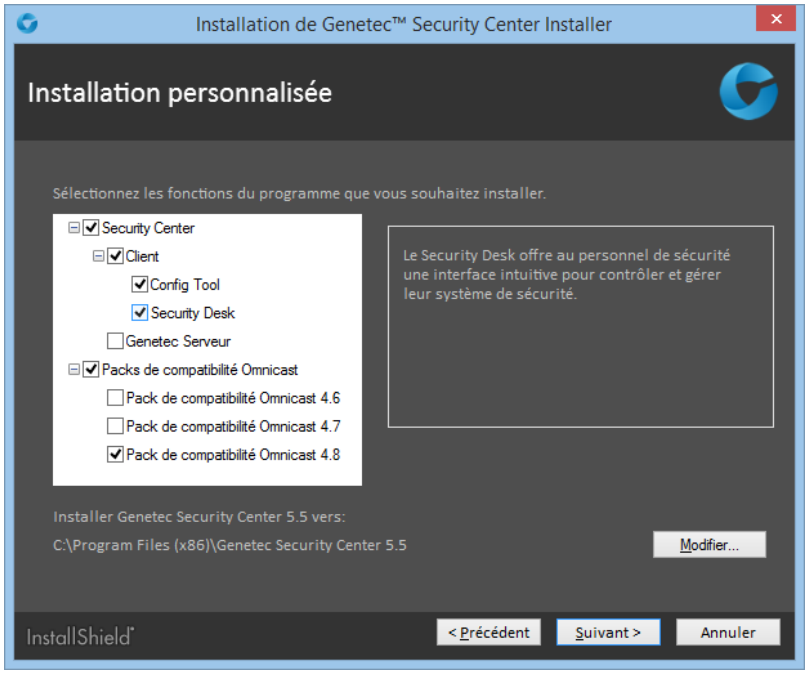
3 Sur la page de *Bienvenue*, cliquez sur **Suivant**.

Des liens sont fournis pour consulter la documentation Security Center pertinente en ligne ou au format PDF.

4 Sur la page *Contrat de licence*, lisez les conditions du *Contrat de licence logicielle Genetec*, sélectionnez **J'accepte les termes de ce contrat de licence**, et cliquez sur **Suivant**.

5 Sur la page *Installation personnalisée*, sélectionnez **Client**, puis les applications client à installer. Vous disposez des options suivantes :

- **Config Tool:** Sert à configurer toutes les propriétés de Security Center.
- **Security Desk:** Permet de contrôler et surveiller efficacement de nombreuses applications de sécurité et de sûreté.
- **Packs de compatibilité Omnicast:** Si vous comptez fédérer les systèmes Omnicast, sélectionnez les packs de compatibilité Omnicast nécessaires.



6 Pour changer le dossier d'installation, cliquez sur **Modifier**, puis cliquez sur **Suivant**.

7 Sur la page *Sélection de la langue*, sélectionnez la langue de l'interface utilisateur des applications Security Center, et cliquez sur **Suivant**.

REMARQUE : L'aide en ligne des applications Security Center n'est pas disponible dans toutes les langues. Pour la liste des langues disponibles, voir les *Notes de version Security Center*.

CONSEIL : Après l'installation, vous pouvez modifier la langue de l'interface à tout moment à l'aide de l'*outil langue* disponible dans le sous-dossier Outils du groupe de programmes Genetec Security Center.

8 Sur la page *Règles de pare-feu*, sélectionnez l'option **Autoriser Genetec Security Center 5.5 à créer les règles de pare-feu nécessaires pour ses applications**, puis cliquez sur **Suivant**.

Cette option permet de configurer correctement les règles de sécurité du pare-feu Windows.

REMARQUE : Vous devez également configurer les ports Security Center sur le pare-feu de votre société après l'installation.

9 Sur la page *Réglages de sécurité*, configurez les options suivantes :

- **Activer l'authentification du Répertoire:** Sélectionnez cette option pour forcer toutes les applications client et serveur sur le poste actuel à valider le certificat d'identité du Répertoire avant de s'y connecter (désactivé par défaut).

  BONNE PRATIQUE : Si vous décidez d'activer l'authentification du Répertoire, il est recommandé d'utiliser un certificat émis par une autorité de certification (AC) de confiance. Sinon, l'utilisateur sera invité à confirmer l'identité du serveur de Répertoire lors de la première connexion au Répertoire.

  Pour en savoir plus sur l'authentification du Répertoire, voir le *Guide de l'administrateur Security Center*.

- **Désactiver l'authentification de base:** L'authentification de base des caméras est désactivée par défaut pour empêcher l'interception des identifiants des caméras lorsque l'Archiveur se connecte à une unité vidéo.

  IMPORTANT : Lorsque cette option est sélectionnée, les caméras qui ne prennent en charge que le mode authentification de base ne peuvent pas être utilisées avec Security Center.

  REMARQUE : Le cas échéant, vous pouvez configurer cette option individuellement pour chaque extension de fabricant de caméras dans Config Tool, dans l'onglet **Extensions** de l'Archiveur.

10 Sélectionnez **Je confirme que j'ai lu et compris les implications de l'activation de ces réglages de sécurité**, puis cliquez sur **Suivant**.

   Le **Programme d'installation de Genetec Security Center 5.4** est lancé et démarre l'installation.

11 Cliquez sur **Terminer**.

Lorsque vous avez terminé

Procédez de la manière suivante :

- Configurez les ports Security Center sur le pare-feu de votre société.

Ports utilisés par défaut par Security Center

Après l'installation de Security Center, vous devez vérifier que tous les ports utilisés sont ouverts sur votre pare-feu et redirigés si vous utilisez la traduction d'adresses réseau, afin que tous les composants de Security Center puissent communiquer correctement.

Durant l'installation de Security Center, vous avez pu autoriser Security Center à créer les règles de pare-feu nécessaires pour ses applications. Lorsque vous sélectionnez cette option, toutes les applications Security Center sont ajoutées en tant qu'exceptions dans le pare-feu Windows. Toutefois, vous devez malgré tout vérifier que tous les ports utilisés par Security Center sont bien ouverts.

Vous pouvez configurer des numéros de ports autres que les numéros utilisés par défaut.

Ports de communication communs

Le tableau suivant présente les ports utilisés par défaut par les applications Security Center :

Ordinateur	Entrant	Sortant	Utilisation du port
Serveur principal	TCP 5500		Demandes de connexion au Répertoire
Postes client (Security Desk et Config Tool)		TCP 5500	Demandes de connexion au Répertoire
Postes client (Config Tool)		TCP 443	Communication avec GTAP pour la validation de CMA/l'envoi de commentaires
Serveurs (nouvelle installation)	TCP 5500	TCP 5500	Communication avec les autres serveurs
	TCP 4502	TCP 4502	Rétrocompatibilité. Pour les connexions depuis les serveurs équipés de Security Center 5.3 ou antérieur.
	HTTP 80		Connexion par les Server Admin
serveurs (mis à niveau depuis la version 5.3 ou antérieure)	TCP 4502	TCP 4502	Si le port serveur 4502 était utilisé avant la mise à niveau, le port 4502 est conservé après la mise à niveau, et le port 4503 est utilisé pour la rétrocompatibilité. Si un autre port serveur était utilisé avant la mise à niveau, ce port est conservé après la mise à niveau, le port 4502 est utilisé pour la rétrocompatibilité, et le port 4503 n'est pas utilisé.
	TCP 4503	TCP 4503	
Gestionnaire de cartes	HTTP 8012		Communication avec les applications client pour le téléchargement des cartes.
Moniteur de disponibilité du système (SAMA)	TCP 4592		Connexion depuis les serveurs Security Center.
		TCP 443	Connexion au Health Service dans le nuage.

Ordinateur	Entrant	Sortant	Utilisation du port
Genetec[MC] Update Service (GUS)	TCP 4595	TCP 4595	Connexion depuis les applications Security Center et communication avec d'autres serveurs GUS.
		TCP 443	Connexion à Internet.

Ports Omnicast

Le tableau suivant présente les ports utilisés par défaut par les applications Omnicast dans Security Center.

Ordinateur	Entrant	Sortant	Utilisation du port
Archiveur	TCP 555		Demandes de flux en direct et enregistrés
	UDP 15000-20000[1]	UDP 15000-20000[1]	Flux audio et vidéo monodiffusés en direct
	TCP et UDP		Ports propres aux fabricants pour événements et découverte d'unités
	UDP 47806	UDP 47806	Flux audio et vidéo multidiffusés en direct
	UDP 47807	UDP 47807	Flux audio et vidéo multidiffusés en direct
		TCP 554 ou HTTP 80	Port généralement utilisé pour demander de la vidéo à une unité
	Telnet 5602		Demandes de connexion Telnet
Archiveur auxiliaire	TCP 558		Demandes de flux enregistrés
Routeur multimédia	TCP 554		Demandes de flux en direct et enregistrés
Redirecteur	TCP 560		Demandes de flux en direct et enregistrés
	UDP 8000-12000		Flux audio et vidéo monodiffusés en direct
	UDP 47806	UDP 47806	Flux audio et vidéo multidiffusés en direct
		TCP 555	Communication avec l'Archiveur
Routeur multimédia RTSP	TCP 654		Demandes de flux en direct et enregistrés
	UDP 51914	UDP 51914	Flux audio et vidéo multidiffusés en direct

Ordinateur	Entrant	Sortant	Utilisation du port
Fédération Omnicast	UDP 1024-2048		Security Desk lors du visionnement de vidéo provenant d'une fédération Omnicast dans Security Center
Postes client (Security Desk et Config Tool)	UDP 6000-6500		Flux audio et vidéo monodiffusés en direct
	UDP 47806		Flux vidéo en direct multidiffusés
	UDP 47807		Flux audio en direct multidiffusés
		TCP 554-560	Demandes de flux audio et vidéo en direct et enregistrés

[1]Vous pouvez avoir plusieurs agents Archiveur par serveur. Chaque agent Archiveur affecte un port UDP unique à chaque unité vidéo qu'il contrôle. Pour s'assurer que chaque port UDP sur un serveur est unique, chaque nouvel agent Archiveur sur un serveur ajoute 5000 à son numéro de port UDP de départ. Par exemple, le premier agent Archiveur utilise les ports 15000 à 20000, le second les ports 20000 à 25000, le troisième les ports 25000 à 30000, etc.

Ports Synergis

Le tableau suivant présente les ports utilisés par défaut par les applications Synergis dans Security Center.

Ordinateur	Entrant	Sortant	Utilisation du port
Gestionnaire d'accès	UDP/TCP 4070	UDP/TCP 4070	Contrôleurs HID VertX/Edge
			Contrôleurs HID VertX/Edge EVO
	TCP 20	TCP 21, 23	Contrôleurs HID VertX/Edge
		TCP 4050	Contrôleurs HID VertX/Edge
			Contrôleurs HID VertX/Edge EVO
		TCP 22	Contrôleurs HID VertX/Edge EVO
		TCP 2000	Port de découverte par défaut des unités Synergis (ce port peut être modifié dans Config Tool)

Le *port de découverte* d'une unité HID est fixe, à 4070. Une fois découverte, l'unité est affectée à un *Gestionnaire d'accès* qui utilise les ports indiqués dans le tableau ci-dessus pour la contrôler.

Pour en savoir plus sur la configuration initiale du matériel HID, téléchargez la documentation sur http://www.HIDglobal.com.

AutoVu^{MC}- ports

Le tableau suivant présente les ports utilisés par défaut par les applications AutoVu^{MC} dans Security Center.

Ordinateur	Entrant	Sortant	Utilisation du port
Gestionnaire RAPI		UDP 5000	Découverte des unités Sharp fixes
	TCP 8731		Unités Sharp fixes et Patroller
	TCP 8832		Patroller demandes de correctifs
	TCP 8787		Pay-by-Plate

Installer BeNomad

Si votre licence Security Center prend en charge la cartographie, vous pouvez utiliser la solution de cartographie par défaut *BeNomad* pour obtenir des informations de cartographie et de géolocalisation inversée.

À savoir

- Lorsque votre licence est créée, vous recevez un e-mail automatique avec un fichier zip qui contient les cartes BeNomad pour votre emplacement géographique, ainsi qu'un fichier *.glic* unique qui contient vos informations de licence. Ces deux fichiers sont nécessaires pour installer BeNomad.
- BeNomad doit également être installé sur tout poste client exécutant Security Desk.

Pour installer BeNomad :

1 Décompactez le contenu du fichier zip BeNomad sur votre ordinateur.

Un dossier nommé BeNomad est créé.

2 Copiez le dossier BeNomad dans le dossier principal du programme, où Security Center est installé. Pour une installation Security Center par défaut, il s'agit du dossier : *C:\Program Files (x86)\Genetec Security Center SR4*.

3 Copiez le fichier de licence *.glic* de l'e-mail vers le dossier *BeNomad*.

Les cartes *BeNomad* seront activées au démarrage de Security Center.

Désactiver la rétrocompatibilité

Les anciennes versions de Security Center (antérieures à la 5.4) ne prennent pas en charge le protocole. Par conséquent, leur prise en charge rend votre système plus vulnérable aux attaques en réseau. Pour renforcer la sécurité de votre système, vous pouvez désactiver la rétrocompatibilité.

À savoir

La rétrocompatibilité est activée par défaut à l'installation du système. Cette option s'applique à l'intégralité du système.

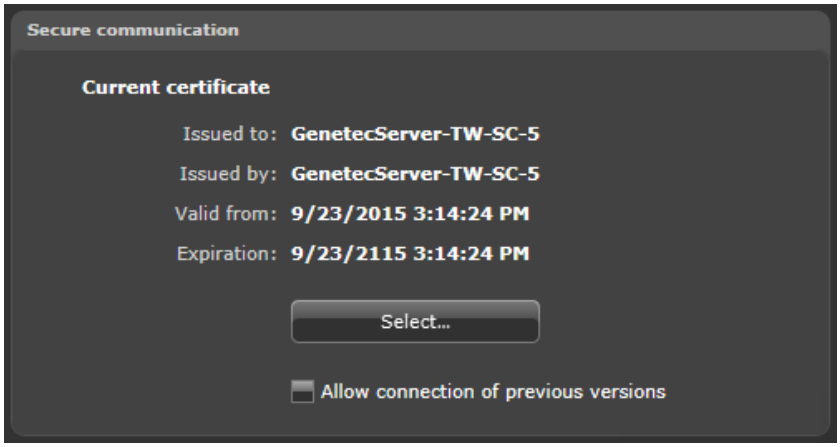
ATTENTION : Mobile Server 4.0 ne prend pas en charge le TLS. La désactivation de la rétrocompatibilité signifie que les apps mobiles et les clients web ne pourront plus se connecter à Security Center. Tous les serveurs d'extension qui n'ont pas encore été mis à niveau vers la version 5.5 cesseront également de fonctionner.

Pour désactiver la rétrocompatibilité :

1 Connectez-vous au Server Admin de votre serveur principal avec un navigateur web.

2 Cliquez sur le serveur principal ( ) dans la liste des serveurs.

3 Dans la section *Sécuriser les communications*, décochez l'option **Autoriser la connexion de versions antérieures**.



4 Cliquez sur **Enregistrer**

La rétrocompatibilité est désactivée. Les personnes qui essaieront de se connecter à votre système avec une ancienne application Security Center recevront le message d'erreur *Les versions client-serveur sont incompatibles*.

Désinstaller Security Center

Si vous voulez entièrement supprimer Security Center de votre système, dont toutes les données, réglages de configuration et archives vidéo, avant de le réinstaller, vous devez suivre une série d'étapes.

À savoir

ATTENTION : Si vous désinstallez une version précédente de Security Center Client et qu'un serveur Security Center 5.5 est installé sur le même ordinateur, le composant serveur est également désinstallé. Vous devrez réinstaller Security Center Server.

Pour désinstaller Security Center de votre système :

1 Dans Server Admin, sauvegardez la base de données Directory en cliquant sur **Sauvegarder/restaurer** dans la section Base de données de l'onglet **Répertoire**.

2 Sauvegardez la base de données de chaque rôle configuré au sein du système.

3 Fermez toutes les applications Security Center (Security Desk, Config Tool et Server Admin).

4 Sélectionnez **Démarrer** > **Panneau de configuration** > **Programmes et fonctionnalités**.

5 Dans la fenêtre *Programmes et fonctionnalités*, faites un clic droit sur **Genetec Security Center 5.5 Installer**, puis cliquez sur **Désinstaller**.

6 Dans la boîte de dialogue *Supprimer le programme*, cliquez sur **Supprimer**.

7 Lorsque le message **Désinstallation terminée** apparaît, cliquez sur **Terminer**.

Genetec Security Center 5.5, le programme d'installation et tous les packs de compatibilité Omnicast sont supprimés.

8 (Facultatif) Si vous ne souhaitez pas conserver les données de base de données, dont les archives vidéo, désinstallez SQL Server.

9 Dans le menu **Démarrer** de Windows, tapez `regedit`, puis appuyez sur **ENTRÉE**.

10 Dans l'*Éditeur du Registre*, exportez les clés suivantes pour les réutiliser en cas de besoin, puis supprimez-les du Registre.

- Sur les systèmes 32 bits : HKEY_LOCAL_MACHINE\SOFTWARE\Genetec
- Sur les systèmes 64 bits : HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Genetec

11 Faites une copie des dossiers suivants pour les réutiliser en cas de besoin, puis supprimez-les.

- Sur les systèmes 32 bits : C:\Program Files\Genetec Security Center 5.5
- Sur les systèmes 64 bits : C:\Program Files (x86)\Genetec Security Center 5.5
- Sur tous les systèmes :
  - C:\ProgramData\Genetec Security Center
  - C:\ProgramData\Genetec Security Center 5.5
  - C:\ProgramData\Genetec Update Service
  - C:\ProgramData\AppData\Local\Genetec Security Center 5.5
  - C:\Users\<username>\AppData\Local\Genetec Inc
  - C:\Users\<username>\AppData\Local\Genetec Security Center 5.5
  - C:\Users\<username>\AppData\Local\IsolatedStorage

    REMARQUE : Vous ne pourrez pas supprimer ce dossier s'il est utilisé par d'autres applications.

12 (Facultatif) Supprimez les archives vidéo (fichiers G64) créées par l'Archiveur.

IMPORTANT : Ne supprimez pas les archives vidéo si vous conservez la base de données de l'Archiveur.

Terminer le processus d'installation

Après l'installation de Security Center, vous pouvez effectuer une série de tâches pour vérifier l'état de bon fonctionnement de votre système.

Avant de commencer

Installez Security Center.

Pour terminer le processus d'installation :

1 Connectez-vous à Server Admin sur le serveur principal, et vérifiez les points suivants dans l'onglet **Directory** :
   - Directory est démarré.
   - Directory , la base de données est connectée.
   - La licence est activée et toutes les fonctionnalités sont confirmées.
   - Le numéro de CMA est confirmé avec date d'expiration.
   - La sauvegarde automatique de la base de données du Directory est activée et configurée.

2 Cliquez sur l'onglet **Genetec Server** et vérifiez les points suivants :
   - Les mots de passe d'Authentification et de Console sont définis.
   - La bonne carte réseau est sélectionnée.
   - Le serveur de messagerie est configuré (si nécessaire).

3 Connectez-vous à Server Admin sur chaque serveur d'extension et vérifiez les points suivants :
   - Le serveur d'extension est connecté au serveur principal.
   - La bonne carte réseau est sélectionnée.

4 Connectez-vous à Config Tool, ouvrez la **Vue réseau** et vérifiez les points suivants :
   - Tous les serveurs sont en ligne et ne présentent pas de dysfonctionnements.
   - Le bon protocole réseau est utilisé en fonction des capacités du réseau.
   - Les adresses publiques sont configurées correctement.

5 Ouvrez la tâche **Système**, puis cliquez sur la **Rôles**

6 Pour chaque rôle Security Center, vérifiez les points suivants :
   - Le rôle est en ligne sans dysfonctionnements (il n'est pas affiché en jaune).
   - La base de données du rôle est connectée.
   - La sauvegarde automatique de la base de données du rôle est configurée (si nécessaire).
   - La bonne carte réseau est sélectionnée pour le rôle, et dans le cas du Media Router, pour chaque redirecteur.

7 Ouvrez la tâche **Gestion des utilisateurs**, et vérifiez les points suivants :
   - Les groupes d'utilisateurs et partitions sont configurés conformément au cahier des charges de déploiement.
   - Un mot de passe est configuré pour l'utilisateur *Admin*.
   - Les partitions utilisées sont configurées conformément au cahier des charges de déploiement.

8 Vérifiez que vous parvenez à vous connecter à Security Center depuis Security Desk.

9 Sur le serveur, vérifiez les points suivants :
   - Le disque de stockage dispose de suffisamment d'espace libre.

- L'indexation du stockage Windows est désactivé sur tous les disques qui serviront à l'archivage vidéo.
- L'ordre des cartes réseau affiché dans les réglages de *Cartes et liaisons* est correct.
- Les cartes réseau inutilisées sont désactivées.
- Le serveur n'est pas un contrôleur de domaine.
- Windows Update n'est pas configuré pour redémarrer automatiquement le serveur après l'installation de mises à jour.
- L'horloge Windows est synchronisée à une source d'heure.
- Aucune application indésirable n'est lancée.
- Aucun blocage ou redémarrage n'est indiqué dans l'Observateur d'événements Windows.
- L'antivirus système est bien configuré (si nécessaire) et toutes les exclusions sont spécifiées.

Lorsque vous avez terminé

Selon les besoins de votre déploiement, configurez les fonctions suivantes de votre système :

- Vidéosurveillance
- Contrôle d'accès
- Reconnaissance de plaques d'immatriculation

Pour en savoir plus sur le déploiement du système, voir le *Guide de l'administrateur Security Center*.

Pour plus d'information sur comment améliorer la sécurity de votre système Genetec[MC] Security Center, voir le Security Center Hardening Guide.

2

Mise à niveau vers Security Center 5.5

Cette section aborde les sujets suivants:

Mises à niveau prises en charge d'une version antérieure de Security Center

Il est important de savoir quelles anciennes versions de Security Center peuvent être mises à niveau vers Security Center 5.5 SR4.

La mise à niveau en une étape est prise en charge pour les versions suivantes de Security Center :

- Security Center 5.2 GA/SR2/SR3/SR4/SR5/SR6/SR7/SR8/SR9/SR10/SR11
- Security Center 5.3 GA/SR1/SR2/SR3/SR4
- Security Center 5.4 GA/SR2/SR3
- Security Center 5.5 GA/SR1/SR2/SR3/SR4

Security Center 5.1 et les versions antérieures nécessitent une mise à niveau en deux étapes.

Préparer la mise à niveau d'une ancienne version de Security Center 5.5

Si vous devez mettre à jour une version plus ancienne de Security Center vers la version 5.5 SR4 , vous devez effectuer les étapes de préparation suivantes :

À savoir

Pour préparer la mise à niveau d'une ancienne version de Security Center vers la version 5.5 SR4 :

- Vous devez disposer des informations suivantes :
  - Le nom d'utilisateur et mot de passe de connexion au service pour tous vos serveurs.
  - Le nom du serveur de bases de données qui gère la base de données du Répertoire.

  Vous devrez saisir à nouveau ces valeurs à l'installation de Security Center Server 5.5 SR4 .

Préparer la mise à niveau de Security Center 5.4 vers 5.5

Pour mettre à niveau votre système 5.4 vers la 5.5, vous devez préparer les éléments suivants.

À savoir

- Différentes versions de Security Center Client peuvent coexister sur un même ordinateur, contrairement à différentes versions de Security Center Server. Tous les réglages actuels ne sont pas conservés lorsque vous désinstallez la version actuelle avant l'installation de la nouvelle version.
- Si le rôle Active Directory ne se trouve pas sur le même domaine que le domaine Active Directory avec lequel il est synchronisé, vous devez configurer une relation d'approbation de domaine. Pour plus d'informations sur la configuration de relations d'approbation de domaine, reportez-vous à votre documentation Microsoft.

Pour préparer la mise à niveau de Security Center 5.4 vers la 5.5 :

1 Si vous utilisez Windows Server 2008, Windows 7 ou Windows Server 2008 R2, vous devez installer Microsoft hotfix KB2588507.

REMARQUE : Ce correctif n'est pas requis pour les Appareils SV.

2 Si vous utilisez Windows 7, Windows 8, Windows 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 ou Windows Server 2012 R2, vous devez installer Microsoft hotfix KB2999226.

3 Si vous utilisez Microsoft SQL Server 2005, installez une version plus récente du serveur de base de données.

Security Center 5.5 n'est pas compatible avec Microsoft SQL Server 2005.(voir la configuration système requise pour la liste des versions compatibles).

4 Si votre système actuel comprend un rôle Active Directory, vérifiez impérativement avant d'effectuer la mise à niveau que l'utilisateur Windows configuré pour la connexion à Windows dispose d'un accès en écriture au champ *accountExpires*.

À compter de Security Center 5.2 SR6, un nouvel attribut standard Windows Active Directory (*accountExpires*) est utilisé par le rôle Active Directory pour importer les utilisateurs et titulaires de cartes dans Security Center. Le nouvel attribut définit une date d'expiration des titulaires de cartes importés dans Security Center, et règle l'état des utilisateurs importés sur inactif à la date d'échéance spécifiée.

ATTENTION : Si l'utilisateur Windows n'a pas un accès en écriture à l'attribut *accountExpires*, tous les titulaires de cartes et identifiants déjà importés depuis Windows Active Directory sont supprimés lors de la première synchronisation de Security Center avec Windows Active Directory après la mise à niveau.

Préparer la mise à niveau de Security Center 5.3 vers 5.5

Pour mettre à niveau votre système 5.3 vers la 5.5, vous devez préparer les éléments suivants.

À savoir

- Différentes versions de Security Center Client peuvent coexister sur un même ordinateur, contrairement à différentes versions de Security Center Server. Tous les réglages actuels ne sont pas conservés lorsque vous désinstallez la version actuelle avant l'installation de la nouvelle version.
- Si le rôle Active Directory ne se trouve pas sur le même domaine que le domaine Active Directory avec lequel il est synchronisé, vous devez configurer une relation d'approbation de domaine. Pour plus d'informations sur la configuration de relations d'approbation de domaine, reportez-vous à votre documentation Microsoft.

Pour préparer la mise à niveau de Security Center 5.3 vers la 5.5 :

1 Si vous utilisez Windows Server 2008, Windows 7 ou Windows Server 2008 R2, vous devez installer Microsoft hotfix KB2588507.

REMARQUE : Ce correctif n'est pas requis pour les Appareils SV.

2 Si vous utilisez Windows 7, Windows 8, Windows 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 ou Windows Server 2012 R2, vous devez installer Microsoft hotfix KB2999226.

3 Si vous utilisez Microsoft SQL Server 2005, installez une version plus récente du serveur de base de données.

Security Center 5.5 n'est pas compatible avec Microsoft SQL Server 2005.(voir la configuration système requise pour la liste des versions compatibles).

4 Si votre système actuel comprend un rôle Active Directory, vérifiez impérativement avant d'effectuer la mise à niveau que l'utilisateur Windows configuré pour la connexion à Windows dispose d'un accès en écriture au champ *accountExpires*.

À compter de Security Center 5.2 SR6, un nouvel attribut standard Windows Active Directory (*accountExpires*) est utilisé par le rôle Active Directory pour importer les utilisateurs et titulaires de cartes dans Security Center. Le nouvel attribut définit une date d'expiration des titulaires de cartes importés dans Security Center, et règle l'état des utilisateurs importés sur inactif à la date d'échéance spécifiée.

ATTENTION : Si l'utilisateur Windows n'a pas un accès en écriture à l'attribut *accountExpires*, tous les titulaires de cartes et identifiants déjà importés depuis Windows Active Directory sont supprimés lors de la première synchronisation de Security Center avec Windows Active Directory après la mise à niveau.

Préparer la mise à niveau de Security Center 5.2 vers 5.5

Pour mettre à niveau votre système 5.2 vers la 5.5, vous devez préparer les éléments suivants.

À savoir

- Différentes versions de Security Center Client peuvent coexister sur un même ordinateur, contrairement à différentes versions de Security Center Server. Tous les réglages actuels ne sont pas conservés lorsque vous désinstallez la version actuelle avant l'installation de la nouvelle version.
- Si le rôle Active Directory ne se trouve pas sur le même domaine que le domaine Active Directory avec lequel il est synchronisé, vous devez configurer une relation d'approbation de domaine. Pour plus d'informations sur la configuration de relations d'approbation de domaine, reportez-vous à votre documentation Microsoft.

Pour préparer la mise à niveau de Security Center 5.2 vers la 5.5 :

1 Si vous utilisez Windows Server 2008, Windows 7 ou Windows Server 2008 R2, vous devez installer Microsoft hotfix KB2588507.

REMARQUE : Ce correctif n'est pas requis pour les Appareils SV.

2 Si vous utilisez Windows 7, Windows 8, Windows 8.1, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 ou Windows Server 2012 R2, vous devez installer Microsoft hotfix KB2999226.

3 Si vous utilisez Microsoft SQL Server 2005, installez une version plus récente du serveur de base de données.

Security Center 5.5 n'est pas compatible avec Microsoft SQL Server 2005.(voir la configuration système requise pour la liste des versions compatibles).

4 Si votre système actuel comprend un rôle Active Directory, vérifiez impérativement avant d'effectuer la mise à niveau que l'utilisateur Windows configuré pour la connexion à Windows dispose d'un accès en écriture au champ *accountExpires*.

À compter de Security Center 5.2 SR6, un nouvel attribut standard Windows Active Directory (*accountExpires*) est utilisé par le rôle Active Directory pour importer les utilisateurs et titulaires de cartes dans Security Center. Le nouvel attribut définit une date d'expiration des titulaires de cartes importés dans Security Center, et règle l'état des utilisateurs importés sur inactif à la date d'échéance spécifiée.

ATTENTION : Si l'utilisateur Windows n'a pas un accès en écriture à l'attribut *accountExpires*, tous les titulaires de cartes et identifiants déjà importés depuis Windows Active Directory sont supprimés lors de la première synchronisation de Security Center avec Windows Active Directory après la mise à niveau.

Différences entre Server Admin 5.x et 5.5

À compter de Security Center 5.5, Server Admin est doté d'une interface utilisateur entièrement repensée qui fonctionne sur tous les navigateurs (sur ordinateurs et appareils mobiles), prend en charge les connexions multi-serveur et gère les connexions sécurisées (HTTPS).

Caractéristiques	Server Admin 5.4 et versions antérieures	Server Admin 5.5 et ultérieur
Navigateurs pris en charge	Internet Explorer 8, 9, 10 et 11. Le module externe Microsoft Silverlight doit être installé.	• Internet Explorer 9, 10, et 11 • Chrome 46 (ou ultérieur) • Firefox 42 (ou ultérieur) • Safari 9 (ou ultérieur) Microsoft Silverlight n'est plus nécessaire.
URL de connexion	`http://<serveur>/Genetec` où `<serveur>` est le nom DNS ou l'adresse IP du serveur.	`https://<serveur>/Genetec` où `<serveur>` est le nom DNS ou l'adresse IP du serveur.
Connexion multi-serveur	Non. Se connecte à un serveur à la fois.	Oui. Affiche tous les serveurs du système, et vous permet d'afficher et de modifier les réglages de chacun d'eux.
Aperçu de l'état du système	Affiché dans l'onglet **Répertoire**. Seulement visible lorsque Server Admin est connecté au serveur principal.	Affiché sur le tableau de bord. Trois témoins LED de couleur indiquent en permanence l'état du système : **Base de données**, **Répertoire** et **Licence**. Cliquez sur une erreur pour basculer vers la section qui permet de résoudre le problème.
Configuration globale	Non. Chaque serveur doit être configuré séparément.	Oui. Les réglages globaux comme le mot de passe serveur, Watchdog et les réglages SMTP sont appliqués à tous les serveurs.
Redémarrer le service Genetec Server	Non.	Oui.
Langue de l'interface utilisateur	Définie avec *l'outil langue*. Le service Genetec Server doit être redémarré et la page web doit être actualisée.	Commande dans Server Admin. Inutile de redémarrer ou d'actualiser quoi que ce soit.
Choisir un thème visuel	Non.	Choix entre un habillage **Sombre** (par défaut) et **Clair**.
Vérifier la version logicielle	Sur la page d'accueil de Config Tool, cliquez sur le bouton  .	Cliquez sur **À propos**.

Caractéristiques	Server Admin 5.4 et versions antérieures	Server Admin 5.5 et ultérieur
Désactiver le Répertoire	1 Connectez Server Admin au serveur principal. 2 Dans l'onglet **Répertoire**, cliquez sur **Désactiver le Répertoire**.	Dans la liste de serveurs à gauche, sélectionnez le serveur principal ( ), puis cliquez sur **Actions** > **Désactiver**.
Activer le Répertoire	1 Connecter Server Admin à un serveur d'extension. 2 Dans l'onglet **Genetec Server**, cliquez sur **Activer le Répertoire**.	Dans la liste de serveurs à gauche, sélectionnez le serveur d'extension, puis cliquez sur **Actions** > **Activer**.
Console de débogage[1]	Non intégrée à Server Admin.	Intégrée à Server Admin, avec de nombreuses améliorations.
Accès à la console de débogage	Peut être désactivé et protégé par mot de passe pour chaque serveur.	La console de débogage adopte le mot de passe de Server Admin, et ne peut pas être désactivée séparément.

[1] La console de débogage est réservée aux ingénieurs de l'assistance technique de Genetec[MC].

Différences entre les partitions dans Security Center 5.x et 5.5

À compter de Security Center 5.3, le modèle de partition a changé, ce qui affecte l'utilisation et la configuration des partitions.

Le tableau suivant résume les modifications apportées aux partitions dans Security Center 5.3 ou ultérieur :

REMARQUE : Pour en savoir plus sur la création et la configuration des partitions dans Security Center 5.5, voir le *Guide de l'administrateur Security Center*.

	Security Center 5.0, 5.1 ou 5.2	Security Center 5.3 et ultérieur
Terminologie	• Utilisateurs autorisés • Gestionnaire de partition	• Utilisateurs autorisés • Administrateur de partition
Configuration de la sécurité	Tâche *Sécurité* : Permet de configurer les utilisateurs, groupes d'utilisateurs et partitions dans trois onglets distincts.	Tâche *Gestion des utilisateurs* : Permet de configurer les utilisateurs, groupes d'utilisateurs et partitions dans une même arborescence d'entités.
Configuration des partitions	• Ne peuvent être créées que dans l'onglet **Partitions** de la tâche *Sécurité* dans Config Tool. • Les partitions sont toujours affichées dans l'onglet **Partitions** de la tâche *Sécurité* dans Config Tool. • Le contenu d'une partition ne peut être modifié que dans l'onglet **Propriétés** de la partition.	• Peut être créée à partir de n'importe quelle tâche d'administration qui affiche une arborescence d'entités. • Les utilisateurs peuvent choisir d'afficher ou de masquer les partitions dans n'importe quelle tâche d'administration en cliquant sur **Afficher les partitions** ( ) dans le champ de **Recherche**. Les partitions sont entièrement masquées lorsqu'aucune partition n'a été créée par les utilisateurs. • Le contenu des partitions peut être directement modifié dans n'importe quelle arborescence d'entités par glisser-déposer des entités vers les partitions auxquelles les entités doivent appartenir.

	Security Center 5.0, 5.1 ou 5.2	Security Center 5.3 et ultérieur
Configuration des droits d'accès aux partitions	• Les droits d'accès des utilisateurs aux partitions sont configurés dans l'onglet **Utilisateurs autorisés** de chaque entité partition. • Les droits d'accès sont hérités implicitement des groupes d'utilisateurs parents. Les membres d'un groupe d'utilisateurs ont accès à la partition, même s'ils n'apparaissent pas dans l'onglet **Utilisateurs autorisés**. • Les droits d'accès accordés à une partition parent sont également accordés aux partitions enfants.	• Les droits d'accès des utilisateurs aux partitions sont configurés dans l'onglet *Droits d'accès* de chaque entité utilisateur et groupe d'utilisateurs. • Les droits d'accès sont explicitement hérités des groupes d'utilisateurs parents et son clairement visibles dans l'onglet *Droits d'accès* des utilisateurs individuels. • Les droits d'accès accordés à une partition parent sont également accordés aux partitions enfants, mais peuvent être révoqués au cas par cas.
Configuration de l'appartenance aux partitions	• Une entité donnée ne peut pas appartenir à plus de trois partitions. • Il n'existe pas de règles gouvernant l'appartenance des entités associées aux partitions. L'appartenance de chaque entité à une partition doit être définie individuellement. Par exemple, l'ajout d'un groupe de titulaires de cartes à une partition n'ajoute pas automatiquement les membres du groupe à la partition.	• Une entité peut appartenir à un nombre de partitions illimité. • Le système applique automatiquement un ensemble de règles basées sur des pratiques courantes concernant l'appartenance des entités associées aux partitions. Par exemple, l'ajout d'un groupe de titulaires de cartes à une partition ajoute automatiquement les membres du groupe à la partition. L'administrateur de la partition peut ensuite modifier les appartenances au cas par cas.

	Security Center 5.0, 5.1 ou 5.2	Security Center 5.3 et ultérieur

Partition publique	• Tous les utilisateurs peuvent voir les entités de la *Partition publique* dans les listes d'entités, y compris les utilisateurs non autorisés.
	• Seuls les utilisateurs autorisés dotés de droits d'administration peuvent afficher les propriétés des entités de la *Partition publique*.
	• La *Partition publique* ne peut pas être renommée ou supprimée.
		• La *Partition publique* n'existe plus.
		• Lorsque les partitions ne sont pas nécessaires, la partition *racine* (nommée d'après le *serveur principal*) contient tout ce que vous créez, et est accessible par défaut à tous les utilisateurs.
		• Lorsque vous faites la mise à niveau d'un système qui contient plusieurs partitions vers la version 5.5, la *Partition publique* est migrée, sachant que les caractéristiques de la *Partition publique* dans la version 5.5 sont différentes.
		  • Les utilisateurs qui n'étaient pas des utilisateurs autorisés de la *Partition publique* dans la version 5.0, 5.1 ou 5.2 n'auront aucun accès à la *Partition publique* dans la version 5.5.
		  • Vous pouvez renommer, modifier et supprimer la *Partition publique* dans la version 5.5.

Partition *Système*	• La partition *Système* est une partition masquée dont la caractéristique est que seuls les administrateurs peuvent accéder à son contenu. • Les entités qui n'appartiennent pas à une partition créée par un utilisateur appartiennent à la partition *Système*.	• La partition *Système* contient toutes les entités auxquelles tous les utilisateurs doivent pouvoir accéder à tout moment. Par exemple, l'horaire *Toujours*, le rôle *Surveillance de l'état* et le rôle *Routeur multimédia* appartiennent tous à la partition *Système*. • La partition *Système* est gérée exclusivement par le système. Elle n'est pas modifiable, même par les administrateurs. • Les entités qui n'appartiennent pas à une partition créée par un utilisateur appartiennent à la partition *racine*.

Mettre à niveau la partition publique de 5.x vers 5.4

Après la mise à niveau d'un système Security Center 5.0, 5.1 ou 5.2 qui utilise plusieurs partitions vers la 5.4, vous devrez parfois accorder des droits d'accès à la *Partition publique* à certains utilisateurs pour qu'ils disposent de tous les droits d'accès nécessaires sous la 5.4. Cela ne concerne pas les mises à niveau de la 5.3 vers la 5.4.

Avant de commencer

- Mettre à niveau Security Center Server vers la 5.4.
- Mettre à niveau Security Center Client vers la 5.4.

À savoir

Si la *Partition publique* est la seule partition du système précédent, tout est migré vers la partition *racine* sous 5.4, et les partitions sont masquées. Si le système précédent utilisait d'autres partitions, la *Partition publique* est migrée avec les différences suivantes :

- Les utilisateurs qui n'étaient pas des utilisateurs autorisés de la *Partition publique* dans la version 5.x n'auront aucun accès à la *Partition publique* dans la version 5.4.
- Vous pouvez renommer, modifier et supprimer la *Partition publique* dans la version 5.4.

Pour que tous les utilisateurs disposent des droits d'accès nécessaires après une mise à niveau de la 5.x vers la 5.4 :

1 Identifiez les utilisateurs et groupes d'utilisateurs qui doivent référencer des entités situées dans la *Partition publique* et qui ne sont pas des utilisateurs autorisés de cette partition.

Exemple: Vous aurez parfois des entités horaire dans la *Partition publique* que seuls les administrateurs peuvent modifier. D'autres utilisateurs peuvent avoir besoin d'accéder à ces horaires pour configurer des règles d'accès ou la détection de mouvement sur les caméras. Sur un système 5.0, 5.1 ou 5.2, ces utilisateurs n'ont pas besoin d'être des utilisateurs acceptés de la *Partition publique*, ce qui n'est pas le cas sur un système 5.4.

Si votre système n'a pas d'utilisateurs de ce type, aucune intervention supplémentaire n'est requise.

2 Ouvrez la tâche *Gestion des utilisateurs*.

3 Créez un groupe d'utilisateurs, nommez-le *UtilisateursPartitionPublique* (ou tout autre nom facile à mémoriser), et accordez-lui les droits d'accès à la *Partition publique*.

Ne créez pas ce groupe d'utilisateurs sous un groupe parent, et ne lui accordez pas de privilèges.

4 Cliquez sur l'onglet **Propriétés** du groupe et ajoutez les utilisateurs et groupes d'utilisateurs qui doivent pouvoir référencer les entités situées dans la *Partition publique* que vous avez identifiés plus tôt.

5 Cliquez sur **Appliquer**.

Configuration requise pour la rétrocompatibilité de Security Center

Security Center 5.5 SR4 est rétrocompatible avec de nombreux composants Security Center 5.x, ce qui signifie que vous pouvez mettre à niveau votre système Security Center en plusieurs étapes.

Voici la configuration requise pour la rétrocompatibilité de Security Center :

- **Mettre à niveau vers la dernière version:** Lors de la mise à niveau, vous devez toujours mettre à niveau le serveur principal qui héberge le rôle Directory et Config Tool. Vous devez toujours mettre à niveau tout serveur d'extension qui héberge un type de rôle qui n'est pas rétrocompatible.
- **Utiliser les nouvelles fonctionnalités:** Pour utiliser les nouveautés de la version 5.5 SR4, faites la mise à niveau de vos serveurs Security Center.
- **Rôle affecté à plusieurs serveurs:** Lorsqu'un rôle est affecté à plusieurs serveurs, comme pour la configuration du basculement, tous ses serveurs doivent exécuter la même version de Security Center.
- **Répertoire affecté à plusieurs serveurs:** Tous les serveurs de Répertoire doivent utiliser exactement la même version du logiciel. Par exemple, si vous faites la mise à niveau vers Security Center 5.5 SR4, vous devez mettre à niveau tous vos serveurs de Répertoire vers la 5.5 SR4.
- **SQL Server:** Security Center 5.5 n'est pas compatible avec Microsoft SQL Server 2005, et vous devez donc installer une version plus récente du serveur de base de données (voir la configuration système requise pour la liste des versions compatibles). Pour en savoir plus sur comment mettre à jour votre SQL Server, consultez la documentation de Microsoft.

IMPORTANT : L'ajout de connexions rétrocompatibles ralentit les performances du Répertoire, et n'est donc conseillé qu'à titre temporaire, tant que vous n'avez pas mis à niveau tous les postes et serveurs.

Rétrocompatibilité des rôles Security Center

Chaque nouvelle version de Security Center 5.5 inclut des nouvelles fonctionnalités de rôles, compatibles ou non avec les versions précédentes des mêmes rôles. Les rôles Security Center rétrocompatibles sont répertoriés dans le tableau suivant.

IMPORTANT : Tout serveur d'extension qui héberge un rôle qui n'est pas rétrocompatible doit être mis à niveau vers la même version que celle du serveur principal qui héberge le Directory.

5.5 rôle	Rétrocompatible avec les versions 5.3 à 5.4
Gestionnaire d'accès	Oui
Active Directory	Non
Archiveur	Oui
Archiveur auxiliaire	Oui
Gestionnaire de Répertoire	Non
Synchroniseur de titulaires de cartes globaux	Oui
Surveillance de l'état	Non
Gestionnaire d'intrusions	Oui

5.5 rôle	Rétrocompatible avec les versions 5.3 à 5.4
Gestionnaire RAPI	Oui
Routeur multimédia	Non
Fédération Omnicast	Oui
Module externe (toutes les instances)	Non
Point de vente	Non
Gestionnaire de rapports	Oui
Routeur multimédia RTSP	Oui
Security Center Federation[MC]	Oui
Gestionnaire de zones	Oui

Rétrocompatibilité des tâches Security Center

Les tâches Security Center 5.5 rétrocompatibles avec Security Desk 5.3 et 5.4 sont répertoriées dans le tableau suivant.

Catégorie de tâche	Type de tâche	Rétrocompatible avec Security Desk 5.3 à 5.4
Exploitation	Surveillance[a]	Oui
	Gestion des titulaires de cartes	Oui
	Gestion des visiteurs	Oui
	Comptage d'individus	Oui
	Gestion des identifiants	Oui
	Éditeur de permis et de liste de véhicules recherchés	Oui
	Gestion d'inventaire	Oui
	Distant	Non
Gestion des alarmes	Surveillance d'alarmes	Oui
	Rapport d'alarmes	Oui
Investigation	Incidents	Oui
	Transactions	Non
	Activités de zones	Oui

Catégorie de tâche	Type de tâche	Rétrocompatible avec Security Desk 5.3 à 5.4
Investigation > Contrôle d'accès	Activités de secteurs	Oui
	Activités de portes	Oui
	Activités de titulaires de cartes	Oui
	Activités de visiteurs	Oui
	Présence dans un secteur	Oui
	Présence	Oui
	Activités d'identifiants	Oui
	Historique de demande d'identifiants	Oui
	Activités d'ascenseurs	Oui
	Détails de visite	Oui
Investigation > Gestion des actifs	Activités d'actifs	Non
	Inventaire d'actifs	Non
Investigation > Détection d'intrusion	Activités de secteurs de détection d'intrusion	Oui
	Événements d'unités de détection d'intrusion	Oui
Investigation > RAPI	Alertes	Oui
	Alertes (multi-région)	Oui
	Lectures	Oui
	Lectures (multi-région)	Oui
	Lecture d'itinéraire (5.2 et antérieur)	Oui
	Pistage Patroller (5.3 et antérieur)	Oui
	Rapport d'inventaire	Oui
	Utilisation quotidienne par Patroller	Oui
	Connexions par Patroller	Oui
	Lectures/alertes par jour	Oui
	Lectures/alertes par zone	Oui

Catégorie de tâche	Type de tâche	Rétrocompatible avec Security Desk 5.3 à 5.4
	Occupation par zone	Oui
Investigation > Vidéo	Archives	Oui
	Signets	Oui
	Recherche de mouvement	Oui
	Événements de caméra	Oui
	Recherche analytique	Oui
Maintenance	État du système	Oui
	Historiques de configuration	Oui
	Historiques d'activité	Oui
	Rapport d'état	Oui
	Statistiques de fonctionnement	Oui
	Inventaire matériel	Oui
Maintenance > Contrôle d'accès	Rapport d'état de contrôle d'accès	Oui
	Événements d'unité de contrôle d'accès	Oui
	Droits d'accès de titulaire de cartes	Oui
	Diagnostic de porte	Oui
	Configuration de règle d'accès	Oui
	Configuration de titulaires de cartes	Oui
	Configuration d'identifiants	Oui
	Configuration d'E/S	Oui
Maintenance > Vidéo	Configuration des caméras	Oui
	Événements d'Archiveur	Oui
	Détails de stockage d'archive	Oui

[a]Comprend la vidéo en temps réel et enregistrée.

Fédérations prises en charge pour Security Center5.5 SR4

Security Center 5.5 SR4 peut fédérer et être fédéré avec d'autres systèmes Security Center exécutant des versions différentes.

Security Center 5.5 peut fédérer ce qui suit :

- Security Center Systèmes 5.5, 5.4, 5.3 et 5.2.
- Omnicast^{MC} Systèmes 4.6, 4.7 et 4.8.
- Stratocast^{MC} Systèmes 1.7.

Security Center 5.5 peut être fédéré par les systèmes suivants :

- Security Center Systèmes 5.4 et 5.5.

IMPORTANT : En règle générale, un système qui exécute la dernière version de Security Center peut :

- Fédérer les systèmes jusqu'à trois versions antérieures.
- Être fédéré par un système exécutant la version précédente de Security Center.

  Par exemple, les systèmes Security Center 5.5 peuvent fédérer Security Center 5.4, 5.3 et 5.2. Un système Security Center 5.3 ne peut fédérer qu'un système 5.4, pas un système 5.5.

Pour en savoir plus sur les limitations des entités fédérées, voir la section *À propos des entités fédérées* du *Guide de l'administrateur Security Center*. Ces limitations s'appliquent tant aux fédérations ascendantes que descendantes.

Mettre à niveau une version plus ancienne de Security Center 5.5

Pour disposer de la dernière version de Security Center 5.5, vous pouvez mettre à niveau une ancienne version de 5.5 vers la SR4 une fois que vous avez effectué les étapes préparatoires.

Avant de commencer

- Prenez connaissance de ce que vous devez savoir et faire avant la mise à niveau.
- Sauvegardez les bases de données du Répertoire et des autres rôles.

À savoir

Vous ne devez pas modifier votre licence lorsque vous effectuez la mise à niveau d'une ancienne version du même produit Security Center.

Les précédents choix d'installation, comme la langue et les types d'installation, sont conservés et l'Assistant InstallShield ne vous les proposera pas.

Pour effectuer la mise à niveau d'une ancienne version de Security Center vers la version 5.5 SR4 :

1 Installez Security Center 5.5 SR4 sur le serveur principal.
2 Installez Security Center 5.5 SR4 sur vos serveurs d'extension, en fonction de vos priorités.
3 Installez Security Center Client 5.5 SR4 sur vos postes client, en fonction de vos priorités.

Lorsque vous avez terminé

Si vous avez utilisé le fichier *AllowedSynchronizationConfiguration.xml* pour configurer les horaires de synchronisation de vos unités HID VertX, vous devez les appliquer à nouveau manuellement dans Config Tool après la mise à niveau.

CONSEIL : Configurez les réglages de synchronisation sur une unité, puis utilisez l'outil *Copy configuration tool* pour définir les mêmes réglages sur plusieurs unités à la fois.

Mise à niveau de Security Center 5.4 vers 5.5

Pour disposer de la dernière version de Security Center, vous pouvez mettre à niveau votre système 5.4 vers la 5.5 une fois que vous avez effectué les étapes préparatoires.

Avant de commencer

- Prenez connaissance de ce que vous devez savoir et faire avant la mise à niveau.
- Prenez connaissance de la rétrocompatibilité.

À savoir

Pour les chemins de mise à niveau pris en charge, voir les *Notes de version Security Center*.

Pour effectuer la mise à niveau de Security Center 5.4 vers la 5.5 :

1 Si votre ancien système Security Center fédérait des systèmes Omnicast, désinstallez les packs de compatibilité installés.

2 Faites la mise à niveau du serveur principal.

3 Faites la mise à niveau des serveurs d'extension et postes de travail de votre système en fonction de vos priorités.

Si Security Center Client et Server sont installés sur un même poste, faites leur mise à niveau en même temps.

IMPORTANT : Veillez à noter puis à appliquer les mêmes réglages que pour l'ancienne installation : mots de passe, base de données, ports, propriétés générales, etc..

Lorsque vous avez terminé

Si le fichier *AllowedSynchronizationConfiguration.xml* était utilisé pour configurer les horaires de synchronisation d'unités HID VertX, les réglages doivent être appliqués à nouveau manuellement dans Config Tool après la mise à niveau.

CONSEIL : Configurez les réglages de synchronisation sur une unité, puis utilisez l'Copy configuration tool pour définir les mêmes réglages sur plusieurs unités à la fois.

Mise à niveau de Security Center 5.3 vers 5.5

Pour disposer de la dernière version de Security Center, vous pouvez mettre à niveau votre système 5.3 vers la 5.5 une fois que vous avez effectué les étapes préliminaires.

Avant de commencer

- Prenez connaissance de ce que vous devez savoir et faire avant la mise à niveau.
- Prenez connaissance de la rétrocompatibilité.

À savoir

Pour les chemins de mise à niveau pris en charge, voir les *Notes de version Security Center*.

Pour effectuer la mise à niveau de Security Center 5.3 vers la 5.5 :

1 Si votre ancien système Security Center fédérait des systèmes Omnicast, désinstallez les packs de compatibilité installés.

2 Faites la mise à niveau du serveur principal.

3 Faites la mise à niveau des serveurs d'extension et postes de travail de votre système en fonction de vos priorités.

Si Security Center Client et Server sont installés sur un même poste, faites leur mise à niveau en même temps.

IMPORTANT : Veillez à noter puis à appliquer les mêmes réglages que pour l'ancienne installation :mots de passe, bases de données, ports, propriétés générales, etc.

Lorsque vous avez terminé

Si vous avez utilisé le fichier *AllowedSynchronizationConfiguration.xml* pour configurer les horaires de synchronisation de vos unités HID VertX, vous devez les appliquer à nouveau manuellement dans Config Tool après la mise à niveau.

CONSEIL : Configurez les réglages de synchronisation sur une unité, puis utilisez l'outil *Copy configuration tool* pour définir les mêmes réglages sur plusieurs unités à la fois.

Mise à niveau de Security Center 5.2 vers 5.5

Pour disposer de la dernière version de Security Center, vous pouvez mettre à niveau votre système 5.2 vers la 5.5 une fois que vous avez effectué les étapes préliminaires.

Avant de commencer

- Prenez connaissance de ce que vous devez savoir et faire avant la mise à niveau.
- Prenez connaissance de la rétrocompatibilité.
- Prenez connaissances des différences entre les partitions dans Security Center 5.x et 5.4.

À savoir

Pour les chemins de mise à niveau pris en charge, voir les *Notes de version Security Center*.

Si votre ancien système n'avait pas de partitions hormis la *Partition publique*, toutes les entités sont déplacées vers la partition *racine* après la mise à niveau vers la 5.5, et toutes les partitions sont masquées. Tous les utilisateurs auront accès à la partition *racine*.

Si votre ancien système utilisait des partitions en plus de la *Partition publique*, les anciennes partitions sont migrées vers la 5.5 avec les mêmes contenus et les mêmes membres (appelés *utilisateurs autorisés* dans la version 5.5). Les règles suivantes s'appliquent :

- Toutes les entités qui étaient masquées sous la 5.x sont déplacées vers la partition *racine* de la 5.5.
- Seuls les administrateurs auront accès à la partition *racine*.
- Seuls les utilisateurs autorisés dotés de droits d'administration peuvent afficher les propriétés des entités de la *Partition publique*.
- Vous pouvez renommer, modifier et supprimer la *Partition publique* dans la version 5.5.

Pour effectuer la mise à niveau de Security Center 5.2 vers la 5.5 :

1. Si votre ancien système Security Center fédérait des systèmes Omnicast, désinstallez les packs de compatibilité installés.
2. Faites la mise à niveau du serveur principal.
3. Si votre ancien système utilisait des partitions autres que la *Partition publique*, mettez à niveau la *Partition publique*.
4. Faites la mise à niveau des serveurs d'extension et postes de travail de votre système en fonction de vos priorités.

   Si Security Center Client et Server sont installés sur un même poste, faites leur mise à niveau en même temps.

   IMPORTANT : Veillez à noter puis à appliquer les mêmes réglages que pour l'ancienne installation :mots de passe, bases de données, ports, propriétés générales, etc.

Lorsque vous avez terminé

Si vous avez utilisé le fichier *AllowedSynchronizationConfiguration.xml* pour configurer les horaires de synchronisation de vos unités HID VertX, vous devez les appliquer à nouveau manuellement dans Config Tool après la mise à niveau.

CONSEIL : Configurez les réglages de synchronisation sur une unité, puis utilisez l'outil *Copy configuration tool* pour définir les mêmes réglages sur plusieurs unités à la fois.

Mise à niveau de Security Center 5.1 vers 5.5

La mise à niveau directe depuis Security Center 5.1 vers la 5.5 n'est pas possible. Vous devez d'abord mettre à niveau votre système vers Security Center 5.3, puis vers la 5.5.

Pour effectuer la mise à niveau de Security Center 5.1 vers la 5.5 :

1 Faites la mise à niveau de votre système Security Center 5.1 vers la version 5.3.

Pour en savoir plus, voir le *Guide d'installation et de mise à jour de Security Center 5.3* de la dernière version de service.

2 Préparez la mise à niveau de Security Center 5.3 vers la 5.5

3 Faites la mise à niveau vers Security Center 5.5.

Mise à niveau de Security Center 5.0 vers 5.5

La mise à niveau directe depuis Security Center 5.0 vers la 5.5 n'est pas possible. Vous devez d'abord mettre à niveau votre système vers Security Center 5.3, puis vers la 5.5.

Pour effectuer la mise à niveau de Security Center 5.0 vers la 5.5 :

1 Faites la mise à niveau de votre système Security Center 5.0 vers la version 5.3.

Pour en savoir plus, voir le *Guide d'installation et de mise à jour de Security Center 5.3* de la dernière version de service.

2 Préparez la mise à niveau de Security Center 5.3 vers la 5.5

3 Faites la mise à niveau vers Security Center 5.5.

Mise à niveau de Security Center 4.0 vers 5.5

La mise à niveau directe depuis Security Center 4.0 vers la 5.5 n'est pas possible. Vous devez d'abord mettre à niveau votre système vers Security Center 5.2, puis vers la 5.5.

Pour effectuer la mise à niveau de Security Center 4.0 vers la 5.5 :

1 Faites la mise à niveau de votre système Security Center 4.0 vers la version 5.2.

Pour en savoir plus, voir le *Guide d'installation et de mise à jour de Security Center 5.2* de la dernière version de service.

2 Préparez la mise à niveau de Security Center 5.2 vers la 5.5

3 Faites la mise à niveau vers Security Center 5.5.

Mettre à niveau les systèmes de basculement de Répertoire depuis une version précédente

Les serveurs de Répertoire ne sont pas rétrocompatibles. Suivez cette procédure si vous faites la mise à niveau d'un système Security Center doté de plusieurs serveurs de Répertoire vers la dernière version.

Avant de commencer

- Lisez les notes de version Security Center pour prendre connaissance des problèmes connus, limitations, micrologiciels pris en charge et autres informations concernant cette version.
- Prévoyez une fenêtre d'une heure pour mettre à niveau tous les serveurs de Répertoire. Cette période doit être planifiée en heures creuses lorsque vous pouvez exécuter le système avec un nombre de fonctionnalités limité.
- Sauvegardez les bases de données du Répertoire et les fichiers de configuration.
- Veillez à noter puis à appliquer les mêmes réglages dans InstallShield que pour l'ancienne installation :mots de passe, bases de données, ports, propriétés générales, etc.
- Config Tool et le Répertoire doivent avoir la même version.
- Si Config Tool et le Répertoire sont sur des ordinateurs différents, faites la mise à niveau de Config Tool avant de mettre à niveau le Répertoire.
- Ne modifiez pas la configuration de basculement du Répertoire avant la mise à niveau. En d'autres termes, ne supprimez pas les serveurs de Répertoire secondaires de la liste de serveurs de Répertoire.

À savoir

- Pendant la mise à niveau, le rôle Répertoire est arrêté. Par conséquent, Config Tool et la majorité des fonctionnalités de Security Desk sont indisponibles. Toutefois, la vidéo affichée avant l'interruption du service Répertoire continue a être diffusée dans la tâche *Surveillance* de Security Desk et enregistrée sur l'Archiveur. Par exemple, les murs vidéo continuent à afficher les flux vidéo. Le contrôle d'accès continue également à fonctionner, mais les opérateurs ne peuvent pas utiliser Security Desk pour ouvrir les portes manuellement, etc.
- Pendant la mise à niveau, chaque serveur de Répertoire est mis à niveau indépendamment. Par conséquent, la fonction de basculement est indisponible.
- La mise à niveau des licences n'est nécessaire qu'en cas de changement de version (par exemple de la version 5.x vers la 5.5). Il n'est pas nécessaire de mettre à niveau la licence pour les mises à niveau de service (par exemple de SRx vers SRy).

Pour mettre à niveau un système à plusieurs serveurs de Répertoire :

1 Sur chaque serveur de Répertoire secondaire de la liste des serveurs de Répertoire, arrêtez le service Genetec Watchdog depuis la fenêtre du service Console de gestion Microsoft (MMC).

Les serveurs de Répertoire secondaires sont représentés par l'icône de serveur d'extension ( ). N'arrêtez pas le serveur principal ( ).

Le service Genetec Server est arrêté sur les serveurs de Répertoire secondaires. Tous les rôles qui ne sont exécutés que sur les serveurs de Répertoire secondaires basculent hors ligne. Généralement, chaque serveur de Répertoire gère une part égale des connexions de rôles et de clients. Une fois que les serveurs de Répertoire secondaires sont arrêtés, tout rôle ou client qui était connecté à l'un de ces serveurs est forcé à se reconnecter au serveur de Répertoire principal. Les clients affichent brièvement le message « Connexion perdue... » pendant ce processus. Les rôles et leurs entités sont affichés comme étant hors ligne jusqu'à leur reconnexion.

2 Faites la mise à niveau du serveur de Répertoire principal en tant que serveur principal.

Le serveur de Répertoire principal, également appelé serveur principal ( ), est le seul serveur qui est encore actif avant de lancer la procédure de mise à niveau. Pendant la mise à niveau du serveur principal, aucun service du Répertoire n'est disponible. Seules quelques fonctionnalités continuent à fonctionner.

Security Center installer arrête automatiquement le service Genetec Server sur le serveur principal, puis le redémarre après la mise à niveau.

3 (Ne s'applique qu'aux changements de version) Activez votre licence Security Center 5.5 en procédant de l'une des manières suivantes :

- sur le Web
- sans accès à Internet

Le service Répertoire est hors ligne. Tous les serveurs d'extension (à l'exception des serveurs de Répertoire) et postes client qui ne sont pas encore mis à niveau sont exécutés en mode rétrocompatibilité. Le basculement de Répertoire et l'équilibrage de charge ne sont pas encore disponibles.

4 Dans Config Tool, connectez-vous au serveur principal. Vérifiez que tous les rôles, serveurs et unités fonctionnent normalement.

Les serveurs de Répertoire secondaires sont toujours arrêtés (en rouge). Tous les rôles qui ne sont exécutés que sur les serveurs de Répertoire secondaires sont toujours hors ligne.

5 Faites la mise à niveau des serveurs de Répertoire restants en tant que serveurs d'extension.

Security Center installer redémarre le service Genetec Server après chaque mise à niveau. Le basculement de Répertoire et l'équilibrage de charge sont toujours indisponibles.

6 (Ne s'applique qu'aux changements de version) Réactivez la licence Security Center 5.5 pour tous les serveurs de Répertoire.

Le basculement de Répertoire et l'équilibrage de charge sont maintenant disponibles.

Lorsque vous avez terminé

Faites la mise à niveau du reste du système en fonction de vos priorités et disponibilités.

IMPORTANT : L'ajout de connexions rétrocompatibles ralentit les performances du Répertoire, et n'est donc conseillé qu'à titre temporaire, tant que vous n'avez pas mis à niveau tous les postes et serveurs.

Rubriques connexes

Configuration requise pour la rétrocompatibilité de Security Center, page 65

Fonctionnalités Security Center client disponibles lorsque le service Répertoire est inaccessible

En cas de mise à niveau d'un système Security Center, tous les serveurs de Répertoire doivent être arrêtés pendant un certain temps. Aucun service fourni par le Répertoire n'est disponible durant l'interruption. Seules certaines fonctionnalités continuent à fonctionner.

Fonctionnalités Security Center qui restent disponibles en l'absence du service Répertoire :

- Security Desk continue à diffuser de la vidéo en direct des caméras.
- L'enregistrement vidéo se poursuit en fonction des horaires, dès lors que les rôles Archiveur sont en ligne.
- Toutes les fonctionnalités de contrôle d'accès continuent à fonctionner normalement, à l'exception des commandes qui doivent être relayées par le service Répertoire, comme les associations événement-action, ainsi que toutes les opérations d'ouverture ou déverrouillage de portes émises depuis Security Desk.
- Les portes peuvent être ouvertes par l'intermédiaire d'un interrupteur (entrée) si toutes les entrées et sorties sont contrôlées par une même unité de contrôle d'accès.

Fonctionnalités Security Center qui ne sont pas disponibles en l'absence du service Répertoire :

- Config Tool et Security Desk : les fonctionnalités sont indisponibles.
- Toutes les actions manuelles (enregistrement, verrouillage/déverrouillage de portes, etc.) effectuées avec les widgets Security Desk sont désactivées, y compris les accès aux caméras.
- Les alarmes et événements en temps réel ne peuvent pas être affichés dans Security Desk.

Réactiver la licence Security Center sur les systèmes de basculement de Répertoire

Vous devez réactiver votre licence Security Center avec une nouvelle clé de validation, chaque fois que vous ajoutez ou supprimez des serveurs à partir de la liste des serveurs de Répertoire.

Avant de commencer

Pour mettre à jour votre licence, vous devez disposer des éléments suivants :

- **ID système et mot de passe:** L'ID système et mot de passe sont disponibles dans le document *Informations de licence Security Center*. Le service client de Genetec vous envoie ce document à l'achat du produit.

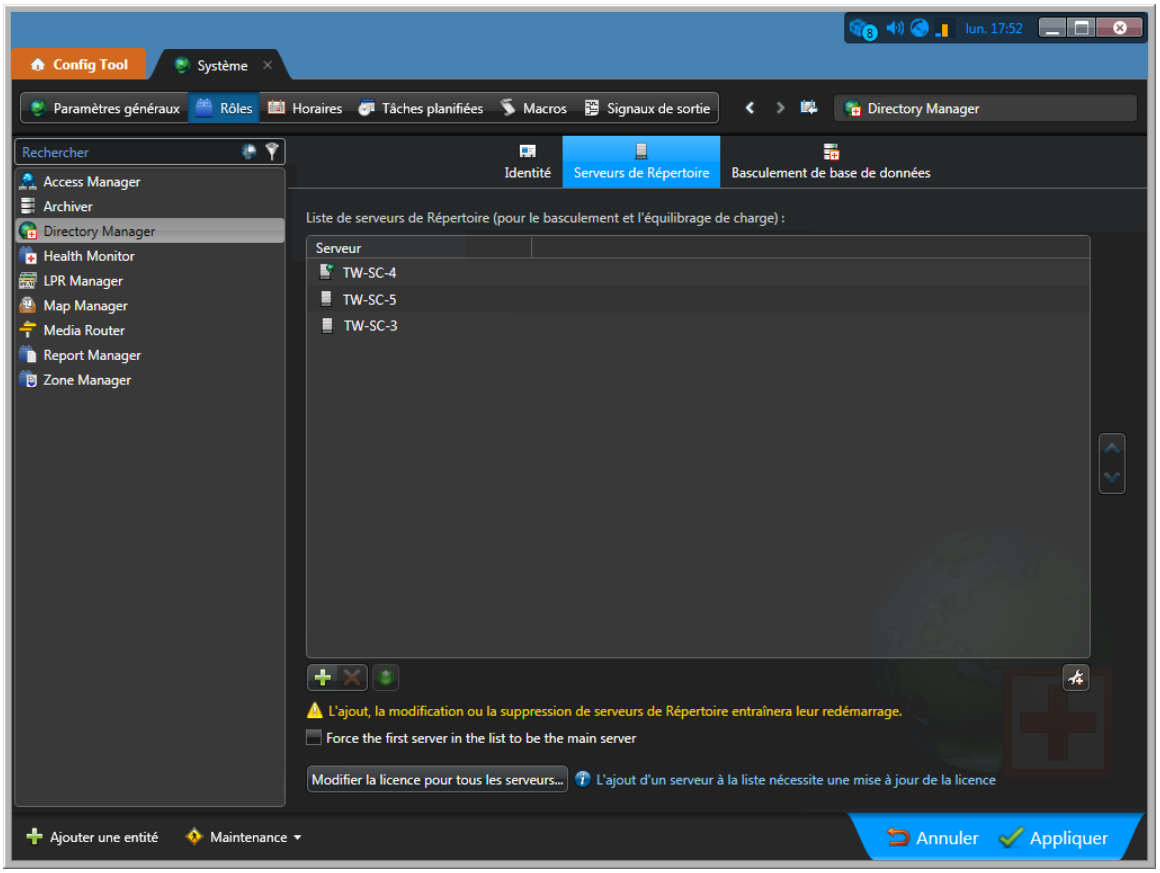
À savoir

IMPORTANT : Server Admin ne peut être utilisé que pour activer une licence de serveur unique. Si vous avez une configuration à plusieurs serveurs de Répertoire, la création de la clé de validation et l'application de la clé de licence doivent être effectuées dans Config Tool. Tous les serveurs de Répertoire doivent être en cours d'exécution pour mettre à jour la licence depuis Config Tool.

Pour activer la licence Security Center sur un système à plusieurs serveurs de Répertoire :

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Système*, puis cliquez sur la vue **Rôles**.

2 Sélectionnez le rôle **Gestionnaire de Répertoire** (), puis cliquez sur l'onglet **Serveurs de Répertoire**.



3 Cliquez sur **Modifier la licence pour tous les serveurs**.

4 Dans la boîte de dialogue **Gestion de licences**, activez votre licence de l'une des manières suivantes :

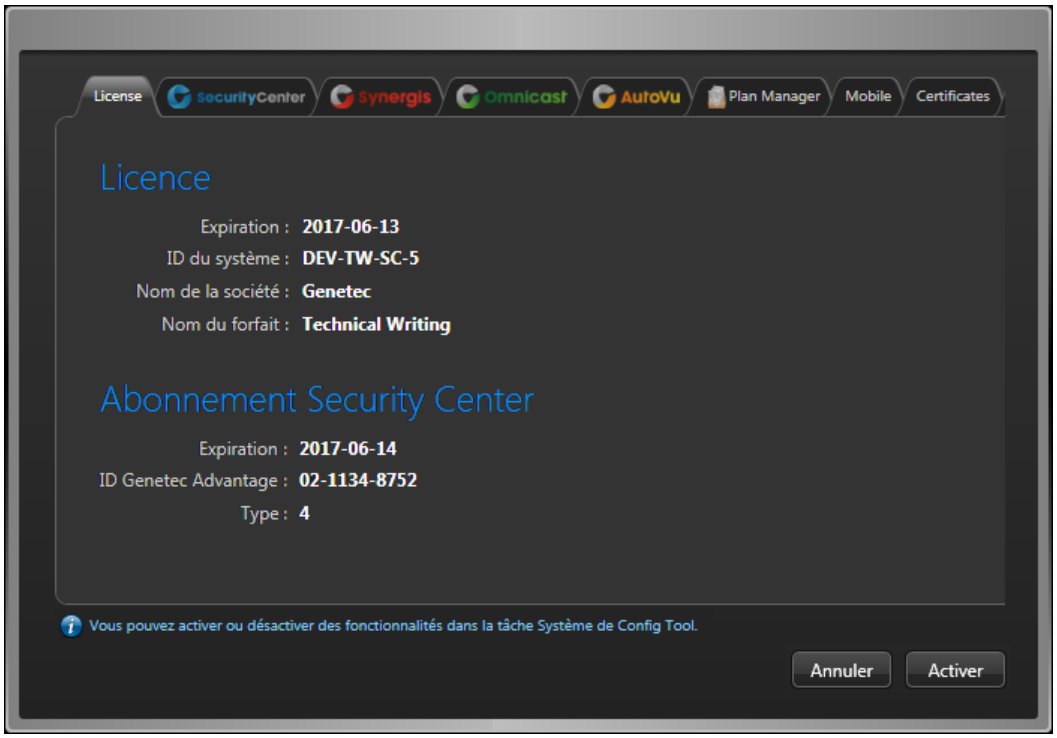
- **Activation Web:** (Recommandé) Réactivez votre licence via Internet.

  Dans la boîte de dialogue qui apparaît, entrez votre *ID système* et votre *mot de passe*, puis cliquez sur **Activer**.

- **Activation manuelle:** Si votre poste Config Tool n'a pas d'accès à Internet, réactivez votre licence Security Center manuellement en vous servant d'un fichier de licence.

IMPORTANT : Envoyez la clé de validation composite (qui comprend tous les serveurs de Répertoire) ; sans quoi la réactivation de licence échoue sans message et le basculement de Répertoire ne fonctionne pas.

Une boîte de dialogue affichant vos informations de licence s'ouvre.



Cliquez sur les onglets colorés pour afficher vos options de licence.

5 Cliquez sur **Appliquer** pour fermer la boîte de dialogue, et cliquez sur **Appliquer** en bas de la fenêtre Config Tool pour enregistrer vos modifications.

Réactivation de votre licence Security Center à l'aide d'un fichier de licence.

Pour réactiver votre licence Security Center pour les changements que vous avez apportés à la liste des serveurs de Répertoire quand le poste Config Tool n'a pas accès à Internet, vous devez utiliser un second poste pour télécharger votre fichier de licence à partir de GTAP, puis appliquer le fichier de licence à en vous servant du premier poste

À savoir

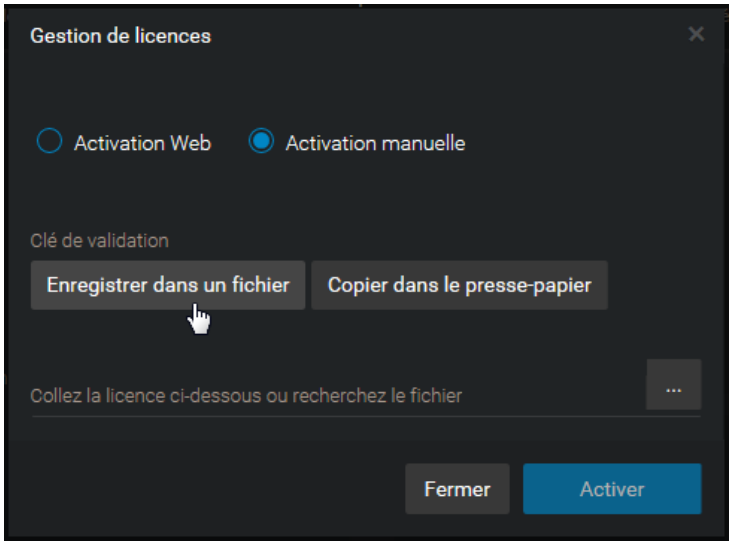
Cette procédure s'inscrit dans le cadre de la réactivation de votre licence Security Center sur un système de basculement de Répertoire.

Pour mettre à jour votre licence à l'aide d'un fichier de licence :

1 Dans la boîte de dialogue *Gestion de licences*, cliquez sur **Enregistrer dans un fichier** pour enregistrer la clé de validation composite dans un fichier.

La clé de validation est une séquence de chiffres (en hexadécimal au format texte) unique générée par Security Center qui identifie votre serveur. Elle sert à générer la clé de licence qui déverrouille votre logiciel Security Center. La clé de licence générée ne peut être appliquée qu'au serveur identifié par la clé de validation.

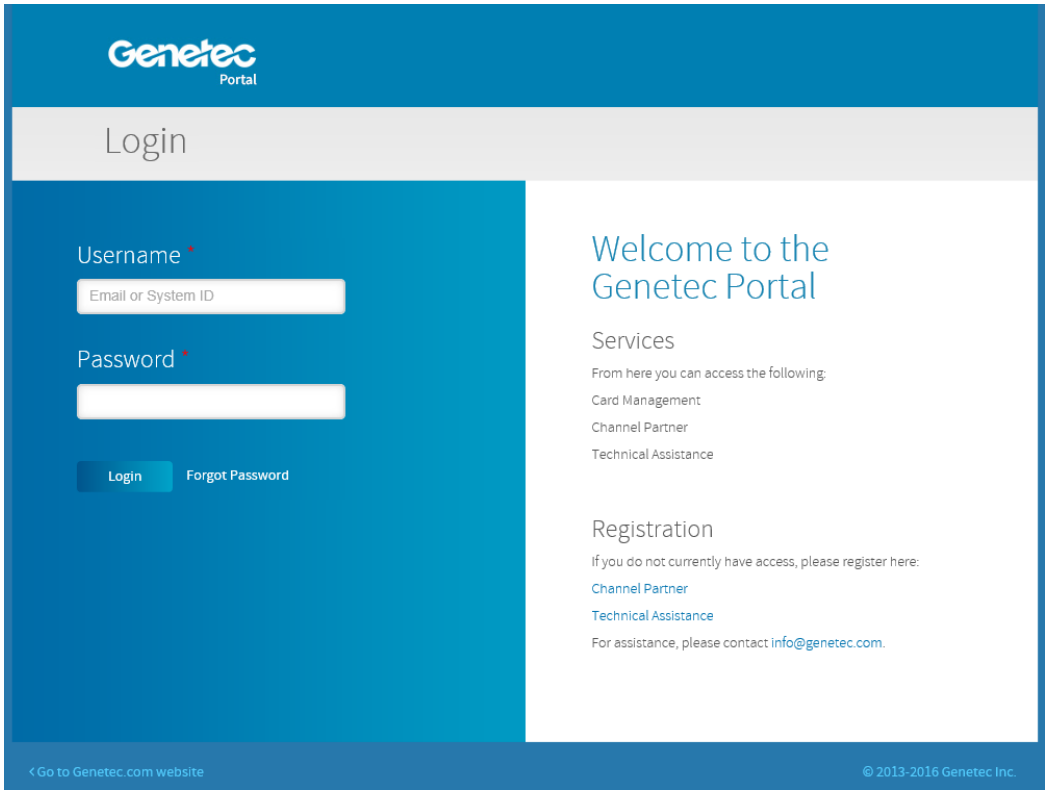
2 Dans la boîte de dialogue *Gestion de licences*, cliquez sur **Activation manuelle**, puis sous *Clé de validation*, cliquez sur **Enregistrer dans un fichier**.



La clé de validation est une séquence de chiffres (en hexadécimal au format texte) unique générée par Security Center qui identifie votre serveur. Elle sert à générer la clé de licence qui déverrouille votre logiciel Security Center. La clé de licence générée ne peut être appliquée qu'au serveur identifié par la clé de validation.

Un fichier texte nommé *validation.vk* est enregistré dans votre dossier *Téléchargements* par défaut. Veillez à copier ce fichier dans un emplacement (il peut s'agir d'une clé USB) auquel vous pouvez accéder depuis un autre poste connecté à Internet.

3 Sur un autre ordinateur connecté à Internet, connectez-vous sur GTAP à l'adresse : https://gtap.genetec.com

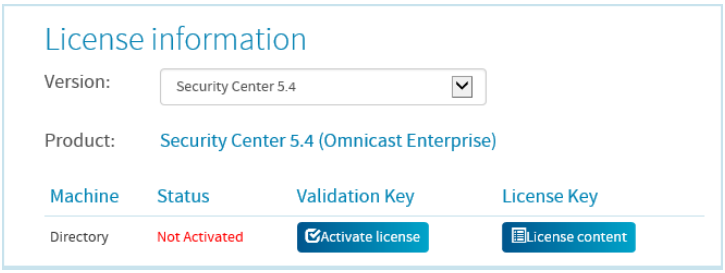


4 Sur la page de connexion GTAP, procédez de l'une des manières suivantes :

- Entrez l'ID système et le mot de passe spécifiés dans le document *Informations de licence Security Center*, et cliquez sur **Connexion**.
- Entrez votre compte utilisateur GTAP (votre adresse de messagerie électronique) et votre mot de passe, puis cliquez sur **Connexion**.
  1 Sur la page *Portail Genetec - Accueil*, cliquez sur **Activer le nouveau système**.
  2 Dans la liste déroulante **ID du système**, sélectionnez votre système et cliquez sur **Envoyer**.

Le navigateur s'ouvre à la page *Informations système*.

5 Défilez jusqu'à la section *Informations de licence* et cliquez sur **Activer la licence**.



6 Dans la boîte de dialogue qui s'ouvre, parcourrez jusqu'à votre clé de validation (.vk file), et cliquez sur **Envoyer**.

Le message **License activation successful** (Activation de licence réussie) s'affiche.

7 Cliquez sur **Télécharger la licence**, et enregistrez la clé de licence dans un fichier.

Le nom par défaut est votre ID système suivi de *_Directory_License.lic*.

8 Revenez au posteConfig Tool.

9 Dans la boîte de dialogue *Gestion de licences*, cliquez sur **Activation manuelle**.

10 Dans la boîte de dialogue *Activation manuelle*, accédez à la clé de licence (fichier .lic), et cliquez sur **Ouvrir**.

11 Cliquez sur **Activer**.

Mettre à niveau le serveur principal Security Center

Le serveur principal de votre système Security Center actuel doit être mis à niveau en premier. Vous devez appliquer une nouvelle licence et mettre à niveau la base de données du Répertoire.

Avant de commencer

- Prenez connaissance de ce que vous devez savoir et faire avant la mise à niveau (voir les sujets connexes).
- Sauvegardez la base de données du Répertoire et toutes les bases de données de rôles interrogées par le serveur principal.

À savoir

Le Config Tool de Security Center 5.5 est nécessaire pour la connexion au Répertoire 5.5. Si Security Center Client est installé sur le serveur principal, faites sa mise à niveau en même temps.

REMARQUE : La mise à niveau de Security Center 5.1 vers Security Center 5.5 n'est pas prise en charge. Security Center 5.5 Client est installé aux côtés des anciennes versions de Security Center Client. Après l'installation, vous pouvez supprimer l'ancienne version.

En cas de message d'alerte de redémarrage durant la mise à niveau, acceptez le message et poursuivez la procédure de mise à niveau. Vous devez redémarrer une fois la mise à niveau terminée.

Pour mettre à niveau le serveur principal :

1 Installez Security Center 5.5 sur le serveur principal.
Utilisez le type d'installation **Serveur principal**.

L'Assistant InstallShield détecte automatiquement l'ancienne version de Security Center, et la met à niveau vers Security Center 5.5.

2 Lorsque vous êtes invité à confirmer que vous avez une sauvegarde à jour de vos bases de données, cochez la case de confirmation, cliquez sur **Suivant**, et suivez les instructions de l'Assistant InstallShield.

Le programme d'installation met à jour votre logiciel Security Center et le schéma de la base de données du Répertoire.

3 Activez votre nouvelle licence Security Center 5.5.

Rubriques connexes

Sauvegarder les bases de données, page 89
Mettre à niveau la base de données du Répertoire Security Center, page 90
Activer la licence Security Center sur le Web, page 23
Activer la licence Security Center sans accès à Internet, page 26
Préparer la mise à niveau de Security Center 5.4 vers 5.5, page 56
Préparer la mise à niveau de Security Center 5.3 vers 5.5, page 57
Préparer la mise à niveau de Security Center 5.2 vers 5.5, page 58

Mettre à niveau les serveurs d'extension dans Security Center

Pour bénéficier des dernières améliorations apportées à Security Center, vous devez mettre à niveau les serveurs d'extension. Pour faire la mise à niveau, installez Security Center Server sur les serveurs d'extension, et suivez les instructions de l'Assistant InstallShield.

Avant de commencer

- Si vous migrez depuis Omnicast 4.x, voir le *Guide de migration Omnicast*.
- Sauvegardez toutes les bases de données de rôles interrogées par le serveur d'extension que vous mettez à niveau.

À savoir

En cas de message d'alerte de redémarrage durant la mise à niveau, acceptez le message et poursuivez la procédure de mise à niveau. Vous devez redémarrer une fois la mise à niveau terminée.

Pour mettre à niveau un serveur d'extension :

1 Installez Security Center 5.5 sur le serveur d'extension.

Utilisez le type d'installation **Serveur d'extension**.

Le programme d'installation détecte automatiquement l'ancienne version de Security Center, et la met à niveau vers la 5.5.

2 Répétez cette procédure sur tous les serveurs d'extension de votre système.

Lorsque vous avez terminé

Pour vérifier que tous les serveurs de votre système sont actifs, connectez-vous au serveur principal avec Config Tool. Dans la tâche *Vue réseau*, tous les serveurs de votre système doivent être affichés en noir (état actif). Si certains rôles ne sont toujours pas actifs, vous devez peut-être mettre à niveau la base de données du Répertoire.

Rubriques connexes

Sauvegarder les bases de données, page 89

Mettre à niveau Security Center Client

Une fois que vous avez mis à niveau le serveur principal et les serveurs d'extension de Security Center, vous pouvez effectuer la mise à niveau de Security Center Client.

À savoir

La mise à niveau de Security Center 5.1 vers Security Center 5.5 n'est pas prise en charge. Security Center 5.5 Client est installé aux côtés des anciennes versions de Security Center Client. Après l'installation, vous pouvez supprimer l'ancienne version.

Pour effectuer la mise à niveau de Security Center 5.1 vers la 5.5 :

1 Installez Security Center Client.

REMARQUE : La configuration de l'espace de travail de l'utilisateur n'est pas conservée. Dans les versions précédentes de Security Center, l'espace de travail utilisateur était enregistré sous forme de configuration de poste de travail. À compter de la 5.4, l'espace de travail de l'utilisateur est enregistré au sein du profil utilisateur dans le Répertoire. La mise à niveau ne convertit pas ces réglages.

2 Dans le Panneau de configuration de Windows, désinstallez l'ancienne version de Security Center Client.

Pour effectuer la mise à niveau de Security Center 5.2, 5.3 ou 5.4 vers la 5.5 :

1 Installez Security Center Client.

Le programme d'installation détecte automatiquement l'ancienne version de Security Center, et la met à niveau vers la 5.5.

Sauvegarder les bases de données

Vous pouvez protéger les données stockées dans une base de données de rôle en sauvegardant régulièrement la base de données. En outre, il est toujours conseillé de sauvegarder vos bases de données avant une mise à niveau.

À savoir

Toutes les bases de données de rôles sont sauvegardées depuis Config Tool, à l'exception de la base de données du Répertoire qui doit être sauvegardée depuis la page Serveur principal de Server Admin. La procédure est très similaire dans les deux cas. C'est pourquoi seule la sauvegarde depuis Config Tool est décrite ici.

REMARQUE : Les cas suivants sont des exceptions :

- Pour sauvegarder les bases de données des rôles Archiveur et Archiveur auxiliaire avec les fichiers vidéo associés, voir Transférer manuellement des archives vidéo.
- Pour sauvegarder la base de données du Répertoire lorsque le mode de basculement *Sauvegarde et restauration* est activé, voir Créer une sauvegarde complète de la base de données du Répertoire.
- D'autres restrictions doivent être prises en compte pour la sauvegarde et restauration de la base de données du Répertoire lorsque le mode de basculement *Miroir* est activé. Pour en savoir plus, reportez-vous à la documentation de Microsoft sur la mise en miroir de SQL Server.

Pour sauvegarder la base de données d'un rôle :

1 Sur la page d'accueil de Config Tool, ouvrez la tâche *Système*, puis cliquez sur la vue **Rôles**.
2 Sélectionnez un rôle et cliquez sur l'onglet **Ressources**.
3 Cliquez sur **Sauvegarder/restaurer** ( ).
4 Dans la boîte de dialogue *Sauvegarder/restaurer* en regard du champ **Dossier de sauvegarde**, cliquez sur **Sélectionner un dossier** ( ), et sélectionnez un emplacement pour le fichier de sauvegarde.

   REMARQUE : Le chemin est relatif au serveur qui héberge le rôle, pas au poste sur lequel vous exécutez Config Tool. Pour sélectionner un disque réseau, entrez le chemin manuellement, et vérifiez que l'utilisateur du service à un accès en écriture à ce dossier.

5 (Facultatif) **Activez** l'option **Compacter le fichier de sauvegarde** pour créer un fichier ZIP au lieu d'un fichier BAK.

   Si vous sélectionnez cette option, vous devrez décompacter le fichier de sauvegarde avant de le restaurer.
6 Cliquez sur **Sauvegarder maintenant**.

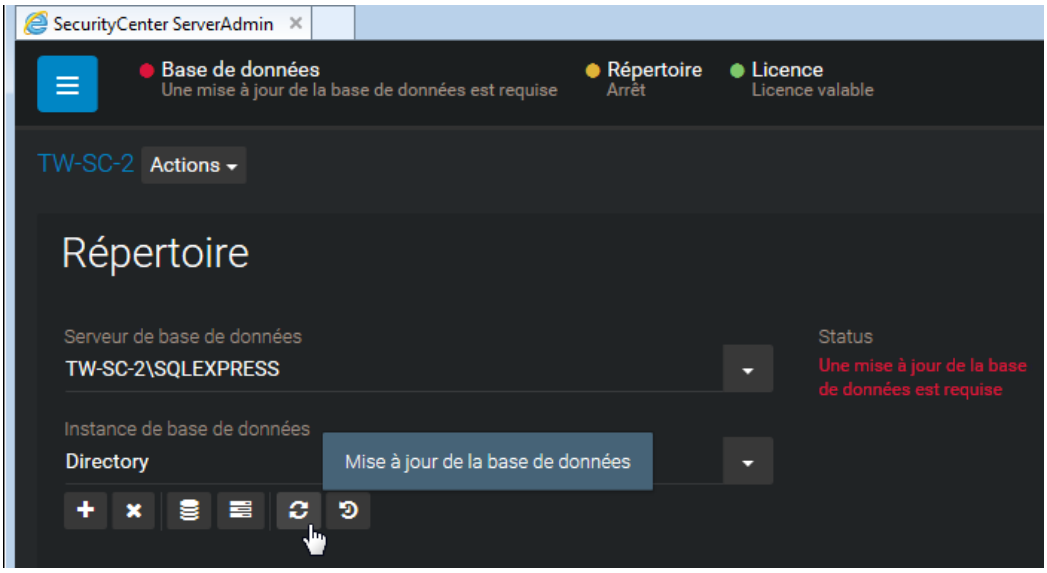
Un fichier de sauvegarde doté de l'extension BAK est créé dans le dossier de sauvegarde. Le nom du fichier correspond au nom de la base de données, suivi par « _ManualBackup_ », suivi par la date (mm-jj-aaaa).

Mettre à niveau la base de données du Répertoire Security Center

Le programme d'installation de Security Center 5.5 met à niveau la base de données du Répertoire dans le cadre de la mise à niveau du serveur principal. La mise à niveau manuelle de la base de données du Répertoire n'est nécessaire que si vous avez restauré une ancienne version de la base de données.

À savoir

Après la restauration d'une ancienne version de la base de données du Répertoire, Server Admin vous informe qu'une mise à jour de la base de données est nécessaire. Pour en savoir plus sur la restauration des bases de données, voir le *Guide de l'administrateur Security Center*.



Pour mettre à jour la base de données de Répertoire :

1 Procédez de l'une des manières suivantes :

- Cliquez sur **Base de données** avec le voyant LED rouge clignotant.
- Cliquez sur **Mise à jour de la base de données** () dans la section *Répertoire*.

La mise à jour de la base de données démarre, et l'état du serveur de base de données indique **Mise à niveau**.

2 Pendant la mise à niveau de la base de données, cliquez sur **Afficher la progression** () pour suivre la progression de la mise à niveau.

Lorsque la mise à niveau est terminée, l'**État** indique **OK**.

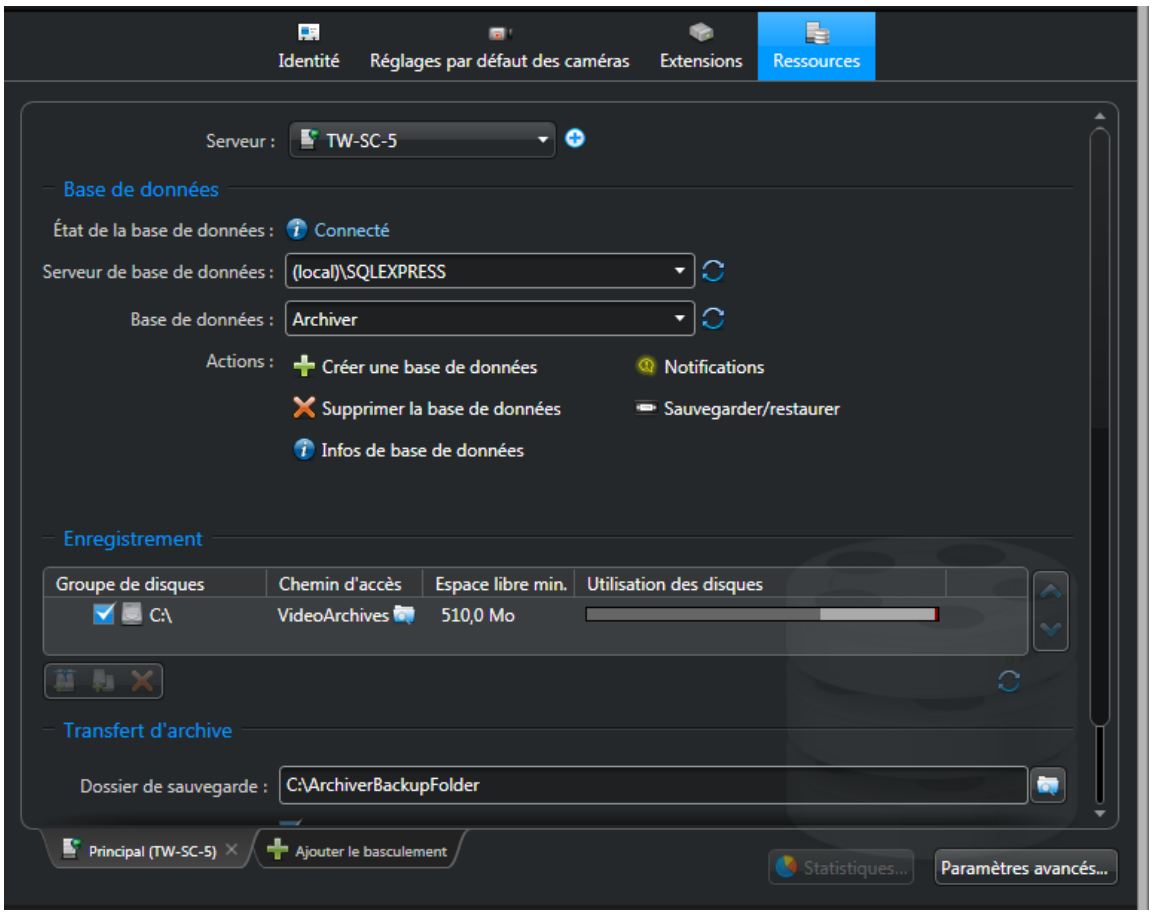
3 Cliquez sur **Propriétés de la base de données** () pour vérifier la version et le nombre d'enregistrements de la base de données.

4 Déconnectez-vous de Server Admin, puis connectez-vous à Config Tool.

5 Ouvrez la tâche **Système** et sélectionnez **Rôles**.

6 Sélectionnez le rôle Archiveur et cliquez sur **Ressources**.

7 Dans la section **Actions**, cliquez sur **Mettre à jour la base de données** ().



Une fois la mise à niveau terminée, l'option **État de la base de données** doit indiquer *Connecté*.

8 Répétez les étapes pour chaque rôle qui nécessite une mise à niveau de sa base de données. Les rôles de votre système varient en fonction de vos options de licence.

Lorsque vous avez terminé

Réduisez la base de données de l'Archiveur, et le cas échéant, d'autres bases de données que vous avez mises à niveau.

Réduire une base de données Security Center après une mise à niveau

Après la mise à niveau d'une base de données, l'espace de stockage utilisé peut considérablement augmenter en raison du stockage temporaire nécessaire pour exécuter les transactions de mise à niveau. L'espace utilisé durant la mise à niveau n'est pas automatiquement libéré une fois la mise à niveau terminée. Pour récupérer l'espace disque inutilisé, vous devez réduire la base de données.

Avant de commencer

Les mises à niveau n'entraînent pas toutes le gonflement de la base de données. Toutefois, après la mise à niveau de la base de données de l'Archiveur de la version 5.3 vers la 5.4, nous recommandons de réduire la base de données. Si vous n'êtes pas sûr de devoir réduire votre base de données après une mise à niveau, consultez son occupation du disque avec SQL Server Management Studio.

À savoir

Selon le modèle de récupération de votre base de données, une sauvegarde du journal des transactions peut être nécessaire pour récupérer l'espace disque inutilisé. Pour en savoir plus, consultez les articles en ligne suivants : Modes de récupération (SQL Server) et Troncation du journal des transactions.

Pour réduire une base de données :

1 Suivez la procédure Réduire une base de données publiée en ligne par Microsoft.
2 Suivez la même procédure pour toutes les bases de données qui doivent être réduites.

À propos de Genetec[MC] Update Service

Genetec[MC] Update Service est un service web qui permet de mettre à jour vos produits Security Center lorsqu'une nouvelle version est disponible.

À compter de Security Center 5.4 GA, Genetec[MC] Update Service est automatiquement installé avec Security Center et vous permet d'effectuer les tâches suivantes :

- Mettre à jour vos produits Security Center lors de la sortie de nouvelles versions.
- Rechercher des mises à jour à intervalles réguliers.
- Télécharger automatiquement les mises à jour lorsqu'elles sont disponibles.

  REMARQUE : les mises à jour peuvent être téléchargées en arrière-plan, mais elles exigent toujours une intervention manuelle pour leur installation.
- Consulter la date de la dernière vérification.
- Configurer le partage poste-à-poste avec plusieurs postes connectés à Internet, ou un seul poste connecté à Internet. Les fichiers de mise à jour ne sont téléchargés qu'une seule fois, puis partagés avec les autres postes.

IMPORTANT : Pour en savoir plus sur la connexion au Genetec Update Service, voir Se connecter à Genetec™ Update Service, page 94.

Se connecter à Genetec[MC] Update Service

Pour vous connecter à Genetec[MC] Update Service, vous devez ouvrir l'application et (le cas échéant) entrer votre mot de passe Genetec[MC] Update Service.

Avant de commencer

Vous devez vous munir de votre mot de passe Genetec[MC] Update Service (si un mot de passe a été défini).

À savoir

Vous pouvez accéder à Genetec[MC] Update Service dans un navigateur web en tapant l'adresse `https://localhost:4595`, ou depuis le menu Démarrer.

REMARQUE : Lorsque vous installez Genetec[MC] Update Service manuellement, vous ne pouvez pas y accéder depuis le menu Démarrer.

Pour se connecter au Genetec[MC] Update Service :

1 Procédez de l'une des manières suivantes :

- Cliquez sur **Démarrer** > **Tous les programmes** > **Genetec Security Center 5.x** > **Genetec[MC] Update Service**.
- Tapez `http://localhost:4595` dans votre navigateur web.

2 Dans la boîte de dialogue **Se connecter**, procédez de l'une des manières suivantes :

- Connectez-vous avec le mot de passe vide par défaut.
- Entrez le mot de passe Genetec[MC] Update Service.

  REMARQUE : Le mot de passe Genetec[MC] Update Service peut être configuré sur la page de la section **Avancé**.

  Pour en savoir plus sur l'utilisation du Genetec[MC] Update Service, ouvrez-le et cliquez sur **Aide**.

3

Automatisation de l'installation de Security Center

Cette section aborde les sujets suivants:

Installation silencieuse de Security Center

L'installation silencieuse est une manière automatisée d'installer le logiciel, sans intervention de l'utilisateur. L'installation silencieuse est exécutée à l'invite de commande, avec le fichier exécutable *Security Center setup.exe* et des commandes du programme d'installation de Windows.

Vous pouvez personnaliser les options suivantes depuis l'invite de commande :

- Langue de l'installation
- Langue de l'application
- Chemin d'installation du client ou serveur
- Fonctionnalités du client ou serveur à installer
- Nom d'utilisateur et mot de passe du serveur pour l'exécution des services
- Nom de la base de données et du serveur

Limitations

Prenez en compte les limitations suivantes avant d'effectuer une installation silencieuse :

- Vous ne pouvez pas mettre à jour votre licence en mode silencieux. Vous devrez exécuter l'application Web Server Admin après l'installation de Security Center pour activer la licence.
- L'invite de commande est limitée à 850 caractères.

  CONSEIL : Un moyen de raccourcir la longueur de la commande consiste à réduire la longueur du chemin d'installation. Pour ce faire, vous pouvez copier les fichiers d'installation sur un disque local.
- Vous ne pouvez pas utiliser de lecteurs mappés dans la spécification du chemin.
- Vous ne pouvez pas installer WinPcap (utilitaire de capture de données de diagnostic) en mode silencieux.

Préparer une installation silencieuse

Certaines tâches doivent être effectuées en amont de l'installation pour éviter les problèmes.

Avant d'effectuer une installation silencieuse :

1 Installez tous les logiciels prérequis.

Security Center installe automatiquement les logiciels prérequis sur votre système. Cela peut entraîner le redémarrage de votre ordinateur. Dès lors, il est recommandé d'installer les logiciels prérequis manuellement avant de lancer l'installation silencieuse.

2 Si vous comptez spécifier un utilisateur Windows autre que l'utilisateur par défaut (système local) pour exécuter les services, vous devez avoir créé cet utilisateur avant de lancer le processus d'installation.

L'utilisateur doit être un membre du groupe Administrateurs et doit disposer du droit d'utilisateur *Ouverture de session en tant que service*.

Rubriques connexes

Installer SQL Server sur un disque distinct, page 5

Commandes d'installation silencieuse de Security Center

Lors d'une installation silencieuse, des options de programme particulières sont nécessaires pour exécuter le programme d'installation de Security Center.

Voici la syntaxe pour exécuter le programme d'installation en mode silencieux :

```
<setup_exe> <setup_options> <msi_options>
```

où :

- `<setup_exe>`**:** Est le fichier .exe du programme d'installation de Security Center. Vous pouvez soit utiliser la version autonome (`"Security Center Setup.exe"`), soit la version web (`SecurityCenterWebSetup.exe`).

  N'utilisez pas le fichier *setup.exe* situé dans le dossier racine du pack d'installation. Il s'agit d'une version à exécution automatique du programme d'installation autonome qui n'accepte pas les arguments à l'invite de commande.
- `<setup_options>`**:** Il s'agit des options d'installation. Elles commencent toutes par une barre oblique (/).
- `<msi_options>`**:** Il s'agit des options du programme d'installation (MSI). Elles s'écrivent en majuscules.

Le tableau suivant présente les options d'installation.

Option d'installation	Description
`/ISInstallDir`	Spécifie le chemin dans lequel le logiciel doit être installé. **EXEMPLES** : • `/ISInstallDir=C:\MonDossier` • `/ISInstallDir="D:\Program Files\MonDossier"` **REMARQUE :** Dans le deuxième exemple, les (") sont requis car la valeur contient des espaces. S'il n'est pas spécifié, l'emplacement par défaut est `<ProgramFiles>\Genetec Security Center 5.5`, où `<ProgramFiles>` correspond soit à %PROGRAMFILES%, soit à %PROGRAMFILES(X86)%, selon la version de votre système d'exploitation.
`/ISFeatureInstall`	Spécifie les fonctionnalités à installer. Les valeurs possibles sont: • `Server` (Genetec Server avec ou sans Répertoire, selon l'option d'installation `SERVER_TYPE`) • `Client` (Security Desk et Config Tool) • `SecurityDesk` (Security Desk seul) • `ConfigTool` (Config Tool seul) • `CompPacks,CompPack4x[,CompPack4x]` (packs de compatibilité Omnicast ; vous devez spécifier au moins un pack) **EXEMPLES** : • `/ISFeatureInstall=Server,Client` (valeur par défaut) • `/ISFeatureInstall=Client,CompPacks,CompPack48`
`/silent`	Configure l'exécution du programme Security Center setup.exe en mode silencieux sans intervention de l'utilisateur.

Option d'installation	Description
`/debuglog<CheminFichier>`	Active le fichier journal de débogage et spécifie son chemin. **REMARQUE :** Le chemin spécifié par `<CheminFichier>` doit exister. Le programme d'installation ne le créera pas. **EXEMPLE** : `/debuglog"C:\DebugLog.log"`
`/log<CheminDossier>`	Active la création de fichiers journaux et spécifie le chemin du dossier. **REMARQUE :** `<CheminDossier>` doit exister. Le programme d'installation ne le créera pas. **EXEMPLE** : `/log"C:\TousMesFichiersJournaux\"`
`/language:`	Définit la langue utilisée par le programme d'installation. Précède immédiatement le code de langue à quatre chiffres. Les espaces ne sont pas autorisés. **EXEMPLES** • `/language:1033` pour l'anglais (valeur par défaut) • `/language:3084` pour le français
`<msi_options>`	Définit la liste des options du programme d'installation (MSI) de Security Center. Chaque option de la liste utilise la syntaxe suivante : `<option>=<valeurs>` où `<option>` est le nom d'une option et `<valeurs>` est une liste de valeurs séparées par des virgules. Aucun espace n'est autorisé de part et d'autre du signe égal (=). Si la liste de valeurs doit contenir des espaces, l'intégralité de la liste de valeurs doit être placée entre guillemets doubles précédés d'une barre oblique inverse (\").

Options du programme d'installation (MSI)

Lors d'une installation silencieuse, vous pouvez spécifier des options d'installation supplémentaires pour le programme d'installation (MSI) de Security Center.

Le tableau suivant présente les options du programme d'installation (MSI) de Security Center. Toutes les options du programme d'installation s'écrivent en majuscules. Contrairement aux options d'installation, elles ne sont pas précédées d'une barre oblique (/). Le nom des options est sensible à la casse.

Option du programme d'installation (MSI)	Description
SERVER_TYPE	Spécifie l'installation d'un serveur principal ou d'extension. Les valeurs possibles sont: • Main: Installer Genetec Server avec le Répertoire (VALEUR PAR DÉFAUT) • Expansion: Installer Genetec Server sans Répertoire
SQLSERVER_GROUP	Spécifie l'installation ou non d'un serveur SQL existant en mode silencieux. Les valeurs possibles sont: • NewServer (doit être utilisé avec SQL_INSTANCE_NAME) • ExistingServer (VALEUR PAR DÉFAUT)
SQL_INSTANCE_NAME	Spécifie le nom de la nouvelle instance de SQL Server. Cette option doit être spécifiée lorsque SQLSERVER_GROUP a la valeur NewServer.
GLOBAL_SERVER	Spécifie le nom du serveur de base de données pour tous les rôles installés par défaut. En cas d'omission, la valeur par défaut est (local)\SQLEXPRESS. **EXEMPLE** : GLOBAL_SERVER=BLADE32\SQLServerEnterprise
DATABASE_SERVER	Pareil que pour l'option GLOBAL_SERVER. Ce paramètre assure la rétrocompatibilité avec d'anciens scripts d'installation silencieuse.
DATABASE_INSTANCE	Utilisé en conjonction avec l'option BACKUP_DATABASE. Spécifie le nom d'instance de base de données du Répertoire, si différent de la valeur par défaut.
UPGRADE_DATABASE	Spécifie que la base de données de Répertoire doit être automatiquement mise à niveau. En l'absence de base de données existante, cette option est ignorée. Les valeurs autorisées sont Y ou N. La valeur par défaut est N. **EXEMPLE** : UPGRADE_DATABASE=Y
BACKUP_DATABASE	Spécifie que la base de données du Répertoire doit être sauvegardée avant l'installation (et avant la mise à niveau de la base de données). Les fichiers de configuration sont également sauvegardés dans le même dossier que la base de données. Si la base de données n'existe pas, les fichiers de configuration sont quand même sauvegardés. Les valeurs autorisées sont Y ou N. En cas d'omission, la valeur par défaut est N. Lorsqu'elle est réglée sur Y, un dossier valable doit être spécifié pour la propriété BACKUP_DATABASE_PATH. **EXEMPLE** : BACKUP_DATABASE=Y

Option du programme d'installation (MSI)	Description
BACKUP_DATABASE_PATH	Utilisé en conjonction avec l'option BACKUP_DATABASE. Spécifie le dossier de sauvegarde de la base de données. Si le chemin n'existe pas, il est créé. **EXEMPLE** : BACKUP_DATABASE_PATH=C:\Backups
SERVICEUSERNAME	Spécifie le nom d'utilisateur utilisé pour les services. **EXEMPLE** : SERVICEUSERNAME=.\admin
SERVICEPASSWORD	Spécifie le mot de passe utilisé pour les services. **EXEMPLE** : SERVICEPASSWORD=unmotdepasse L'utilisateur et le mot de passe doivent être créés avec les bons identifiants avant d'utiliser ces propriétés. En cas d'omission, la valeur par défaut est vide.
SERVERADMIN_PORT	Spécifie le port HTTP pour l'application web Server Admin. **EXEMPLE** : SERVERADMIN_PORT=8080 En cas d'omission, la valeur par défaut est 5500.
SERVERADMIN_PASSWORD	Spécifiez le mot de passe (8 caractères minimum) pour ouvrir l'app web Server Admin.

Option du programme d'installation (MSI)	Description
LANGUAGECHOSEN	Langue utilisée par Security Center. Les valeurs de code autorisées sont : • Arabe - 1025 • Chinois (Simplifié) - 2052 • Chinois (Traditionnel) - 1028 • Tchèque - 1029 • Néerlandais - 1043 • Anglais - 1033 • Français - 3084 • Allemand - 1031 • Hébreu - 1037 • Hongrois - 1038 • Italien - 1040 • Japonais - 1041 • Coréen - 1042 • Norvégien - 1044 • Persan - 1065 • Polonais - 1045 • Portugais (Brésil) - 2070 • Russe - 1049 • Espagnol - 1034 • Suédois - 1053 • Thaïlandais - 1054 • Turc - 1055 • Vietnamien - 1066 **EXEMPLE** : LANGUAGECHOSEN=3084 Si le code est incorrect, l'anglais est utilisé. En cas d'omission, la langue d'installation (spécifiée par l'option d'installation /language:) est utilisée.
WEBSERVER_PORT	Spécifie le port HTTP pour l'application Web Server Admin. En cas d'omission, la valeur par défaut est 80.
CREATE_FIREWALL_RULES	Ajoute les applications Security Center installées à la liste des exceptions du pare-feu de Windows. Les valeurs autorisées sont 0 ou 1. • 0 = Ne pas créer de règles de pare-feu • 1 = Créer des règles de pare-feu (VALEUR PAR DÉFAUT) **EXEMPLE** : CREATE_FIREWALL_RULES=1
MAINSERVER_ENDPOINT	Utilisé pour l'installation d'un serveur d'extension. Spécifiez le nom DNS ou l'adresse IP du serveur principal. **EXEMPLE** : MAINSERVER_ENDPOINT=MYMAINSERVER

Option du programme d'installation (MSI)	Description
MAINSERVER_PASSWORD	Utilisé pour l'installation d'un serveur d'extension. Entrez le mot de passe du serveur principal auquel il doit se connecter.
DATACOLLPOLICY	Cette option permet la configuration du Service Availability Monitor (SAM). Les valeurs possibles sont: • Anonymous: SAM recueillera des données anonymes (VALEUR PAR DÉFAUT) • On: SAM recueillera des données accompagnées d'informations système. Nécessite ACTIVATIONCODE. • Off: SAM ne recueillera pas de données.
ACTIVATIONCODE	Il s'agit du code d'activation requis pour autoriser SAM à recueillir des données système. **EXEMPLE** : DATACOLLPOLICY=On ACTIVATIONCODE=mycode
SECURE_COMMUNICATION	Valeur booléenne qui spécifie si la communication sécurisée (l'authentification du Répertoire) doit être appliquée. • 0 = Non appliqué ; l'authentification du Répertoire est désactivée (VALEUR PAR DÉFAUT) • 1 = Appliquée ; l'authentification du Répertoire est activée **EXEMPLE** : SECURE_COMMUNICATION=1
DEACTIVBASIC	Valeur booléenne qui indique si l'authentification de base pour les caméras doit être désactivée. • 0 = Authentification de base activée • 1 = Authentification de base désactivée (VALEUR PAR DÉFAUT) **EXEMPLE** : DEACTIVBASIC=0
REBOOT	Cette option permet de forcer ou d'empêcher le redémarrage une fois l'installation Server terminée. Les valeurs autorisées sont : • F - Pour forcer un redémarrage une fois l'installation terminée. • S - Pour empêcher le redémarrage, sauf en cas de recours à l'action ForceReboot. • R - Pour empêcher tout redémarrage entraîné par les actions du programme d'installation de Windows. (VALEUR PAR DÉFAUT)
SKIPSERVICESTART	Cette option permet d'éviter de démarrer les services Security Center immédiatement après l'installation (le comportement par défaut), si vous devez installer des correctifs après l'installation par exemple. Si vous utilisez cette option, n'oubliez pas de démarrer les services Security Center (NET START GenetecServer et NET START GenetecWatchdog) après l'installation des correctifs. **EXEMPLE** : SKIPSERVICESTART=Y

Exemples de commandes d'installation de Security Center Server

Les différentes options de commande vous permettent de personnaliser votre installation silencieuse de Security Center Server.

Exemple

Genetec Server et le Répertoire sont installés en anglais avec un nom d'utilisateur et un mot de passe particuliers pour l'exécution du service. Les fichiers sont placés dans un nouveau dossier, le serveur de base de données est spécifié, et le redémarrage est bloqué. L'installation est exécutée en mode silencieux, sans questions.

```
"Security Center Setup.exe" /silent /language:1033 ISFeatureInstall=Server /
ISInstallDir=C:\NewServer SERVICEUSERNAME=.\toto SERVICEPASSWORD=motdepasse
 DATABASE_SERVER=(local)\Genetec DATABASE_INSTANCE=RépertoireSecurityCenter REBOOT=S
```

Exemple

Installation standard de Genetec Server en tant que serveur principal, avec Répertoire et sans questions. Seul le chemin d'installation est différent.

```
"Security Center Setup.exe" /language:1033 /silent /ISInstallLDir=c:\GENETEC_PATH /
ISFeatureInstall=Server
```

Exemple

Installation standard de Genetec Server en tant que serveur d'extension, sans questions. Seul le chemin d'installation est différent.

```
"Security Center Setup.exe" /language:1033 /silent /ISInstallLDir=c:\GENETEC_PATH /
ISFeatureInstall=Server SERVER_TYPE=Expansion
```

Exemple

Installation standard en mode silencieux, sans questions, en français.

```
"Security Center Setup.exe" /language:3084 /silent
```

Exemple

Installation complète en anglais, avec les packs de compatibilité Omnicast 4.7 et 4.8, en mode silencieux et sans questions. Le nom de serveur de base de données par défaut, (local)\SQLExpress, est utilisé pour le Répertoire.

```
"Security Center Setup.exe" /language:1033 /silent /
ISFeatureInstall=Client,Server,CompPacks,CompPack47,CompPack48
```

Exemple

Installation complète en mode silencieux, sans questions, en anglais. Cette installation crée un fichier journal sur le disque C:.

```
"Security Center Setup.exe" /language:1033 /silent /ISFeatureInstall=Client,Server /
log"C:\" /debuglog"C:\DebugLog.log"
```

Exemple

Installation complète en mode silencieux, sans questions, en anglais. Security Center Les applications utiliseront l'arabe.

```
"Security Center Setup.exe" /language:1033 /silent /ISFeatureInstall=Client,Server
 LANGUAGECHOSEN=1025
```

Exemples de commandes d'installation de Security Center Client

Les différentes options de commande vous permettent de personnaliser votre installation silencieuse de Security Center Client.

Exemple

Security Desk Installation en mode silencieux, sans questions, en anglais.

```
"Security Center Setup.exe" /language:1033 /silent /ISInstallDir=c:\GENETEC_PATH /
ISFeatureInstall=SecurityDesk
```

Exemple

Config Tool et Security Desk sont installés en mode silencieux, sans questions, en français.

```
"Security Center Setup.exe" /language:3084 /silent /ISInstallDir=c:\GENETEC_PATH /
ISFeatureInstall=ConfigTool,SecurityDesk
```

Exemple

Config Tool et Security Desk sont installés en mode silencieux, sans questions, en anglais.

```
"Security Center Setup.exe" /language:1033 /silent /ISInstallDir=c:\GENETEC_PATH /
ISFeatureInstall=ConfigTool,SecurityDesk
```

Exemple

Installation standard en français, en mode silencieux et sans questions.

```
"Security Center Setup.exe" /language:3084 /silent
```

Exemple

Installation complète en anglais, avec le pack de compatibilité Omnicast 4.8, en mode silencieux et sans questions.

```
"Security Center Setup.exe" /language:1033 /silent /
IsInstallFeature=Client,Server,CompPacks,CompPack48
```

Exemple

Installation complète en mode silencieux, sans questions, en anglais. Security Center Les applications utiliseront l'arabe.

```
"Security Center Setup.exe" /language:1033 /silent /ISFeatureInstall=Client,Server
 LANGUAGECHOSEN=1025
```

Désinstaller Security Center en mode silencieux

Security Center peut être désinstallé en mode silencieux.

Pour désinstaller Security Center (composants Client et Server) en mode silencieux :

1 Exécutez la commande suivante depuis le dossier *SC Packages* du pack d'installation de Security Center :
```
"Security Center Setup.exe" /silent /remove
```

Pour désinstaller les composants Security Center Client (lorsque Server est également installé) :

1 Exécutez la commande suivante depuis le dossier *SC Packages* du pack d'installation de Security Center :
```
"Security Center Setup.exe" /silent /ISFeatureRemove=Client
```

Pour désinstaller les composants Security Center Server (lorsque Client est également installé) :

1 Exécutez la commande suivante depuis le dossier *SC Packages* du pack d'installation de Security Center :
```
"Security Center Setup.exe" /silent /ISFeatureRemove=Server
```

4

Dépannage

Cette section aborde les sujets suivants:

Dépannage :problèmes de stabilité et de performances vidéo

Après l'installation de Security Center, vous devrez parfois installer des correctifs Microsoft pour assurer le bon fonctionnement de Security Center.

À savoir

Les situations suivantes nécessitent l'installation d'un correctif Microsoft :

- Vous vous connectez à Config Tool ou à Security Desk après l'installation de Security Center, et vous recevez le message : « Une dépendance requise pour cette application est introuvable sur le système. La stabilité et les performances vidéo ne seront pas garanties sans le correctif KB2494124/KB2468871 ».
- Vous installez Security Center sur un système 64 bits. Pour améliorer les performances, vous devez installer le correctif KB2588507.

Pour installer les correctifs Microsoft :

1 Fermez Config Tool et Security Desk.
2 Téléchargez les correctifs nécessaires sur Internet :
   - Pour les ordinateurs 64 bits, téléchargez les fichiers suivants :
     - *NDP40-KB2468871-v2-IA64.exe*
     - *NDP40-KB2468871-v2-x64.exe*
     - *NDP40-KB294124-x64.exe*
     - *Windows6.1-KB2588507-v2-x64.msu*
   - Pour les ordinateurs 32 bits, téléchargez les fichiers suivants :
     - *NDP40-KB2468871-v2-x86.exe*
     - *NDP40-KB294124-x86.exe*
3 Exécutez les correctifs les uns après les autres, en suivant l'ordre de téléchargement.
4 Redémarrez votre ordinateur.

Dépannage : Des fichiers restent bloqués après un déblocage manuel

Utilisez *streams.exe* pour débloquer les fichiers du pack d'installation Security Center qui restent bloqués après une intervention manuelle.

À savoir

Vous ne devez exécuter *streams.exe* que sur les fichiers qui restent bloqués après l'échec d'une tentative de les débloquer manuellement. Le message d'erreur qui apparaît pendant l'installation ressemble à : « Ficher(s) bloqué(s) détecté(s) dans le pack de téléchargement. Le programme d'installation va s'arrêter. Pour relancer l'installation, débloquez le pack téléchargé. »

Pour débloquer des fichiers avec *streams.exe* :

1 Téléchargez *streams.exe* sur https://technet.microsoft.com/en-ca/sysinternals/bb897440.aspx.

2 Ouvrez l'invite de commande.

3 Entrez `streams.exe -d` <nom de fichier>, où <nom de fichier> est le nom du fichier à débloquer.

Lorsque vous avez terminé

Si vous avez débloqué le fichier d'installation ZIP (au lieu de son contenu), vous devez à nouveau extraire son contenu avant de procéder à l'installation de Security Center.

Rubriques connexes

Débloquer des fichiers manuellement, page 13

Glossaire

A

action	Une action est une fonction programmable par l'utilisateur pouvant être déclenchée automatiquement en réaction à un événement, comme une porte entrebâillée trop longtemps ou un objet laissé sans surveillance, ou pouvant être exécutée en fonction d'un horaire particulier.
alarme active	Une alarme active est une alarme qui n'a pas encore été acquittée.
Active Directory	Service d'annuaire créé par Microsoft, et type de rôle qui importe les utilisateurs et titulaires de cartes d'un annuaire Active Directory et assure leur synchronisation.
Advanced Systems Format	Le format ASF (Advanced Systems Format) est un format de streaming vidéo de Microsoft. Le format ASF ne peut être affiché que par des logiciels de lecture multimédias compatibles, comme Windows Media Player.
agent	Sous-processus créé par un rôle Security Center pour une exécution simultanée sur plusieurs serveurs afin de répartir la charge.
alarme	Type d'entité qui décrit une situation problématique particulière qui nécessite une attention immédiate, et la manière dont elle doit être traitée dans Security Center. Par exemple, une alarme peut indiquer les entités impliquées (généralement des caméras et des portes), les personnes à notifier, la manière de l'afficher pour l'utilisateur, etc.
acquittement d'une alarme	Un acquittement d'alarme est la réponse de l'utilisateur à une alarme. Il existe deux variantes d'acquittement d'alarmes dans Security Center : l'acquittement par défaut et l'acquittement secondaire. Chaque variante est associée à un événement différent pour permettre la programmation de différentes actions en fonction du type d'acquittement sélectionné par l'utilisateur.
Alarmes	Type de tâche d'administration qui permet de configurer les alarmes et les groupes de moniteurs analogiques.
antiretour	L'antiretour correspond à une restriction d'accès à un secteur sécurisé empêchant un titulaire de cartes de pénétrer dans un secteur qu'il n'a pas encore quitté, ou inversement.

Archiveur	Type de rôle responsable de la découverte, la vérification de l'état et le contrôle des unités vidéo. L'Archiveur gère également l'archivage vidéo, et effectue la détection de mouvement si elle n'est pas réalisée sur l'unité elle-même.
Archives	Type de tâche d'investigation qui permet de rechercher et d'afficher les archives vidéo disponibles, par caméra et par horaire.
Activités de secteurs	Type de tâche de maintenance qui répertorie les événements relatifs à certains rôles Archiveur.
actif	Type d'entité qui représente tout objet de valeur équipé d'une puce RFID qui permet de le surveiller avec un logiciel de gestion d'actifs.
AutoVu^{MC}	AutoVu^{MC} est le système de reconnaissance automatique de plaques d'immatriculation (RPI) sur IP de Security Center qui automatise la lecture et la vérification de plaques d'immatriculation de véhicules. Les caméras AutoVu^{MC} enregistrent des images de plaques d'immatriculation et envoient ces données aux patrouilleurs ou au centre de sécurité afin que ceux-ci puissent les comparer aux listes des véhicules recherchés (liste critique) et à la liste des véhicules autorisés (liste d'autorisations). Vous pouvez installer AutoVu^{MC} pour des applications d'identification de contrevenants et de véhicules recherchés, de surveillance urbaine, de contrôle du stationnement, de contrôle d'accès aux aires de stationnement, d'inventaire de véhicules, de sécurité et de contrôle d'accès.
Archiveur auxiliaire	Type de rôle qui complète l'archive vidéo créée par l'Archiveur. Contrairement à l'Archiveur, l'Archiveur auxiliaire n'est pas lié à un *port de découverte* particulier. Il peut donc archiver n'importe quelle caméra du système, dont les caméras fédérées depuis d'autres systèmes Security Center. L'Archiveur auxiliaire s'appuie sur l'Archiveur principal pour communiquer avec les unités vidéo. Il ne peut pas fonctionner seul.
Activités de titulaires de cartes	Type de tâche d'investigation qui répertorie les activés liées à un titulaire de cartes (accès refusé, premier entré, dernier sorti, violation antiretour, etc.).
alerte fantôme	Lecture (capture de plaque d'immatriculation) comparée à une liste de véhicules recherchés fantômes. Les alertes fantômes ne sont pas affichées sur l'écran du Patroller, mais sont affichées dans Security Desk par un utilisateur disposant des privilèges nécessaires.
Activités d'identifiants	Type de tâche d'investigation qui répertorie les activités liées aux identifiants (accès refusé en cas d'expiration, identifiants inactifs, perdus ou volés, etc.).

antirebond	Temps nécessaire pour le changement d'état d'une entrée (ex. : actif vers inactif) avant que ce changement soit signalé. Les commutateurs électriques peuvent entraîner des signaux temporaires instables en cas de changement d'état qui peuvent déboussoler les circuits logiques. L'antirebond sert à filtrer les signaux instables en ignorant tous les changements d'états dont la durée est inférieure à un laps de temps déterminé (en millisecondes).
Activités de portes	Type de tâche d'investigation qui analyse les activités liées aux portes (accès refusé, porte forcée, porte ouverte trop longtemps, sabotage matériel, etc.).
ascenseur	Type d'entité qui dote les ascenseurs de propriétés de contrôle d'accès. Pour un ascenseur, chaque étage est considéré en tant que point d'entrée.
Activités d'ascenseurs	Type de tâche d'investigation qui analyse les activités liées aux ascenseurs (accès refusé, accès à l'étage, unité hors ligne, sabotage matériel, etc.).
appliquer	Entreprendre une action suite à une infraction confirmée. Un agent de stationnement peut par exemple appliquer une violation à un contrevenant (contraventions impayées) en plaçant un sabot sur une roue d'un véhicule.
arborescence des entités	Représentation graphique des entités de Security Center sous forme d'arborescence afin d'illustrer les relations hiérarchiques entre les entités.
accès libre	Point d'accès à un secteur sécurisé pour lequel aucun identifiant n'est requis. La porte est déverrouillée. Il s'agit généralement d'un état durant les heures de bureau, d'une mesure temporaire en cas de maintenance ou lors du lancement du système de contrôle d'accès, avant sa configuration.
alerte	Lecture de plaque d'immatriculation qui correspond à une règle d'alerte associée à une liste de véhicules recherchés, une règle de dépassement horaire, un permis ou une restriction de permis. Dans Patroller, l'utilisateur peut accepter ou refuser une alerte. Une alerte acceptée peut alors être appliquée.
Alertes	Type de tâche d'investigation qui analyse les alertes rapportées durant une période donnée et dans une zone géographique donnée.
action éclair	Action affectée à une touche de fonction du clavier du PC (Ctrl +F1 à Ctrl+F12) dans Security Desk pour un accès rapide.
Activités de secteurs de détection d'intrusion	Type de tâche d'investigation qui analyse des activités (armement global, armement du périmètre, contrainte,

	problème d'entrée, etc.) dans certains secteurs de détection d'intrusion.
alerte en temps réel	Alerte identifiée par Patroller et immédiatement envoyée à Security Center par réseau sans fil.
affichage de carte	Un affichage est une position et un facteur de zoom prédéfinis sur une carte donnée.
armement global	L'armement global consiste à armer un secteur de détection d'intrusion de manière à ce que tous les capteurs affectés au secteur déclenchent l'alarme en cas d'activation de l'un d'eux.
aire de stationnement	Polygone définissant le lieu et la forme d'une aire de stationnement sur une carte. En définissant le nombre de places de l'aire de stationnement, Security Center peut calculer son pourcentage d'occupation sur une période donnée.
administrateur de partition	Un administrateur de partition est un utilisateur autorisé d'une partition disposant des droits d'administration sur la partition et ses membres. Il peut ajouter, modifier et supprimer la plupart des entités au sein de la partition, dont les utilisateurs, groupes d'utilisateurs et les partitions enfant, à l'exception des rôles. L'administrateur de partition peut modifier les rôles au sein de la partition, mais il ne peut ni en ajouter, ni en effacer.
armer le périmètre	Armement d'un secteur de détection d'intrusion de manière à ce que seuls les capteurs affectés au périmètre du secteur déclenchent l'alarme en cas d'activation de l'un d'eux. Les autres capteurs, comme les capteurs de mouvement à l'intérieur du secteur, sont ignorés.
alerte de permis	Alerte générée lorsqu'une lecture (de numéro de plaque d'immatriculation) ne correspond pas à un permis ou correspond à un permis non valable.
adresse IP privée	Adresse IP sélectionnée au sein d'une plage d'adresses qui ne sont valables que pour une utilisation sur un réseau local. Les plages d'adresses IP privées sont : 10.0.0.0 à 10.255.255.255, 172.16.0.0 à 172.16.255.255 et 192.168.0.0 à 192.168.255.255. Les routeurs sur Internet sont généralement configurés pour ignorer tout trafic utilisant des adresses IP privées.
agent de redirection	Agent créé par le rôle Routeur multimédia pour rediriger les flux de données d'un point d'extrémité IP vers un autre.
archivage redondant	Option permettant l'archivage simultané d'une copie de tous les flux vidéo d'un rôle Archiveur sur un serveur de secours, afin d'éviter les pertes de données.
antiretour strict	Option de l'antiretour. Lorsque cette option est activée, un événement antiretour est généré lorsqu'un titulaire de cartes tente de quitter un secteur auquel l'accès ne lui a pas été

	accordé. Lorsqu'elle est désactivée, Security Center ne génère un événement antiretour que lorsqu'un titulaire pénètre dans un secteur qu'il n'a jamais quitté.
antiretour avec délai	Option de l'antiretour. Lorsque Security Center considère qu'un titulaire de cartes est déjà présent dans un secteur, un événement antiretour est généré si ce titulaire tente d'accéder de nouveau au même secteur durant un laps de temps défini par le *Délai d'expiration de présence*. Une fois ce laps de temps écoulé, le titulaire peut à nouveau accéder au secteur sans générer d'événement antiretour.
analyse vidéo	Technologie logicielle servant à analyser le contenu vidéo à la recherche d'informations particulières. Le comptage des individus passant une porte, la reconnaissance de plaques d'immatriculation, la détection d'objets sans surveillance ou la direction d'individus qui marchent/courent sont tous des exemples d'analyse vidéo.
archive vidéo	Une archive vidéo contient les séquences audio et vidéo, ainsi qu'une base de données qui documente l'enregistrement (caméra source, horodatage, événements, signets, etc.).
Activités de visiteurs	Type de tâche d'investigation qui répertorie les activés liées aux visiteurs (accès refusé, premier entré, dernier sorti, violation antiretour, etc.).
Activités de zones	Type de tâche d'investigation qui analyse des activités liées à une zone (armement ou désarmement d'une zone, serrure verrouillée ou déverrouillée, etc.).

B

Boîte de dérivation	Boîte de dérivation propriétaire de Genetec pour les solutions AutoVu mobiles qui utilisent les caméras Sharp. La boîte de dérivation fournit l'alimentation et la connectivité réseau aux unités Sharp et à l'ordinateur embarqué dans le véhicule.
blocage de caméra	Fonctionnalité Omnicast qui permet de restreindre l'affichage de la vidéo (en direct ou enregistrée) provenant de certaines caméras aux utilisateurs dotés d'un niveau utilisateur minimum.
basculement	Mode d'exploitation de secours dans lequel un rôle (fonction du système) est automatiquement transféré d'un serveur principal à un serveur secondaire en attente. Ce transfert entre serveurs ne survient qu'en cas d'indisponibilité du serveur principal en raison d'une panne ou pour cause de maintenance programmée.
barre des tâches	Élément d'interface de la fenêtre de l'application client de Security Center composé de l'onglet Accueil et de la liste de tâches actives. La barre des tâches peut être configurée

	de manière à apparaître sur un des bords de la fenêtre de l'application.

C

Contrôle d'accès	Type de tâche d'administration qui permet de configurer les rôles, unités, règles, titulaires de cartes et identifiants de contrôle d'accès, ainsi que les entités et réglages associés.
Configuration de règle d'accès	Type de tâche maintenance qui répertorie les entités et points d'accès affectés par une règle d'accès donnée.
codeur audio	Périphérique ou logiciel qui code les flux audio en utilisant un algorithme de compression. Synonyme de *microphone*.
Concepteur de badges	Outil qui permet de concevoir et modifier des modèles de badges.
caméra	Type d'unité vidéo représentant une source vidéo unique du système. La source vidéo peut être une caméra IP, ou une caméra analogique connectée au codeur vidéo d'une unité vidéo. Plusieurs flux vidéo peuvent être générés à partir d'une même source vidéo.
Configuration des caméras	Type de tâche de maintenance qui permet de consulter les propriétés et les réglages des caméras locales (fabricant, résolution, débit d'image, etc.).
canevas	Le canevas est l'un des volets de l'espace de travail de Security Desk. Le canevas permet d'afficher les informations multimédias, telles que les vidéos, les cartes et les photos. Il est divisé en trois volets :les tuiles, le tableau de bord et les propriétés.
carte et code PIN	Mode de point d'accès qui oblige le titulaire de cartes à passer une carte dans un lecteur, puis à saisir un code PIN.
Configuration de titulaires de cartes	Type de tâche de maintenance qui répertorie les propriétés de titulaires de cartes (nom, prénom, photo, état, propriétés personnalisées, etc.).
caisse enregistreuse	Type d'entité qui représente une caisse enregistreuse (ou un terminal) d'un système de point de vente.
certificat	Désigne l'une des options suivantes : *certificat d'identité* ; (2) *certificat de SDK*.
Config Tool	Application d'administration de Security Center qui sert à gérer tous les utilisateurs de Security Center et à configurer toutes les entités Security Center, comme les secteurs, caméras, portes, horaires, titulaires de cartes, unités Patroller/RAPI et périphériques matériels.

caméra contextuelle	Caméra connectée à une unité de RAPI qui génère une image grand-angle en couleur du véhicule dont la plaque a été lue par la caméra de RAPI.
code d'identifiant	Représentation textuelle de l'identifiant permettant d'afficher les données de l'identifiant (généralement le code d'installation et le numéro de carte). Pour les identifiants basés sur des formats de carte personnalisés, l'utilisateur peut choisir les données incluses dans le code d'identifiant.
Configuration d'identifiants	Type de tâche de maintenance qui répertorie les propriétés d'identifiants (état, titulaire de cartes affecté, format de carte, code d'identifiant, propriétés personnalisées, etc.).
champ personnalisé	Propriété définie par l'utilisateur associée à un type d'entité servant à stocker des informations complémentaires utiles à votre organisation.
contact de porte	Un contact de porte surveille l'état d'une porte (ouverte ou fermée). Il peut également servir à détecter un état anormal (porte ouverte trop longtemps).
côté de porte	Chaque porte a deux côtés, appelés *Entrée* et *Sortie* par défaut. Chaque côté est un point d'accès à un secteur. Par exemple, le passage par un côté permet de pénétrer dans un secteur et le passage par l'autre côté permet de le quitter. Dans le cadre de la gestion des accès, les identifiants requis pour passer une porte dans un sens ne sont pas forcément les mêmes que pour passer cette porte dans le sens inverse.
contrainte	Code spécial servant à désarmer un système d'alarme. Ce code alerte silencieusement un poste de surveillance que le système d'alarme a été désarmé sous la contrainte.
caméra fantôme	Entité utilisée en tant que caméra de substitution. Cette entité est créée automatiquement par Omnicast lorsque des archives vidéo doivent être restaurées pour une caméra dont la définition a été supprimée du Répertoire, soit parce que le périphérique matériel n'existe plus, soit parce que l'entité a été supprimée par erreur. Elles n'existent que pour que les utilisateurs puissent référencer une archive vidéo qui serait orpheline en l'absence de ce mécanisme.
Configuration d'E/S	Type de tâche de maintenance qui répertorie les configurations d'E/S (points d'accès contrôlés, portes et ascenseurs) d'unités de contrôle d'accès.
caméra IP	Unité vidéo intégrant une caméra.
clé de licence	Clé logicielle permettant de déverrouiller le logiciel Security Center. Cette clé de licence est générée spécifiquement pour chaque ordinateur sur lequel le service Répertoire est installé. Pour obtenir votre clé de licence, vous devez fournir l'*ID*

	du système (identification du système) et la *clé de validation* (identifiant du PC).
Connexions par Patroller	Type de tâche d'investigation qui répertorie les connexions effectuées par un Patroller donné.
Caméra de RAPI	Caméra connectée à une unité de RAPI qui produit des gros plans en haute résolution des plaques d'immatriculation.
capture manuelle	Saisie d'informations de plaque d'immatriculation par l'utilisateur au lieu de la RAPI.
Comptage d'individus	Type de tâche d'exploitation qui suit en temps réel le nombre de titulaires de cartes au sein des secteurs sécurisés de votre système.
client de partage	Système Security Center autorisé à afficher et modifier des entités partagées par un autre système.
cycle de tâches	Fonctionnalité de Security Desk qui permet de faire défiler les tâches de la liste de tâches active, en fonction d'une durée d'affichage prédéfinie.
clé de validation	Numéro de série unique qui identifie un ordinateur, nécessaire pour obtenir la clé de licence.
Coffre-fort	Outil permettant d'afficher les instantanés enregistrés et les fichiers vidéo exportés au format G64, G64x et GEK (chiffré). Dans le Coffre-fort, vous pouvez lire les fichiers vidéo, chiffrer et déchiffrer les fichiers, les convertir au format ASF et les préparer avec Genetec Video Player.
codeur vidéo	Un codeur vidéo est un appareil vidéo qui convertit une source vidéo analogique en un format numérique à l'aide d'un algorithme de compression standard, comme le H.264, MPEG-4, MPEG-2 ou M-JPEG. Le codeur vidéo est l'un des nombreux équipements dont sont dotées les unités de codage vidéo.
chien de garde	Service Security Center installé avec le service Genetec Server sur chaque ordinateur serveur. Le chien de garde surveille le bon fonctionnement du service Genetec Server, et le relance en cas de détection de conditions anormales.

D

droit d'accès	Droit de base dont les utilisateurs doivent disposer sur une partie du système pour pouvoir interagir avec lui. D'autres droits, comme afficher et modifier la configuration d'entités, sont accordés par le biais des privilèges. Dans le contexte du système Synergis^{MC}, un droit d'accès est accordé au détenteur de la carte pour lui permettre de passer par un point d'accès à une date et une heure données.

Détails de stockage d'archive	Type de tâche de maintenance qui répertorie les fichiers vidéo (nom de fichier, heure de début et de fin, taille du fichier, état de la protection, etc.) utilisés pour stocker les archives vidéo, et qui permet de modifier l'état de protection des fichiers, parmi d'autres choses.
décodeur audio	Périphérique ou logiciel qui décode les flux audio compactés pour leur lecture. Synonyme de *haut-parleur*.
diffusion	Technique de communication entre un seul émetteur et tous les récepteurs d'un réseau.
Droits d'accès de titulaire de cartes	Type de tâche de maintenance qui répertorie les titulaires de cartes et groupes de titulaires de cartes qui sont autorisés ou non à accéder à des secteurs, portes ou ascenseurs.
Data Server	Module serveur Plan Manager qui gère la base de données Plan Manager qui stocke la configuration de la carte.
Diagnostic de porte	Type de tâche de maintenance qui recense tous les titulaires de cartes ayant accès à un côté de porte particulier ou à un étage d'ascenseur à un moment donné.
Détection d'intrusion	Type de tâche d'administration qui permet de configurer les rôles et unités de détection d'intrusion.
détection de mouvement	Fonctionnalité qui permet de détecter les changements au sein d'une série d'images vidéo. La définition de ce qui constitue du « mouvement » dans une vidéo peut relever de critères très sophistiqués.
Déplacer l'unité	Outil servant à déplacer une unité d'un rôle gestionnaire vers un autre. La configuration et les données de l'unité sont conservées lors du déplacement. Après le déplacement, le nouveau gestionnaire assume le contrôle de l'unité, tandis que l'ancien gestionnaire continue à gérer les données recueillies par l'unité avant son déplacement.
Distant	Type de tâche d'exploitation qui permet de surveiller et contrôler à distance d'autres postes Security Desk de votre système, par le biais de la tâche Surveillance et de la tache Surveillance d'alarmes.
demande de passage	La demande de passage (REX ou request to exit) est un bouton de déverrouillage de porte généralement situé à l'intérieur d'un secteur sécurisé et qui permet à un individu de quitter le secteur sécurisé sans présenter d'identifiants. Il peut également s'agir du signal d'un capteur de mouvement. Il s'agit également du signal reçu par le contrôleur pour une requête de sortie.
décodeur vidéo	Un codeur vidéo est un périphérique qui convertit un flux vidéo numérique en signaux analogiques (NTSC ou PAL) pour lecture sur un moniteur analogique. Le décodeur vidéo est un

	des nombreux périphériques dont sont équipées les unités de décodage vidéo.
Détails de visite	Type de tâche d'investigation qui analyse le séjour (inscription et radiation) de visiteurs (présents et passés).

E

enregistrement sur périphérique	Processus d'enregistrement et de stockage vidéo en local, sans recours à un serveur d'enregistrement centralisé. L'enregistrement sur périphérique permet de stocker la vidéo directement sur le support de stockage intégré à la caméra.
entité	Les entités sont les composants de base de Security Center. Tout ce qui requiert une configuration est représenté par une entité. Les entités peuvent représenter un objet physique, comme une caméra ou une porte, ou une notion abstraite, comme une alarme, un horaire, un utilisateur, un rôle, un module externe ou un composant logiciel.
entité fédérée	Toute entité importée d'un système indépendant par l'intermédiaire d'un rôle Fédération.
entité globale	Entité partagée par plusieurs systèmes Security Center indépendants en vertu de son appartenance à une partition globale. Seuls les titulaires de cartes, groupes de titulaires de cartes et modèles de badge sont éligibles pour le partage.
entité inactive	Entité teintée en rouge dans le navigateur d'entités. Signale que l'entité physique représentée par l'entité est en panne, hors ligne ou mal configurée.
extension de fabricant	Réglages propres à un fabricant d'unités de contrôle d'accès, d'unités vidéo et d'unités de détection d'intrusion.
espace de travail	Zone de l'application client de Security Center réservée pour la tâche en cours. L'espace de travail est composé des volets suivants :canevas, volet de rapport, tableau de bord et vue secteur.
Explorateur de fichiers vidéo	Type de tâche d'investigation qui recherche des fichiers vidéo (G64 et G64x) dans le système de fichiers et permet de les lire, les convertir au format ASF et en vérifier l'authenticité.

F

Federation[MC]	La fonctionnalité Federation[MC] réunit plusieurs systèmes de sécurité sur IP Genetec[MC] indépendants dans un système virtuel unique. Grâce à cette fonctionnalité, les utilisateurs de Security Center peuvent afficher et contrôler les entités qui appartiennent aux systèmes fédérés directement depuis leur système Security Center local.

fournisseur d'identité	Site Internet qui gère les comptes utilisateur et qui est responsable de générer et de gérer les informations d'identité et d'authentification des utilisateurs. Par exemple, Google gère les comptes Gmail de ses utilisateurs, qui permettent un accès par connexion unique à d'autres sites web.
Forces de l'ordre	Installation du logiciel Patroller configurée pour les forces de l'ordre :les lectures de plaques sont comparées à des listes de plaques recherchées (listes de véhicules recherchés). L'utilisation de cartes est facultative.
frise chronologique	Représentation graphique d'une séquence vidéo, avec des repères temporels représentant du mouvement et des signets. Des vignettes peuvent être ajoutées à la frise pour aider à identifier les sections dignes d'intérêt.
fichier vidéo	Fichier créé par un rôle d'archivage (Archiveur ou Archiveur auxiliaire) pour stocker de la vidéo. L'extension de fichier utilisée est G64 ou G64x. Vous devez disposer de Security Desk ou de Genetec Video Player pour lire les fichiers vidéo.
flux vidéo	Entité représentant une configuration de qualité vidéo particulière (format de données, résolution de l'image, débit binaire, débit d'image, etc.) pour une caméra.
filature visuelle	Fonctionnalité de Security Desk qui permet de suivre un individu lorsqu'il se déplace de secteur en secteur, sans perdre le contact visuel dès lors que les secteurs sont surveillés par des caméras.Cette fonctionnalité affiche des incrustations semi-opaques sur la vidéo qui indiquent où cliquer pour basculer vers une caméra adjacente.

G

Gestionnaire d'accès	Gestionnaire d'accès est le rôle qui gère et surveille les unités de contrôle d'accès du système.
groupe de titulaires de cartes	Type d'entité permettant de configurer les droits d'accès en commun d'un groupe de titulaires de cartes.
Gestion des titulaires de cartes	Type de tâche d'exploitation qui permet de créer, modifier et supprimer des titulaires de cartes. Cette tâche permet également de gérer leurs identifiants, y compris les cartes temporaires.
Gestion des identifiants	Type de tâche d'exploitation qui permet de créer, modifier et supprimer des identifiants. Elle permet également d'imprimer des badges et d'inscrire un grand nombre de cartes d'accès dans le système, soit en les passant dans un lecteur de cartes particulier, soit en saisissant des plages de valeurs.

Gestionnaire de Répertoire	Rôle qui gère le basculement du Répertoire et la répartition de la charge afin d'obtenir la disponibilité élevée qui caractérise Security Center.
gâche de porte électrique	Dispositif électrique qui libère le verrou de porte lorsqu'un courant est envoyé.
G64	Format Security Center utilisé par les rôles d'archivage (Archiveur et Archiveur auxiliaire) pour stocker les séquences vidéo issues d'une caméra unique. Ce format de données prend en charge l'audio, les signets, les métadonnées en surimpression, l'horodatage, les marqueurs de mouvements et d'événements, ainsi que le débit et la résolution variables.
G64x	Format Security Center servant à stocker plusieurs séquences vidéo provenant de plusieurs caméras et exportées ou sauvegardées en même temps. Ce format de données prend en charge l'audio, les signets, les métadonnées en surimpression, l'horodatage, les marqueurs de mouvements et d'événements, ainsi que le débit et la résolution variables et le tatouage numérique.
Genetec Server	Service Windows au cœur de l'architecture de Security Center devant être installé sur tout ordinateur faisant partie de l'ensemble de serveurs de Security Center. Chacun de ces serveurs est une ressource informatique générique apte à accueillir n'importe quel rôle (ensemble de fonctions) que vous lui affectez.
Genetec Video Player	Lecteur multimédia servant à lire les fichiers vidéo exportés depuis Security Desk aux formats G64 et G64x, sur un ordinateur qui n'est pas équipé de Security Center.
géocodage	Processus de déduction de coordonnées géographiques (latitude et longitude) à partir d'une adresse postale.
Geographic information system	Geographic information system (GIS) est un système qui capture des données géographiques. Map Manager peut se connecter à des fournisseurs de services GIS tiers pour fournir des cartes et autres données géolocalisées à Security Center.
Gestionnaire d'intrusions	Type de rôle qui surveille et contrôle les *tableaux d'intrusion* (ou tableaux d'alarmes). Il recueille les événements rapportés par les tableaux d'intrusion, les signale en temps réel dans Security Center, et les consigne dans une base de données pour une utilisation ultérieure.
Gestion d'inventaire	Type de tâche d'exploitation qui permet d'ajouter et rapprocher les lectures de plaques à un inventaire de parc de stationnement.
Gestionnaire RAPI	Type de rôle qui gère et contrôle les Patroller et les unités Sharp fixes. Le Gestionnaire RAPI stocke toutes les données de

	RAPI (lectures, alertes, images, états de véhicules, données GPS etc.) recueillies par les unités de RAPI qu'il gère dans une base de données centralisée à des fins de reporting. Le Gestionnaire RAPI est également chargé de mettre à jour les Sharp fixes et les Patroller sur le terrain avec des correctifs, des mises à jour de listes de véhicules recherchés, etc.
groupe de moniteurs	Type d'entité servant à désigner des moniteurs analogiques pour l'affichage d'alarmes. À part les groupes de moniteurs, le seul autre moyen d'afficher des alarmes en temps réel est d'utiliser la tâche Surveillance d'alarmes dans Security Desk.
Gestionnaire de rapports	Type de rôle qui automatise l'envoi et l'impression de rapports en fonction d'un horaire.
géocodage inversé	Fonctionnalité AutoVu qui traduit une longitude et une latitude en adresse postale.
groupe de transfert	Scénario de transfert d'archive intégrant des réglages particuliers, comme les caméras ou Archiveurs inclus dans le transfert en cours, l'horaire de transfert des archives, les données transférées, etc.
groupe d'utilisateurs	Type d'entité qui définit un groupe d'utilisateurs ayant des propriétés et privilèges en commun. Lorsqu'il rejoint un groupe, un utilisateur hérite automatiquement de toutes les propriétés du groupe. Un utilisateur peut appartenir à plusieurs groupes. Les groupes d'utilisateurs peuvent également être imbriqués.
Gestion des utilisateurs	Type de tâche d'administration qui permet de configurer les utilisateurs, groupes d'utilisateurs et partitions.
Gestion des visiteurs	Type de tâche d'exploitation qui permet d'inscrire, de radier et de modifier les visiteurs, et de gérer leurs identifiants, y compris les cartes temporaires.
Gestionnaire de zones	Type de rôle qui gère les zones virtuelles et déclenche des événements ou des relais de sortie en fonction des entrées configurées pour chaque zone. Il consigne également les événements de zone dans une base de données pour les rapports d'activité de zone.

H

Historiques d'activité	Type de tâche de maintenance qui répertorie les activités des utilisateurs relatives aux fonctions vidéo, de contrôle d'accès et de RAPI. Cette tâche peut fournir diverses informations, comme les personnes ayant lancé la lecture d'un enregistrement vidéo donné, ayant utilisé l'éditeur de liste de véhicules recherchés et de permis, ayant activé le

	filtrage de liste de véhicules recherchés, parmi bien d'autres informations.
Historiques de configuration	Type de tâche de maintenance qui répertorie les modifications de configuration de certaines entités du système, et les personnes responsables de ces modifications.
Historique de demande d'identifiants	Type de tâche d'investigation qui répertorie les utilisateurs ayant demandé, annulé ou imprimé des identifiants de titulaires de cartes.
Haute disponibilité	Approche architecturale permettant à un système de fonctionner à un niveau plus élevé que la normale. S'appuie généralement sur le basculement et l'équilibrage de charge.
horaire	Type d'entité qui définit des contraintes horaires qui peuvent être appliquées à de nombreuses situations au sein du système. Chaque contrainte horaire est décrite par une plage de dates (quotidien, hebdomadaire, mensuel, annuel ou à dates spécifiques) et par une plage horaire (toute la journée, plage fixe, journée ou nuit).
hôte de partage	Système Security Center qui comporte des partitions qui sont partagées avec d'autres systèmes Security Center.
horaire standard	Type d'entité horaire exploitable en toute situation. Sa seule limite est qu'il ne prend pas en charge la couverture de jour ou de nuit.
horaire demi-jour	Type d'entité horaire qui autorise une couverture de jour et de nuit. Les horaires demi-jour ne sont pas adaptés à toutes les situations. Il sert surtout à contrôler des comportements liés à la vidéo.
horaire de déverrouillage	Définit les plages de temps durant lesquelles le passage d'un point d'accès (côté de porte ou étage d'ascenseur) est accordé librement.

I

inscription automatique	Processus selon lequel les unités IP du réseau sont découvertes automatiquement par Security Center. Le rôle chargé des unités envoie en *diffusion générale* un message de découverte sur un port particulier, et les unités qui écoutent sur ce port répondent par un message contenant les informations permettant de se connecter. Le rôle utilise ensuite ces informations pour paramétrer automatiquement la connexion à l'unité et établir les communications.
identifiant	Type d'entité qui représente une carte de proximité, un modèle biométrique ou un code PIN exigé pour accéder à un secteur sécurisé. Un identifiant ne peut être affecté qu'à un titulaire à la fois.

Inventaire matériel	Type de tâche de maintenance qui recense les caractéristiques (modèle, version du micrologiciel, adresse IP, fuseau horaire, etc.) des unités vidéo, de contrôle d'accès, de détection d'intrusion et de RAPI du système.
incident	Tout événement inattendu signalé par un utilisateur de Security Desk. Les rapports d'incident peuvent contenir du texte enrichi et des informations complémentaires sous forme d'événements et d'entités.
Incidents	Type de tâche d'investigation qui permet de rechercher, de valider et de modifier des rapports d'incident.
IPv4	Protocole IP de première génération utilisant un espace d'adresses sur 32 bits.
IPv6	Protocole Internet de nouvelle génération qui amène notamment un espace d'adressage beaucoup plus étendu que le protocole IPv4 actuellement utilisé.
inventaire de plaques d'immatriculation	Liste de numéros de plaques d'immatriculation de véhicules d'un parc de stationnement durant une période donnée, indiquant l'emplacement des véhicules (secteur et rangée).
ID logique	Numéros uniques affectés à chaque entité du système pour pouvoir les identifier facilement. Les identifiants logiques sont uniques seulement pour un type d'entité particulier.
Inventaire mobile de plaques d'immatriculation	Installation logicielle Patroller conçue pour recueillir des numéros d'immatriculation et d'autres informations associées pour créer et actualiser un inventaire de plaques d'immatriculation dans des parcs de stationnement de taille importante.
ID de moniteur	Identifiant unique servant à identifiant un écran de poste de travail contrôlé par Security Desk.
ID de tuile	Numéro affiché dans le coin supérieur gauche d'une tuile de visionnement. Ce numéro identifie de manière unique la tuile sur le canevas.
imagerie des roues	Technologie de marquage virtuel des roues qui capture des images des roues de véhicules afin de savoir s'ils ont été déplacés entre deux lectures de plaques.

K

Kit de développement de pilotes	SDK servant à développer des pilotes de périphériques.
Keyhole Markup Language	Keyhole Markup Language (KML) est un format de fichier conçu pour l'affichage de données géographiques dans un navigateur géographique comme Google Earth et Google Maps.

Kit de développement logiciel	Le SDK (Software Development Kit) permet aux utilisateurs finaux de développer des applications personnalisées ou des extensions pour Security Center.

L

liste de véhicules recherchés fantômes	Liste de véhicules recherchés masquée des utilisateurs d'AutoVu Patroller. Les lectures détectées dans une liste de véhicules recherchés fantômes génèrent des alertes fantômes.
liste de véhicules recherchés	Type d'entité qui définit une liste de véhicules recherchés dans laquelle chaque véhicule est identifié par un numéro de plaque d'immatriculation, l'État émetteur et la raison pour laquelle le véhicule est recherché (volé, personne recherchée, alerte enlèvement, VIP, etc.). D'autres informations peuvent être utilisées, comme le modèle, la couleur et le numéro d'identification du véhicule (VIN).
Liens E/S	Les liens d'entrée/sortie contrôlent un relais de sortie en fonction de l'état combiné (normal, actif ou problème) d'un ensemble d'entrées surveillées. Ils peuvent par exemple servir à déclencher un avertisseur sonore (via un relais de sortie) lorsqu'une fenêtre du rez-de-chaussée d'un immeuble est brisée (si chaque fenêtre est équipée d'un capteur de « bris de glace » relié à une entrée).
lecture de plaque d'immatriculation	Numéro de plaque minéralogique capturé dans une image vidéo par le biais de la technologie de RAPI.
lecture en temps réel	Lecture identifiée par Patroller et immédiatement envoyée à Security Center par réseau sans fil.
long terme	Type de règle de stationnement qui caractérise une règle de dépassement horaire. La règle *long terme* s'appuie sur le même principe que la règle *même position*, sauf que la durée de stationnement est supérieure à 24 heures. Une seule règle de dépassement horaire peut utiliser la règle long terme à l'échelle du système.
lien cartographique	Objet cartographique qui vous redirige vers une autre carte d'un simple clic.
lecteur	Capteur qui lit les identifiants dans le cadre d'un système de contrôle d'accès. Par exemple, il peut s'agir d'un lecteur de cartes ou d'un capteur biométrique.
Lectures	Type de tâche d'investigation qui répertorie les lectures de plaques d'immatriculation effectuées sur une période donnée et dans une zone géographique donnée.
Lectures/alertes par jour	Type de tâche d'investigation qui répertorie les lectures et alertes de plaques d'immatriculation effectuées sur une période donnée et dans une zone géographique donnée.

Lectures/alertes par zone	Type de tâche d'investigation qui répertorie le nombre lectures et d'alertes par zone de stationnement pour une plage de dates donnée.
lecture non rapprochée	Lecture de plaque IMPI qui n'a pas été rapprochée avec un inventaire.

M

moniteur analogique	Type d'entité qui représente un moniteur qui affiche de la vidéo provenant d'une source analogique, comme un décodeur vidéo ou une caméra analogique. Dans Security Center, ce terme désigne les moniteurs qui ne sont pas contrôlés par un poste de travail.
modèle de badge	Type d'entité servant à configurer un modèle d'impression de badges.
module contrôleur	Composant de traitement de données de Synergis Master Controller compatible IP. Module préchargé avec le micrologiciel du contrôleur et un outil d'administration web, Synergis Appliance Portal.
mode dégradé	Mode de fonctionnement hors ligne du module d'interface en cas de perte de connexion à l'unité Synergis. Le module d'interface accorde l'accès à tous les identifiants correspondant à un code d'installation particulier. Seuls les modules d'interface Mercury et HID VertX prennent en charge le mode dégradé.
mode dépendant	Mode de fonctionnement en ligne du module d'interface, lorsque l'unité Synergis prend toutes les décisions de contrôle d'accès. Certains modules d'interface ne prennent pas en charge le mode dépendant.
mécanisme événement-action	Mécanisme permettant de déclencher une action suite à un événement. Par exemple, vous pouvez configurer Security Center pour déclencher une alarme en cas de porte forcée.
module RS-485 à quatre ports	Composant de communication RS-485 du Synergis Master Controller avec quatre ports (ou canaux) nommés A, B, C et D. Le nombre de modules d'interface que vous pouvez connecter à chaque canal dépend du type de matériel dont vous disposez.
module d'interface	Un module d'interface est un périphérique de sécurité tiers qui communique avec une unité de contrôle d'accès via une connexion IP ou RS-485, et qui fournit des connexions d'entrée, de sortie et de lecteur supplémentaires à l'unité.
macro	Type d'entité qui encapsule un programme C# qui ajoute des fonctionnalités à Security Center.

Map Generator	Module Map Server qui importe les cartes vectorielles et bitmap dans la base de données de Plan Manager.
mode Carte	Mode de fonctionnement de Security Desk où la zone principale du canevas est occupée par une carte géographique, dédiée à l'affichage d'événements de RAPI.
Map Server	Module serveur Plan Manager qui gère les cartes privées importées par l'administrateur Plan Manager. Map Server inclut deux modules : Map Generator et Tile Server.
Media Gateway	Rôle utilisé par des applications externes pour demander de la vidéo en direct ou enregistrée par l'intermédiaire du protocole RTSP (Real Time Streaming Protocol), et pour recevoir des flux vidéo bruts directement depuis des caméras gérées par des systèmes Security Center.
Migration tool	Outil servant à faire migrer les systèmes Omnicast 4.x vers Security Center 5. Cet outil doit être exécuté sur chaque serveur qui héberge des composants Omnicast 4.x.
Mobile Admin	Outil d'administration web servant à configurer Mobile Server.
Mobile app	Composant client de Security Center Mobile installé sur appareils mobiles. Les utilisateurs de Mobile app se connectent à Mobile Server pour recevoir des alarmes, visionner de la vidéo en direct, consulter l'état des portes et davantage, depuis Security Center.
Mobile Server	Le composant serveur de Security Center Mobile qui assure la connexion des appareils mobiles (via Mobile app ou Web Client) à Security Center. Mobile Server se connecte à Security Center, puis synchronise les données et la vidéo entre Security Center et les composants client Mobile pris en charge.
module externe	Un module externe est un composant logiciel qui ajoute une fonctionnalité ou un service particulier à un système plus important.
Module externe	Type de rôle qui héberge un module externe particulier.
Modules externes	Type de tâche d'administration qui permet de configurer les rôles et unités de type module externe.
mode d'enregistrement	Critères utilisés par l'Archiveur pour planifier l'enregistrement de flux vidéo. Il existe quatre modes d'enregistrement : • Désactivé (aucun enregistrement autorisé) • Manuel (enregistrement à la demande de l'utilisateur) • Continu (enregistrement permanent) • Mouvement/manuel (enregistrement selon les paramètres de détection de mouvement ou à la demande)

même position Type de règle de stationnement qui caractérise une règle de dépassement horaire. Un véhicule est en infraction s'il est garé à exactement le même endroit au delà d'une période donnée. Patroller doit être équipé de fonctions GPS pour appliquer ce type de réglementation.

mode serveur Mode de fonctionnement en ligne spécial réservé aux unités Synergis, où l'unité délègue toutes les décisions de contrôle d'accès au Gestionnaire d'accès (au serveur). L'unité doit être connectée au Gestionnaire d'accès en permanence pour fonctionner selon ce mode.

mode autonome Mode de fonctionnement hors ligne du module d'interface, lorsqu'il fonctionne en mode autonome et prend des décisions en fonction des réglages de contrôle d'accès préalablement téléchargés depuis l'unité Synergis. Le rapport d'activité est effectué sur horaire ou lorsque la connexion à l'unité est disponible. Certains modules d'interface ne prennent pas en charge le mode autonome.

mode supervisé Mode de fonctionnement en ligne du module d'interface, lorsqu'il prend des décisions en fonction des réglages de contrôle d'accès préalablement téléchargés depuis l'unité Synergis. Le module d'interface signale son activité en temps réel à l'unité, et permet à l'unité d'ignorer les décisions qui contredisent les réglages actuels de l'unité. Certains modules d'interface ne prennent pas en charge le mode supervisé.

mode Tuile Mode de fonctionnement de Security Desk où la zone principale du canevas est occupée par le volet des tuiles et le tableau de bord.

mosaïque Disposition des tuiles sur le canevas.

module externe de tuile Type d'entité qui représente une application exécutée dans une tuile Security Desk.

N

Navigator Appareil embarqué dans le véhicule propriétaire de Genetec qui fournit des coordonnées GPS et des relevés de compteur à Patroller. Raccordé au compteur kilométrique du véhicule, il est plus précis qu'un appareil GPS standard. Le boîtier Navigator peut être utilisé avec tout type de déploiement AutoVu mobile qui dépend de coordonnées géographiques, mais il est obligatoire pour les installations Stationnement urbain avec imagerie des roues

nouveau véhicule recherché Élément de liste de véhicules recherchés saisi manuellement dans Patroller. Lorsque vous recherchez une plaque qui n'est pas trouvée dans les listes chargées dans Patroller, vous pouvez saisir la plaque afin de déclencher une alerte en cas de lecture de la plaque concernée.

niveau d'accès Valeur numérique servant à restreindre l'accès à un secteur lorsqu'un niveau de risque est activé. Un titulaire de cartes ne peut accéder (entrée ou sortie) à un secteur que si son niveau d'accès est supérieur ou égal à celui du secteur.

niveau de risque Procédure d'urgence qu'un opérateur Security Desk peut activer pour un secteur ou l'ensemble du système pour réagir rapidement à une situation dangereuse, comme un incendie ou une fusillade.

niveau utilisateur Valeur numérique affectée aux utilisateurs pour restreindre leur capacité à effectuer certaines opérations, comme contrôler une caméra PTZ, afficher le flux vidéo d'une caméra ou rester connecté lorsqu'un niveau de risque est activé. Plus la valeur est faible, plus la priorité est élevée.

numéro d'identification de véhicule Numéro d'identification de véhicule (vehicle identification number ou VIN) attribué par le constructeur à un véhicule. Ce numéro est souvent affiché sur une petite plaque du tableau de bord, visible depuis l'extérieur du véhicule. Les listes de véhicules recherchés et de permis peuvent inclure un VIN en plus du numéro de plaque d'immatriculation, pour confirmer une alerte l'identification d'un véhicule recherché.

O

Outil de diagnostic d'accès L'outil de diagnostic d'accès est un utilitaire qui aide à détecter et diagnostiquer les problèmes de configuration d'accès. Il permet d'obtenir les informations suivantes :

- Qui est autorisé à passer un point d'accès à un instant donné
- Quels points d'accès un titulaire de cartes est autorisé à utiliser à un instant donné
- La raison pour laquelle un titulaire de carte est autorisé ou non à utiliser un point d'accès à un instant donné

Outil Copie de configuration L'Outil de copie de configuration permet de gagner du temps de configuration en copiant les paramètres d'une entité vers d'autres entités qui doivent avoir des paramètres similaires.

objet cartographique Un objet cartographique est une représentation graphique d'entités Security Center sur vos cartes. Ils vous permettent d'interagir avec votre système sans quitter la carte.

Ordinateur portable embarqué Tablette ou ordinateur portable renforcé utilisé embarqué dans les véhicules et qui sert à exécuter l'application AutoVu Patroller. Il est généralement équipé d'un écran tactile d'une résolution d'au moins 800 x 600 pixels, et capable de se connecter aux réseaux sans fil.

Omnicast Omnicast est le système de vidéosurveillance sur IP de Security Center qui offre une gestion transparente de la

	vidéo numérique. Omnicast permet l'utilisation de modules et de CODEC (codeurs/décodeurs) tiers au sein d'une même installation, ce qui permet de sélectionner les équipements adaptés à chaque application pour une souplesse optimale.
Omnicast[MC] Federation[MC]	Omnicast[MC] Federation[MC] peuvent être utilisés dans votre système Security Center.
Outil Découverte des unités	À compter de Security Center 5.4 GA, l'Outil Découverte des unités a été remplacé par l'Outil d'inscription d'unités.
Occupation par zone	Type de tâche d'investigation qui répertorie le nombre de véhicules stationnant dans une zone de stationnement donnée, ainsi que le pourcentage d'occupation.

P

point d'accès	Un point d'accès est un point d'entrée (ou de sortie) d'un secteur physique pour lequel le passage peut être surveillé et soumis à des règles d'accès. Il s'agit généralement d'un côté de porte ou d'un étage d'ascenseur.
Présence dans un secteur	Tâche d'investigation qui fournit un instantané de tous les titulaires de cartes et visiteurs présents dans un secteur donné.
pâté (2 côtés)	Type de règle de stationnement qui caractérise une règle de dépassement horaire. Un pâté définit la longueur d'une rue entre deux croisements. Un véhicule est en infraction s'il est garé sur le même pâté durant une période donnée. Le déplacement du véhicule d'un côté ou l'autre de la rue n'a pas d'incidence.
port de découverte	Port utilisé par certains rôles Security Center (Gestionnaire d'accès, Archiveur, Gestionnaire RAPI) pour détecter les unités dont ils sont responsables sur le réseau local. Il ne peut pas y avoir deux ports de découverte identiques sur un même système.
porte	Type d'entité qui représente une barrière physique. Il peut s'agir d'une porte, mais aussi d'une grille, d'un tourniquet ou de tout autre passage contrôlable. Chaque porte a deux côtés, appelés *Entrée* et *Sortie* par défaut. Chaque côté est un point d'accès (entrée ou sorite) à un secteur sécurisé.
Patroller fantôme	Entité créée automatiquement par le Gestionnaire RAPI lorsque la licence AutoVu inclut le module d'importation XML. Dans Security Center, toutes les données de RAPI doivent être associées à une entité Patroller ou à une entité de RAPI correspondant à une caméra Sharp fixe. Lorsque vous importez des données de RAPI depuis un Gestionnaire RAPI particulier module d'importation XML, le système utilise l'entité fantôme pour représenter la source de données de

	RAPI. Vous pouvez rédiger des requêtes qui référencent l'entité fantôme comme pour une entité normale.
partition globale	Partition partagée à l'échelle de plusieurs systèmes Security Center indépendants par le propriétaire de la partition, appelé hôte de partage.
pack d'intégration matérielle	Un pack d'intégration matérielle (hardware integration package ou HIP) est une mise à jour pouvant être appliquée à Security Center. Il permet la prise en charge de nouvelles fonctionnalités (comme de nouveaux types d'unités vidéo), sans effectuer la mise à niveau vers une nouvelle version de Security Center.
point chaud	Type d'objet cartographique qui représente un emplacement sur la carte et qui requiert une attention particulière. Un clic sur un point chaud affiche les caméras fixes et PTZ associées.
packs de compatibilité Omnicast	Composant logiciel à installer pour assurer la compatibilité de Security Center avec un système Omnicast 4.x.
parc de stationnement	Type d'entité qui représente une zone de stationnement de taille importante sous forme de secteurs et de rangées, à des fins d'inventaire.
partition	Type d'entité qui définit un ensemble d'entités qui ne sont visibles que par un groupe particulier d'utilisateurs. Une partition peut par exemple inclure tous les secteurs, portes, caméras et zones d'un immeuble.
Patroller	1 Application logicielle AutoVu installée sur un ordinateur embarqué dans le véhicule. Patroller se connecte à Security Center. Il est contrôlé par le Gestionnaire RAPI. Patroller compare les lectures de plaques d'immatriculation effectuées par les caméras de RAPI à des listes de véhicules recherchés et de véhicules ayant des permis. Il recueille également des données pour l'application d'horaires de stationnement. Patroller vous notifie en cas d'alerte de liste de véhicules recherchés ou de permis, afin que vous puissiez immédiatement réagir. 2 Type d'entité qui représente un véhicule équipé du logiciel Patroller.
Patroller Config Tool	Application de gestion de Patroller servant à configurer les réglages propres à Patroller, comme ajouter des caméras Sharp au réseau du véhicule, activer des fonctions comme la capture manuelle et les Nouveaux véhicules recherchés, et spécifier un nom d'utilisateur et mot de passe pour la connexion à Patroller.

Pistage Patroller	Type de tâche d'investigation qui représente l'itinéraire d'un Patroller un jour donné sur une carte, ou la position actuelle de véhicules Patroller sur la carte.
permis	Type d'entité qui définit une liste de détenteurs de permis de stationnement. Chaque détenteur de permis est caractérisé par une catégorie (zone de permis), un numéro de plaque d'immatriculation, l'État émetteur de la plaque, une plage de validité (date d'entrée en vigueur et date d'expiration). Les permis sont utilisés dans le cadre du stationnement urbain et universitaire.
Plan Manager	Plan Manager est un module Security Center qui ajoute des fonctionnalités de cartographie interactives pour mieux visualiser votre environnement de sécurité.
Plan Manager Client	Composant client de Plan Manager qui est exécuté en tant que module externe de tuile dans Security Desk. Il permet aux opérateurs d'utiliser des cartes pour surveiller et contrôler des caméras, portes et autres dispositifs de sécurité, et aux administrateurs de créer des objets cartographiques.
Plan Manager Server	Composant serveur de Plan Manager hébergé par un rôle Module externe Security Center. Plan Manager Server comprend deux modules serveur, Data Server et Map Server, qui peuvent être hébergés par un même rôle Module externe ou par deux rôles Module externe distincts.
Plate Reader	Composant logiciel de l'unité Sharp qui traite les images capturées par la caméra de RAPI pour la lecture de plaques d'immatriculation, et qui associe la lecture à une image contextuelle capturée par la caméra contextuelle. Plate Reader gère également la communication avec Patroller et le Gestionnaire RAPI. Lorsqu'une caméra externe d'imagerie des roues est connectée à l'unité Sharp, Plate Reader capture également les images des roues fournies par cette caméra.
Point de vente	Les points de vente désignent généralement le matériel et les logiciels utilisés pour contrôler les sorties. Équivalent électronique d'une caisse enregistreuse. Ces systèmes servent à capturer des transactions détaillées, à autoriser des paiements, à surveiller les stocks, à effectuer des audits et à gérer les employés. Les systèmes de point de vente sont utilisés dans les supermarchés, les restaurants, les hôtels, les stades, les casinos et autres types d'établissements pratiquant la vente au détail.
privilège	Les privilèges déterminent les tâches que peuvent effectuer les utilisateurs, comme armer les zones, bloquer les caméras ou débloquer les portes, au sein de la partie du système à laquelle ils peuvent accéder.
Portail Sharp	Application Web d'administration servant à configurer les caméras Sharp pour les systèmes AutoVu fixes ou mobiles.

	Vous utilisez un navigateur web pour vous connecter à une adresse IP particulière (ou à un nom de l'unité Sharp dans certains cas) correspondant à la Sharp que vous souhaitez configurer. Une fois connecté, vous pouvez configurer des options comme le contexte de RAPI (Alabama, Oregon, Québec, etc.), la stratégie de lecture (véhicules circulant lentement ou rapidement), afficher le flux vidéo en direct de l'unité Sharp, etc.
Présence	Type de tâche d'investigation qui répertorie les personnes ayant accédé à un secteur donné et la durée totale de leur séjour, durant une période donnée.
Port VSIP	Nom donné au port de découverte des unités Verint. Un Archiver peut être configuré de manière à écouter sur plusieurs ports VSIP.

Q

quartier	Type de règle de stationnement qui caractérise une règle de dépassement horaire. Un quartier est une zone géographique au sein d'une ville. Un véhicule est en infraction s'il est garé au sein d'un même quartier durant une période donnée.

R

Rapport d'état de contrôle d'accès	Type de tâche de maintenance qui signale les dysfonctionnements qui affectent certaines unités de contrôle d'accès.
règle d'accès	Type d'entité qui définit une liste de titulaires de cartes auxquels un accès est accordé ou refusé en fonction d'un horaire. Une règle d'accès peut être affectée à un point d'accès ou à un secteur sécurisé.
Rapport d'alarmes	Tâche d'investigation qui permet de rechercher les alarmes actuelles et les anciennes alarmes.
redressement	Transformation visant à redresser une image numérique capturée par un objectif grand-angle.
Répertoire	Le Répertoire est le rôle principal qui identifie un système. Il gère toutes les configurations d'entités et réglages à l'échelle du système dans Security Center. Une seule instance de ce rôle est autorisée par système. Le serveur qui héberge le rôle Répertoire est appelé le *serveur principal*, et vous devez le configurer en premier. Tous les autres serveurs que vous ajoutez à Security Center sont appelés *serveurs d'extension* et doivent se connecter au serveur principal pour appartenir au même système.

règle de superviseur présent	Restriction d'accès à un secteur sécurisé empêchant quiconque de pénétrer le secteur tant qu'un superviseur n'est pas présent sur site. La restriction peut être appliquée en cas d'accès libre (horaires de déverrouillage des portes) ou d'accès contrôlé (règles d'accès en vigueur).
Recherche analytique	Type de tâche d'investigation qui permet de rechercher des enregistrements vidéo en fonction d'événements d'analyse vidéo.
Rapport d'état	Type de tâche de maintenance qui signale les problèmes de fonctionnement.
règle d'alerte	Type de règle de RAPI servant à identifier les véhicules recherchés (appelés « alertes ») par le biais de la lecture de plaques d'immatriculation. Les types de règles d'alertes suivants sont disponibles :liste de véhicules recherchés, règle de dépassement horaire, permis et restriction de permis.
Rapport d'inventaire	Type de tâche d'investigation qui permet d'afficher un inventaire particulier (lieu de véhicule, durée de séjour, etc.) ou de comparer deux inventaires d'un parc de stationnement (véhicules ajoutés, véhicules supprimés, etc.).
Reconnaissance de plaques d'immatriculation	La Reconnaissance automatique de plaques d'immatriculation (RAPI) est une technologie de traitement de l'image utilisée pour lire les numéros de plaques d'immatriculation. La reconnaissance automatique de plaques d'immatriculation (RAPI) convertit des gros plans de numéros de plaques capturées par des caméras en un format de base de données interrogeable.
RAPI	Type de tâche d'administration qui permet de configurer les rôles, unités, règles, listes de véhicules recherchés, permis, règles de dépassement horaire de RAPI, ainsi que les entités et réglages associés.
Règle de RAPI	Méthode utilisée par Security Center et AutoVu pour le traitement d'une lecture de plaque d'immatriculation. Une règle de RAPI peut être une règle d'alerte ou un parc de stationnement.
Routeur multimédia	Rôle central qui gère toutes les demandes de flux (audio et vidéo) dans Security Center. Il établit des sessions de diffusion entre la source du flux (caméra ou Archiveur) et les demandeurs (applications clientes). Les décisions de routage dépendent du lieu (adresse IP) et des capacités de transmission de tous les composants impliqués (source, destinations, réseaux et serveurs).
Recherche de mouvement	Type de tâche d'investigation qui recherche des mouvements détectés dans une partie particulière du champ de vision d'une caméra.

réseau	Les entités Réseau servent à capturer les caractéristiques des réseaux utilisés par votre système, afin d'optimiser les décisions d'acheminement des flux.
règle de dépassement horaire	Type d'entité qui définit une durée maximale de durée de stationnement et le nombre maximum d'infractions pouvant être sanctionnées au cours d'une journée. Cette règle est utilisée dans l'application du stationnement urbain et universitaire. Pour le stationnement universitaire, une règle de dépassement horaire spécifie également la zone de stationnement concernée.
restriction de permis	Type d'entité qui applique des restrictions horaires à une série de permis de stationnement pour une zone de stationnement donnée. Les restrictions de permis ne sont applicables qu'aux Patroller configurés pour l'application de stationnement universitaire.
redirecteur	Serveur désigné pour l'hébergement d'un agent de redirection créé par le rôle Routeur multimédia.
rôle	Un rôle est un module logiciel qui effectue une tâche particulière au sein de Security Center. Les rôles doivent être affectés à un ou plusieurs serveurs pour exécution.
route	Réglage servant à configurer les capacités de transmission entre deux extrémités d'un réseau, pour l'acheminement de flux multimédias.
Routeur multimédia RTSP	Rôle utilisé par des applications externes pour demander de la vidéo en direct ou enregistrée par l'intermédiaire du protocole RTSP (Real Time Streaming Protocol), et pour recevoir des flux vidéo bruts directement depuis les caméras source.
règle de deuxième personne	Restriction d'accès à une porte qui oblige deux titulaires de cartes (y compris les visiteurs) à présenter leurs identifiants dans un certain laps de temps afin d'obtenir un accès.
Remplacement d'unité	L'outil de permutation d'unités sert à remplacer un appareil défaillant par un autre appareil compatible, en assurant le transfert des données de l'ancienne unité vers la nouvelle unité. Dans le cas d'une unité de contrôle d'accès, la configuration de l'ancienne unité est copiée vers la nouvelle unité. Dans le cadre d'une unité vidéo, l'archive vidéo associée à l'ancienne unité est associée à la nouvelle unité, mais la configuration de l'ancienne unité n'est pas copiée.
règle d'escorte de visiteur	Restriction d'accès à un secteur sécurisé qui requiert l'accompagnement des visiteurs par un titulaire de cartes durant leur visite. Pour que le passage par un point d'accès soit accordé, le visiteur et son escorte attitrée (un titulaire de cartes) doivent tous les deux présenter leurs identifiants dans un délai donné.

S

Surveillance d'alarmes	Type de tâche d'exploitation qui permet de surveiller et de répondre aux alarmes (acquitter, transférer, mettre en veille, etc.) en temps réel, et d'analyser les anciennes alarmes.
secteur	Type d'entité qui représente un concept ou un lieu physique (pièce, étage, bâtiment, site, etc.) utilisé pour le regroupement logique des entités du système.
signet	Fragment de texte qui sert à repérer un emplacement particulier d'une séquence vidéo. Vous pouvez ensuite utiliser les signets pour rechercher les séquences vidéo associées.
Signets	Type de tâche d'investigation qui recherche des signets associés à certaines caméras durant une période donnée.
séquence de caméras	Type d'entité qui définit une liste de caméras qui sont affichées successivement en boucle dans une même tuile dans Security Desk.
Stationnement urbain	Installation du logiciel Patroller configurée pour l'application des restrictions de permis et des règles de dépassement horaire.
Stationnement urbain avec imagerie des roues	Installation Patroller particulière de type *Stationnement urbain* qui intègre l'imagerie des roues. L'utilisation de cartes et du navigateur est obligatoire.
sortie contrôlée	Point d'accès permettant de quitter un secteur sécurisé sur présentation d'un identifiant.
serveur de base de données	Application qui gère le contenu des bases de données et qui traite les requêtes de données émises par les applications clientes. Security Center utilise Microsoft SQL Server en tant que serveur de base de données.
Serveur de Répertoire	Un des multiples serveurs qui exécute simultanément le rôle Répertoire dans le cadre d'une configuration à haute disponibilité.
serveur d'extension	Tout ordinateur serveur du système Security Center qui n'héberge pas le rôle Répertoire. Les serveurs d'extension servent à renforcer la capacité de traitement du système.
système fédéré	Système indépendant (Omnicast ou Security Center) intégré Security Center local par le biais d'un rôle Fédération, afin que les utilisateurs locaux puissent consulter et manipuler ces entités comme si elles appartenaient au système local.
sortie libre	Point de sortie d'un secteur sécurisé pour lequel aucun identifiant n'est requis. L'utilisateur ouvre la porte en tournant la poignée ou en appuyant sur le bouton REX, puis il sort. Un

	système automatique referme la porte afin qu'elle puisse être verrouillée après qu'elle ait été ouverte.
Synchroniseur de titulaires de cartes globaux	Type de rôle qui assure la synchronisation bidirectionnelle des titulaires de cartes partagés et des entités associées entre le système local (participant au partage) et le système central (hôte de partage).
Surveillance de l'état	Le rôle central qui surveille les entités système comme les serveurs, rôles, unités et applications client à l'affût de dysfonctionnements.
Statistiques de fonctionnement	Type de tâche de maintenance qui fournit une vue d'ensemble du fonctionnement de votre système.
sas	Restriction d'accès affectée à un secteur sécurisé qui n'autorise l'ouverture que d'une porte à la fois.
secteur de détection d'intrusion	Type d'entité correspondant à une zone ou partition (groupe de capteurs) d'un tableau d'intrusion.
serveur principal	Le seul serveur d'un système Security Center qui héberge le rôle Répertoire. Tous les autres serveurs doivent se connecter au serveur principal afin d'appartenir au même système. Dans le cadre d'une configuration à haute disponibilité où le rôle Répertoire est hébergé sur plusieurs serveurs, il s'agit du seul serveur autorisé à écrire dans la base de données du Répertoire.
Surveillance	La tâche de *Surveillance* permet de surveiller et de réagir en temps réel à des événements liés à des entités sélectionnées. La tâche *Surveillance* vous permet également de surveiller et de répondre à des alarmes.
signal de sortie	Type d'entité qui définit le format du signal de sortie, comme une impulsion, avec un délai et une durée.
serveur principal	Serveur par défaut sélectionné pour effectuer une fonction particulière (ou rôle) du système. Pour améliorer la tolérance aux pannes du système, le serveur premier peut s'appuyer sur un serveur de secours. En cas d'indisponibilité du serveur principal, le serveur secondaire prend automatiquement le relais.
serveur secondaire	Tout serveur alternatif de secours devant remplacer le serveur principal en cas d'indisponibilité de celui-ci.
secteur sécurisé	Entité secteur qui représente un site physique auquel l'accès est contrôlé. Un secteur sécurisé est constitué de portes de périmètre (portes servant à pénétrer et à quitter le secteur) et de restrictions d'accès (règles régissant l'accès au secteur).
Security Center	Security Center est la plate-forme de sécurité unifiée qui intègre de manière transparente les systèmes de sécurité IP

	de Genetec[MC] au sein d'une même solution innovante. Les systèmes unifiés au sein de Security Center sont Genetec[MC] de reconnaissance automatique de plaques d'immatriculation (RAPI).
Security Center Federation[MC]	Security Center Federation[MC] est le rôle qui connecte un système Security Center distant et indépendant à votre Security Center local. Ainsi, les entités et événements du système distant peuvent être utilisés dans votre système local.
Security Center Mobile	Security Center Mobile est une fonctionnalité de la plateforme unifiée de Genetec qui vous permet de vous connecter à votre système Security Center par le biais d'un réseau IP sans fil. Des composants client Mobile sont disponibles sous forme du client Web Client unifié et universel et de diverses apps mobiles pour smartphones et tablettes.
Security Desk	Security Desk est l'interface utilisateur unifiée de Security Center. Il fournit des processus cohérents à l'échelle d'Omnicast, Synergis et AutoVu, les principaux composants de Security Center. La conception centrée sur les tâches de Security Desk permet aux opérateurs de contrôler et surveiller efficacement de nombreuses applications de sécurité et de sûreté.
serveur	Type d'entité qui représente un ordinateur sur lequel Genetec Server est installé.
Server Admin	Application Web hébergée sur chaque ordinateur serveur de Security Center permettant de configurer Genetec Server. Server Admin permet également de configurer le rôle Répertoire sur le serveur principal.
Sharp EX	Unité Sharp incluant un processeur d'image intégré avec deux entrées NTSC ou PAL de définition standard pour caméras externes (caméras de RAPI et contextuelles).
SharpOS	Composant logiciel des unités Sharp ou SharpX. SharpOS est responsable de toutes les tâches de capture, collection, traitement et analyse de plaques. Par exemple, une mise à jour SharpOS peut intégrer de nouveaux contextes de RAPI, un nouveau micrologiciel, des mises à jour du Portail Sharp ou des services Windows de la Sharp (Plate Reader, HAL, service de mise à jour, etc.).
Sharp VGA	Unité Sharp qui intègre les composants suivants :illuminateur à infrarouge ; caméra de RAPI en définition standard (640 x 480) pour la capture de plaques ; processeur de traitement de l'image ; caméra contextuelle couleur NTSC ou PAL avec gestion de flux vidéo.
SharpX	Composant caméra du système SharpX. L'unité caméra Sharp X intègre un illuminateur LED à impulsions qui fonctionne dans

	l'obscurité totale (0 lux), une caméra de RAPI monochrome (1024 x 946 @ 30 ips) et une caméra contextuelle couleur (640 x 480 @ 30 ips). Les données de RAPI capturées par l'unité caméra SharpX sont traitées par un composant matériel distinct appelé Unité de traitement de RAPI AutoVu.
Sharp XGA	Unité Sharp qui intègre les composants suivants :illuminateur à infrarouge ; caméra de RPM haute définition (1024 x 768) pour la capture de plaques ; processeur de traitement de l'image ; caméra contextuelle couleur NTSC ou PAL avec gestion de flux vidéo et GPS en option.
SharpX VGA	Composant caméra du système SharpX. L'unité caméra Sharp X VGA intègre un illuminateur LED à impulsions qui fonctionne dans l'obscurité totale (0 lux), une caméra de RAPI monochrome (640 x 480 @ 30 ips) et une caméra contextuelle couleur (640 x 480 @ 30 ips). Les données de RAPI capturées par l'unité caméra SharpX VGA sont traitées par un composant matériel distinct appelé Unité de traitement de RAPI AutoVu.
Synergis Appliance Portal	Outil d'administration web servant à configurer et gérer l'appareil Synergis, ainsi qu'à mettre à niveau son micrologiciel.
Synergis	Synergis, le système de contrôle d'accès sur IP de Security Center, est conçu pour offrir une connectivité IP de bout en bout, du lecteur de contrôle d'accès jusqu'au poste de travail client. Synergis intègre de manière transparente de nombreuses fonctionnalités de contrôle d'accès, dont la conception de badges, la gestion des visiteurs, le contrôle des ascenseurs et la surveillance de zones, parmi bien d'autres.
Synergis Master Controller	Synergis Master Controller (SMC) est l'appareil de contrôle d'accès de Genetec assurant la prise en charge de divers modules d'interface tiers sur IP et RS-485. Le SMC s'intègre de manière transparente au sein de Security Center, et peut prendre des décisions de contrôle d'accès indépendamment du Gestionnaire d'accès.
Système	Tâche d'administration qui permet de configurer les rôles, macros, horaires, ainsi que d'autres entités et réglages du système.
Stationnement universitaire	Installation du logiciel Patroller configurée pour l'application de stationnement universitaire :application des permis de stationnement et des dépassements horaire. L'utilisation de cartes est obligatoire. Gère également les listes de véhicules recherchés.
séquence vidéo	Tout flux vidéo enregistré d'une quelconque durée.

SDK Web	Le rôle SDK Web expose les méthodes et objets du SDK Security Center en tant que services web, pour permettre le développement multiplate-forme.

T

Transfert d'archive	Type de tâche d'administration qui permet de configurer les réglages de récupération des enregistrements des unités vidéo, de duplication des archives entre Archiveurs, ou de sauvegarde des archives vers un emplacement particulier.
transfert d'archive	Processus de transfert des données vidéo d'un site vers un autre. La vidéo est enregistrée et stockée sur l'unité vidéo elle-même ou sur un disque de stockage de l'Archiveur, puis les enregistrements sont transférés vers un autre site.
titulaire de cartes	Type d'entité qui représente un individu autorisé à pénétrer et à quitter des secteurs sécurisés en fonction de ses identifiants (généralement des cartes d'accès), et dont les activités peuvent être surveillées.
tableau de bord	L'un des trois volets du canevas de Security Desk. Il contient les commandes graphiques (ou widgets) associées à l'entité affichée dans la tuile actuelle.
tableau d'intrusion	Unité fixée au mur où les capteurs d'alarmes (détecteurs de mouvement, détecteurs de fumée, capteurs de portes, etc.) et le câblage des alarmes d'intrusion sont branchés et gérés.
translation d'adresses réseau (NAT)	Processus de modification des informations d'adresse réseau dans les en-têtes de paquets de datagrammes (IP) transitant dans un appareil de routage, afin de traduire un espace d'adresses IP vers une autre.
tâche privée	Tâche enregistrée qui n'est visible que par l'utilisateur qui l'a créée.
tâche publique	Tâche enregistrée pouvant être partagée par plusieurs utilisateurs de Security Center.
tâche planifiée	Type d'entité qui définit une action exécutée automatiquement à un instant précis ou selon un horaire récurrent.
talonnage	Entrée d'une personne dans un secteur sécurisé sans lecture d'identifiant en passant derrière une autre personne qui a passé son identifiant dans un lecteur.
tâche	Notion sur laquelle repose l'interface utilisateur de Security Center. Chaque tâche correspond à un aspect de votre travail en tant que professionnel de la sécurité. Par exemple, vous utilisez une tâche de surveillance pour surveiller les événements du système en temps réel, ou une tâche d'investigation pour déceler des comportements suspects,

	ou encore une tâche d'administration pour configurer votre système. Les tâches peuvent être personnalisées et plusieurs tâches peuvent être effectuées en même temps.
tuile	Fenêtre individuelle sur le canevas utilisée pour afficher une seule entité. L'entité affichée est généralement la vidéo provenant d'une caméra, une carte ou tout autre élément graphique. Son aspect dépend de l'entité affichée.
Tile Server	Module Map Server qui répond aux requêtes de cartes émises par Plan Manager Client.
Transmission Control Protocol (protocole de contrôle des transmissions)	Ensemble de règles de connexion (protocole) associé au protocole IP (Internet Protocol) servant à transmettre des données sur un réseau IP. Le protocole TCP/IP définit la manière dont les données peuvent être transmises de façon fiable entre les réseaux. TCP/IP est la norme de communications la plus répandue et est à la base d'Internet.
tatouage numérique de la vidéo	Le tatouage est le processus d'ajout d'une signature numérique à chaque image vidéo enregistrée afin d'assurer son authenticité. Si quelqu'un tente d'apporter ultérieurement des modifications à la vidéo (ajout, suppression ou retouche d'une image), les signatures ne correspondent plus, indiquant que la vidéo a été altérée.

U

unité de contrôle d'accès	Type d'entité qui représente un périphérique de contrôle d'accès intelligent, comme un appareil Synergis ou un contrôleur réseau HID, et qui communique directement avec le Gestionnaire d'accès sur un réseau IP. Une unité de contrôle d'accès fonctionne de manière autonome si elle est déconnectée du Gestionnaire d'accès.
utilisateur autorisé	Un utilisateur autorisé est un utilisateur qui peut voir les (ou accéder aux) entités contenues dans la partition. Les utilisateurs ne peuvent exercer leurs privilèges que sur les entités qu'ils peuvent voir.
Unité de traitement de RPI AutoVu^{MC}	L'unité de traitement de RPI AutoVu^{MC} est l'unité de traitement du système SharpX. L'unité de traitement de RPI AutoVu est disponible avec deux ou quatre entrées pour les caméras, avec un processeur dédié par caméra (avec caméras SharpX) ou pour deux caméras (avec caméras SharpX VGA). Des performances de traitement par caméra optimales sont ainsi garanties. L'unité de traitement de RPI AutoVu est parfois appelée *unité de coffre*, puisqu'elle est généralement installée dans le coffre du véhicule.

Utilitaire Résolution de conflits	Outil permettant de résoudre les conflits générés par l'importation d'utilisateurs et de titulaires de cartes depuis Active Directory.
Utilisation quotidienne par Patroller	Type de tâche d'investigation qui répertorie les statistiques d'utilisation quotidienne d'un Patroller particulier (durée de fonctionnement, arrêt le plus long, extinction la plus longue, etc.) sur une période donnée.
unité de détection d'intrusion	Type d'entité qui représente un tableau d'intrusion (ou tableau d'alarme) surveillé et contrôlé par Security Center.
Unité de RAPI	Type d'entité qui représente un dispositif matériel dédié à la capture de numéros de plaques d'immatriculation. Les unités de RAPI sont généralement reliées à une caméra de RAPI et à une caméra contextuelle. Ces caméras peuvent être extérieures ou intégrées à l'unité.
unité Sharp	Unité de RAPI propriétaire de Genetec qui intègre les composants de capture et de traitement de plaques d'immatriculation, ainsi que des fonctions de traitement vidéo, le tout dans un boîtier renforcé.
unité	Dispositif matériel qui communique sur un réseau IP pouvant être contrôlé directement par un rôle Security Center. Security Center distingue quatre types d'entités : • Unités de contrôle d'accès, gérées par le rôle Gestionnaire d'accès • Unités vidéo, gérées par le rôle Archiveur • Unités de RAPI, gérées par le rôle Gestionnaire RAPI • Unités de détection d'intrusion, gérées par le rôle Gestionnaire d'intrusions.
utilisateur	Type d'entité qui identifie une personne qui utilise les applications Security Center et définit ses droits et privilèges au sein du système. Les utilisateurs peuvent être créés manuellement ou importés depuis Active Directory.
unité vidéo	Type d'appareil de codage ou décodage vidéo capable de communiquer sur réseau IP et d'intégrer un ou plusieurs codeurs vidéo. Tout un éventail de marques et de modèles d'unités vidéo sont disponibles, dont certaines prennent en charge les données audio ou encore la communication sans fil. Les modèles de codage haut de gamme intègrent leurs propres dispositifs d'enregistrement et d'analyse vidéo. Les caméras (IP ou analogiques), les codeurs vidéo et les décodeurs vidéo sont tous des exemples d'unités vidéo. Dans le cadre de Security Center, les unités vidéo sont des types d'entités qui représentent un appareil de codage ou décodage vidéo.

V

Vue secteur	Type de tâche d'administration qui permet de configurer les secteurs, portes, caméras, modules externes de tuile, secteurs de détection d'intrusion, zones et autres entités affichées dans la vue secteur.
vue secteur	Classe les entités couramment utilisées comme les portes, caméras, modules externes de tuiles, secteurs de détection d'intrusion, zones, etc. par secteurs. Cette vue est généralement créée pour le travail au quotidien des opérateurs de sécurité.
vidéo asynchrone	Type d'entité qui représente tout objet de valeur équipé d'une puce RFID qui permet de le surveiller avec un logiciel de gestion d'actifs.
vue réseau	Vue du navigateur qui illustre votre environnement réseau en représentant chaque serveur sur le réseau auquel il appartient.
Vue réseau	Type de tâche d'administration qui permet de configurer les réseaux et serveurs.
volet de rapport	Le volet de rapport est l'un des volets de l'espace de travail de Security Desk. Il affiche les résultats de recherche ou les événements en temps réel sous forme de tableau.
vue rôles et unités	Affichage du navigateur qui présente tous les rôles du système, ainsi que les unités qu'ils contrôlent sous forme d'entités enfant.
vidéo synchrone	Lecture simultanée de vidéo en direct ou enregistrée provenant de plusieurs caméras synchronisées.
Vidéo	Type de tâche d'administration qui permet de configurer les rôles de gestion, les unités, les moniteurs analogiques et les caméras vidéo.

W

Web Client	Composant client de Security Center Mobile qui fournit un accès aux fonctionnalités de Security Center via un navigateur web. Les utilisateurs de Web Client se connectent à Mobile Server pour configurer et surveiller différents aspects du système Security Center.
Web Map Service	Web Map Service (WMS) est un protocole normalisé pour servir par Internet des images cartographiques géolocalisées générées par un serveur de cartographie exploitant une base de données GIS.
widget	Composant de l'interface utilisateur.
Windows Communication Foundation	Windows Communication Foundation (WCF) est une architecture de communication qui permet aux applications installées sur une ou plusieurs machines de communiquer en

	réseau. AutoVu Patroller utilise WCF pour communiquer à distance avec Security Center.

Z

zone matérielle	Une zone matérielle est une entité zone dont les liens d'E/S sont gérés par une seule unité de contrôle d'accès. Les zones matérielles fonctionnent indépendamment du Gestionnaire d'accès et ne peuvent donc pas être armées ou désarmées depuis Security Desk.
zone de mouvement	Zones d'une image vidéo définies par l'utilisateur dans lesquelles les mouvements sont recherchés.
zone de notification	La zone de notification contient des icônes qui offrent un accès rapide à certaines fonctionnalités du système, et des indicateurs d'événements système et d'informations d'état. Les réglages de zone de notification sont conservés dans votre profil utilisateur et s'appliquent à Security Desk et Config Tool.
zone de stationnement	Notion d'ordre général désignant la zone dans laquelle une règle de stationnement donnée (dépassement horaire, restriction de permis) est en vigueur. Dans le contexte du stationnement universitaire, la zone de stationnement doit être expressément définie sous forme de liste de parcs de stationnement.
zone virtuelle	Une zone virtuelle est une entité zone dont les liens d'E/S sont effectués au niveau logiciel. Les appareils d'entrée et de sortie peuvent appartenir à différentes unités de types distincts. Les zones virtuelles sont contrôlées par le Gestionnaire de zones, et ne fonctionnent que lorsque toutes les unités sont connectées. Elles peuvent être armées et désarmées avec Security Desk.
zone	Type d'entité qui surveille un ensemble d'entrées et déclenche des événements en fonction de leurs états. Ces événements peuvent servir à contrôler des relais de sortie.

Informations complémentaires sur les produits

Vous trouverez la documentation sur les produits aux endroits suivants :

- **Site d'information technique Genetec[MC]:** La dernière version de la documentation est disponible sur le Site d'information technique Pour accéder au Site d'information technique, connectez-vous au Portail Genetec[MC] et cliquez sur Information technique. 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 intègrent par ailleurs un lien permettant de télécharger la dernière version du document.
- **Aide:** Les applications Security Centerclient et web offrent une aide en ligne qui décrit le fonctionnement du produit et la marche à suivre pour utiliser ses fonctionnalités. Patroller et le Sharp Portal proposent également une aide contextuelle pour chaque écran. Pour accéder à l'aide en ligne, cliquez sur **Aide**, appuyez sur F1 ou touchez le **?** (point d'interrogation) au sein des différentes applications client.

Assistance technique

Le centre d'assistance technique de Genetec[MC] (GTAC) s'engage à fournir le meilleur service d'assistance technique possible à ses clients du monde entier. En tant que client Genetec[MC], vous avez accès au Site d'information technique de Genetec[MC], où vous pouvez trouver des informations et chercher des réponses à vos questions sur les produits.

- **Site d'information technique Genetec[MC]:** Consultez des articles, des manuels et des vidéos qui répondront à vos interrogations ou vous aideront à résoudre des problèmes techniques.

  Avant de contacter GTAC ou d'ouvrir un ticket d'assistance, il est important de consulter le Site d'information technique qui propose des informations sur comment corriger ou contourner certains problèmes et sur les problèmes connus.

  Pour accéder au Site d'information technique, connectez-vous au Portail Genetec[MC] et cliquez sur Information technique. Vous ne trouvez pas ce que vous cherchez ? Contactez documentation@genetec.com.

- **Centre d'assistance technique de Genetec[MC] (GTAC):** La procédure pour contacter GTAC est décrite dans les documents sur Genetec[MC] Lifecycle Management : FR_GLM_ASSURANCE et FR_GLM_ADVANTAGE.

Ressources complémentaires

Si vous souhaitez obtenir une assistance complémentaire, en plus du centre d'assistance technique de Genetec[MC], vous disposez des ressources suivantes :

- **Forum:** Le Forum est un forum de discussion convivial qui permet aux clients et aux employés de Genetec[MC] de communiquer et de converser sur différents sujets, qu'il s'agisse de questions ou de conseils techniques. Vous pouvez vous y connecter ou vous y inscrire sur https://gtapforum.genetec.com.
- **Formation technique:** Nos formateurs agréés peuvent vous aider à concevoir, installer, exploiter et dépanner votre système dans un environnement de formation professionnel ou dans vos propres locaux. Des services de formation technique sont proposés pour tous les produits et pour différents niveaux d'expérience, et peuvent en outre être personnalisés pour répondre à vos besoins ou objectifs particuliers. Pour plus de détails, reportez-vous à http://www.genetec.com/support/training/training-calendar.

Licences

- Pour l'activation ou la réinitialisation de licences, veuillez contacter GTAC sur https://gtap.genetec.com.
- Pour des problèmes de contenu de licences ou de références ou concernant une commande, veuillez contacter le service clientèle de Genetec[MC] à l'adresse customerservice@genetec.com, ou appelez le 1-866-684-8006 (option 3).
- Pour obtenir une licence de démo ou pour des questions sur les tarifs, veuillez contacter le service commercial de Genetec[MC] à l'adresse sales@genetec.com, ou appelez le 1-866-684-8006 (option 2).

Problèmes et pannes des produits matériels

Veuillez contacter GTAC sur https://gtap.genetec.com pour tout problème lié aux appareils Genetec[MC] ou au matériel acheté auprès de Genetec Inc.

L'index

P

R

S

T