SOPHOS
Security made simple.

SafeGuard Enterprise
Guide d'installation

Version du produit : 7
Date du document : décembre 2014

Table des matières

1 À propos de SafeGuard Enterprise

SafeGuard Enterprise est une solution de sécurité des données complète et modulaire, qui utilise une stratégie de chiffrement basée sur une règle pour protéger les informations et les partager sur les serveurs, les ordinateurs et les appareils mobiles.

L'administration centralisée est effectuée avec SafeGuard Management Center. Les stratégies de sécurité, les clés, les certificats, les cartes à puce et les tokens peuvent être gérés à l'aide d'une stratégie d'administration basée sur des rôles clairement définis. Les journaux détaillés et les rapports garantissent aux utilisateurs et aux administrateurs de toujours être informés de l'ensemble des événements.

Du côté des utilisateurs, le chiffrement des données et leur protection contre tout accès non autorisé constituent les principales fonctions de sécurité de SafeGuard Enterprise. SafeGuard Enterprise peut être intégré de façon transparente à l'environnement normal de l'utilisateur, et son utilisation est facile et intuitive. Le système d'authentification SafeGuard, l'authentification au démarrage (POA, Power-On Authentication), assure une protection nécessaire des accès et une prise en charge conviviale lors de la récupération des codes d'accès.

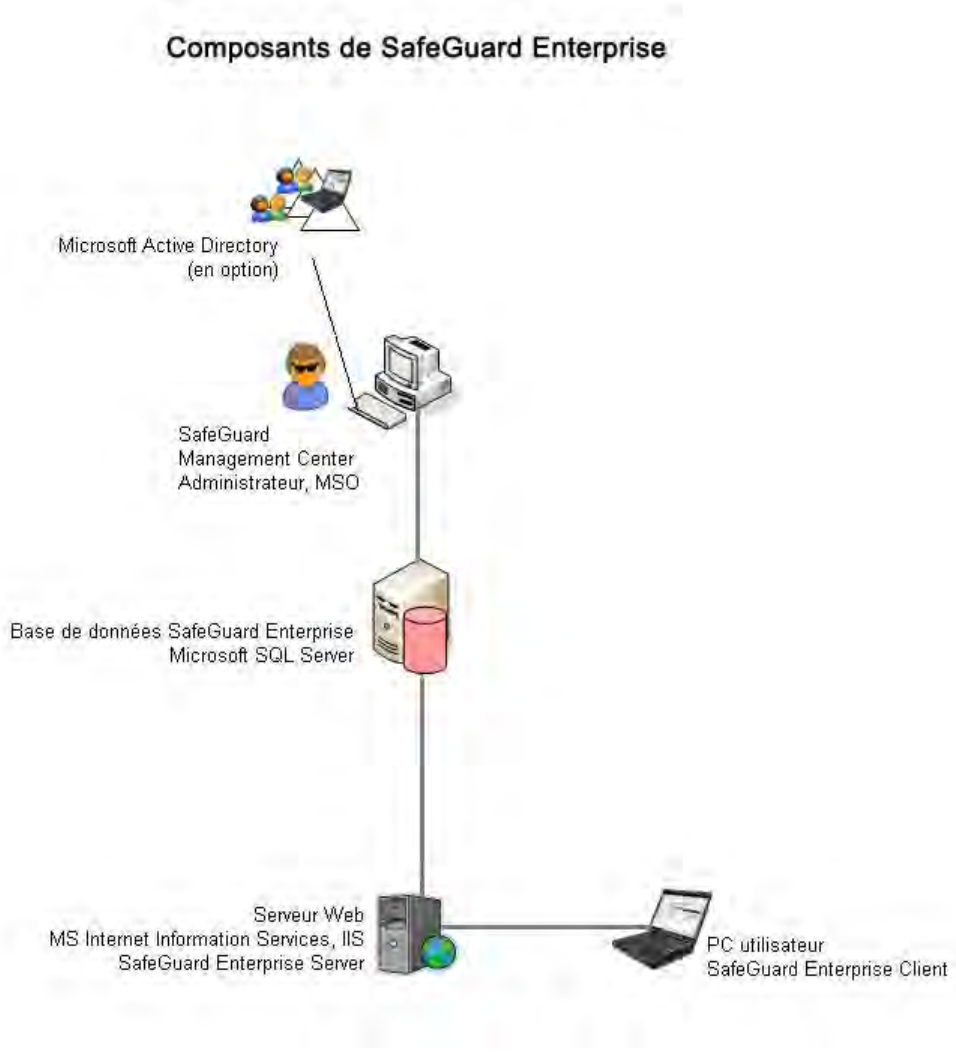
Remarque : certaines fonctions ne sont pas incluses dans toutes les licences. Veuillez contacter votre Partenaire commercial pour obtenir plus de renseignements sur ce qui est inclus dans votre licence.

1.1 Composants de SafeGuard Enterprise

Cette section constitue un aperçu des composants SafeGuard Enterprise et explique comment ils interagissent.

Une ou plusieurs bases de données Microsoft SQL stockent les informations sur les ordinateurs d'extrémité sur le réseau d'entreprise. L'administrateur, appelé dans SafeGuard Enterprise responsable principal de la sécurité (MSO, Master Security Officer), utilise SafeGuard Management Center pour gérer le contenu de la base de données et créer des instructions de sécurité (stratégies).

Les ordinateurs d'extrémité lisent les stratégies dans la base de données et signalent à celle-ci qu'ils fonctionnent correctement. La communication entre la base de données et les ordinateurs d'extrémité est établie par le serveur Web IIS (Internet Information Services) sur lequel le serveur SafeGuard Enterprise est installé.



Le tableau suivant décrit les composants individuels :

Composant	Description
Bases de données SafeGuard Enterprise basées sur la base de données Microsoft SQL Server	Les bases de données SafeGuard Enterprise contiennent toutes les données nécessaires, telles que les clés/certificats, les informations sur les utilisateurs et les ordinateurs, les événements et les paramètres de stratégie. Les bases de données sont accessibles via le serveur SafeGuard Enterprise et uniquement par un seul responsable de la sécurité via SafeGuard Management Center, généralement le responsable principal de la sécurité. Les bases de données SafeGuard Enterprise peuvent être générées et configurées à l'aide d'un assistant ou de scripts.
Serveur SafeGuard Enterprise sur serveur Web IIS	Services Internet (ISS) de Microsoft. .NET Framework 4 et ASP.NET 4 sont requis. Le serveur Web utilisé pour SafeGuard Enterprise doit être basé sur IIS. Nous vous conseillons d'utiliser un serveur IIS dédié pour le serveur SafeGuard Enterprise.

Composant	Description
	Le serveur SafeGuard Enterprise sert d'interface entre la base de données SafeGuard Enterprise et l'ordinateur d'extrémité SafeGuard Enterprise. Sur demande, le serveur SafeGuard Enterprise envoie les paramètres de stratégie aux ordinateurs d'extrémité. Il doit pouvoir accéder à la base de données. Il s'exécute en tant qu'application sur un serveur Web IIS.
	Authentification de base et ASP .NET 4.5 Lorsque vous choisissez SSL en tant que méthode de chiffrement du transport pour la communication du serveur client, veuillez installer le rôle *Authentification de base* en plus d'ASP.NET 4.5.
SafeGuard Management Center sur l'ordinateur de l'administrateur	Outil d'administration centralisée pour les ordinateurs d'extrémité protégés par SafeGuard Enterprise, la gestion des clés et des certificats, les utilisateurs et les ordinateurs et la création des stratégies SafeGuard Enterprise. SafeGuard Management Center communique avec la base de données SafeGuard Enterprise. .NET Framework 4 est requis.
Services d'annuaire (facultatif)	Importation d'Active Directory. qui contient la structure organisationnelle de l'entreprise avec les utilisateurs et les ordinateurs.
Logiciel de chiffrement SafeGuard Enterprise sur les ordinateurs d'extrémité	Logiciel de chiffrement pour une authentification et un chiffrement des données sécurisés sur les ordinateurs d'extrémité. Les ordinateurs d'extrémité protégés par SafeGuard Enterprise peuvent soit être connectés au serveur SafeGuard Enterprise (administré), soit pas connectés du tout à un serveur SafeGuard Enterprise (non administré). Les ordinateurs d'extrémité reçoivent leurs stratégies directement du serveur SafeGuard Enterprise. Les ordinateurs d'extrémité non administrés reçoivent leurs stratégies à l'intérieur des packages de configuration pouvant être déployés à l'aide de mécanismes de distribution tiers.

2 Démarrage

Cette section vous explique comment préparer avec succès l'installation de SafeGuard Enterprise.

- Première installation : le Conseiller d'installation SGN simplifie la première installation des composants d'administration, notamment les stratégies par défaut. Pour lancer le Conseiller d'installation SGN pour les nouvelles installations de SafeGuard Enterprise, démarrez **`SGNInstallAdvisor.bat`** fourni avec le produit. Un assistant vous guide tout au long de l'installation.

- Installation de mise à jour : suivez les étapes décrites dans ce guide.

Remarque : nos vidéos de démonstration sont idéales pour découvrir SafeGuard Enterprise. Elles décrivent l'installation de SafeGuard Enterprise et l'utilisation de SafeGuard Management Center. Retrouvez plus d'informations sur notre site Web : http://www.sophos.com/fr-fr/.

2.1 Quelles sont les étapes clés ?

Pour installer SafeGuard Enterprise, suivez les étapes d'installation mentionnées ci-dessous.

Remarque : SafeGuard Enterprise pour Windows ne prend pas en charge le matériel d'Apple et ne peut pas être installé dans un environnement Boot Camp.

Tous les composants SafeGuard Enterprise (packages .msi) sont disponibles dans le produit.

Étape	Description	Package/Outil
1	Téléchargement des programmes d'installation.	
2	Installation de .NET Framework 4 avec ASP.NET 4. Si vous utilisez .NET 4.5 et souhaitez choisir SSL en tant que méthode de chiffrement du transport pour la communication du serveur client, veuillez installer le rôle *Authentification de base* en plus d'ASP.NET 4.5.	
3	Configuration des services Internet (IIS) pour SafeGuard Enterprise.	
4	Installation du serveur SafeGuard Enterprise.	SGNServer.msi
5	Configuration de l'authentification de la base de données Microsoft SQL Server pour le responsable principal de la sécurité de SafeGuard Enterprise.	
6	Génération des bases de données SafeGuard Enterprise à l'aide d'un script.	Scripts fournis avec le produit dans le répertoire Tools\Database scripts

Étape	Description	Package/Outil
7	Installation de la console d'administration de SafeGuard Management Center pour la gestion centralisée des utilisateurs, ordinateurs, stratégies, clés et rapports.	SGNManagementCenter.msi
8	Configuration de SafeGuard Management Center : connexion base de données et serveur de base de données, certificats, informations d'identification du responsable principal de la sécurité.	Assistant de configuration de SafeGuard Management Center
9	Enregistrement et configuration du serveur SafeGuard Enterprise : création du package de configuration du serveur et déploiement de ce dernier sur le serveur Web.	Outil de package de configuration de SafeGuard Management Center
10	Création de la structure organisationnelle depuis Active Directory ou manuellement.	SafeGuard Management Center
11	Préparation des ordinateurs d'extrémité au chiffrement.	SGxClientPreinstall.msi
12	Création du package de configuration initiale pour la configuration des ordinateurs d'extrémité.	Outil de package de configuration de SafeGuard Management Center
13	Installation du logiciel de chiffrement et du package de configuration initiale sur les ordinateurs d'extrémité	Retrouvez plus d'informations sur les packages disponibles à la section À propos des ordinateurs d'extrémité administrés et non administrés à la page 49.

2.2 Vérification de la configuration système requise

Avant de déployer SafeGuard Enterprise, vérifiez la configuration système requise.

Retrouvez plus d'informations sur la configuration matérielle et logicielle, sur les service packs et sur l'espace disque requis pour effectuer l'installation ainsi que pour bénéficier d'un fonctionnement optimal de votre produit dans les Notes de publication de SafeGuard sur : http://www.sophos.com/fr-fr/support/knowledgebase/112776.aspx.

2.3 Téléchargement des programmes d'installation

1. À l'aide de l'adresse Web et des codes d'accès de téléchargement fournis par votre administrateur système, allez sur le site Web Sophos et téléchargez les programmes d'installation.
2. Placez-les à un emplacement auquel vous pouvez accéder pour effectuer l'installation.

2.4 Paramètres de langue

Les paramètres de langue pour les assistants de configuration et les composants SafeGuard Enterprise sont décrits ci-dessous.

Assistants

Les assistants d'installation et de configuration des packages d'installation différents utilisent le paramètre de langue du système d'exploitation. Si la langue du système d'exploitation n'est pas disponible pour ces assistants, la langue par défaut est automatiquement l'anglais.

SafeGuard Management Center

Vous pouvez définir la langue de SafeGuard Management Center comme suit :

- Dans SafeGuard Management Center, cliquez sur **Outils > Options > Général**. Sélectionnez **Utiliser la langue définie par l'utilisateur** et sélectionnez une langue disponible. Les langues prises en charge sont l'anglais, l'allemand, le français et le japonais.
- Redémarrez SafeGuard Management Center. Il apparaît dans la langue sélectionnée.

SafeGuard Enterprise sur les ordinateurs d'extrémité

Vous définissez la langue de SafeGuard Enterprise sur les ordinateurs d'extrémité dans une stratégie de type **Paramètres généraux** dans SafeGuard Management Center en utilisant le paramètre **Personnalisation > Langue utilisée sur le client** :

- Si la langue du système d'exploitation est sélectionnée, SafeGuard Enterprise utilise le paramètre de langue du système d'exploitation. Si la langue du système d'exploitation n'est pas disponible dans SafeGuard Enterprise, la langue de SafeGuard Enterprise est définie par défaut sur l'anglais.
- Si l'une des langues disponibles est sélectionnée, les fonctions de SafeGuard Enterprise apparaissent dans la langue sélectionnée sur l'ordinateur d'extrémité.

2.5 Compatibilité avec les autres produits Sophos

Cette section décrit la compatibilité de SafeGuard Enterprise 7.0 avec les autres produits Sophos.

2.5.1 Compatibilité avec SafeGuard LAN Crypt

La version 3.7x de SafeGuard LAN Crypt et la version 7.0 de SafeGuard Enterprise peuvent cohabiter sur un ordinateur. Si vous voulez utiliser la fonction SafeGuard Data Exchange, veuillez installer un composant de compatibilité supplémentaire pour assurer le bon fonctionnement des versions du produit sur un ordinateur d'extrémité.

Remarque : le composant de compatibilité est fourni avec votre produit : Installez `SGFileEncCompLayer.msi` sur les systèmes 32 bits et `SGFileEncCompLayer_x64.msi` sur les systèmes 64 bits.

Si SafeGuard LAN Crypt 3.7x est déjà installé :

1. Installez le composant de compatibilité sur l'ordinateur d'extrémité.
2. Installez le package de préinstallation SafeGuard sur l'ordinateur d'extrémité.
3. Installez SafeGuard Data Exchange sur l'ordinateur d'extrémité.
4. Installez le package de configuration du client SafeGuard sur l'ordinateur d'extrémité.
5. Redémarrez l'ordinateur d'extrémité.

Remarque : au cours de l'installation, vous allez voir apparaître un message vous informant que le composant SGLC Profile Loader est déjà en cours d'installation. Vous pouvez ignorer ce message. Il apparaît car SafeGuard LAN Crypt et SafeGuard Enterprise ont des composants communs. Les composants affectés seront mis à jour au redémarrage.

Si SafeGuard Enterprise 7.0 est déjà installé :

1. Installez SafeGuard LAN Crypt 3.7x sur l'ordinateur d'extrémité.
2. Installez le composant de compatibilité sur l'ordinateur d'extrémité.
3. Redémarrez l'ordinateur d'extrémité.

Remarque : les versions précédentes des deux produits ne peuvent pas cohabiter sur un seul ordinateur. Par exemple, si vous essayez d'installer la version 3.6x de SafeGuard LAN Crypt sur un ordinateur sur lequel la version 7.0 de SafeGuard Enterprise est déjà installée, l'installation est annulée et un message d'erreur apparaît.

2.5.2 Compatibilité avec SafeGuard PrivateCrypto et SafeGuard PrivateDisk

SafeGuard Enterprise 7.0 et les produits autonomes SafeGuard PrivateCrypto (à partir de la version 2.30 ou supérieure) et SafeGuard PrivateDisk (à partir de la version 2.30 et supérieure) peuvent cohabiter sur le même ordinateur.

SafeGuard PrivateCrypto et SafeGuard PrivateDisk peuvent alors partager la gestion des clés de SafeGuard Enterprise.

2.5.3 Compatibilité avec SafeGuard RemovableMedia

Le composant SafeGuard Data Exchange et SafeGuard RemovableMedia ne peuvent pas cohabiter sur le même ordinateur. Avant d'installer SafeGuard Data Exchange sur un ordinateur d'extrémité, vérifiez si SafeGuard RemovableMedia est déjà installé. Dans ce cas, assurez-vous d'avoir désinstallé SafeGuard RemovableMedia avant d'installer SafeGuard Data Exchange.

Les clés locales créées avec une version de SafeGuard RemovableMedia antérieure à la version 1.20 avant de passer à SafeGuard Data Exchange peuvent être utilisées sur l'ordinateur protégé par SafeGuard Enterprise. En revanche, elles ne sont pas transférées automatiquement dans la base de données SafeGuard Enterprise.

2.5.4 Compatibilité avec Sophos Enterprise Console

Si vous utilisez Sophos Enterprise Console (SEC) pour administrer le chiffrement, n'installez pas le serveur SafeGuard Enterprise ou SafeGuard Management Center sur le serveur sur lequel le serveur d'administration SEC est installé.

2.6 Restrictions générales

Notez les restrictions générales suivantes pour SafeGuard Enterprise sur les ordinateurs d'extrémité :

- SafeGuard Enterprise pour Windows ne prend pas en charge le matériel d'Apple et ne peut pas être installé dans un environnement Boot Camp.
- Si vous utilisez le mécanisme Intel Advanced Host Controller Interface (AHCI) sur l'ordinateur d'extrémité, le disque dur d'initialisation doit être installé dans le connecteur 0 ou le connecteur 1. Vous pouvez insérer jusqu'à 32 disques durs. SafeGuard Enterprise ne s'exécute que sur les deux premiers connecteurs.

- Le chiffrement basé sur volume de SafeGuard pour les volumes se trouvant sur les disques dynamiques et sur les disques de table de partition GUID (GPT) n'est pas pris en charge. Dans ces cas-là, l'installation est interrompue. Si de tels disques sont trouvés sur l'ordinateur d'extrémité, ils ne sont pas pris en charge.

- Les modules de chiffrement intégral du disque SafeGuard (chiffrement de volumes SafeGuard et prise en charge de BitLocker) ne sont pas compatibles avec les systèmes équipés de disques durs reliés par un bus SCSI.

- La fonction de **Changement rapide d'utilisateur** n'est pas prise en charge.

- L'utilisation de SafeGuard Enterprise dans un environnement Terminal Server n'est pas prise en charge.

3 Configuration du serveur SafeGuard Enterprise

Le serveur SafeGuard Enterprise sert d'interface avec les clients SafeGuard Enterprise. Comme SafeGuard Management Center, il permet d'accéder à la base de données. Il s'exécute en tant qu'application sur un serveur Web basé sur les services Internet (IIS) de Microsoft.

Le serveur SafeGuard Enterprise inclut le Planificateur de tâches pour créer et planifier des tâches périodiques basées sur des scripts. Les tâches sont automatiquement exécutées sur le serveur SafeGuard Enterprise. Les scripts sont fournis avec le produit SafeGuard Enterprise. Retrouvez plus d'informations dans le *Manuel d'administration de SafeGuard Enterprise*.

Nous vous conseillons d'installer le serveur SafeGuard Enterprise sur un IIS dédié. Les performances s'en trouvent ainsi améliorées. En outre, il garantit l'absence de conflits entre d'autres applications et SafeGuard Enterprise comme, par exemple, avec la version d'ASP.NET à utiliser.

Ce chapitre décrit comment installer le serveur SafeGuard Enterprise, avec le Planificateur de tâches sous IIS. Commencez par installer et configurer les services Internet (IIS) de Microsoft.

3.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies :

- Vous devez disposer de droits d'administrateur Windows.
- Les services Internet (IIS) de Microsoft doivent être disponibles.

  IIS est gratuit. Ce programme se trouve, par exemple, sur votre DVD Windows ou sur le site Web de Microsoft.
- Si vous utilisez le chiffrement de transport SSL entre le serveur SafeGuard Enterprise et le client SafeGuard Enterprise, veuillez configurer IIS à l'avance. Retrouvez plus d'informations à la section Sécurisation des connexions de transport avec SSL à la page 40.

  Un certificat doit être généré et le serveur des services Internet (IIS) configuré pour utiliser SSL et sélectionner le certificat.

  Le nom du serveur spécifié lors de la configuration du serveur SafeGuard Enterprise doit être identique à celui spécifié dans le certificat SSL. Faute de quoi, la communication entre le client et le serveur est impossible. Un certificat distinct est nécessaire pour chaque serveur SafeGuard Enterprise.

  Si vous utilisez un équilibreur de charge réseau, vérifiez que la plage de ports inclut le port SSL.
- .NET Framework 4 et ASP.NET 4 doivent être installés. Il sont fournis avec le produit SafeGuard Enterprise.

3.2 Installation et configuration des services Internet (IIS) de Microsoft

Cette section vous explique comment préparer l'exécution des services Internet (IIS) de Microsoft avec le serveur SafeGuard Enterprise.

3.2.1 Installation et configuration des services Internet (IIS) 7/7.5 sur Microsoft Windows Server 2008/2008 R2

IIS est gratuit. Ce programme se trouve, par exemple, sur votre DVD Windows ou sur le site Web de Microsoft.

1. Dans le menu **Démarrer**, cliquez sur **Tous les programmes**, **Outils d'administration**, puis sur **Gestionnaire de serveur**.
2. Dans le **Gestionnaire de serveur**, cliquez sur **Rôles**, puis cliquez sur **Ajouter des rôles**.
3. Dans l'**Assistant d'ajout de rôles**, sur la page **Avant de commencer**, vérifiez les éléments suivants :
   - Le compte administrateur a un mot de passe fort.
   - Les paramètres réseau, par exemple les adresses IP, sont configurés.
   - Les dernières mises à jour de sécurité de Windows Update sont installées.
4. Sélectionnez **Sélectionner les rôles** à droite, puis **Serveur Web (IIS)**. Sur la page qui suit, cliquez sur **Ajouter les fonctionnalités requises**. Le **Serveur Web (IIS)** apparaît dans la zone de navigation de l'**Assistant d'ajout de rôles**.
5. Cliquez sur **Serveur Web (IIS)**, puis sur **Services de rôles**. Conservez les services de rôles par défaut.
6. À droite, sélectionnez **ASP.NET**, ce qui sélectionne également tous les services des sous-rôles.
7. Sélectionnez les **Scripts et outils de gestion IIS** nécessaire à une configuration correcte de IIS 7.
8. Cliquez sur **Suivant**, puis sur **Installer** et enfin sur **Fermer**,

   IIS est installé avec une configuration par défaut pour l'hébergement de ASP.NET.
9. Vérifiez que la page Web apparaît correctement à l'aide de http://<nom serveur>. Retrouvez plus d'informations sur : http://support.microsoft.com.

3.2.1.1 Vérification de l'enregistrement de .NET Framework sous IIS 7

.NET Framework 4 est requis. Ce programme est fourni avec le produit SafeGuard Enterprise.

Pour vérifier s'il est installé correctement sur IIS 6 ou IIS 7 :

1. À partir du menu **Démarrer**, sélectionnez **Exécuter...**.
2. Saisissez la commande suivante : **`Appwiz.cpl`**. Tous les programmes installés sur l'ordinateur apparaissent à l'écran.
3. Vérifiez si .NET Framework Version 4 apparaît. Si elle n'apparaît pas, installez cette version. Suivez les étapes de l'assistant d'installation et confirmez tous les paramètres par défaut.

4. Pour vérifier si l'installation est correctement enregistrée, allez dans C:\Windows\Microsoft.NET\Framework. Chaque version installée doit être visible sous la forme d'un dossier distinct montrant la version comme nom de dossier, par exemple "v 4.0".

3.2.1.2 Vérification de l'enregistrement d'ASP.NET sous IIS 7

La version 4.0 de ASP.NET est requise.

1. Pour vérifier qu'ASP.NET est installé et enregistré sous la bonne version, saisissez la commande **aspnet_regiis.exe -lv** à l'invite de commande.

La version 4.0 doit apparaître pour ASP.NET.

3.2.2 Installation et configuration des services Internet (IIS) 8 sur Microsoft Windows Server 2012/2012 R2

IIS est gratuit. Ce programme se trouve, par exemple, sur votre DVD Windows ou sur le site Web de Microsoft.

1. Sur **Gestionnaire de serveursTableau de bord**, cliquez sur **Gérer** et sélectionnez **Ajouter des rôles et des fonctionnalités**.
2. Dans l'**Assistant Ajout de rôles et de fonctionnalités**, sur la page **Avant de commencer**, vérifiez les éléments suivants :
   - Le compte administrateur a un mot de passe fort.
   - Les paramètres réseau, par exemple les adresses IP, sont configurés.
   - Les dernières mises à jour de sécurité de Windows Update sont installées.
3. Sélectionnez **Rôles du serveur** sur le volet de gauche, puis **Serveur Web (IIS)**. Cliquez sur **Ajouter des fonctionnalités** dans la fenêtre qui s'affiche. Le **Rôle Serveur Web (IIS)** apparaît dans la zone de navigation de l'**Assistant Ajout de rôles et de fonctionnalités**.
4. Dans le volet de gauche, sélectionnez **Services de rôle** sous **Rôle Serveur Web (IIS)**. Conservez les services de rôles par défaut.
5. Défilez jusqu'au nœud **Développement d'applications** et vérifiez :
   - **ASP.NET 4.5**
   - **Extensions ISAPI**
   - **Filtres ISAPI**

   Les services de sous-rôles nécessaires sont sélectionnés automatiquement.
6. Sous le nœud **Sécurité**, vérifiez :
   - **Authentification de base**
   - **Authentification Windows**
7. Cliquez sur **Suivant**, puis sur **Installer** et enfin sur **Fermer**.

   Votre service de serveur IIS est installé avec une configuration par défaut pour l'hébergement d'ASP.NET.

3.3 Installation du serveur SafeGuard Enterprise

Après avoir configuré IIS, vous pouvez installer le serveur SafeGuard Enterprise sur le serveur IIS. Le package d'installation **`SGNServer.msi`** est livré avec le produit.

1. Sur le serveur sur lequel vous voulez installer le serveur SafeGuard Enterprise, cliquez deux fois sur **`SGNServer.msi`**. Un assistant vous guide tout au long des étapes nécessaires.
2. Validez les valeurs par défaut dans toutes les boîtes de dialogue qui suivent. Le Planificateur de tâches est automatiquement installé avec une installation de type **Complète**.

Le serveur SafeGuard Enterprise est installé avec le Planificateur de tâches.

Remarque : afin d'améliorer les performances, une fois le serveur SafeGuard Enterprise installé, la connexion des événements consignés dans le journal est désactivée par défaut pour la base de données SafeGuard Enterprise. Toutefois, la connexion des événements journalisés est nécessaire pour la protection de l'intégrité des événements journalisés. La concaténation de toutes les entrées du tableau des événements permet de voir clairement lorsqu'une entrée a été supprimée et de lancer une vérification de l'intégrité. Pour utiliser la protection d'intégrité, vous devez définir manuellement la connexion des événements consignés dans le journal. Retrouvez plus d'informations à la section *Rapports* du *Manuel d'administration de SafeGuard Enterprise*.

4 Configuration de la base de données SafeGuard Enterprise

SafeGuard Enterprise archive toutes les données nécessaires, telles que les clés/certificats, les informations sur les utilisateurs et sur les ordinateurs, les événements et les paramètres de stratégie dans une base de données. La base de données SafeGuard Enterprise se trouve sur Microsoft SQL Server

Vérifiez la liste des types de serveurs SQL actuellement pris en charge dans la section des configurations système requises de la version actuelle des notes de publication sur : http://www.sophos.com/fr-fr/support/knowledgebase/112776.aspx.

Vous pouvez configurer la base de données soit automatiquement à la première configuration dans SafeGuard Management Center soit manuellement à l'aide de scripts SQL fournis avec votre produit. Selon l'environnement de votre entreprise, vérifiez la méthode à choisir. Retrouvez plus d'informations à la section Droits d'accès à la base de données à la page 18.

Afin d'améliorer les performances, la base de données SafeGuard Enterprise peut être répliquée sur plusieurs serveurs SQL. Retrouvez plus d'informations sur le paramétrage de la réplication de la base de données à la section Réplication de la base de données SafeGuard Enterprise à la page 68.

Plusieurs bases de données SafeGuard Enterprise peuvent être créées et maintenues à jour pour différents locataires tels que les différents locaux d'une entreprise, les différentes unités organisationnelles ou les différents domaines (architecture mutualisée). Retrouvez plus d'informations sur la configuration d'une architecture mutualisée à la section Configurations d'architecture mutualisée à la page 28.

Remarque : nous vous conseillons d'effectuer une sauvegarde en ligne permanente de la base de données. Sauvegardez régulièrement votre base de données pour protéger les clés, les certificats d'entreprise et les attributions utilisateur/machine. Les cycles de sauvegarde conseillés sont à effectuer, par exemple, suite à la première importation des données, suite à des modifications importantes ou à intervalles réguliers, par exemple toutes les semaines ou tous les jours.

4.1 Authentification de la base de données

Pour pouvoir accéder à la base de données SafeGuard Enterprise, le responsable principal de la sécurité du SafeGuard Management Center doit être authentifié au niveau du serveur SQL. Cette authentification peut être effectuée comme suit :

- Authentification Windows : promouvoir un utilisateur Windows actuel à un poste d'utilisateur SQL
- Authentification SQL : créer un compte utilisateur SQL

Vous pouvez vous renseigner auprès de votre administrateur SQL pour connaître la méthode d'authentification la mieux adaptée en tant que responsable de la sécurité. Vous devez disposer de cette information avant de pouvoir générer la base de données et avant de procéder à la configuration initiale dans l'Assistant de configuration du SafeGuard Management Center.

Utilisez l'authentification SQL pour des ordinateurs ne faisant pas partie d'un domaine, sinon utilisez l'authentification Windows. Si vous utilisez l'authentification SQL, nous conseillons vivement de protéger la connexion de et vers le serveur de base de données avec SSL. Retrouvez plus d'informations à la section Configuration de SSL à la page 40.

4.1.1 Droits d'accès à la base de données

SafeGuard Enterprise est configuré d'une telle façon que pour utiliser la base de données SQL, vous n'avez besoin que d'un seul compte utilisateur avec des droits d'accès minimaux pour la base de données. Ce compte utilisateur est utilisé par SafeGuard Management Center et délivré uniquement au premier responsable de la sécurité de SafeGuard Management Center. Il garantit la connexion à la base de données SafeGuard Enterprise. Lorsque SafeGuard Enterprise est en cours d'exécution, un seul responsable de la sécurité de SafeGuard Management Center nécessite uniquement les droits en lecture/écriture sur la base de données de SafeGuard Management Center.

La base de données SafeGuard Enterprise peut soit être créée manuellement soit automatiquement lors de la configuration initiale dans SafeGuard Management Center. Si elle est créée automatiquement, les droits d'accès étendus pour la base de données SQL (db_creator) sont nécessaires pour le premier responsable de la sécurité de SafeGuard Management Center. Néanmoins, l'administrateur SQL peut ensuite révoquer ces droits jusqu'à l'installation ou la mise à jour suivante.

Si l'extension des autorisations pendant la configuration de SafeGuard Management Center n'est pas souhaitée, l'administrateur SQL peut générer la base de données SafeGuard Enterprise à l'aide d'un script. Les deux scripts fournis avec le produit, **CreateDatabase.sql** et **CreateTables.sql** peuvent être exécutés à cet effet.

Le tableau suivant affiche les autorisations SQL nécessaires pour Microsoft SQL Server.

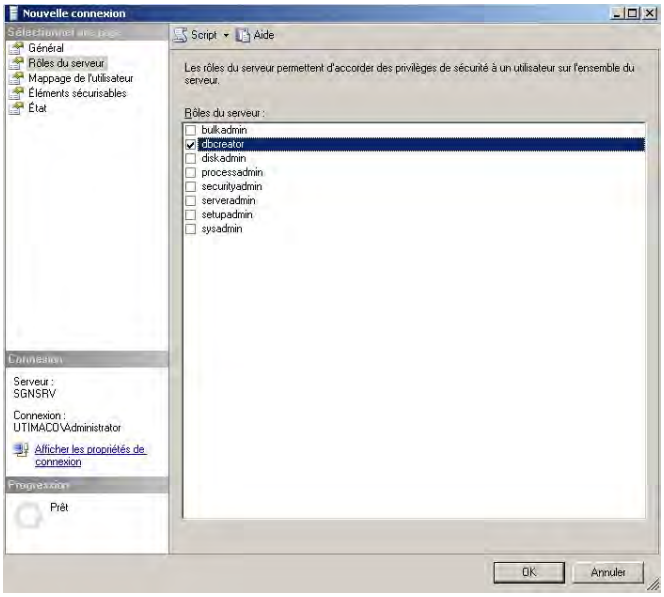
SQL Server 2012, SQL Server 2012 Express	Droit d'accès
Création de la base de données	
Serveur	db_creator
Base de données maître	Aucune
Base de données SafeGuard Enterprise	db_ownerpublic (par défaut)
Utilisation de la base de données	
Serveur	Aucune
Base de données maître	Aucune
Base de données SafeGuard Enterprise	db_datareader db_datawriter publique (par défaut)

4.1.2 Configuration d'un compte Windows pour la connexion au serveur SQL

La description des étapes de configuration individuelle ci-dessous est destinée aux administrateurs SQL et concerne Microsoft Windows Server 2008 et Microsoft SQL Server 2014 Standard ou Express Edition.

En tant qu'administrateur SQL, vous avez besoin du droit de création de comptes utilisateur.

1. Ouvrez SQL Server Management Studio. Connectez-vous à SQL Server à l'aide de vos codes d'accès.
2. Ouvrez l'**Explorateur d'objets**, cliquez avec le bouton droit de la souris sur **Sécurité**, choisissez **Nouveau**, puis cliquez sur **Connexions**.
3. Dans **Connexion - Nouveau** sur la page **Général**, sélectionnez **Authentification Windows**.
4. Cliquez sur **Rechercher**. Recherchez le nom utilisateur Windows respectif et cliquez sur **OK**. Le nom utilisateur apparaît comme **Nom de connexion**.
5. Dans **Base de données par défaut**, si aucun script n'a été utilisé pour créer une base de données SafeGuard Enterprise, sélectionnez **Maître**.
6. Cliquez sur **OK**.
7. Pour créer automatiquement la base de données lors de la première configuration de SafeGuard Management Center, vous devez changer les droits d'accès. Dans **Connexion - Nouveau**, attribuez les droits d'accès/rôles en cliquant à gauche sur **Rôles du serveur** : Sélectionnez **dbcreator**. Dès que SafeGuard Enterprise est installé, vous pouvez réinitialiser le rôle de la base de données sur **dbowner**.



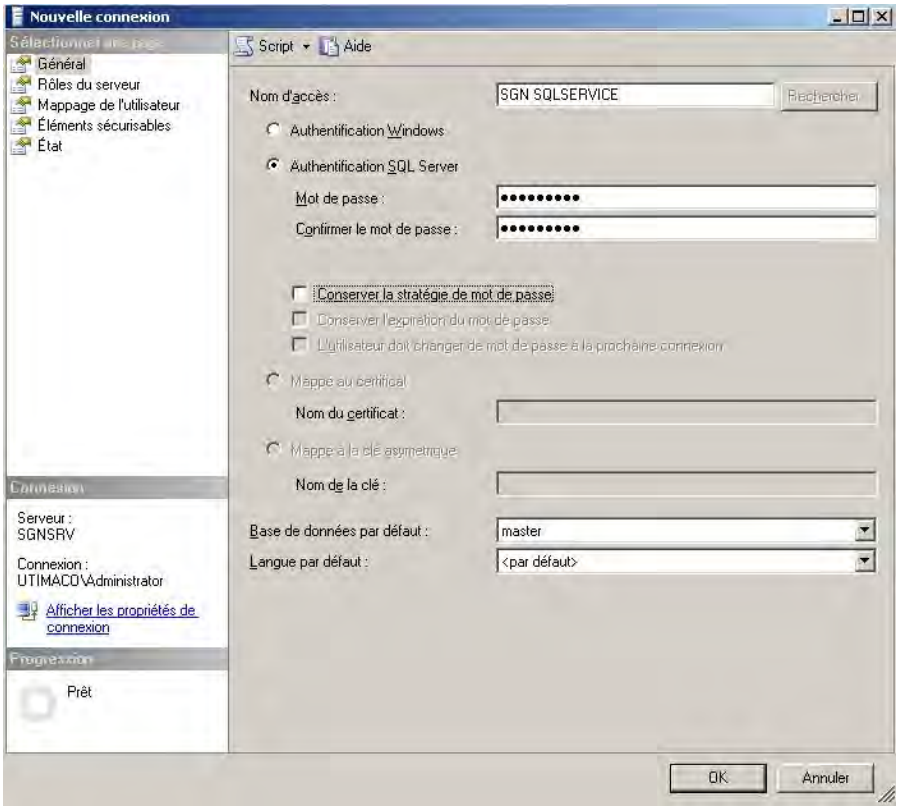
4.1.3 Création d'un compte SQL pour la connexion au serveur SQL

La description des étapes de configuration individuelles ci-dessous est destinée aux administrateurs SQL. Elle concerne toutes les éditions de Microsoft Windows Server 2008 avec Microsoft SQL Server 2008 Standard Edition.

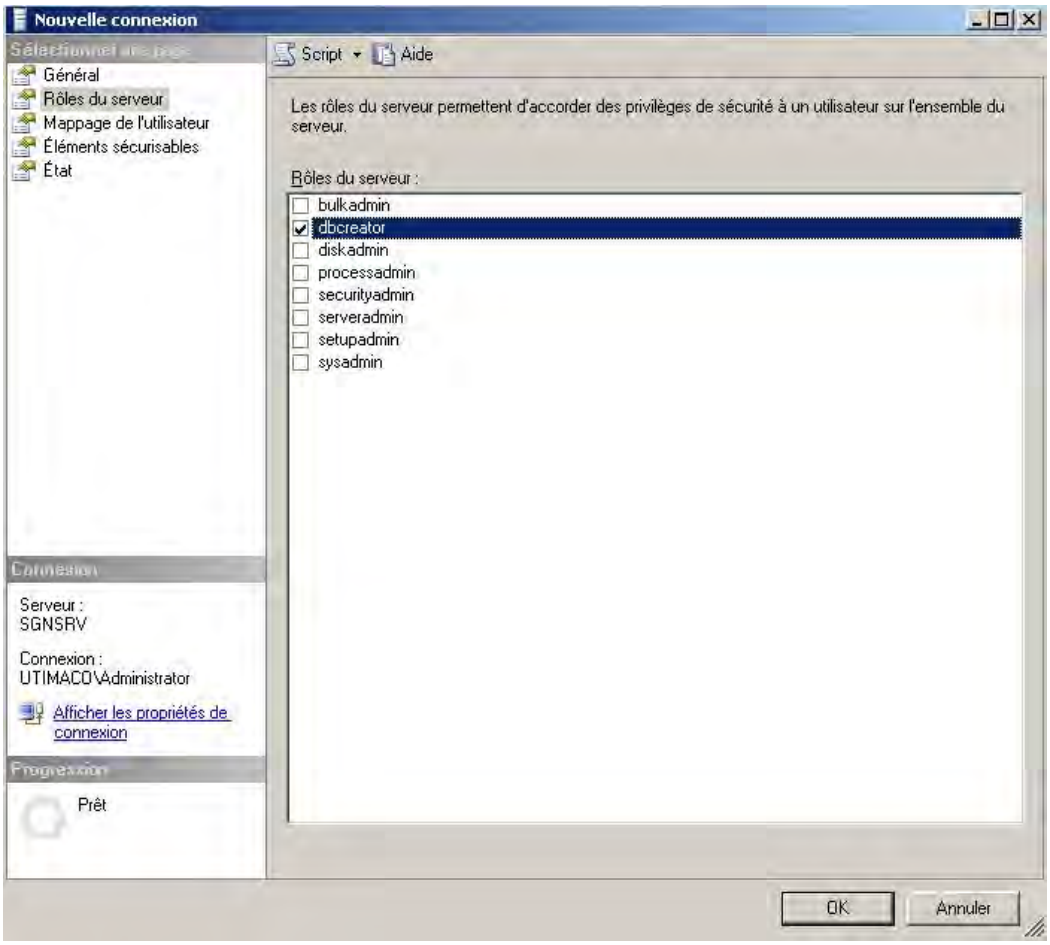
En tant qu'administrateur SQL, vous avez besoin du droit de création d'un compte utilisateur SQL.

1. Ouvrez SQL Server Management Studio. Connectez-vous à SQL Server à l'aide de vos codes d'accès.
2. Ouvrez l'**Explorateur d'objets**, cliquez avec le bouton droit de la souris sur **Sécurité**, choisissez **Nouveau**, puis cliquez sur **Connexions**.
3. Dans **Connexion - Nouveau** sur la page **Général**, sélectionnez **Authentification SQL Server**.
4. Sur la page **Général**, dans **Nom de connexion**, procédez de la manière suivante :
   a) Saisissez le nom du nouvel utilisateur, par exemple SGN SQLSERVICE.
   b) Saisissez et confirmez le mot de passe du compte.
   c) Dessélectionnez **Appliquer la stratégie des mots de passe**.
   d) Dans **Base de données par défaut**, si aucun script n'a été utilisé pour créer une base de données SafeGuard Enterprise, sélectionnez **Maître**. Cliquez sur **OK**.

   Notez la méthode d'authentification et les codes d'accès. Fournissez ces informations au responsable de la sécurité de SafeGuard Management Center.



5. Pour créer la base de données automatiquement lors de la première configuration de SafeGuard Management Center, vous devez changer les droits d'accès ainsi : dans **Connexion - Nouveau** sur la page **Général**, attribuez les droits d'accès/rôles en cliquant sur **Rôles du serveur** à gauche. Sélectionnez **dbcreator**. Dès que SafeGuard Enterprise est installé, vous pouvez réinitialiser le rôle de la base de données sur **dbowner**.



Le compte utilisateur SQL et les droits d'accès sont maintenant configurés pour le responsable de la sécurité de SafeGuard Enterprise.

4.2 Génération de la base de données SafeGuard Enterprise

Une fois le compte utilisateur configuré pour la connexion au serveur SQL, générez la base de données SafeGuard Enterprise. Pour ce faire, vous pouvez procéder de deux façons :

- À l'aide de l'Assistant de configuration de SafeGuard Management Center

  Au titre de responsable de la sécurité, vous pouvez facilement créer la base de données SafeGuard Enterprise suite à l'installation de SafeGuard Management Center. L'assistant de configuration de SafeGuard Management Center vous guide tout au long de la configuration de base qui inclut également la création de la base de données. Pour ce faire, poursuivez l'installation et la configuration de SafeGuard Management Center. Retrouvez plus d'informations à la section Installation de SafeGuard Management Center à la page 26. Puis, continuez à changer les droits d'accès adéquats. Retrouvez plus

d'informations à la section Modification des droits d'accès à la base de données SafeGuard Enterprise à la page 23.

- À l'aide de scripts SQL fournis avec le produit

  Cette procédure est généralement favorisée si l'extension des autorisations SQL pendant la configuration de SafeGuard Management Center n'est pas souhaitée.

  La méthode à appliquer dépend de votre environnement. Contactez votre administrateur SQL et votre responsable de la sécurité SafeGuard Enterprise pour convenir de la méthode à utiliser.

4.2.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies :

- Microsoft SQL Server doit déjà être installé et configuré. Microsoft SQL Express Edition convient bien aux petites entreprises, car il est exempt de frais de licence.
- Pour des raisons de performances, Microsoft SQL Server et le serveur SafeGuard Enterprise ne doivent pas être installés sur le même ordinateur.
- Les méthodes d'authentification de la base de données et les droits d'accès de la base de données doivent être clarifiés.

4.2.2 Génération de la base de données SafeGuard Enterprise à l'aide d'un script

Si vous souhaitez créer automatiquement la base de données SafeGuard Enterprise au cours de la configuration de SafeGuard Management Center, vous pouvez ignorer cette étape. Si vous ne souhaitez pas disposer des autorisations SQL étendues au cours de la configuration de SafeGuard Management Center, veuillez effectuer cette étape. Deux scripts de base de données sont fournis à cet effet avec le produit (dossier Tools) :

- CreateDatabase.sql
- CreateTables.sql

La description des étapes ci-dessous est destinée aux administrateurs SQL et concerne Microsoft SQL Server 2008 Standard Edition.

En tant qu'administrateur SQL, vous avez besoin du droit de création d'une base de données.

1. Copiez les scripts CreateDatabase.sql et CreateTables.sql inclus dans le produit SafeGuard Enterprise sur le serveur SQL.
2. Cliquez deux fois sur le script **CreateDatabase.sql**. Microsoft SQL Server Management Studio démarre.
3. Connectez-vous à SQL Server à l'aide de vos codes d'accès.
4. Assurez-vous que les deux chemins cible se trouvant au début du script, sous **FILENAME** (MDF, LDF), sont bien présents sur le lecteur de disque dur local. Corrigez-les si nécessaire.
5. Cliquez sur le bouton **Exécuter** depuis la barre d'outils pour générer la base de données. Vous avez créé la base de données **SafeGuard**. Utilisez maintenant le script CreateTables.sql fourni avec le produit pour générer les tables.
6. Cliquez deux fois sur **CreateTables.sql** . Un autre volet s'ouvre dans Microsoft SQL Server Management Studio.

7. Dans la partie supérieure du script, saisissez **`use SafeGuard`** pour sélectionner la base de données SafeGuard Enterprise dans laquelle les tables doivent être créées.
8. Cliquez sur le bouton **Exécuter** depuis la barre d'outils pour générer les tables.

La base de données SafeGuard Enterprise et les tables associées ont été créées.

4.3 Modification des droits d'accès à la base de données SafeGuard Enterprise

Dès que la base de données SafeGuard Enterprise a été créée, les autorisations d'accès peuvent être modifiées soit à l'aide d'un script, soit dans SafeGuard Management Center. Il est possible d'affecter différents rôles et autorisations à un utilisateur sur une base de données, par conséquent, seuls les droits minimaux sont requis pour la connexion à la base de données SafeGuard Enterprise.

1. Ouvrez SQL Server Management Studio. Connectez-vous à SQL Server à l'aide de vos codes d'accès.
2. Ouvrez l'**Explorateur d'objets**, cliquez avec le bouton droit de la souris sur **Sécurité**, puis cliquez deux fois sur **Connexions**.
3. Cliquez avec le bouton droit de la souris sur le nom d'utilisateur respectif et cliquez sur **Propriétés**.
4. Sélectionnez **Mappage des utilisateurs** sur la gauche. Sous **Utilisateurs mappés à cette connexion** , sélectionnez la base de données **SafeGuard**.
5. Sous **Appartenance au rôle de base de données** définissez les droits d'accès minimaux pour utiliser la base de données SafeGuard Enterprise : sélectionnez **db_datareader**, **db_datawriter** et **public**.
6. Cliquez sur **OK**.

4.4 Vérification des services SQL, des canaux nommés et des paramètres TCP/IP

La description concerne Microsoft Windows Server 2008 (R2) et Microsoft SQL Server 2012 Standard ou Express Edition.

1. Ouvrez le Gestionnaire de configuration SQL Server.
2. À partir de l'arborescence de navigation sur la gauche, sélectionnez **Services SQL Server**.
3. Assurez-vous que l'**État** de **SQL Server** et de **Explorateur SQL Server** est **En cours d'exécution** et que le **Mode de démarrage** est défini sur **Automatique**.
4. À partir de l'arborescence de navigation sur la gauche, sélectionnez **Configuration du réseau SQL Server** et sélectionnez l'instance en cours.
5. Cliquez avec le bouton droit de la souris sur le protocole **Canaux nommés** et cliquez sur **Activé**.
6. Cliquez avec le bouton droit de la souris sur le protocole **TCP/IP** et cliquez sur **Activé**.
7. Ensuite, cliquez avec le bouton droit de la souris sur le protocole **TCP/IP** et cliquez sur **Propriétés**. Dans l'onglet **Adresses IP**, sous **IPAll**, laissez le champ **Ports TCP dynamiques** vide. Définissez le **Port TCP** sur 1433.
8. Redémarrez les services SQL.

4.5 Création d'une règle de pare-feu Windows sur Windows Server 2008 (R2)

La description concerne Microsoft Windows Server 2008 (R2) avec Microsoft SQL Server 2012 Standard ou Express Edition. Lorsque vous utilisez cette configuration, effectuez les étapes ci-dessous afin de vous assurer que la connexion peut être établie entre la base de données SafeGuard Enterprise et SafeGuard Management Center.

1. Sur l'ordinateur hébergeant l'instance de SQL Server, cliquez sur **Démarrer**, sélectionnez **Outils d'administration**, puis cliquez sur **Pare-feu Windows avec fonctions avancées de sécurité**.
2. À partir de l'arborescence de navigation sur la gauche, sélectionnez **Règles de trafic entrant**.
3. Cliquez sur **Action** dans la barre de menus, puis sur **Nouvelle règle**. L'**Assistant Nouvelle règle de trafic entrant** démarre.
4. Sur la page **Type de règle** , sélectionnez **Personnaliser** et cliquez sur **Suivant**.
5. Sur la page **Programme**, sélectionnez le programme et les services auxquels cette règle doit s'appliquer et cliquez sur **Suivant**.
6. Sur la page **Protocole et ports**, sélectionnez **TCP** en tant que **Type de protocole**. Pour le **Port local**, sélectionnez **Ports spécifiques** et saisissez **1433**. Pour le **Port distant** , sélectionnez **Tous les ports**. Cliquez sur **Suivant**.
7. Sur la page **Étendue**, vous pouvez spécifier que la règle s'applique uniquement au trafic réseau allant vers ou provenant d'adresses IP saisies sur cette page. Configurez de manière adéquate et cliquez sur **Suivant**.
8. Sur la page **Action**, sélectionnez **Autoriser la connexion** et cliquez sur **Suivant**.
9. Sur la page **Profil**, sélectionnez l'emplacement sur lequel la règle s'applique et cliquez sur **Suivant**.
10. Sur la page **Nom**, saisissez un nom et une description pour votre règle et cliquez sur **Terminer**.

4.6 Configuration de l'authentification Windows pour la connexion au serveur SQL

La description concerne Microsoft Windows Server 2008 avec Microsoft SQL Server 2012 Standard Edition et IIS 7.

Pour activer la communication entre le serveur SafeGuard Enterprise et la base de données SafeGuard Enterprise lors de l'utilisation de l'authentification Windows, l'utilisateur doit devenir membre des groupes Active Directory. Les autorisations des fichiers locaux doivent être ajustées et le compte utilisateur SQL doit être renseigné dans le pool d'applications de l'IIS.

1. Sélectionnez **Démarrer**, puis **Exécuter**. Saisissez **dsa.msc**. Ouvrez le composant logiciel enfichable Utilisateurs et ordinateurs Active Directory.
2. Dans l'arborescence de navigation sur la gauche, développez l'arborescence du domaine et sélectionnez **Builtin**.
3. Ajoutez l'utilisateur Windows respectif dans les groupes suivants : IIS_IUSRS, Utilisateurs du journal de performance, Utilisateurs de l'Analyseur de performances.
4. Quittez le composant logiciel enfichable.

5. Dans le système de fichiers local, dans l'Explorateur Windows, cliquez avec le bouton droit de la souris sur le dossier C:\Windows\Temp et sélectionnez **Propriétés**. Dans **Propriétés**, sélectionnez l'onglet **Sécurité**.
6. Dans **Sécurité**, cliquez sur **Ajouter** et saisissez le nom d'utilisateur Windows respectif dans le champ **Entrez les noms d'objets à sélectionner**. Cliquez sur **OK**.
7. Dans l'onglet **Sécurité**, sous **Autorisations**, cliquez sur **Avancé**. Dans la boîte de dialogue **Paramètres de sécurité avancés pour Temp**, sous l'onglet **Autorisations**, cliquez sur **Modifier les autorisations**. Puis, modifiez les autorisations dans la boîte de dialogue **Objet** sur **Autoriser** : **Liste du dossier / lecture des données**, **Création de fichier / écriture de données**, **Suppression**.
8. Cliquez sur **OK**, puis fermez la boîte de dialogue **Propriétés de : Temp** et l'Explorateur Windows.
9. Ouvrez le **Gestionnaire des services IIS**.
10. Dans le volet **Connexions** à gauche, sélectionnez **Pools d'applications** du nœud serveur correspondant.
11. Dans la liste **Pools d'applications** à droite, sélectionnez **SGNSRV-Pool**.
12. Dans le volet **Actions** à gauche, sélectionnez **Paramètres avancés**.
13. Dans **Paramètres avancés**, sous **Modèle de processus**, pour la propriété **Identité**, cliquez sur le bouton **...**
14. Dans **Identité du pool d'applications**, sélectionnez **Compte personnalisé** et cliquez sur **Définir**.
15. Dans **Définir les codes d'accès**, saisissez le nom d'utilisateur Windows correspondant sous la forme suivante : `Domaine\<nom utilisateur Windows>`. Saisissez et confirmez le mot de passe Windows respectif, puis cliquez sur **OK**.
16. Dans le volet **Connexions** à gauche, sélectionnez le nœud serveur correspondant et cliquez sur **Redémarrer** dans le volet **Actions**.
17. Dans le volet **Connexions** à gauche, sous le nœud serveur correspondant, sous **Sites**, **Sites Web par défaut**, sélectionnez **SGNSRV**.
18. Sur la page d'accueil /SGNSRV, cliquez deux fois sur **Authentification**.
19. Cliquez avec le bouton droit de la souris sur **Authentification anonyme** et sélectionnez **Modifier**.
20. Pour **Identité utilisateur anonyme**, sélectionnez **Utilisateur spécifique** et vérifiez que le nom utilisateur est **IUSR**. Corrigez-le si nécessaire.
21. Cliquez sur **OK**.

La configuration supplémentaire lors de l'utilisation d'un compte Windows pour la connexion au serveur SQL est désormais terminée.

5 Installation de SafeGuard Management Center

Cette section décrit l'installation et la configuration de SafeGuard Management Center.

SafeGuard Management Center est l'outil d'administration central de SafeGuard Enterprise. Il s'installe sur les ordinateurs administrateurs que vous avez l'intention d'utiliser pour la gestion de SafeGuard Enterprise. Il peut être installé sur tout ordinateur du réseau à partir duquel il est possible d'accéder les bases de données SafeGuard Enterprise.

SafeGuard Management Center permet de prendre en charge plusieurs bases de données via les configurations mutualisées de base de données (Multi Tenancy). Vous pouvez configurer et conserver différentes bases de données SafeGuard Enterprise pour différents titulaires, dans le cas par exemple de plusieurs locaux d'entreprise, unités organisationnelles ou domaines. Pour faciliter la gestion, les configurations de ces bases de données peuvent également être exportées vers des fichiers et importées à partir de fichiers.

5.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies :

- Assurez-vous de disposer des droits d'administrateur Windows.
- .NET Framework 4 doit être installé. Il est fourni avec le produit SafeGuard Enterprise.
- Si vous voulez créer une nouvelle base de données SafeGuard Enterprise lors de la configuration de SafeGuard Management Center, vous avez besoin des droits d'accès et des informations d'identification SQL nécessaires. Retrouvez plus d'informations à la section Droits d'accès à la base de données à la page 18.
- Si la base de données SafeGuard Enterprise et SafeGuard Management Center sont installés sur des ordinateurs différents, assurez-vous que SQL Server 2012 Native Client et Utilitaires ligne de comm. SQL Server 2014 sont installés sur l'ordinateur sur lequel SafeGuard Management Center est installé. Ils sont fournis avec le produit SafeGuard Enterprise dans le dossier tiers.

5.2 Installation de SafeGuard Management Center

1. Démarrez SGNManagementCenter.msi à partir du dossier d'installation du produit livré. Un assistant vous guide tout au long des étapes nécessaires.
2. Acceptez les valeurs par défaut des boîtes de dialogue qui suivent exception faite de la suivante : Sur la page de sélection du **Type d'installation**, procédez de l'une des manières suivantes :
   - Pour que SafeGuard Management Center prenne en charge une seule base de données, sélectionnez **Standard**.
   - Pour que SafeGuard Management Center prenne en charge plusieurs bases de données en mode **(Mutualisé)**, sélectionnez **Complète**. Retrouvez plus d'informations à la section Configurations mutualisées à la page 28.

SafeGuard Management Center est installé. Si nécessaire, redémarrez votre ordinateur. Effectuez ensuite la configuration initiale dans SafeGuard Management Center.

5.3 Affichage du système d'aide de SafeGuard Management Center

Le système d'aide de SafeGuard Management Center s'affiche dans votre navigateur. Il fournit des fonctions complètes telle que l'aide spécifique au contexte ainsi que la recherche sur le texte intégral. Il est configuré pour offrir les fonctionnalités complètes des pages de contenu du système d'aide suite à l'activation de JavaScript dans votre navigateur.

Avec Microsoft Internet Explorer, le comportement est le suivant :

- Windows 7 - Internet Explorer 8 - sécurité par défaut :
  - Vous ne voyez pas de barre de sécurité pour vous informer qu'Internet Explorer a bloqué l'exécution des scripts.
  - JavaScript est en cours d'exécution.

Remarque : la désactivation de JavaScript ne vous empêche pas de pouvoir toujours afficher et naviguer dans le système d'aide de SafeGuard Management Center. Toutefois, certaines fonctionnalités, telle que Rechercher, ne pourront pas être utilisées.

5.4 Configuration de SafeGuard Management Center

Après l'installation, vous devez configurer SafeGuard Management Center. L'assistant de configuration de SafeGuard Management Center vous aide, lors de la configuration initiale, à spécifier les paramètres de base de SafeGuard Management Center et la connexion à la base de données. Il s'ouvre automatiquement lorsque vous démarrez SafeGuard Management Center pour la première fois après l'installation.

Vous pouvez configurer SafeGuard Management Center pour l'utiliser avec une base de données ou avec plusieurs (Architecture mutualisée).

Remarque : vous devez exécuter la configuration initiale à l'aide de l'assistant de configuration pour les configurations indépendantes (Single Tenancy) et mutualisées (Multi Tenancy).

5.4.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies :

- Assurez-vous de disposer des droits d'administrateur Windows.
- Munissez-vous des informations suivantes : si nécessaire, vous pouvez les obtenir auprès de votre administrateur SQL.

  Codes d'accès SQL
  Le nom du serveur SQL sur lequel la base de données SafeGuard Enterprise doit être exécutée.
  Le nom de la base de données SafeGuard Enterprise si elle a déjà été créée.

5.4.2 Configurations mutualisées

Vous pouvez configurer différentes bases de données SafeGuard Enterprise et les maintenir à jour pour une instance de SafeGuard Management Center. Cela s'avère particulièrement utile pour disposer de configurations de base de données différentes pour différents domaines, unités organisationnelles ou locaux d'entreprise.

Remarque : configurez une instance séparée du serveur SafeGuard Enterprise pour chaque base de données.

Pour faciliter la configuration, les configurations créées précédemment peuvent aussi être importées à partir de fichiers ou de nouvelles configurations de base de données peuvent être exportées, en vue d'une réutilisation ultérieure.

Pour une configuration mutualisée de SafeGuard Management Center, effectuez d'abord la configuration initiale, puis procédez aux étapes plus spécifiques de la configuration partagée.

5.4.3 Configuration initiale de SafeGuard Management Center

Après l'installation de SafeGuard Management Center, veuillez effectuer la configuration initiale. Vous devez exécuter cette opération en mode indépendant et en mode mutualisé.

Pour lancer l'assistant de configuration de SafeGuard Management Center :

1. Sélectionnez **SafeGuard Management Center** depuis le menu **Démarrer**. L'assistant de configuration démarre et vous guide tout au long des étapes nécessaires.
2. Dans la page **Bienvenue**, cliquez sur **Suivant**.

5.4.4 Configuration de la connexion au serveur de base de données

Une base de données sert à stocker toutes les stratégies et tous les paramètres de chiffrement SafeGuard Enterprise. Pour que SafeGuard Management Center et le serveur SafeGuard Enterprise puissent communiquer avec cette base de données, vous devez spécifier une méthode d'authentification pour l'accès à la base de données, soit l'authentification Windows NT, soit l'authentification SQL. Si vous voulez vous connecter au serveur de base de données avec l'authentification SQL, assurez-vous d'avoir à portée de main les codes d'accès SQL respectives. Si nécessaire, vous pouvez les obtenir auprès de votre administrateur SQL.

1. Sur la page **Connexion au serveur de base de données**, effectuez les opérations suivantes :
   - Sous **Paramètres de connexion**, sélectionnez le serveur de base de données SQL dans la liste **Serveur de base de données**. La liste de tous les ordinateurs d'un réseau sur lequel Microsoft SQL Server est installé est affichée. Si vous ne pouvez pas sélectionner le serveur, saisissez son nom ou son adresse IP avec le nom de l'instance SQL.
   - Sélectionnez **Utiliser SSL** pour protéger la connexion entre le SafeGuard Management Center et le serveur de base de données SQL. Nous vous conseillons fortement d'effectuer cette opération lorsque vous avez sélectionné **Utiliser l'authentification SQL Server avec les codes d'accès suivants** sous **Authentification** car ce paramètre chiffrera le transport des codes d'accès SQL. Le chiffrement SSL requiert un environnement SSL actif sur le serveur de base de données SQL que vous avez préalablement configuré. Retrouvez plus d'informations à la section Sécurisation des connexions de transport avec SSL à la page 40.

2. Sous **Authentification**, activez le type d'authentification à utiliser pour accéder à cette instance du serveur de base de données. Ceci est nécessaire afin que SafeGuard Management Center puisse communiquer avec la base de données :
   - Sélectionnez **Utiliser l'authentification Windows NT** pour utiliser vos codes d'accès Windows.

     Remarque : utilisez ce type d'authentification si votre ordinateur appartient à un domaine. Une configuration supplémentaire est obligatoire car l'utilisateur doit être autorisé à se connecter à la base de données. Retrouvez plus d'informations aux sections Configuration d'un compte Windows pour la connexion au serveur SQL à la page 19 et Configuration de l'authentification Windows pour la connexion au serveur SQL à la page 24.
   - Sélectionnez **Utiliser l'authentification SQL Server avec les codes d'accès suivants** pour accéder à la base de données avec vos codes d'accès SQL respectifs. Saisissez les codes d'accès correspondant au compte utilisateur SQL que votre administrateur SQL a créé. Si nécessaire, vous pouvez les obtenir auprès de votre administrateur SQL.

     Remarque : utilisez ce type d'authentification si votre ordinateur n'appartient à aucun domaine. Assurez-vous d'avoir sélectionné **Utiliser SSL** pour sécuriser la connexion au/du serveur de base de données.

3. Cliquez sur **Suivant**.

La connexion au serveur de base de données a été établie.

5.4.5 Création ou sélection d'une base de données

Sur la page **Paramètres de base de données**, déterminez si une base de données existante ou nouvelle est utilisée pour stocker les données d'administration.

1. Procédez de l'une des manières suivantes :
   - Si aucune base de données n'existe encore, sélectionnez **Créer une base de données nommée**. Saisissez le nom de la nouvelle base de données. Pour ce faire, vous devez disposer des droits d'accès SQL adéquats. Retrouvez plus d'informations à la section Droits d'accès à la base de données à la page 18. Pour empêcher les problèmes de localisation, les noms de la base de données SafeGuard Enterprise doivent seulement contenir les caractères suivants : caractères (A-Z, a-z), nombres (0-9), traits de soulignement (_).
   - Si une base de données a déjà été créée ou si vous avez déjà installé SafeGuard Management Center sur un ordinateur différent, sélectionnez **Sélectionner une base de données disponible**, puis sélectionnez la base de données appropriée dans la liste.

2. Cliquez sur **Suivant**.

5.4.6 Création du responsable principal de la sécurité

En tant que responsable de la sécurité, vous pouvez accéder à SafeGuard Management Center pour créer des stratégies SafeGuard Enterprise et configurer le logiciel de chiffrement pour l'utilisateur final.

Le responsable principal de la sécurité (MSO, Master Security Officer) est l'administrateur au plus haut niveau avec tous les droits et un certificat qui n'expire pas.

1. Sur la page **Données du responsable de la sécurité** sous **Identifiant du responsable principal de la sécurité**, saisissez un nom de responsable principal de la sécurité.
2. Dans **Certificat du responsable principal de la sécurité**, procédez d'une des manières suivantes :
   - Cliquez sur **Créer** pour créer un nouveau certificat pour le responsable principal de la sécurité. Vous êtes invité à saisir et à confirmer un mot de passe chacun pour le magasin de certificats et pour le fichier dans lequel les certificats doivent être exportés (fichier de clé privée P12). Le certificat est créé et affiché sous **Certificat du responsable principal de la sécurité**.
   - Cliquez sur **Importer** pour utiliser un certificat du responsable principal de la sécurité déjà disponible sur le réseau. Dans **Importer le certificat d'authentification**, recherchez le fichier de clé sauvegardé. Sous **Mot de passe du fichier de clé**, saisissez le mot de passe de ce fichier. Saisissez le mot de passe du magasin de certificats sous **Mot de passe du magasin de certificats** et confirmez-le. Cliquez sur **OK**. Le certificat est importé et affiché sous **Certificat du responsable principal de la sécurité**.

   Le responsable principal de la sécurité a besoin du magasin de certificats pour se connecter à SafeGuard Management Center. Notez ce mot de passe et conservez-le en lieu sûr ! Si vous le perdez, le responsable principal de la sécurité ne pourra pas se connecter à SafeGuard Management Center.

   Le responsable principal de la sécurité a besoin du fichier de clés privées pour restaurer une installation interrompue de SafeGuard Management Center.
3. Cliquez sur **Suivant**.

Le responsable principal de la sécurité est créé.

5.4.6.1 Création du certificat du responsable principal de la sécurité (MSO)

Dans la boîte de dialogue **Création d'un certificat MSO**, procédez comme suit :

1. Sous **Identifiant du responsable principal de la sécurité**, saisissez un nom de responsable principal de la sécurité.
2. Saisissez deux fois le mot de passe du magasin de certificats et cliquez sur **OK**.

Le certificat MSO est créé et enregistré en local sous la forme d'une sauvegarde (<nom_mso>.cer).

Remarque : notez ce mot de passe et conservez-le en lieu sûr ! Vous en avez besoin pour vous authentifier à SafeGuard Management Center.

5.4.6.2 Exportation du certificat du responsable principal de la sécurité (MSO)

Le certificat MSO est exporté dans un fichier, communément appelé le fichier de clé privées (P12) qui est sécurisé par un mot de passe. Le certificat MSO dispose ainsi d'une protection supplémentaire. Le fichier de clés privées est nécessaire pour restaurer une installation interrompue de SafeGuard Management Center.

Pour exporter un certificat MSO :

1. Dans **Exportation du certificat**, saisissez et confirmez le mot de passe de la clé privée (fichier P12). Le mot de passe doit être composé de 8 caractères alphanumériques.
2. Cliquez sur **OK**.
3. Saisissez un emplacement de stockage du fichier de clé privée.

La clé privée est créée et le fichier est stocké dans l'emplacement défini (nom_mso.p12).

Remarque : créez une sauvegarde de la clé privée (fichier p12) et stockez-la dans un emplacement sûr après la configuration initiale. Si la clé est perdue en cas de panne du PC, vous devrez alors réinstaller SafeGuard Enterprise. Ceci est valable pour tous les certificats des responsables de sécurité générés par SafeGuard. Retrouvez plus d'informations à la section *Exportation du certificat d'entreprise et du responsable principal de la sécurité* du *Manuel d'administration de SafeGuard Enterprise.*

5.4.6.3 Importation du certificat du responsable principal de la sécurité (MSO)

Si un certificat MSO est déjà disponible, vous devez l'importer dans le magasin de certificats.

Remarque : il est impossible d'importer un certificat à partir d'une infrastructure de clé publique (PKI) de Microsoft. Un certificat importé doit avoir 1024 bits au minimum et 4096 bits au maximum.

1. Dans **Importation du fichier de clé pour l'authentification**, cliquez sur **[...]** et sélectionnez le fichier de clé.
2. Veuillez saisir le mot de passe du fichier de clé.
3. Saisissez le mot de passe du magasin de certificats.
4. Confirmez le mot de passe du magasin de certificats.
5. Cliquez sur **OK**.

Les certificats et les clés privées sont à présent dans le magasin de certificats. La connexion à SafeGuard Management Center nécessite ensuite le mot de passe du magasin de certificats.

5.4.7 Création du certificat d'entreprise

Le certificat d'entreprise permet de différencier des installations de SafeGuard Management. En combinaison avec le certificat du MSO, il permet de restaurer une configuration de base de données SafeGuard Enterprise endommagée.

1. Sur la page **Certificat d'entreprise**, sélectionnez **Créer un nouveau certificat d'entreprise**.
2. Saisissez un nom de votre choix.

   Remarque : par défaut, les certificats générés par SafeGuard Enterprise (entreprise, machine, responsable de la sécurité et utilisateur) sont signés par l'algorithme **SHA-256** à la première installation pour une sécurité optimale.

   Si vous avez toujours besoin de gérer SafeGuard Enterprise 6,0 ou une version antérieure avec SafeGuard Management Center 7.0, veuillez sélectionner **SHA-1** sous **Algorithme de hachage pour les certificats générés**. Retrouvez plus d'informations à la section *Modification de l'algorithme pour les certificats autosignés* du *Manuel d'administration de SafeGuard Enterprise*.

   L'algorithme sélectionné est utilisé pour signer tous les certificats générés par SafeGuard Enterprise. Il s'agit de certificats d'entreprise et de la machine et des certificats du responsable de la sécurité et de l'utilisateur.

3. Cliquez sur **Suivant**.

Le nouveau certificat d'entreprise est stocké dans la base de données.

Créez une sauvegarde du certificat d'entreprise et stockez-le dans un emplacement sûr après la configuration initiale.

Retrouvez plus d'informations sur la restauration de la configuration d'une base de données endommagée à la section Restauration de la configuration d'une base de données corrompue à la page 36.

5.4.8 Configuration initiale complète de SafeGuard Management Center

1. Cliquez sur **Terminer** pour terminer la configuration initiale de SafeGuard Management Center.

Un fichier de configuration est créé.

Vous avez créé :

- Une connexion au serveur SafeGuard Enterprise.
- Une base de données SafeGuard Enterprise.
- Un compte de responsable principal de la sécurité pour se connecter au SafeGuard Management Center.
- Tous les certificats nécessaires pour restaurer une configuration de base de données corrompue ou une installation de SafeGuard Management Center.

SafeGuard Management Center démarre une fois que l'assistant de configuration a fermé.

5.5 Création de configurations de base de données supplémentaires (Mutualisées)

Condition préalable : la fonction de configuration mutualisée doit avoir été installée avec une installation de type **Complète**. La configuration initiale de SafeGuard Management doit avoir été effectuée. Retrouvez plus d'informations à la section Démarrage de la configuration initiale de SafeGuard Management Center à la page 28.

Remarque : vous devez configurer une instance distincte par base de données du serveur SafeGuard Enterprise.

Pour créer une configuration de base de données supplémentaire SafeGuard Enterprise à la suite de la configuration initiale :

1. Démarrez SafeGuard Management Center. La boîte de dialogue **Sélection d'une configuration** s'affiche.
2. Cliquez sur **Nouveau**. L'assistant de configuration de SafeGuard Management Center démarre automatiquement
3. L'assistant vous guide tout au long des étapes nécessaires de création d'une nouvelle configuration de base de données. Définissez les paramètres tels que requis. La nouvelle configuration de base de données est générée.
4. Pour vous authentifier dans SafeGuard Management Center, vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Cliquez sur **OK**.

SafeGuard Management Center démarre et se connecte à la nouvelle configuration de base de données. Au prochain lancement de SafeGuard Management Center, la nouvelle configuration de base de données peut être sélectionnée dans la liste.

Remarque : retrouvez plus d'informations sur les autres tâches concernant la configuration mutualisée à la section *Utilisation de plusieurs configurations de base de données* du *Manuel d'administration de SafeGuard Enterprise.*

5.6 Configuration des instances supplémentaires de SafeGuard Management Center

Vous pouvez configurer des instances supplémentaires de SafeGuard Management Center pour donner l'accès aux responsables de la sécurité pour l'exécution des tâches administratives sur différents ordinateurs. Il peut être installé sur tout ordinateur du réseau à partir duquel il est possible d'accéder les bases de données.

SafeGuard Enterprise gère les droits d'accès au SafeGuard Management Center dans son propre répertoire de certificats. Ce répertoire doit contenir tous les certificats de tous les responsables de sécurité autorisés à se connecter au SafeGuard Management Center. La connexion au SafeGuard Management Center nécessite uniquement le mot de passe du magasin de certificats.

1. Installez SGNManagementCenter.msi sur un autre ordinateur avec les fonctionnalités requises.
2. Démarrez SafeGuard Management Center nouvellement installé sur l'ordinateur approprié. L'assistant de configuration démarre et vous guide tout au long des étapes nécessaires.
3. Dans la page **Bienvenue**, cliquez sur **Suivant**.
4. Dans la boîte de dialogue **Connexion au serveur de base de données**, sous **Serveur de base de données**, sélectionnez, dans la liste, l'instance de base de données SQL souhaitée. Tous les serveurs de base de données disponibles sur votre ordinateur ou sur votre réseau s'affichent. Sous **Authentification**, activez le type d'authentification à utiliser pour accéder à cette instance du serveur de base de données. Si vous sélectionnez **Utiliser l'authentification SQL avec les codes d'accès suivants**, saisissez les codes d'accès du compte utilisateur SQL que votre administrateur SQL a créé. Cliquez sur **Suivant**.
5. Sur la page **Paramètres de base de données**, cliquez sur **Sélectionner une base de données disponible** et sélectionnez dans la liste la base de données correspondante. Cliquez sur **Suivant**.
6. Dans **Authentification au SafeGuard Management Center**, sélectionnez une personne autorisée dans la liste. Si le mode Multi Tenancy est activé, la boîte de dialogue s'affiche pour la configuration à laquelle l'utilisateur est sur le point de se connecter. Saisissez et confirmez le mot de passe du magasin de certificats.

   Un magasin de certificats est créé pour le compte utilisateur actuel et il est protégé par ce mot de passe. Pour toute connexion future, vous n'avez besoin que de ce mot de passe.

7. Cliquez sur **OK**.

   Un message s'affiche indiquant que le certificat et la clé privée n'ont pas été trouvés ou sont inaccessibles.

8. Pour importer les données, cliquez sur **Oui**, puis sur **OK**. Cette opération démarre le processus d'importation.
9. Dans **Importation du fichier de clé pour l'authentification**, cliquez sur **[...]** et sélectionnez le fichier de clé. Saisissez maintenant le **mot de passe du fichier de clés**. Saisissez le mot de passe du magasin de certificats précédemment défini dans **Mot de passe du magasin de certificat ou code confidentiel du token**. Sélectionnez **Importer dans le magasin de certificats** ou sélectionnez **Copier sur le token** pour stocker le certificat sur un token.
10. Saisissez le mot de passe une nouvelle fois pour initialiser le magasin de certificats.

Les certificats et les clés privées sont à présent contenus dans le magasin de certificats. La connexion au SafeGuard Management Center nécessite ensuite le mot de passe du magasin de certificats.

5.7 Connexion à SafeGuard Management Center

La connexion à SafeGuard Management Center dépend du mode d'exécution : indépendant (Single Tenancy) ou mutualisé (Multi Tenancy).

Retrouvez plus d'informations sur les premiers pas dans SafeGuard Management Center dans le *Manuel d'administration de SafeGuard Enterprise*.

5.7.1 Connexion en mode indépendant

1. Démarrez SafeGuard Management Center depuis le menu **Démarrer**. Une boîte de dialogue de connexion apparaît.
2. Connectez-vous en tant que responsable principal de la sécurité et saisissez le mot de passe du magasin de certificats spécifié pendant la configuration initiale. Cliquez sur **OK**.

SafeGuard Management Center démarre.

Remarque : si vous saisissez un mot de passe incorrect, un message d'erreur s'affiche et un délai est imposé avant la tentative de connexion suivante. Le délai augmente à chaque échec de tentative de connexion. Les échecs sont consignés dans un journal.

5.7.2 Connexion en mode mutualisé

Le processus de connexion au SafeGuard Management Center est plus long lorsque plusieurs bases de données ont été configurées (Multi Tenancy).

1. Démarrez SafeGuard Management Center à partir du dossier des produits du menu **Démarrer**. La boîte de dialogue **Sélection d'une configuration** s'affiche.
2. Sélectionnez la configuration de base de données que vous souhaitez utiliser et cliquez sur **OK**. La configuration de base de données sélectionnée est reliée à SafeGuard Management Center et devient active.
3. Vous êtes invité à sélectionner le nom du responsable de la sécurité de cette configuration et à saisir son mot de passe de magasin de certificats. Cliquez sur **OK**.

SafeGuard Management Center démarre et se connecte à la configuration de base de données sélectionnée.

Remarque : si vous saisissez un mot de passe incorrect, un message d'erreur s'affiche et un délai est imposé avant la tentative de connexion suivante. Le délai augmente à chaque échec de tentative de connexion. Les échecs sont consignés dans un journal.

5.8 Installation de la structure organisationnelle dans SafeGuard Management Center

Deux méthodes vous permettent de rediriger votre organisation dans SafeGuard Enterprise :

- Importation d'un service d'annuaire, par exemple, Active Directory.

Lors de la synchronisation avec les objets Active Directory comme des ordinateurs, les utilisateurs et les groupes sont importés dans le SafeGuard Management Center et stockés dans la base de données SafeGuard Enterprise.

- Création manuelle d'une structure organisationnelle.

  Si aucun service d'annuaire n'est disponible ou s'il y a seulement quelques unités organisationnelles afin qu'aucun service d'annuaire ne soit nécessaire, vous pouvez créer de nouveaux domaines/groupes de travail auxquels l'utilisateur ou l'ordinateur peut se connecter.

Vous pouvez utiliser l'une de ces deux options ou les combiner. Par exemple, vous pouvez importer un service Active Directory (AD) partiellement ou intégralement, et créer manuellement d'autres unités organisationnelles. L'attribution des stratégies est assurée que la structure organisationnelle soit importée ou créée manuellement.

Remarque : en associant deux méthodes, les unités organisationnelles créées manuellement ne sont pas redirigées vers le service AD. Si les unités organisationnelles créées dans SafeGuard Enterprise doivent être redirigées vers AD, vous devez les ajouter séparément à AD.

Retrouvez plus d'informations sur l'importation ou la création d'une structure organisationnelle au chapitre *Création de la structure organisationnelle* du *Manuel d'administration de SafeGuard Enterprise*.

5.9 Importation du fichier de licence

SafeGuard Enterprise dispose d'un compteur de licences intégré. Par défaut, un nombre fixe de 5 licences pour chaque composant SafeGuard Enterprise disponible fait partie de l'installation. Ceci doit permettre une évaluation facile des autres composants SafeGuard Enterprise sans aucun effet secondaire. Lors de l'achat de SafeGuard Enterprise, chaque client reçoit un fichier de licence personnalisé qui doit être importé dans SafeGuard Management Center.

Retrouvez plus d'informations au chapitre *Licences* du *Manuel d'administration de SafeGuard Enterprise*.

5.10 Restauration de l'installation corrompue de SafeGuard Management Center

Si l'installation de SafeGuard Management Center est corrompue mais la base de données est toujours intacte, l'installation peut être facilement restaurée en installant SafeGuard Management Center et en utilisant la base de données existante ainsi que le certificat sauvegardé du responsable de la sécurité.

- Le certificat du responsable principal de la sécurité de la configuration de la base de données correspondante doit avoir été exporté sous la forme d'un fichier .p12, ainsi qu'être disponible et valide.

- Vous devez connaître les mots de passe du fichier .p12 et du magasin de certificats.

Pour restaurer l'installation corrompue de SafeGuard Management Center :

1. Réinstallez le package d'installation de SafeGuard Management Center. Ouvrez SafeGuard Management Center. L'assistant de configuration démarre automatiquement.

2. Sur la page **Connexion à la base de données**, sélectionnez le serveur de base de données correspondant et configurez la connexion à la base de données, le cas échéant. Cliquez sur **Suivant**.
3. Sur la page **Paramètres de base de données**, cliquez sur **Sélectionner une base de données disponible** et sélectionnez dans la liste la base de données correspondante.
4. Sur la page **Données du responsable de la sécurité**, exécutez l'une des actions suivantes :
   - Si le fichier de certificat sauvegardé se trouve sur l'ordinateur, il s'affiche. Saisissez le mot de passe que vous utilisez pour vous authentifier dans SafeGuard Management Center.
   - Si le fichier de certificat sauvegardé est introuvable sur l'ordinateur, cliquez sur **Importer**. Recherchez le fichier de certificat sauvegardé et cliquez sur **Ouvrir**. Saisissez le mot de passe du fichier de certificat sélectionné. Cliquez sur **Oui**. Saisissez et confirmez le mot de passe d'authentification dans SafeGuard Management Center.
5. Cliquez sur **Suivant**, puis sur **Terminer** pour achever la configuration de SafeGuard Management Center.

L'installation corrompue de SafeGuard Management Center est restaurée.

5.11 Restauration d'une configuration de base de données corrompue

La configuration corrompue d'une base de données peut être restaurée en réinstallant SafeGuard Management Center pour créer une nouvelle instance de la base de données, d'après les fichiers de certificat sauvegardés. Vous garantissez ainsi que tous les ordinateurs d'extrémité SafeGuard Enterprise existants acceptent les stratégies de la nouvelle installation.

- Les certificats d'entreprise et du responsable principal de la sécurité pour la configuration de la base de données correspondante doivent avoir été exportés sous la forme de fichiers .p12, ainsi qu'être disponibles et valides. Vous sauvegardez les certificats dans SafeGuard Management Center.
- Vous devez également connaître les mots de passe de ces deux fichiers .p12, ainsi que du magasin de certificats.

Remarque : nous conseillons seulement ce type de restauration si aucune sauvegarde de base de données valide n'est disponible. Tous les ordinateurs connectés à un client qui a été restauré de cette façon perdront leurs attributions utilisateur/machine, conduisant à une authentification au démarrage provisoirement désactivée. Les mécanismes de challenge/réponse ne seront pas disponibles tant que l'ordinateur d'extrémité correspondant n'aura pas renvoyé avec succès les informations sur sa clé.

Pour restaurer une base de données corrompue :

1. Réinstallez le package d'installation de SafeGuard Management Center. Ouvrez SafeGuard Management Center. L'assistant de configuration démarre automatiquement.
2. Sur la page **Connexion à la base de données**, sélectionnez **Créer une base de données**. Sous **Paramètres de base de données**, configurez la connexion à la base de données. Cliquez sur **Suivant**.
3. Sur la page **Données du responsable de la sécurité**, sélectionnez le responsable principal de la sécurité correspondant, puis cliquez sur **Importer**.

4. Dans **Importation du certificat d'authentification**, recherchez le fichier de clé sauvegardé. Sous **Mot de passe du fichier de clé**, saisissez et confirmez le mot de passe spécifié pour ce fichier. Sélectionnez **Stocker le fichier de clé dans le magasin de certificats** et saisissez le mot de passe pour le magasin. Cliquez sur **OK**.
5. Le certificat du responsable principal de la sécurité est alors importé. Cliquez sur **Suivant**.
6. Sur la page **Certificat d'entreprise**, sélectionnez **Restaurer à l'aide d'un certificat d'entreprise existant**. Cliquez sur **Importer** pour rechercher le fichier de certificat sauvegardé qui contient le certificat d'entreprise valide. Vous êtes invité à saisir le mot de passe défini pour le magasin de certificats. Saisissez votre mot de passe et cliquez sur **OK**. Cliquez sur **Oui** pour confirmer le message. Le certificat d'entreprise est alors importé.
7. Cliquez sur **Suivant**, puis sur **Terminer**.

La configuration de la base de données est restaurée.

6 Test de la communication

Une fois le serveur SafeGuard Enterprise, la base de données et SafeGuard Management Center configurés, veuillez tester la connexion. Cette section décrit les étapes à suivre.

6.1 Conditions préalables

Définissez ou vérifiez les paramètres suivants avant de tester la connexion :

6.1.1 Ports/connexions

Les ordinateurs d'extrémité doivent créer les connexions suivantes :

Connexion de l'ordinateur d'extrémité SafeGuard à	Port
Serveur SafeGuard Enterprise	Port 80/TCP Port 443 lors de l'utilisation de la connexion de transport SSL

SafeGuard Management Center doit créer les connexions suivantes :

Connexion de SafeGuard Management Center à	Port
Base de données SQL	Port dynamique SQL Server 2012 : Port 1433/TCP et port 1434/TCP
Active Directory	Port 389/TCP
SLDAP	Port 636 pour l'importation du service Active Directory

Le serveur SafeGuard Enterprise doit créer les connexions suivantes :

Connexion du serveur SafeGuard Enterprise à	Port
Base de données SQL	Port 1433/TCP et port 1434/TCP pour le port dynamique SQL 2012 (Express)
Active Directory	Port 389/TCP

6.1.2 Méthode d'authentification

1. Sur l'ordinateur sur lequel est installé le serveur SafeGuard Enterprise, ouvrez le **Gestionnaire des services Internet (IIS)**.
2. Dans l'arborescence, cliquez sur **Services Internet (IIS)**. Cliquez sur **« Nomserveur »**, **Sites Web**, **Site Web par défaut**.
3. Cliquez avec le bouton droit de la souris sur **SGNSRV**, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Sécurité de répertoire**.
5. Sous **Authentification et contrôle d'accès**, cliquez sur **Modifier**. Dans **Méthodes d'authentification**, sélectionnez **Activer la connexion anonyme**. Sous **Accès authentifié**, dessélectionnez la case **Authentification Windows intégrée**.

6.1.3 Paramètres du serveur proxy pour le serveur Web et l'ordinateur

Déterminez les paramètres du serveur proxy comme suit :

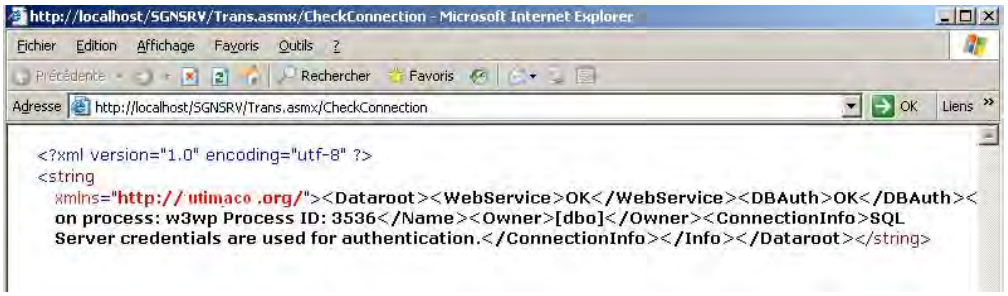
1. Dans Internet Explorer, dans le menu **Outils**, cliquez sur **Options Internet**. Puis cliquez sur **Connexions** et ensuite sur **Paramètres du réseau local**.
2. Dans **Paramètres du réseau local**, sous **Serveurs proxy**, dessélectionnez **Utiliser un serveur proxy pour votre réseau local**.

   Si un serveur proxy est nécessaire, cliquez sur **Ne pas utiliser de serveur proxy pour les adresses locales**.

6.2 Test de connexion (IIS 7 sous Windows Server 2008)

1. Sur l'ordinateur sur lequel est installé le serveur SafeGuard Enterprise, ouvrez le **Gestionnaire des services Internet (IIS)**.
2. Dans l'arborescence, cliquez sur **« Nom du serveur »**, **Sites**, **Site Web par défaut**. Vérifiez que la page Web **SGNSRV** est disponible dans le dossier **Site Web par défaut**.
3. Cliquez avec le bouton droit de la souris sur **SGNSRV**, sélectionnez **Gérer une application** et cliquez sur **Parcourir** pour ouvrir la page **Accueil de SGNSRV Sophos SafeGuard Web Service**.
4. Sur la page **Sophos SafeGuard Web Service**, une liste des actions possibles apparaît. Dans cette liste, cliquez sur **CheckConnection**.
5. Sur la page **CheckConnection**, cliquez sur **Appeler**.

Le test de connexion a réussi lorsque les résultats suivants apparaissent :



7 Sécurisation des connexions de transport avec SSL

Pour renforcer la sécurité, SafeGuard Enterprise prend en charge le chiffrement des connexions de transport avec SSL entre ses composants :

- La connexion entre le serveur de base de données et le serveur Web ainsi que la connexion entre le serveur de base de données et l'ordinateur sur lequel se trouve SafeGuard Management Center peuvent être chiffrées avec SSL.

- La connexion entre le serveur SafeGuard Enterprise et l'ordinateur administré par SafeGuard Enterprise peut être protégée via SSL ou par un chiffrement exclusif SafeGuard. Le protocole SSL présente l'avantage d'être standard et de permettre d'établir une connexion plus rapidement qu'en utilisant le chiffrement de transport SafeGuard.

  Mac : SSL doit être utilisé pour sécuriser la connexion entre le serveur SafeGuard Enterprise Server et les ordinateurs d'extrémité Mac.

  Remarque : nous vous conseillons vivement d'utiliser la communication chiffrée SSL, sauf pour des configurations de démonstration ou de test. Si, pour quelque raison que ce soit, vous ne pouvez pas le faire et que le chiffrement SafeGuard est utilisé, la connexion à une instance unique du serveur est limité à 1000 clients maximum.

Avant d'activer SSL dans SafeGuard Enterprise, il est nécessaire de configurer un environnement SSL.

7.1 Configuration de SSL

Les tâches générales suivantes sont nécessaires pour configurer le serveur Web avec SSL :

- Une autorité de certification doit être installée pour générer des certificats utilisés pour le chiffrement SSL.

- Un certificat doit être généré et le serveur des services Internet (IIS) configuré pour utiliser SSL et sélectionner le certificat.

- Le nom du serveur spécifié lors de la configuration du serveur SafeGuard Enterprise doit être identique à celui spécifié dans le certificat SSL. Faute de quoi, la communication entre le client et le serveur est impossible. Un certificat distinct est nécessaire pour chaque serveur SafeGuard Enterprise.

- Si vous utilisez un équilibreur de charge réseau, vérifiez que la plage de ports inclut le port SSL.

Retrouvez plus d'informations auprès de notre support technique ou consultez :

- http://msdn2.microsoft.com/fr-fr/library/ms998300.aspx

- http://support.microsoft.com/default.aspx?scid=kb;fr-fr;316898

- https://blogs.msdn.com/sql_protocols/archive/2005/11/10/491563.aspx

7.2 Activation du chiffrement SSL dans SafeGuard Enterprise

Vous pouvez activer le chiffrement SSL dans SafeGuard Enterprise comme suit :

- Connexion entre le serveur web et le serveur de base de données :

  Activez le chiffrement SSL en enregistrant le serveur SafeGuard Enterprise à l'aide de l'outil de package de configuration de SafeGuard Management Center. Retrouvez plus d'informations à la section Configuration de la connexion au serveur de base de données à la page 28 ou sur : http://www.sophos.com/fr-fr/support/knowledgebase/109012.aspx.

- Connexion entre le serveur de base de données et SafeGuard Management Center

  Activez le chiffrement SSL dans l'Assistant de configuration initiale de SafeGuard Management Center. Retrouvez plus d'informations à la section Configuration de la connexion au serveur de base de données à la page 28.

- Connexion entre le serveur SafeGuard Enterprise et l'ordinateur d'extrémité protégé par SafeGuard Enterprise :

  Activez le chiffrement SSL lors de la création du package de configuration pour les ordinateurs d'extrémité administrés SafeGuard Enterprise dans l'outil de package de configuration de SafeGuard Management Center. Retrouvez plus d'informations à la section Création d'un package de configuration pour les ordinateurs administrés à la page 53. Retrouvez plus d'informations sur la configuration du serveur SafeGuard Enterprise et de l'ordinateur protégé par SafeGuard Enterprise pour qu'ils utilisent SSL pour sécuriser la communication à la section Sécurisation de la communication entre le serveur et l'ordinateur d'extrémité avec SSL à la page 41.

Vous pouvez définir le chiffrement SSL pour SafeGuard Enterprise lors de la première configuration des composants SafeGuard Enterprise ou ultérieurement à tout moment. Créez ensuite un nouveau package de configuration et déployez-le sur le serveur ou sur l'ordinateur administré correspondant.

7.3 Sécurisation de la communication entre le serveur et l'ordinateur d'extrémité avec SSL

7.3.1 Conditions préalables

La sécurisation de la communication entre le serveur SafeGuard Enterprise et l'ordinateur protégé par SafeGuard Enterprise avec SSL nécessite un certificat valide. Vous pouvez utiliser les types de certificat suivants :

- Un certificat autosigné. Retrouvez plus d'informations à la section Utilisation d'un certificat autosigné à la page 42.
- Un certificat émis par une infrastructure de clés publiques (PKI) avec un certificat privé ou un certificat racine public. Retrouvez plus d'informations à la section Utilisation d'un certificat généré par une infrastructure de clés publiques à la page 43.

  D'un point de vue technique, le fait que vous utilisiez un certificat racine public ou privé ne fait aucune différence.

Remarque : si un certificat créé par une infrastructure de clés publique est disponible mais qu'aucune infrastructure de clés publiques ne l'est, vous n'allez pas pouvoir utiliser ce certificat pour sécuriser la communication avec SSL. Dans ce cas, veuillez installer une infrastructure de clés publiques ou créer un certificat autosigné.

7.3.2 Paramétrage du serveur SafeGuard Enterprise

Pour configurer l'utilisation du serveur SafeGuard Enterprise avec SSL dans le but de sécuriser la communication entre le serveur et l'ordinateur d'extrémité protégé par SafeGuard Enterprise, veuillez procéder aux tâches générales suivantes :

1. Installez SafeGuard Management Center. Retrouvez plus d'informations à la section Installation de SafeGuard Management Center à la page 26.
2. Installez le serveur SafeGuard Enterprise. Retrouvez plus d'informations à la section Installation du serveur SafeGuard Enterprise à la page 16.
3. Vérifiez la communication entre le serveur SafeGuard Enterprise et la base de données SQL à l'aide d'un test d'appel.

Après avoir terminé toutes les étapes de configuration, importez le certificat à utiliser pour la communication SSL. Vous pouvez soit utiliser un certificat autosigné, soit un certificat existant. Si vous avez déjà une infrastructure de clés publiques, vous pouvez utiliser un certificat généré par une infrastructure de clés publiques.

7.3.3 Utilisation d'un certificat autosigné

Pour créer un certificat autosigné avec SafeGuard Enterprise :

1. Ouvrez le Gestionnaire des services Internet (IIS) sur la machine qui héberge le serveur SafeGuard Enterprise.
2. Vérifiez le nom du serveur affiché sur le nœud supérieur.
3. Sur la machine sur laquelle SafeGuard Management Center est installé, sélectionnez **Programmes**, **Sophos**, **SafeGuard** et **SafeGuard Certificate Manager**.

   SafeGuard Certificate Manager s'affiche.

4. Saisissez le mot de passe pour ouvrir le magasin de certificats SafeGuard.
5. Cliquez sur le bouton **Créer un certificat**.

   La boîte de dialogue **Création d'un nouveau certificat** s'affiche.

6. Pour créer un certificat :

   a) Saisissez le nom du certificat correspondant à celui de la machine qui apparaît sur le nœud supérieur dans le Gestionnaire des services Internet (IIS).

   b) Conservez la valeur par défaut pour la longueur de la clé.

   c) Saisissez un mot de passe.

   d) Cliquez sur **OK**.

7. Enregistrez les fichiers cert et p12 à un emplacement joignable par la machine qui héberge les services Internet IIS.

7.3.4 Utilisation d'un certificat généré par une infrastructure de clés publiques

Si vous voulez utiliser un certificat généré par une infrastructure de clés publiques pour la communication SSL, veuillez créer un certificat pour la machine exécutant le serveur SafeGuard Enterprise. Les conditions suivantes sont requises :

- Le nom du certificat doit correspondre à celui de la machine qui apparaît sur le nœud supérieur dans le gestionnaire d'Internet Information Services (IIS).
- Le certificat doit être émis sur la machine à l'aide du nom FQDN.

Remarque : si, seul un certificat créé par une infrastructure de clés publique est disponible mais qu'aucune infrastructure de clés publiques ne l'est, vous n'allez pas pouvoir utiliser ce certificat pour sécuriser la communication avec SSL. Dans ce cas, veuillez installer une infrastructure de clés publiques ou créer un certificat autosigné.

7.3.5 Configuration de la page Web SGNSRV pour accepter un certificat

Condition préalable : un certificat valide d'utilisation de SSL doit être disponible.

Remarque : la description suivante fait référence à Microsoft Windows Server 2012.

1. Ouvrez le **Gestionnaire des services Internet (IIS)**.
2. Dans le volet de navigation, sélectionnez le serveur qui héberge la page Web SGNSRV.
3. Dans le volet de droite, sélectionnez **Certificats de serveur** dans la section **IIS**.
4. Sur la page **Certificats de serveur**, cliquez sur **Importer** dans le volet **Actions**.
5. Sélectionnez le certificat à utiliser pour sécuriser la connexion SSL. Saisissez votre mot de passe et cliquez sur **OK**.
6. Dans le volet de navigation, cliquez avec le bouton droit de la souris sur **Site Web par défaut**, puis cliquez sur **Modifier les liaisons**.
7. Cliquez sur **Ajouter** dans la boîte de dialogue **Liaisons de sites**.
8. Sous **Type :**, sélectionnez **https** et sous **Certificat SSL :**, sélectionnez le certificat à utiliser pour sécuriser la connexion SSL.
9. Cliquez sur **OK** et fermez la boîte de dialogue **Liaisons de sites**.
10. Dans le volet de navigation, sélectionnez le serveur et cliquez sur **Redémarrer** dans le volet **Actions**.

7.3.6 Configuration de l'utilisation de l'ordinateur d'extrémité avec SSL

Pour utiliser SSL sur un ordinateur d'extrémité protégé par SafeGuard Enterprise, procédez aux étapes suivantes :

1. Attribuez le certificat au client.
2. Créez un package de configuration client qui inclut SSL. Retrouvez plus d'informations à la section Création d'un package de configuration pour les ordinateurs administrés à la page 53.

7.3.6.1 Attribution de certificats

Il existe plusieurs façons d'attribuer un certificat à un ordinateur d'extrémité. L'une d'entre elles consiste à l'attribuer à l'aide d'une stratégie de groupe Microsoft, décrite dans cette

section. Si vous voulez utiliser une méthode différente, assurez-vous que le certificat est enregistré dans le magasin de certificats de l'ordinateur local.

Pour attribuer un certificat à l'aide d'une stratégie de groupe :

1. Ouvrez la console **Gestion de la stratégie de groupe**.
2. Recherchez un Objet de stratégie de groupe ou créez-en un nouveau qui contient les paramètres du certificat. Assurez-vous que l'Objet de stratégie de groupe est associé au domaine, au site ou à une unité organisationnelle auquel appartiennent les utilisateurs que vous souhaitez gérer avec la stratégie.
3. Cliquez avec le bouton droit de la souris sur l'Objet de stratégie de groupe et sélectionnez **Modifier**.

   L'**Éditeur de gestion des stratégies de groupe** s'ouvre et affiche le contenu de l'objet de stratégie.
4. Dans le volet de navigation, ouvrez **Configuration ordinateur** > **Paramètres Windows** > **Paramètres de sécurité** > **Stratégies de clé publique** > **Éditeurs approuvés**.
5. Cliquez sur le menu **Action**, puis cliquez sur **Importer**.
6. Suivez les instructions de l'**Assistant Importation de certificat** pour rechercher et importer le certificat.
7. Si le certificat est autosigné mais qu'aucun historique ne permet de remonter jusqu'à un certificat se trouvant dans le magasin de certificats **Autorités de certification racines de confiance**, veuillez également copier le certificat dans ce magasin. Dans le volet de navigation, cliquez sur **Autorités de certification racines de confiance**, puis, répétez les étapes 5 et 6 pour installer une copie du certificat dans ce magasin.

8 Enregistrement et configuration du serveur SafeGuard Enterprise

Le serveur SafeGuard Enterprise doit être enregistré et configuré pour mettre en place les informations de communication entre le serveur IIS, la base de données et l'ordinateur d'extrémité protégé par SafeGuard. Les informations sont stockées dans un package de configuration de serveur.

Effectuez cette tâche dans SafeGuard Management Center. Le flux de travail est différent si le serveur SafeGuard Enterprise est installé sur le même ordinateur que SafeGuard Management Center ou sur un ordinateur différent.

Vous pouvez définir d'autres propriétés comme l'ajout de responsables de sécurité supplémentaires pour le serveur sélectionné ou la configuration de la connexion à la base de données.

8.1 Enregistrement et configuration du serveur SafeGuard Enterprise pour l'ordinateur en cours d'utilisation

Au moment de l'installation de SafeGuard Management Center et du serveur SafeGuard Enterprise sur l'ordinateur sur lequel vous travaillez actuellement, enregistrez et configurez le serveur SafeGuard Enterprise.

Remarque : cette option n'est pas disponible si le mode mutualisé est activé.

1. Démarrez SafeGuard Management Center.
2. Dans le menu **Outils**, cliquez sur **Outil de package de configuration**.
3. Sélectionnez l'onglet **Serveurs**, puis **Faire de cet ordinateur un serveur SGN**.

   La configuration du serveur SafeGuard Enterprise démarre automatiquement.

4. Acceptez les valeurs par défaut dans toutes les boîtes de dialogue suivantes.

Le serveur SafeGuard Enterprise est enregistré. Un package de configuration serveur (MSI) appelé **`<Serveur>.msi`** est créé et directement installé sur l'ordinateur en cours. Les informations du serveur sont affichées dans l'onglet **Serveurs**. Vous pouvez exécuter une configuration supplémentaire.

Remarque : si vous voulez installer un nouveau package de configuration du serveur (MSI) sur le serveur SafeGuard Enterprise, veillez à désinstaller d'abord l'ancien package de configuration du serveur. Par ailleurs, supprimez manuellement la mémoire cache locale de manière à ce qu'il puisse être mis à jour correctement avec les nouvelles données de configuration, telles que les paramètres SSL. Puis installez le nouveau package de configuration sur le serveur.

8.2 Enregistrement et configuration du serveur SafeGuard Enterprise pour un ordinateur différent

Lorsque le serveur SafeGuard Enterprise est installé sur un ordinateur différent de celui sur lequel se trouve SafeGuard Management Center, enregistrez et configurez le serveur SafeGuard Enterprise :

1. Démarrez SafeGuard Management Center.
2. Dans le menu **Outils**, cliquez sur **Outil de package de configuration**.
3. Sélectionnez l'onglet **Serveurs**, puis cliquez sur **Ajouter...**.
4. Dans **Enregistrement du serveur**, cliquez sur **[...]** pour sélectionner le certificat machine du serveur. Ce dernier est généré lors de l'installation du serveur SafeGuard Enterprise. Par défaut, il se trouve dans le répertoire **`MachCert`** du répertoire d'installation du serveur SafeGuard Enterprise. Son nom de fichier est **`<Nomordinateur>.cer`**. Si le serveur SafeGuard Enterprise est installé sur un autre ordinateur que SafeGuard Management Center, ce fichier .cer doit être accessible sous la forme d'une copie ou en utilisant une autorisation réseau.

   Ne sélectionnez pas le certificat MSO.

   Le nom complet (FQDN), par exemple **`serveur.monentreprise.com`** et les informations de certificat apparaissent.

   Remarque : si vous utilisez le chiffrement de transport SSL entre l'ordinateur d'extrémité et le serveur, le nom du serveur spécifié ici doit être identique à celui qui est spécifié dans le certificat SSL, Faute de quoi, ils ne peuvent pas communiquer.

5. Cliquez sur **OK**.

   Les informations du serveur sont affichées dans l'onglet **Serveurs**.

6. Cliquez sur l'onglet **Packages du serveur**. Les serveurs disponibles sont affichés. Sélectionnez le serveur requis. Indiquez le chemin de sortie pour le package de configuration du serveur. Cliquez sur **Créer un package de configuration**.

   Un package de configuration (MSI) appelé **`<Serveur>.msi`** est créé à l'emplacement spécifié.

7. Confirmez le message de réussite en cliquant sur **OK**.
8. Dans l'onglet **Serveurs**, cliquez sur **Fermer**.

Vous avez terminé l'enregistrement et la configuration du serveur SafeGuard Enterprise. Installez le package de configuration du serveur (MSI) sur l'ordinateur exécutant le serveur SafeGuard Enterprise. À tout moment, vous pouvez changer la configuration du serveur dans l'onglet **Serveurs**.

Remarque : si vous voulez installer un nouveau package de configuration du serveur (MSI) sur le serveur SafeGuard Enterprise, veillez à désinstaller d'abord l'ancien package de configuration du serveur. Par ailleurs, supprimez manuellement la mémoire cache locale de manière à ce qu'il puisse être mis à jour correctement avec les nouvelles données de configuration, telles que les paramètres SSL. Puis installez le nouveau package de configuration sur le serveur.

8.3 Modification des propriétés du serveur SafeGuard Enterprise

À tout moment, vous pouvez modifier les propriétés et paramètres de tout serveur enregistré et de sa connexion à la base de données.

1. Dans le menu **Outils**, cliquez sur **Outil de package de configuration**.
2. Cliquez sur l'onglet **Serveurs** et sélectionnez le serveur requis.
3. Effectuez l'une des opérations suivantes :

Élément	Description
Scripts autorisés	Cliquez pour activer l'utilisation de l'API de SafeGuard Enterprise Management. Ceci autorise les tâches administratives de création de scripts.
Win. Auth. WHD	Cliquez pour activer l'authentification Windows pour Web Helpdesk. Par défaut, cette option est désactivée.
Rôles du serveur	Cliquez pour sélectionner/dessélectionner un rôle de responsable de la sécurité responsable du serveur sélectionné.
Ajouter un rôle de serveur...	Cliquez pour ajouter d'autres rôles spécifiques de responsable de la sécurité du serveur sélectionné si besoin est. Vous êtes invité à sélectionner le certificat du serveur. Le rôle de responsable de la sécurité est ajouté et peut être affiché sous **Rôles de serveur**.
Connexion à la base de données	Cliquez sur **[...]** pour configurer une connexion à une base de données spécifique pour un serveur Web enregistré, notamment les codes d'accès de base de données et le chiffrement de transport entre le serveur Web et le serveur de base de données. Retrouvez plus d'informations à la section Configuration de la connexion au serveur de base de données à la page 28. Même si la vérification de la connexion à la base de données n'a pas réussi, un nouveau package de configuration du serveur peut être créé. **Remarque :** Il n'est pas nécessaire de relancer l'assistant de configuration de Management Center pour mettre à jour la configuration de la base de données. Veillez simplement à créer un nouveau package de configuration du serveur et à le distribuer ensuite au serveur concerné. La nouvelle connexion à la base de données peut être utilisée lorsque le package du serveur mis à jour est installé sur le serveur.

4. Créez un nouveau package de configuration du serveur dans l'onglet **Packages du serveur**.
5. Désinstallez l'ancien package de configuration du serveur, puis installez le nouveau sur le serveur respectif.

La nouvelle configuration de serveur devient active.

8.4 Enregistrement du serveur SafeGuard Enterprise avec le pare-feu Sophos activé

un ordinateur d'extrémité protégé par SafeGuard Enterprise ne parvient pas à se connecter au serveur SafeGuard Enterprise lorsqu'un pare-feu Sophos avec des paramètres par défaut est installé sur l'ordinateur d'extrémité. Par défaut, le pare-feu Sophos bloque les connexions NetBIOS nécessaire pour la résolution du nom de réseau du serveur SafeGuard Enterprise.

1. Pour contourner le problème, effectuez l'une des opérations suivantes :
   - Débloquez les connexions NetBIOS dans le pare-feu.
   - Incluez le nom pleinement qualifié du serveur SafeGuard Enterprise dans le package de configuration du serveur. Retrouvez plus d'informations à la section Enregistrement et configuration du serveur SafeGuard Enterprise sur un ordinateur différent à la page 46.

9 Configuration de SafeGuard Enterprise sur les ordinateurs d'extrémité

Le logiciel de chiffrement SafeGuard Enterprise peut être intégré de façon transparente à l'environnement normal de l'utilisateur, et son utilisation est facile et intuitive. En fonction de votre stratégie de déploiement, les ordinateurs d'extrémité peuvent être équipés de différents modules SafeGuard Enterprise et configurés selon vos besoins.

Les responsables de la sécurité peuvent effectuer l'installation et la configuration en local sur les ordinateurs d'extrémité ou dans le cadre d'une distribution logicielle centralisée. Grâce à l'installation centralisée, une installation standardisée est garantie sur plusieurs ordinateurs d'extrémité.

9.1 À propos des ordinateurs d'extrémité administrés et non administrés

Vous pouvez configurer les ordinateurs d'extrémité comme suit :

- **Administré - Client SafeGuard Enterprise (administré)**

  Administration centralisée basée sur serveur dans SafeGuard Management Center.

  Il existe une connexion au serveur SafeGuard Enterprise pour les ordinateurs d'extrémité administrés. Ils reçoivent leurs stratégies par le biais du serveur SafeGuard Enterprise. La connexion peut être désactivée provisoirement, par exemple lors d'un déplacement professionnel, même si l'ordinateur d'extrémité est défini comme administré.

- **Non administré - Client Sophos SafeGuard (autonome)**

  Administration locale via des packages de configuration créés dans SafeGuard Management Center.

  Les ordinateurs d'extrémité non administrés ne sont jamais connectés au serveur SafeGuard Enterprise et ne sont pas connectés à l'administration centralisée de SafeGuard Enterprise. Ils fonctionnent en mode autonome.

  Les ordinateurs d'extrémité non administrés reçoivent les stratégies SafeGuard Enterprise au moyen de packages de configuration. Ils ne reçoivent jamais de stratégies via une connexion établie avec le serveur SafeGuard Enterprise.

  Les stratégies SafeGuard Enterprise sont créées dans SafeGuard Management Center et exportées dans des packages de configuration. Les packages de configuration doivent ensuite être déployés par les mécanismes de distribution de logiciels de l'entreprise ou installés manuellement sur les ordinateurs d'extrémité.

Différents packages d'installation et modules sont fournis pour chaque type d'ordinateur d'extrémité.

9.2 Restrictions

Notez les restrictions pour SafeGuard Enterprise sur les ordinateurs d'extrémité dans les sections suivantes.

9.2.1 Restrictions pour les ordinateurs d'extrémité administrés

Notez les restrictions suivantes pour les ordinateurs d'extrémité administrés.

- **Restrictions pour le chiffrement initial :**

  La configuration initiale des ordinateurs d'extrémité administrés peut impliquer la création de stratégies de chiffrement pouvant être distribuées aux ordinateurs d'extrémité protégés par SafeGuard Enterprise sous forme de package de configuration.

  Toutefois, lorsque l'ordinateur d'extrémité protégé par SafeGuard Enterprise n'est pas connecté à un serveur SafeGuard Enterprise juste après l'installation du package de configuration, mais est temporairement hors ligne, seules les stratégies de chiffrement présentant les paramètres spécifiques suivants sont immédiatement actives :

  Protection des périphériques basés sur le volume avec la **Clé machine définie** comme clé de chiffrement.

  Pour que toutes les autres stratégies impliquant le chiffrement à l'aide de clés définies par l'utilisateur soient activées sur l'ordinateur d'extrémité protégé par SafeGuard Enterprise, le package de configuration correspondant doit également être réaffecté à l'unité organisationnelle de l'ordinateur d'extrémité. Les clés définies par l'utilisateur sont alors créées uniquement lorsque la connexion entre l'ordinateur d'extrémité et le serveur SafeGuard Enterprise est rétablie.

  En effet, la **Clé machine définie** est directement créée sur l'ordinateur d'extrémité protégé par SafeGuard Enterprise lors du premier redémarrage après installation, alors que les clés définies par l'utilisateur ne peuvent être créées qu'une fois que l'ordinateur d'extrémité a été enregistré sur le serveur SafeGuard Enterprise.

- **Restrictions pour la prise en charge du Chiffrement de lecteur BitLocker :**

  Le chiffrement de volumes SafeGuard Enterprise ou le Chiffrement de lecteur BitLocker peuvent être utilisés séparément mais pas en même temps. Pour changer de type de chiffrement, déchiffrez d'abord tous les lecteurs chiffrés, désinstallez le logiciel de chiffrement SafeGuard Enterprise, puis réinstallez-le avec les fonctions souhaitées. Le programme d'installation empêche le déploiement des deux fonctions en même temps. La désinstallation et la réinstallation sont nécessaires même lorsqu'aucun package de configuration prévu pour déclencher le chiffrement n'a été installé.

9.2.2 Restrictions pour les ordinateurs d'extrémité non administrés

Le chiffrement de fichiers n'est pas pris en charge pour les ordinateurs d'extrémité non administrés (clients Sophos SafeGuard autonomes).

9.3 Préparation des ordinateurs d'extrémité au chiffrement

Avant de déployer SafeGuard Enterprise, nous vous conseillons de vous préparer comme suit :

- Un compte d'utilisateur doit être configuré et actif sur les ordinateurs d'extrémité.
- Assurez-vous de disposer des droits d'administrateur Windows.
- Créez une sauvegarde complète des données sur l'ordinateur d'extrémité.

- Les lecteurs à chiffrer doivent être complètement formatés et disposer d'une lettre de lecteur.
- Sophos fournit un fichier de configuration matérielle pour réduire le risque de conflits entre l'authentification au démarrage et le matériel de votre ordinateur d'extrémité. Le fichier est contenu dans le package du logiciel de chiffrement. Nous vous conseillons d'installer une version mise à jour de ce fichier avant de procéder au déploiement de SafeGuard Enterprise. Ce fichier bénéficie d'une mise à jour mensuelle et peut être téléchargé depuis l'emplacement suivant : http://www.sophos.com/fr-fr/support/knowledgebase/65700.aspx

  Vous pouvez nous aider à améliorer la compatibilité en exécutant un outil que nous vous fournissons pour recueillir seulement les informations matérielles correspondantes. L'outil est très simple à utiliser. Les informations recueillies sont ajoutées au fichier de configuration matérielle. Retrouvez plus d'informations sur http://www.sophos.com/fr-fr/support/knowledgebase/110285.aspx.

- Recherchez les erreurs sur le(s) disque(s) dur(s) à l'aide de la commande suivante :

  `chkdsk %lecteur% /F /V /X`

  Dans certains cas, vous pouvez être invité à redémarrer votre ordinateur d'extrémité et à exécuter de nouveau la commande **chkdsk**. Retrouvez plus d'informations sur : http://www.sophos.com/fr-fr/support/knowledgebase/107799.aspx.

  Pour vérifier les résultats (fichier journal) dans l'Observateur d'événements Windows :

  Windows 7 : Sélectionnez **Journaux Windows**, **Application**, **Wininit**.

- Utilisez l'outil de défragmentation de Windows appelé « defrag » pour localiser et consolider les éléments fragmentés, notamment les fichiers de démarrage, les fichiers de données et les dossiers sur les volumes locaux. Retrouvez plus d'informations sur : http://www.sophos.com/fr-fr/support/knowledgebase/109226.aspx.

- Désinstallez les gestionnaires de démarrage tiers, tels que PROnetworks Boot Pro et Boot-US.

- Nous vous conseillons d'installer une version mise à jour du fichier de configuration matérielle avant de procéder au déploiement de SafeGuard Enterprise. Ce fichier bénéficie d'une mise à jour mensuelle et peut être téléchargé depuis l'emplacement suivant : http://www.sophos.com/fr-fr/support/knowledgebase/65700.aspx.

- Si la partition de démarrage de l'ordinateur d'extrémité a été convertie du format FAT au format NTFS et si l'ordinateur n'a pas été redémarré depuis, redémarrez l'ordinateur une fois. Sinon, il se peut que l'installation ne se soit pas terminée avec succès.

- Pour les clients SafeGuard Enterprise (administrés) seulement : vérifiez s'il existe une connexion au serveur SafeGuard Enterprise. Sélectionnez cette adresse Web dans Internet Explorer sur les ordinateurs d'extrémité : http://<AdresseIPServeur>/sgnsrv. Si la page **Trans** affiche **Vérifier la connexion**, la connexion avec le serveur SafeGuard Enterprise a été établie avec succès.

9.3.1 Préparation pour Cloud Storage

Le module Cloud Storage de SafeGuard Enterprise offre un chiffrement basé sur fichier des données stockées dans le Cloud.

Cloud Storage s'assure que les copies locales des données du Cloud sont chiffrées de manière transparente et restent chiffrées une fois stockées dans le Cloud.

La façon dont l'utilisateur exploite les données stockées dans le Cloud reste inchangée. Le logiciel de stockage dans le Cloud recommandé par le fournisseur n'est pas affecté et peut être utilisé de la même façon qu'avant pour envoyer des données vers le Cloud ou recevoir des données de celui-ci.

Pour préparer les ordinateurs d'extrémité à utiliser Cloud Storage :

- Le logiciel du fournisseur de stockage dans le Cloud doit être installé sur les ordinateurs d'extrémité sur lesquels vous voulez installer Cloud Storage.
- Ce logiciel doit avoir une application (ou un service système) stockée dans le système de fichiers local et synchroniser les données entre le Cloud et le système local.
- Il doit aussi stocker les données synchronisées dans le système de fichiers local.

Remarque : Cloud Storage chiffre uniquement les nouvelles données stockées dans le Cloud. Si des données étaient déjà stockées dans le Cloud avant l'installation de Cloud Storage, elles ne seront pas automatiquement chiffrées. Si elles doivent être chiffrées, l'utilisateur doit tout d'abord les supprimer du Cloud, puis les saisir de nouveau une fois que Cloud Storage a été installé.

9.3.2 Préparation pour la prise en charge du Chiffrement de lecteur BitLocker

Remarque : avant de commencer l'installation, veuillez décider si vous souhaitez utiliser SafeGuard Enterprise en association avec le Chiffrement de lecteur BitLocker ou avec le chiffrement intégral du disque de SafeGuard Enterprise. L'installation est interrompue si vous essayez d'installer les deux en même temps.

Si vous souhaitez utiliser SafeGuard Enterprise pour administrer les ordinateurs d'extrémité BitLocker, effectuez les préparations spécifiques suivantes sur l'ordinateur d'extrémité :

- Windows 7 ou Windows 8 doit être installé sur l'ordinateur d'extrémité.
- Le Chiffrement de lecteur BitLocker doit être installé et activé.
- Si TPM doit être utilisé pour l'authentification, TPM doit être initialisé, assigné à un propriétaire et activé.
- Si vous souhaitez installer le chiffrement basé sur volume de SafeGuard Enterprise, assurez-vous qu'aucun volume n'a encore été chiffré avec le Chiffrement de lecteur BitLocker. Dans le cas contraire, le système risque d'être endommagé.
- Pour installer la prise en charge du Chiffrement de lecteur BitLocker, désactivez le contrôle d’accès d’utilisateur ou ouvrez une session à l'aide du compte administrateur intégré.

9.3.3 Préparation d'une installation « Modifier »

Si une installation SafeGuard Enterprise existante est modifiée ou si des fonctions sont installées ultérieurement, le programme d'installation peut générer une message d'avertissement vous informant que certains composants (par exemple, SafeGuard Removable Media Manager) sont actuellement en cours d'utilisation. Ce message est généré lorsque les fonctions sélectionnées, partageant des composants en cours d'utilisation, ne peuvent pas être mises à jour immédiatement. Vous pouvez ignorer ce message car les composants affectés seront automatiquement mis à jour au redémarrage.

Ce comportement s'applique à une installation en mode surveillé et sans surveillance.

9.4 Création des packages de configuration

En fonction de la configuration requise, créez les packages de configuration appropriés pour les ordinateurs d'extrémité dans SafeGuard Management Center :

- Pour les ordinateurs d'extrémité Windows administrés - Packages client administrés
- Pour les ordinateurs d'extrémité Windows non administrés - Packages client autonomes
- Pour les Macs - Packages client administrés
- Lors de l'utilisation de comptes de service pour les tâches d'après installation

Le package de configuration initiale doit être installé sur les ordinateurs d'extrémité avec le logiciel de chiffrement.

9.4.1 Création d'un package de configuration pour ordinateurs administrés

1. Dans le menu **Outils** de SafeGuard Management Center, cliquez sur **Outil de package de configuration**.
2. Sélectionnez **Packages du client administré**.
3. Cliquez sur **Ajouter un package de configuration**.
4. Donnez un nom au package de configuration.
5. Attribuez un serveur SafeGuard Enterprise principal (le serveur secondaire n'est pas nécessaire).
6. Si besoin est, spécifiez un groupe de stratégies, préalablement créé dans SafeGuard Management Center et que vous souhaitez appliquer aux ordinateurs. Si vous voulez utiliser des comptes de service utilisateur pour les tâches postérieures à l'installation sur l'ordinateur, assurez-vous d'inclure le paramètre de stratégie respectif dans ce premier groupe de stratégie. Retrouvez plus d'informations à la section Comptes de service pour les tâches postérieures à l'installation à la page 55.
7. Sélectionnez le mode **Chiffrement du transport** définissant la manière de chiffrer la connexion entre le client et le serveur SafeGuard Enterprise : chiffrement du transport SafeGuard ou chiffrement SSL.

   Le protocole SSL présente l'avantage d'être standard et de permettre d'établir une connexion plus rapidement qu'en utilisant le chiffrement du transport SafeGuard. Le chiffrement SSL est sélectionné par défaut. Retrouvez plus d'informations à la section Sécurisation des connexions de transport avec SSL à la page 40.

8. Indiquez un chemin de sortie pour le package de configuration (MSI).
9. Cliquez sur **Créer un package de configuration**.

   Si vous avez sélectionnez le chiffrement SSL en tant que mode de **Chiffrement du transport**, la connexion au serveur est validée. En cas d'échec de la connexion, un message d'avertissement s'affiche.

Le package de configuration (MSI) a été créé dans le répertoire spécifié. Vous devez maintenant distribuer et déployer ce package sur les ordinateurs d'extrémité.

9.4.2 Création d'un package de configuration pour les ordinateurs non administrés

1. Dans le menu **Outils** de SafeGuard Management Center, cliquez sur **Outil de package de configuration**.
2. Sélectionnez **Packages du client autonome**.
3. Cliquez sur **Ajouter un package de configuration**.
4. Donnez un nom au package de configuration.
5. Spécifiez un **Groupe de stratégies** préalablement créé dans SafeGuard Management Center et que vous souhaitez appliquer aux ordinateurs.
6. Sous **Emplacement de la sauvegarde de la clé**, indiquez ou sélectionnez un chemin réseau partagé pour le stockage du fichier de récupération de clé. Saisissez le chemin de partage sous la forme suivante : **`\\ordinateur réseau\`**, par exemple **`\\monentreprise.edu\`**. Si vous n'indiquez pas de chemin ici, l'utilisateur final sera invité à indiquer l'emplacement de stockage de ce fichier lors de sa première connexion à l'ordinateur d'extrémité, suite à l'installation.

   Le fichier de récupération de clé (XML) est requis pour activer la récupération des ordinateurs protégés par SafeGuard Enterprise. Il est généré sur chaque ordinateur protégé par SafeGuard Enterprise.

   Remarque : assurez-vous d'enregistrer ce fichier de récupération de clé à un emplacement de fichier accessible pour le support. Les fichiers peuvent également être fournis au support à l'aide de différents mécanismes. Ce fichier est chiffré par le certificat d'entreprise. Il peut donc être enregistré sur un support externe ou sur le réseau pour être fourni au support technique à des fins de récupération. Il peut également être envoyé par courriel.

7. Sous **Groupe d'authentification au démarrage**, vous pouvez sélectionner le groupe d'utilisateurs de l'authentification au démarrage à attribuer à l'ordinateur d'extrémité. Les utilisateurs de l'authentification au démarrage peuvent accéder à l'ordinateur d'extrémité pour des tâches administratives après activation de l'authentification au démarrage. Pour attribuer des utilisateurs de l'authentification au démarrage, le groupe d'authentification au démarrage doit avoir été préalablement créé dans la zone **Utilisateurs et ordinateurs** de SafeGuard Management Center.
8. Indiquez un chemin de sortie pour le package de configuration (MSI).
9. Cliquez sur **Créer un package de configuration**.

Le package de configuration (MSI) a été créé dans le répertoire spécifié. Vous devez maintenant distribuer et déployer ce package sur les ordinateurs d'extrémité.

9.4.3 Création d'un package de configuration pour les Macs

Un package de configuration pour un Mac contient les informations sur le serveur et le certificat d'entreprise. Le Mac utilise ces informations pour signaler les informations d'état (authentification au démarrage active/inactive, état de chiffrement,...). Les informations d'état sont affichées dans SafeGuard Management Center.

1. Dans le menu **Outils** de SafeGuard Management Center, cliquez sur **Outil de package de configuration**.
2. Sélectionnez **Packages du client administré**.
3. Cliquez sur **Ajouter un package de configuration**.
4. Donnez un nom au package de configuration.

5. Attribuez un serveur SafeGuard Enterprise principal (le serveur secondaire n'est pas nécessaire).
6. Sélectionnez **SSL** comme **Chiffrement du transport** pour la connexion entre l'ordinateur d'extrémité et le serveur SafeGuard Enterprise. **Sophos** en tant que **Chiffrement de transport** n'est pas pris en charge pour Mac.
7. Indiquez un chemin de sortie pour le package de configuration (ZIP).
8. Cliquez sur **Créer un package de configuration**.

   La connexion au serveur pour le mode **Chiffrement du transport** SSL est validé. En cas d'échec de la connexion, un message d'avertissement s'affiche.

Le package de configuration (ZIP) a été créé dans le répertoire spécifié. Vous devez maintenant distribuer et déployer ce package sur vos Macs.

9.4.4 Comptes de service pour les tâches postérieures à l'installation

Si vous souhaitez installer SafeGuard Enterprise via un déploiement centralisé, nous vous conseillons de configurer une liste de comptes de service. Une fois qu'un administrateur informatique a été ajouté à la liste de comptes de service, il peut se connecter aux ordinateurs d'extrémité sur lesquels SafeGuard Enterprise est installé, et ce, sans activer l'authentification au démarrage. Cette opération est fortement recommandée car, par défaut, le premier utilisateur qui se connecte à un ordinateur d'extrémité après l'installation est ajouté à l'authentification au démarrage en tant que compte principal. Les utilisateurs inclus dans ces listes sont, en revanche, traités comme des utilisateurs invités SafeGuard Enterprise.

Avec les comptes de service, les étapes à suivre sont :

- SafeGuard Enterprise est installé sur un ordinateur d'extrémité.
- Après le redémarrage de l'ordinateur d'extrémité, un opérateur en charge du déploiement et figurant sur une liste de comptes de service se connecte à l'ordinateur d'extrémité à l'aide de l'invite de connexion Windows.
- D'après la liste de comptes de service appliquée au ordinateur d'extrémité, l'utilisateur est identifié comme un compte de service et traité comme utilisateur invité.
- Le technicien en charge du déploiement n'est pas ajouté à l'authentification au démarrage et l'authentification au démarrage ne sera pas active. L'utilisateur final peut se connecter et activer l'authentification au démarrage.

Remarque : vous devez créer des listes de comptes de service dans une stratégie et l'attribuer au premier groupe de stratégies du premier package de configuration que vous installez sur l'ordinateur d'extrémité après avoir installé le logiciel de chiffrement. Retrouvez plus d'informations dans le *Manuel d'administration de SafeGuard Enterprise*.

9.5 Installation du logiciel de chiffrement

La configuration du logiciel de chiffrement SafeGuard Enterprise sur les ordinateurs d'extrémité peut être effectuée de deux manières :

- Installation locale du logiciel de chiffrement. Ce type d'installation est conseillée, par exemple, lors d'une installation de test.
- Installation centralisée du logiciel de chiffrement. L'installation standard sur plusieurs ordinateurs d'extrémité est ainsi garantie.

Avant de commencer, vérifiez les packages et les fonctions d'installation disponibles pour les ordinateurs d'extrémité administrés et non administrés. Les étapes d'installation pour les deux variantes sont identiques sauf que vous attribuez un package de configuration différent pour chacun.

Le comportement des ordinateurs d'extrémité lors de la première connexion suite à l'installation de SafeGuard Enterprise et à l'activation de l'authentification au démarrage est décrit dans le *Manuel d'utilisation de SafeGuard Enterprise*.

9.5.1 Packages d'installation et fonctions

Le tableau suivant montre les packages d'installation et les fonctions du logiciel de chiffrement SafeGuard Enterprise sur les ordinateurs d'extrémité. Les packages d'installation se trouvent dans le dossier « Installers » de votre produit.

Remarque : si l'ordinateur d'extrémité fonctionne sous un système d'exploitation Windows 64 bits, installez la variante 64 bits des packages d'installation (<nom du package>_x64.msi).

Même s'il est possible d'installer seulement un sous-ensemble de fonctions lors d'une première installation, nous vous conseillons de commencer par installer le package de chiffrement intégral SafeGuard Enterprise.

Package	Contenu	Disponible pour les ordinateurs d'extrémité administrés	Disponible pour les ordinateurs d'extrémité non administrés
SGxClientPreinstall.msi	**Package de préinstallation** Le package doit être installé avant d'installer tout package d'installation de chiffrement. Fournit aux ordinateurs d'extrémité les configurations requises pour une installation réussie du logiciel de chiffrement actuel.	 obligatoire	 obligatoire
SGNClient.msi SGNClient_x64.msi	**Package d'installation du client SafeGuard** Fournit aux ordinateurs d'extrémité les configurations requises pour une installation réussie du logiciel de chiffrement actuel. Pour le chiffrement intégral des disques durs internes et externes, SafeGuard Enterprise offre les alternatives **Chiffrement basé sur volume SafeGuard** ou **BitLocker**.		
	Chiffrement basé sur volume SafeGuard (uniquement sur Windows 7 BIOS) Chiffrement intégral du disque SafeGuard. Inclut l'authentification au démarrage SafeGuard.		

Package	Contenu	Disponible pour les ordinateurs d'extrémité administrés	Disponible pour les ordinateurs d'extrémité non administrés
	Sélectionnez le type d'installation **Complète**, **Standard** , ou **Personnalisée**.		
	BitLocker ou **C/R BitLocker** SafeGuard Enterprise gère le moteur de chiffrement Microsoft BitLocker. Sur les plates-formes UEFI, l'authentification préalable au démarrage BitLocker s'effectue à l'aide d'un mécanisme de Challenge / Réponse SafeGuard tandis que la version BIOS permet d'obtenir la clé de récupération à partir de SafeGuard Management Center. Sélectionnez le type d'installation **Personnalisée**.		
	Échange de données SafeGuard Data Exchange : chiffrement basé sur fichier des données présentes sur les supports amovibles sur toutes les plates-formes sans nouveau chiffrement nécessaire. Sélectionnez le type d'installation **Complète** ou **Personnalisée**.		
	Chiffrement de fichiers Chiffrement basé sur fichier des données présentes sur les disques durs locaux et sur les partages réseau, surtout pour les groupes de travail. Sélectionnez le type d'installation **Complète** ou **Personnalisée**.		
	Cloud Storage Chiffrement basé sur fichier des données stockées dans le Cloud. Les copies locales des données stockées dans le Cloud sont toujours chiffrées de manière transparente. Pour envoyer ou recevoir des données depuis le Cloud, le logiciel recommandé par le fournisseur doit être utilisé. Sélectionnez le type d'installation **Complète** ou **Personnalisée**.		

9.5.2 Installation locale du logiciel de chiffrement

Conditions préalables :

- Les ordinateurs d'extrémité doivent avoir été préparés pour le chiffrement. Retrouvez plus d'informations à la section Préparation des ordinateurs d'extrémité au chiffrement à la page 50.
- Décidez du package de chiffrement et des fonctions à installer.

Pour installer localement le logiciel de chiffrement :

1. Ouvrez une session sur l'ordinateur d'extrémité en tant qu'administrateur.
2. Si SafeGuard LAN Crypt 3.7 x est installé sur l'ordinateur d'extrémité et que vous souhaitez installer SafeGuard Data Exchange, commencez par installer le composant de compatibilité `SGFileEncCompLayer.msi` ou `SGFileEncCompLayer_x64.msi`. Ils sont livrés avec votre produit. Retrouvez plus d'informations à la section Compatibilité avec SafeGuard LAN Crypt à la page 10.
3. Installez le package de préinstallation **`SGxClientPreinstall.msi`** le plus récent. Il va fournir à l'ordinateur d'extrémité la configuration requise pour une installation réussie du logiciel de chiffrement courant.

   Remarque : vous pouvez également installer **`vcredist_x86.exe`** en le téléchargeant sur : http://www.microsoft.com/downloads/details.aspx?FamilyID=766a6af7-ec73-40ff-b072-9112bab119c2 ou vérifiez que le fichier **`MSVCR100.dll`** est présent dans le dossier Windows\WinSxS sur l'ordinateur.
4. Cliquez deux fois sur le package logiciel de chiffrement (MSI). Un assistant vous guide tout au long des étapes nécessaires.
5. Dans l'assistant, validez les valeurs par défaut dans toutes les boîtes de dialogue qui suivent.

   Remarque : dans une première installation, nous vous conseillons de sélectionner une installation **Complète** dès le départ. Pour installer seulement un sous-ensemble de fonctions, choisissez une installation **Personnalisée** et activez/désactivez les fonctions désirées.

   SafeGuard Enterprise est installé sur l'ordinateur d'extrémité.
6. Accédez à l'emplacement d'enregistrement du package de configuration correspondant (MSI) créé auparavant dans SafeGuard Management Center. Des packages de configuration spécifiques doivent être installés pour les ordinateurs d'extrémité administrés et non administrés. Retrouvez plus d'informations à la section Création de packages de configuration à la page 53.
7. Installez le package de configuration (MSI) correspondant sur l'ordinateur.
8. Après l'installation, assurez-vous que les ordinateurs d'extrémité ont été redémarrés deux fois pour activer l'authentification au démarrage. L'ordinateur doit être redémarré une troisième fois pour effectuer une sauvegarde des données de noyau à chaque initialisation Windows.

   Assurez-vous que l'ordinateur n'est pas en veille prolongée, en mode de veille ou en mode de veille hybride avant le troisième redémarrage pour exécuter avec succès la sauvegarde du noyau.

SafeGuard Enterprise est installé sur l'ordinateur d'extrémité. Retrouvez plus d'informations sur le comportement de connexion de l'ordinateur après l'installation de SafeGuard Enterprise dans le *Manuel d'utilisation de SafeGuard Enterprise*.

9.5.3 Installation centralisée du logiciel de chiffrement

Grâce à l'installation centralisée du logiciel de chiffrement, une installation standardisée est garantie sur plusieurs ordinateurs d'extrémité.

Remarque : dans le cadre de la distribution centralisée des logiciels, les packages d'installation et de configuration peuvent uniquement être attribués à un ordinateur d'extrémité et non à un utilisateur.

Pour une installation centrale, effectuez les opérations suivantes :

- Vérifiez les packages de chiffrement disponibles pour les ordinateurs d'extrémité administrés et non administrés. Retrouvez plus d'informations à la section Packages d'installation et fonctions à la page 56.
- Vérifiez les options de ligne de commande.
- Vérifiez la liste des paramètres des fonctions pour l'option de ligne de commande ADDLOCAL.
- Vérifiez les exemples de commandes.
- Préparez le script d'installation.

9.5.3.1 Installation centralisée du logiciel de chiffrement avec Active Directory

Veuillez effectuer les étapes suivantes lors de l'installation centralisée du logiciel de chiffrement à l'aide des objets de stratégie de groupe (GPO) dans Active Directory :

Remarque : dans le cadre de la distribution centralisée des logiciels, les packages d'installation et de configuration peuvent uniquement être attribués à un ordinateur d'extrémité et non à un utilisateur.

- Utilisez un objet de stratégie de groupe (GPO) différent pour chaque package d'installation et mettez-les dans l'ordre suivant :

  composant de compatibilité
  package de préinstallation
  package du logiciel de chiffrement
  package de configuration de l'ordinateur d'extrémité

  Retrouvez plus d'informations sur les packages à la section Préparation du script d'installation à la page 59.

- Si la langue de l'ordinateur d'extrémité n'est pas définie sur vos paramètres régionaux, procédez aux modifications supplémentaires suivantes : dans l'Éditeur de stratégies de groupe, sélectionnez l'objet de groupe respectif et **Configuration de l'ordinateur > Paramètres logiciels> Avancés**. Dans la boîte de dialogue **Options de déploiement avancées**, sélectionnez **Ignorer la langue lors du déploiement de ce package** et cliquez sur **OK**.

9.5.3.2 Préparation du script d'installation

Conditions préalables :

- Les ordinateurs d'extrémité doivent avoir été préparés pour le chiffrement.
- Décidez du package de chiffrement et des fonctions à installer.

Pour installer le logiciel de chiffrement de manière centralisée :

1. Créez un dossier appelé **`Logiciels`** à utiliser pour centraliser le stockage de toutes les applications.
2. Utilisez vos propres outils pour créer un package à installer sur les ordinateurs d'extrémité. Le package doit inclure les éléments suivants dans l'ordre mentionné :

Package	Description
Package de préinstallation `SGxClientPreinstall.msi`	Le package obligatoire fournit aux ordinateurs d'extrémité la configuration requise pour une installation réussie du logiciel de chiffrement actuel, par exemple la DLL requise **`MSVCR100.dll`**. **Remarque :** si ce package n'est pas installé, l'installation du logiciel de chiffrement échoue.
Package du logiciel de chiffrement	Retrouvez une liste des packages disponibles à la section Installation des packages et des fonctions à la page 56.
Package de configuration pour les ordinateurs d'extrémité	Utilisez les packages de configuration créés auparavant dans SafeGuard Management Center. Des packages de configuration différents doivent être installés pour les ordinateurs d'extrémité administrés et non administrés. Retrouvez plus d'informations à la section Création de packages de configuration à la page 53. Veillez à d'abord supprimer toutes les anciennes versions.

3. Créez un script avec les commandes de l'installation préconfigurée. Le script doit indiquer quelles fonctions du logiciel de chiffrement vous voulez installer. Retrouvez plus d'informations à la section Paramètres des fonctions de l'option ADDLOCAL à la page 62. Ouvrez une invite de commande et saisissez les commandes de script. Retrouvez plus d'informations sur la syntaxe de ligne de commande à la section Options de ligne de commande pour l'installation centralisée à la page 61.
4. Distribuez ce package sur les ordinateurs d'extrémité à l'aide des mécanismes de distribution de logiciels de l'entreprise.

   L'installation est effectuée sur les ordinateurs d'extrémité. Les ordinateurs d'extrémité sont ensuite prêts à utiliser SafeGuard Enterprise.

5. Après l'installation, assurez-vous que les ordinateurs d'extrémité ont été redémarrés deux fois pour activer l'authentification au démarrage SafeGuard. Ils doivent être redémarrés une troisième fois pour effectuer une sauvegarde des données de noyau à chaque initialisation Windows.

   Assurez-vous que les ordinateurs ne sont pas suspendus ou en veille prolongée avant le troisième redémarrage pour exécuter avec succès la sauvegarde du noyau.

Une configuration supplémentaire peut être requise pour garantir que l'authentification au démarrage fonctionne correctement sur chaque plate-forme matérielle. La plupart des conflits matériels peuvent être résolus à l'aide de la fonctionnalité **Raccourcis clavier** intégrée à l'authentification au démarrage. Les raccourcis clavier peuvent être configurés dans l'authentification au démarrage après l'installation ou via un paramètre de configuration supplémentaire passé à la commande msiexec de Windows Installer. Retrouvez plus d'informations sur :

http://www.sophos.com/fr-fr/support/knowledgebase/107781.aspx

http://www.sophos.com/fr-fr/support/knowledgebase/107785.aspx

9.5.3.3 Options de ligne de commande pour l'installation centralisée

Pour une installation centralisée, nous vous conseillons de préparer un script à l'aide du composant d'installation Windows **`msiexec`**. **`Msiexec`** effectue automatiquement une installation préconfigurée de SafeGuard Enterprise. **`Msiexec`** est inclus dans Windows. Retrouvez plus d'informations sur : http://msdn.microsoft.com/fr-fr/library/aa367988(VS.85).aspx.

Syntaxe de la ligne de commande

```
msiexec /i <chemin+nom du package msi> /qn ADDLOCAL=ALL | <Fonctions
 SGN> <paramètre SGN>
```

La syntaxe de la ligne de commande est constituée des éléments suivants :

- Les paramètres de Windows Installer, par exemple, les avertissements des journaux et les messages d'erreur envoyés dans un fichier lors de l'installation.
- Les fonctions de SafeGuard Enterprise à installer, par exemple, le chiffrement intégral du disque.
- Les paramètres de SafeGuard Enterprise , par exemple pour indiquer le répertoire d'installation.

Options de ligne de commande

Vous pouvez sélectionner toutes les options disponibles en utilisant msiexec.exe à l'invite. Les principales options sont décrites ci-dessous.

Option	Description
`/i`	Indique qu'il s'agit d'une installation.
`/qn`	Exécute une installation sans interaction de l'utilisateur et n'affiche pas d'interface utilisateur.
`ADDLOCAL=`	Répertorie les fonctions SafeGuard Enterprise à installer. Si l'option n'est pas spécifiée, toutes les fonctions d'une installation standard sont installées. Retrouvez une liste des fonctions SafeGuard Enterprise dans chaque package d'installation et leur disponibilité en fonction de la configuration des ordinateurs d'extrémité à la section Packages d'installation et fonctions à la page 56. Retrouvez une liste des paramètres des fonctions pour l'option ADDLOCAL à la section Paramètres des fonctions pour l'option ADDLOCAL à la page 62.
`ADDLOCAL=ALL`	Sous Windows 7 (BIOS), **`ADDLOCAL=ALL`** installe le chiffrement SafeGuard à base de volumes et toutes les autres fonctions disponibles.

Option	Description
	Sous Windows 8, **ADDLOCAL=ALL** installe le chiffrement BitLocker et toutes les autres fonctions disponibles.
REBOOT=Force | NoRestart	Force ou supprime un redémarrage après l'installation. Si rien n'est spécifié, le redémarrage est forcé après l'installation.
/L* <chemin + nom de fichier>	Consigne tous les avertissements et messages d'erreur dans le fichier journal spécifié. Le paramètre **/Le <chemin + nom de fichier>** ne journalise que les messages d'erreur.
Installdir= <répertoire>	Spécifie le répertoire dans lequel installer le logiciel de chiffrement SafeGuard Enterprise. Si aucune valeur n'est spécifiée, le répertoire d'installation par défaut est <SYSTEM>:\PROGRAM FILES\SOPHOS.

9.5.3.4 Paramètres des fonctions pour l'option ADDLOCAL

Vous devez définir à l'avance les fonctions à installer sur les ordinateurs d'extrémité. Les noms des fonctions sont ajoutées en tant que paramètres à l'option de commande ADDLOCAL. Veuillez établir une liste des fonctions après avoir saisi l'option **ADDLOCAL** dans la commande :

- Séparez les fonctions à l'aide d'une virgule et non d'un espace.
- Respectez la casse.
- Si vous sélectionnez une fonction, vous devez également ajouter toutes les fonctions parentes à la ligne de commande.
- Veuillez noter que les noms des fonctions peuvent être différents des noms de modules correspondants. Vous les retrouverez dans le tableau ci-dessous entre parenthèses.
- Veuillez indiquer les fonctions **Client** et **CredentialProvider** par défaut.

Le tableau ci-dessous dresse la liste des fonctions qui peuvent être installées sur les ordinateurs d'extrémité. Retrouvez plus d'informations sur : Packages d'installation et fonctions à la page 56.

Fonctions parentes	Fonction
Client	**CredentialProvider** Obligatoire. La fonction active la connexion avec le fournisseur de codes d'accès.
Client, **BaseEncryption**	**SectorBasedEncryption** (chiffrement de volumes SafeGuard)
	Remarque : SectorBasedEncryption OU **BitLockerSupport** peuvent être spécifiés.

Fonctions parentes	Fonction
Client,**BaseEncryption**	**BitLockerSupport** (BitLocker)
Client,**BaseEncryption**,**BitLockerSupport**	**BitLockerSupportCR** (C/R BitLocker)
Client	**SecureDataExchange** (Data Exchange)
Client	**FileShare** (chiffrement de fichiers)
Client	**CloudStorage** (Cloud Storage)

9.5.3.5 Exemple de commande : chiffrement de volumes SafeGuard avec Chiffrement de fichiers

La commande installe les éléments suivants :

- Les ordinateurs d'extrémité sont fournis avec la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement.
- Connexion aux ordinateurs d'extrémité à l'aide du fournisseur de codes d'accès Windows.
- Authentification au démarrage (POA) de SafeGuard Enterprise.
- Chiffrement de volumes SafeGuard Enterprise.
- SafeGuard File Encryption avec le chiffrement des données basé sur fichier sur le disque dur local et les partages réseau.
- Le package de configuration qui configure l'ordinateur d'extrémité en tant qu'ordinateur d'extrémité administré et permet la connexion au serveur SafeGuard Enterprise.
- Des fichiers journaux sont créés.

Exemple de commande :

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log
I:\Temp\SGxClientPreinstall.log
```

```
msiexec /i F:\Software\SGNClient.msi /qn /log I:\Temp\SGNClient.log

ADDLOCAL=Client,CredentialProvider,BaseEncryption,SectorBasedEncryption,FileShare
 Installdir=C:\Program Files\Sophos\SafeGuard Enterprise
```

```
msiexec /i F:\Software\SGNConfig_managed.msi /qn /log
I:\Temp\SGNConfig_managed.log
```

9.5.3.6 Exemple de commande : prise en charge de SafeGuard BitLocker avec Challenge/Réponse.

La commande installe les éléments suivants :

- Les ordinateurs d'extrémité sont fournis avec la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement.
- Connexion aux ordinateurs d'extrémité à l'aide du fournisseur de codes d'accès Windows.
- Prise en charge de SafeGuard BitLocker.
- Challenge/Réponse SafeGuard pour la récupération de BitLocker
- Le package de configuration qui configure l'ordinateur d'extrémité en tant qu'ordinateur d'extrémité administré et permet la connexion au serveur SafeGuard Enterprise.
- Des fichiers journaux sont créés.

Exemple de commande :

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log
I:\Temp\SGxClientPreinstall.log
```

```
msiexec /i F:\Software\SGNClient.msi /qn /log I:\Temp\SGNClient.log

ADDLOCAL=Client,BaseEncryption,CredentialProvider,BitLockerSupport,BitLockerSupportCR
 Installdir=C:\Program Files\Sophos\SafeGuard Enterprise
```

```
msiexec /i F:\Software\SGNConfig_managed.msi /qn /log
I:\Temp\SGNConfig_managed.log
```

9.5.3.7 Exemple de commande : prise en charge de SafeGuard BitLocker avec Challenge/Réponse et Chiffrement de fichiers

La commande installe les éléments suivants :

- Les ordinateurs d'extrémité sont fournis avec la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement.
- Connexion aux ordinateurs d'extrémité à l'aide du fournisseur de codes d'accès Windows.
- Prise en charge de SafeGuard BitLocker.
- Challenge/Réponse SafeGuard pour la récupération de BitLocker
- SafeGuard File Encryption avec le chiffrement des données basé sur fichier sur le disque dur local et les partages réseau.
- Le package de configuration qui configure l'ordinateur d'extrémité en tant qu'ordinateur d'extrémité administré et permet la connexion au serveur SafeGuard Enterprise.

- Des fichiers journaux sont créés.

Exemple de commande :

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log
I:\Temp\SGxClientPreinstall.log
```

```
msiexec /i F:\Software\SGNClient.msi /qn /log I:\Temp\SGNClient.log

ADDLOCAL=Client,BaseEncryption,CredentialProvider,BitLockerSupport,BitLockerSupportOR,FileShare
 Installdir=C:\Program Files\Sophos\SafeGuard Enterprise
```

```
msiexec /i F:\Software\SGNConfig_managed.msi /qn /log
I:\Temp\SGNConfig_managed.log
```

9.6 Installation du logiciel de chiffrement pour Mac

Retrouvez plus d'informations sur l'installation du logiciel de chiffrement sur les clients Mac OS X dans le *Manuel d'administration de Sophos SafeGuard File Encryption pour Mac* et dans le *Manuel d'administration de Sophos SafeGuard Native Device Encryption pour Mac*.

9.7 Installations conformes à la norme FIPS

La certification FIPS décrit les conditions de sécurité requises des modules de chiffrement. Par exemple, les organismes publics aux États-Unis et au Canada exigent des logiciels certifiés FIPS 140-2 pour des informations particulièrement sensibles en matière de sécurité.

SafeGuard Enterprise utilise les algorithmes AES certifiés par FIPS. Toutefois, une nouvelle mise en place plus rapide des algorithmes AES est installée par défaut mais n'est pas encore certifiée FIPS.

Pour utiliser la variante certifiée FIPS de l'algorithme AES, paramétrez la propriété FIPS sur 1 (un) lors de l'installation du logiciel de chiffrement SafeGuard Enterprise.

Ajoutez la propriété au script de ligne de commande suivant :

```
msiexec /i F:\Software\SGNClient.msi FIPS=1
```

Remarque : ceci s'applique uniquement à SafeGuard Enterprise Device Encryption et à Windows 7.

Remarque : si vous voulez procédez à la mise à niveau d'une installation conforme à la norme FIPS, sachez que les nouvelles versions seront installées en mode FIPS indépendamment du paramètre que vous avez choisi.

9.8 Installations sur les disques durs à chiffrement automatique compatibles Opal

SafeGuard Enterprise prend en charge la norme de l'éditeur indépendant Opal concernant les disques durs à chiffrement automatique et offre la gestion des ordinateurs d'extrémité disposant de tels disques durs.

Pour s'assurer que la prise en charge des disques durs à chiffrement automatique conformes à la norme Opal respectent strictement la norme, vous pouvez effectuer deux types de vérification lors de l'installation de SafeGuard Enterprise sur l'ordinateur d'extrémité :

- **Vérifications fonctionnelles**

  Elles incluent, entre autres, de vérifier que le lecteur s'identifie en tant que lecteur de disque dur « OPAL », que les propriétés de communications sont correctes et que les fonctions Opal requises pour SafeGuard Enterprise sont prises en charge par le lecteur.

- **Vérifications de sécurité**

  Les vérifications de sécurité garantissent que seuls les utilisateurs SafeGuard Enterprise qui sont enregistrés sur le lecteur sont les propriétaires des clés utilisées pour le chiffrement logiciel de lecteurs ne se chiffrant pas automatiquement. Si d'autres utilisateurs se sont enregistrés lors de l'installation, SafeGuard Enterprise tente automatiquement de les désactiver. Cette fonctionnalité est requise par la norme Opal à l'exception de quelques autres « responsabilités » par défaut qui sont requises pour exécuter un système Opal.

  Remarque : les vérifications de sécurité sont répétées lorsqu'une stratégie de chiffrement pour le lecteur est appliquée suite à l'installation réussie du mode Opal. En cas d'échec, ceci signifie que la gestion des lecteurs a été modifiée simultanément en dehors de SafeGuard Enterprise depuis la première vérification lors de l'installation. Dans ce cas, SafeGuard Enterprise ne verrouille pas le disque dur Opal. Un message va s'afficher.

Si l'une de ces vérifications échoue de manière irrécupérable, l'installation ne repasse pas dans le chiffrement basé sur logiciel. À la place, tous les volumes présents sur le lecteur Opal restent non chiffrés.

À partir de la version 7 de SafeGuard Enterprise, les vérifications Opal ne sont plus effectuées par défaut. Ceci signifie que même en présence d'un lecteur Opal, SafeGuard Enterprise chiffrera les volumes présents sur ce lecteur à l'aide du chiffrement de logiciels.

Si vous voulez forcer les vérifications Opal, utilisez la syntaxe de ligne de commande suivante :

```
MSIEXEC /i <nom_du_client_sélectionné_msi>.msi OPALMODE=0
```

Remarque : la mise à niveau de SafeGuard Enterprise 6.x vers SafeGuard Enterprise 7.0 sur un système équipé d'un disque dur Opal utilisé en mode de chiffrement HW Opal conservera le mode de chiffrement HW.

Certains disques durs Opal peuvent avoir des problèmes de sécurité. Il n'est pas possible de savoir automatiquement quels privilèges ont été affectés à un utilisateur/responsable qui a déjà été enregistré sur le lecteur lors de l'installation ou du chiffrement de SafeGuard Enterprise. Si le lecteur refuse la commande de désactivation de ces utilisateurs, SafeGuard Enterprise restaure le chiffrement logiciel afin de garantir une sécurité maximale de l'utilisateur SafeGuard Enterprise. Nous ne sommes pas en position de garantir la sécurité des disques durs, aussi nous avons mis en place un commutateur d'installation qui vous permet d'utiliser à votre propre discrétion les lecteurs affichant des problèmes potentiels de sécurité. Retrouvez

une liste des lecteurs de disque dur nécessitant l'utilisation d'un commutateur d'installation ainsi que plus d'informations sur les lecteurs de disque dur pris en charge dans les *Notes de publication de SafeGuard Enterprise*.

Pour appliquer le commutateur d'installation, utilisez la syntaxe de ligne de commande suivante :

```
MSIEXEC /i <nom_du_client_sélectionné_msi.msi>.msi
IGNORE_OPAL_AUTHORITYCHECK_RESULTS=1
```

La propriété interne du .msi a le même nom, si vous voulez le modifier à l'aide d'une transformation.

Retrouvez plus d'informations sur l'utilisation de SafeGuard Enterprise avec des lecteurs de disque dur conformes à la norme Opal dans le *Manuel d'administration* et dans le *Manuel d'utilisation de SafeGuard Enterprise*.

10 Réplication de la base de données SafeGuard Enterprise

Afin d'améliorer ses performances, la base de données SafeGuard Enterprise peut être répliquée sur plusieurs serveurs SQL.

Ce chapitre décrit comment configurer la réplication pour la base de données SafeGuard Enterprise dans un environnement distribué. Nous considérons que vous avez déjà une certaine expérience concernant l'utilisation du mécanisme de réplication dans Microsoft SQL Server.

Remarque : l'administration doit avoir lieu uniquement sur la base de données principale, et pas sur les bases de données dupliquées.

Important :

La solution proposée ne décrit pas la procédure de réplication de la base de données dans le but d'effectuer des basculements redondants mais dans le but d'améliorer les performances dans des cas de figure de distribution de la base de données sur plusieurs emplacements.

10.1 Réplication de fusion

La réplication de fusion correspond au processus de distribution des données d'un éditeur vers des abonnés. Il permet à l'éditeur et aux abonnés d'effectuer des mises à jour de manière indépendante, puis de les fusionner d'un site à l'autre.

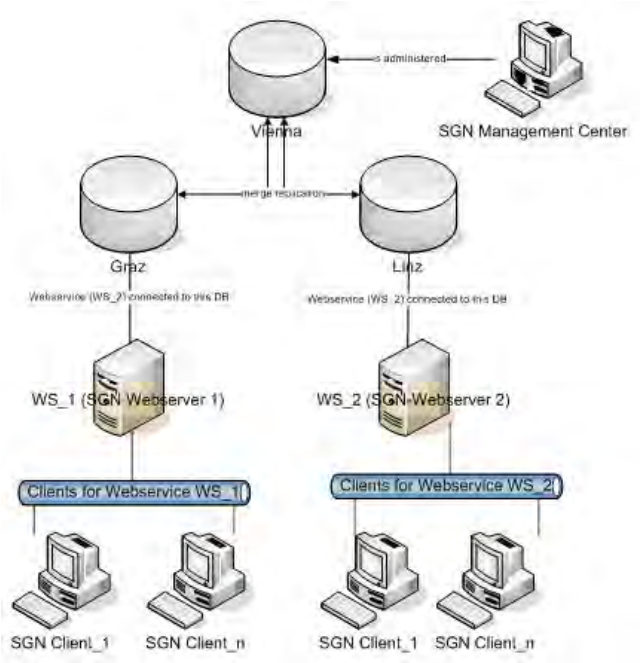
La réplication de fusion permet à plusieurs sites de travailler de façon autonome, puis de fusionner les mises à jour de manière à obtenir un résultat unique et homogène. La capture instantanée initiale est appliquée aux abonnés, puis Microsoft SQL Server effectue un suivi des modifications sur les données publiées par l'éditeur et par les abonnés. Les données sont synchronisées continuellement entre les serveurs, à intervalles réguliers ou sur demande. Puisque les mises à jour sont effectuées sur plusieurs serveurs, les mêmes données peuvent avoir été mises à jour par l'éditeur ou par plusieurs abonnés. Des conflits peuvent donc apparaître lors de la fusion.

La réplication de fusion comprend des choix par défaut et personnalisés de résolution des conflits, que vous pouvez modifier au moment de la configuration d'une publication de fusion. Lorsqu'un conflit survient, un programme de résolution est appelé par l'agent de fusion. Il détermine les données à accepter et à propager vers les autres sites.

10.2 Configuration de la réplication des bases de données

La configuration d'une réplication d'une base de données SafeGuard Enterprise est expliquée à l'aide d'un exemple basé sur Microsoft SQL Server.

Dans l'exemple, SafeGuard Enterprise est administré de manière exclusive depuis la base de données **Vienna**. Toute modification est transmise par SafeGuard Management Center aux bases de données **Graz** et **Linz** par réplication dans Microsoft SQL Server. Les modifications signalées par les ordinateurs client par l'intermédiaire des serveurs Web sont également transmises à Microsoft SQL Server par réplication.



10.2.1 Génération de la base de données principale

Commencez par configurer la base de données SafeGuard Enterprise principale. Dans notre exemple, il s'agit de la base de données VIENNA.

La procédure de génération de la base de données principale est la même que pour une installation de SafeGuard Enterprise sans réplication.

- Générez la base de données principale dans l'assistant de configuration de SafeGuard Management Center.

  Cette procédure exige que SafeGuard Management Center soit déjà installé. Retrouvez plus d'informations à la section Démarrage de la configuration initiale de SafeGuard Management Center à la page 28.

- Générez la base de données principale avec un script SQL. Ils figurent avec le produit livré.

  Cette procédure est généralement préférée si l'extension des autorisations SQL lors de la configuration de SafeGuard Management n'est pas souhaitée. Retrouvez plus d'informations à la section Génération de la base de données SafeGuard Enterprise à l'aide d'un script à la page 22.

10.2.2 Génération des bases de données de réplication Graz et Linz

Une fois la base de données principale configurée, générez les bases de données dupliquées. Dans notre exemple, il s'agit des bases de données Graz et Linz.

Remarque : les tables de données et les tableaux EVENT se trouvent dans des bases de données distinctes. Par défaut, les entrées d'événement ne sont pas connectées, de manière à ce que la base de données des événements puisse être dupliquée sur plusieurs serveurs SQL afin d'améliorer les performances. Si les tableaux EVENT sont connectés, des problèmes peuvent survenir lors de la réplication de ses enregistrements de données.

Pour générer les bases de données de réplication :

1. Créez une publication de la base de données principale dans la console de gestion du serveur SQL.

   Une publication définit la série de données à répliquer.

2. Sélectionnez les tables, les vues et les procédures stockées à synchroniser dans cette publication.
3. Créez les bases de données dupliquées en générant un abonnement pour Graz et un autre pour Linz. Les nouvelles bases de données Graz et Linz apparaissent ensuite également dans l'assistant de configuration des abonnements SQL.
4. Fermez l'assistant de configuration SQL. Le moniteur de réplication indique si la réplication s'exécute correctement ou non.
5. Assurez-vous de saisir le nom de base de données approprié dans la première ligne du script SQL. Par exemple, utilisez **`Graz`** ou **`Linz`**.
6. Réalisez à nouveau les captures instantanées à l'aide de l'agent de capture instantanée.

Les bases de données dupliquées Graz et Linz ont été créées.

10.3 Installation et enregistrement des serveurs SafeGuard Enterprise

Pour installer le serveur SafeGuard Enterprise sur les serveurs Web, veuillez procéder comme suit.

1. Installez le serveur SafeGuard Enterprise sur le serveur WS_1.
2. Installez le serveur SafeGuard Enterprise sur le serveur WS_2.
3. Enregistrez les deux serveurs dans SafeGuard Management Center : Dans le menu **Outils**, cliquez sur **Outil de package de configuration**, puis cliquez sur **Serveurs**. Dans l'onglet **Serveurs**, cliquez sur **Ajouter**.
4. Vous êtes invité à ajouter les certificats de serveur **`ws_1.cer`** et **`ws_2.cer`**. Ils se trouvent dans le dossier **`\Program Files\Sophos\Sophos SafeGuard\MachCert\`**. Ces certificats sont nécessaires à la création des packages de configuration appropriés.

Les serveurs SafeGuard Enterprise sont installés et enregistrés.

10.4 Création des packages de configuration de la base de données Graz

Veuillez créer les packages de configuration de la base de données Graz : un pour le serveur WS_1 pour communiquer avec la base de données Graz et un pour les clients SafeGuard Enterprise Graz se connectant au service Web WS_1.

1. Dans le menu **Outils** de SafeGuard Management Center, cliquez sur **Options**, puis sur **Base de données**.
2. Sous **Paramètres de connexion**, sélectionnez **`WS_1`** en tant que **Serveur de base de données** et Graz en tant que **Base de données sur serveur**. Cliquez sur **OK**.
3. Dans le menu **Outils**, cliquez sur **Outil de package de configuration**, puis cliquez sur **Packages du serveur**. Sélectionnez le serveur **`WS_1`**, puis, sélectionnez le chemin de sortie et cliquez sur **Créer un package de configuration**.

4. Ouvrez l'onglet **Packages du client administré**. Cliquez sur **Ajouter un package de configuration** et saisissez un nom de package. Sous **Serveur principal**, sélectionnez le serveur auquel les clients SafeGuard Enterprise Graz doivent être connectés : **`WS_1`**. Sélectionnez le chemin de sortie et cliquez sur **Créer un package de configuration.**

Les packages de configuration du serveur et du client SafeGuard Enterprise pour la base de données Graz ont été créés dans l'emplacement défini.

10.5 Création des packages de configuration de la base de données Linz

Veuillez créer les packages de configuration de la base de données Linz : un pour le serveur WS_2 pour communiquer avec la base de données Linz et un pour les clients SafeGuard Enterprise Linz se connectant au service Web WS_2.

1. Dans le menu **Outils** de SafeGuard Management Center, cliquez sur **Options**, puis sur **Base de données**.
2. Sous **Paramètres de connexion**, sélectionnez **`WS_2`** en tant que **Serveur de base de données** et Linz en tant que **Base de données sur serveur**. Cliquez sur **OK**.
3. Dans le menu **Outils**, cliquez sur **Outil de package de configuration**, puis cliquez sur **Packages du serveur**. Sélectionnez le serveur **`WS_2`**, sélectionnez le chemin de sortie et cliquez sur **Créer un package de configuration**.
4. Ouvrez l'onglet **Packages du client administré**. Cliquez sur **Ajouter un package de configuration** et saisissez un nom de package. Sous **Serveur principal**, sélectionnez le serveur auquel les clients SafeGuard Enterprise Linz doivent être connectés : **`WS_2`**. Sélectionnez le chemin de sortie et cliquez sur **Créer un package de configuration**. Cliquez sur **Fermer**.
5. Connectez de nouveau SafeGuard Management Center à la base de données Vienna : dans le menu **Outils**, cliquez sur **Options**, puis cliquez sur **Base de données**.

Les packages de configuration du serveur et du client SafeGuard Enterprise pour la base de données Linz ont été créés dans l'emplacement défini.

10.6 Installation des packages de configuration du serveur SafeGuard Enterprise

1. Installez le package de configuration du serveur **`ws_1.msi`** sur le service Web WS_1 destiné à communiquer avec la base de données Graz.
2. Installez le package de configuration du serveur **`ws_2.msi`** sur le service Web WS_2, destiné à communiquer avec la base de données Linz.

3. Testez la communication entre les serveurs SafeGuard Enterprise et ces bases de données :

   a) Sur l'ordinateur sur lequel est installé le serveur SafeGuard Enterprise, ouvrez le **Gestionnaire des services Internet (IIS)**.

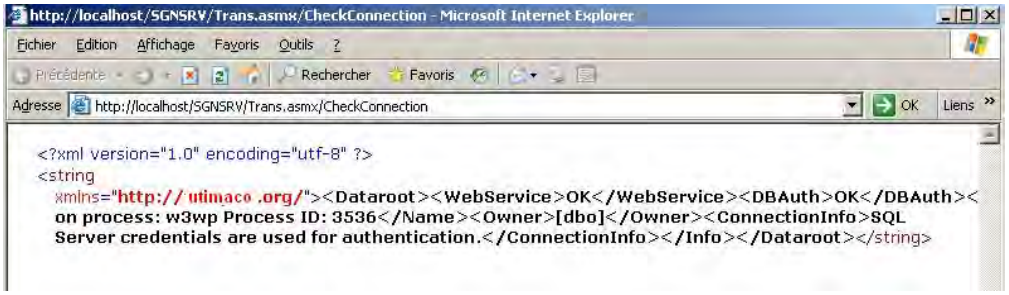
   b) Dans l'arborescence, cliquez sur **Services Internet (IIS)**. Cliquez sur **« Nomserveur »**, **Sites Web**, **Site Web par défaut**. Vérifiez que la page Web **SGNSRV** est disponible dans le dossier **Site Web par défaut**.

   c) Cliquez avec le bouton droit de la souris sur **SGNSRV**, puis cliquez sur **Parcourir**. Une liste d'actions possibles apparaît à droite de la fenêtre.

   d) Dans cette liste, sélectionnez **CheckConnection**. L'action possible apparaît à droite de la fenêtre.

   e) Pour tester la connexion, cliquez sur **Appeler**.

   Le test de connexion est un succès lorsque les résultats suivants apparaissent :



10.7 Configuration de l'ordinateur d'extrémité

Retrouvez plus d'informations sur l'installation du logiciel de chiffrement sur les ordinateurs d'extrémité à la section Installation centralisée du logiciel de chiffrement à la page 59.

Remarque : pour la configuration des ordinateurs d'extrémité, assurez-vous d'installer le package de configuration correct après l'installation :

1. Installez le package de configuration Graz sur les ordinateurs d'extrémité qui doivent être connectés au serveur Graz WS_1.
2. Installez le package de configuration Linz sur les ordinateurs d'extrémité qui doivent être connectés au serveur Linz WS_2.

Retrouvez plus d'informations sur la mise à jour des bases de données SafeGuard Enterprise répliquées dans le *Guide de mise à niveau de SafeGuard Enterprise*.

11 À propos de la désinstallation

Cette section couvre les rubriques suivantes :

- Bon usage en matière de désinstallation
- Désinstallation du logiciel de chiffrement SafeGuard Enterprise
- Interdiction de désinstallation du logiciel de chiffrement SafeGuard Enterprise sur les ordinateurs d'extrémité

11.1 Bon usage en matière de désinstallation

Lorsque le logiciel de chiffrement SafeGuard Enterprise est installé sur le même ordinateur que SafeGuard Management Center, assurez-vous de bien suivre cette procédure de désinstallation afin de pouvoir continuer à les utiliser :

1. Désinstallez SafeGuard Management Center.
2. Désinstallez le package de configuration.
3. Désinstallez le logiciel de chiffrement.
4. Installez à nouveau le package que vous souhaitez continuer à utiliser.

11.2 Désinstallation du logiciel de chiffrement SafeGuard Enterprise

La désinstallation du logiciel de chiffrement SafeGuard Enterprise des ordinateurs d'extrémité implique les étapes suivantes :

- Déchiffrement des données chiffrées.
- Désinstallation du logiciel de chiffrement.

  Les stratégies appropriées doivent être effectives sur les ordinateurs d'extrémité pour permettre le déchiffrement et la désinstallation.

11.2.1 Interdiction de la désinstallation sur les ordinateurs d'extrémité

Pour assurer une protection supplémentaire des ordinateurs d'extrémité, nous vous conseillons d'interdire la désinstallation locale de SafeGuard Enterprise sur les ordinateurs d'extrémité. Définissez l'option **Désinstallation autorisée** de la stratégie **Paramètres de machine spécifiques** sur **Non** et déployez cette stratégie sur les ordinateurs d'extrémité. Les tentatives de désinstallation sont alors annulées et les tentatives non autorisées sont consignées dans le journal.

11.2.2 Déchiffrement des données chiffrées

La condition préalable suivante doit être remplie :

Pour déchiffrer les volumes chiffrés, tous les volumes chiffrés basé sur volume doivent disposer d'une lettre de lecteur qui leur est attribuée.

1. Dans SafeGuard Management Center, modifiez la stratégie en cours du type **Protection des périphériques** qui est attribuée aux ordinateurs que vous voulez déchiffrer. Sélectionnez les cibles et paramétrez **L'utilisateur peut déchiffrer le volume** sur **Oui**. Attribuez la stratégie aux ordinateurs d'extrémité concernés.
2. Créez une stratégie de déchiffrement du type **Protection des périphériques**, sélectionnez les cibles qui doivent être déchiffrées et paramétrez le **Mode de chiffrement du support** sur **Aucun chiffrement**.
3. Dans **Utilisateurs et ordinateurs**, créez un groupe pour les ordinateurs que vous voulez déchiffrer : Cliquez avec le bouton droit de la souris sur le nœud du domaine sur lequel vous voulez créer le groupe. Puis, sélectionnez **Nouveau > Créer un groupe**.
4. Sélectionnez le nœud de domaine de ce groupe et attribuez-lui la stratégie de déchiffrement en faisant glisser la stratégie de la liste des **Stratégies disponibles** dans l'onglet **Stratégies**. Activez la stratégie en faisant glisser le groupe de la liste des **Groupes disponibles** jusqu'à la zone **Activation**. Dans l'onglet **Stratégies** du nœud du domaine, vérifiez que la **Priorité** est définie sur 1 et que l'option **Ne pas remplacer** est activée. Dans la zone **Activation** du nœud du domaine, assurez-vous que la stratégie s'applique uniquement aux membres du groupe.
5. Dans la zone de navigation **Utilisateurs et ordinateurs**, sélectionnez le groupe, cliquez avec le bouton droit de la souris sur l'onglet **Membres** qui s'affiche dans la zone d'action et cliquez sur **Ajouter** pour ajouter au groupe les ordinateurs que vous voulez déchiffrer.
6. Sur l'ordinateur d'extrémité devant être déchiffré, procédez à la synchronisation avec le serveur SafeGuard Enterprise pour vous assurer que la mise à jour des stratégies a été reçue et qu'elle est active.
7. Ouvrez l'Explorateur Windows. Cliquez avec le bouton droit de la souris sur le volume devant être déchiffré et cliquez sur **Chiffrement > Déchiffrement**.

   Assurez-vous que le déchiffrement se termine avec succès.

   Remarque : les ordinateurs d'extrémité peuvent être éteints et redémarrés lors du chiffrement/déchiffrement. Si le déchiffrement est suivi d'une désinstallation, nous conseillons de ne pas suspendre, ni de mettre en veille l'ordinateur d'extrémité lors du déchiffrement.

11.2.3 Désinstallation

Les conditions préalables suivantes doivent être remplies :

- Les données chiffrées doivent être déchiffrées correctement pour qu'elles deviennent accessibles par la suite. Le processus de déchiffrement doit être terminé. Un véritable déchiffrement est particulièrement important lorsque la désinstallation est déclenchée par Active Directory.

  Par ailleurs, tous les supports amovibles chiffrés doivent être déchiffrés avant la désinstallation du dernier ordinateur d'extrémité protégé par SafeGuard Enterprise accessible. Sinon, les utilisateurs pourraient ne plus pouvoir accéder à leurs données. Tant que la base de données SafeGuard Enterprise est disponible, les données présentes sur les supports amovibles peuvent être récupérées.

- Pour désinstaller le chiffrement intégral du disque SafeGuard, tous les volumes chiffrés basé sur volume doivent disposer d'une lettre de lecteur qui leur est attribuée.

- Assurez-vous de toujours désinstaller l'intégralité du package avec toutes les fonctions installées.

1. Dans SafeGuard Management Center, modifiez la stratégie du type **Paramètres de machine spécifiques**. Paramétrez **Désinstallation autorisée** sur **Oui**.
2. Dans **Utilisateurs et ordinateurs**, créez un groupe pour les ordinateurs que vous voulez déchiffrer : Cliquez avec le bouton droit de la souris sur le nœud du domaine sur lequel vous voulez créer le groupe. Puis, sélectionnez **Nouveau > Créer un groupe**.
3. Sélectionnez le nœud de domaine de ce groupe et attribuez-lui la stratégie de désinstallation en faisant glisser la stratégie de la liste des **Stratégies disponibles** dans l'onglet **Stratégies**. Activez la stratégie en faisant glisser le groupe de la liste des **Groupes disponibles** jusqu'à la zone **Activation**. Dans l'onglet **Stratégies** du nœud du domaine, vérifiez que la **Priorité** est définie sur 1 et que l'option **Ne pas remplacer** est activée. Dans la zone **Activation** du nœud du domaine, assurez-vous que la stratégie s'applique uniquement aux membres du groupe.
4. Ajoutez les ordinateurs d'extrémité que vous voulez désinstaller au groupe.
5. Pour démarrer la désinstallation, utilisez l'une des méthodes suivantes :
   - Pour désinstaller localement sur l'ordinateur d'extrémité, synchronisez avec le serveur SafeGuard Enterprise pour vous assurer que la mise à jour des stratégies a été reçue et est active. Puis sélectionnez **Démarrer > Panneau de configuration > Ajout/Suppression de programmes > Client Sophos SafeGuard > Supprimer**.
   - Pour désinstaller de manière centralisée, utilisez le mécanisme de distribution de logiciels de votre choix. Assurez-vous que toutes les données requises ont été déchiffrées correctement avant que la désinstallation démarre.

12 Support technique

Vous bénéficiez du support technique des produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur community.sophos.com/ et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur www.sophos.com/fr-fr/support.aspx.
- Téléchargez la documentation des produits sur www.sophos.com/fr-fr/support/documentation/.
- Ouvrez un incident support sur https://secure2.sophos.com/fr-fr/support/contact-support/support-query.aspx.

13 Mentions légales