

SafeGuard Enterprise Guide d'installation

Version du produit : 5.60
Date du document : avril 2011



Table des matières

| | | |
|----|---|----|
| 1 | Présentation de SafeGuard Enterprise | 3 |
| 2 | Composants de SafeGuard Enterprise..... | 3 |
| 3 | Démarrage..... | 5 |
| 4 | Configuration du serveur SafeGuard Enterprise..... | 13 |
| 5 | Configuration de la base de données SafeGuard Enterprise..... | 21 |
| 6 | Configuration du SafeGuard Management Center..... | 30 |
| 7 | Test de la communication..... | 42 |
| 8 | Enregistrement et configuration du serveur SafeGuard Enterprise..... | 45 |
| 9 | Configuration de SafeGuard Enterprise sur les ordinateurs d'extrémité..... | 49 |
| 10 | Configuration centralisée des ordinateurs d'extrémité..... | 58 |
| 11 | Configuration locale des ordinateurs d'extrémité..... | 68 |
| 12 | Installation de SafeGuard Enterprise sur les ordinateurs disposant de plusieurs systèmes d'exploitation..... | 69 |
| 13 | Configuration de la protection de la configuration SafeGuard..... | 71 |
| 14 | Réplication de la base de données SafeGuard Enterprise..... | 77 |
| 15 | Mise à jour de SafeGuard Enterprise..... | 82 |
| 16 | Mise à jour du système d'exploitation | 88 |
| 17 | Mise à niveau de Sophos SafeGuard vers SafeGuard Enterprise..... | 88 |
| 18 | Mise à niveau de SafeGuard Easy 4.x et de Sophos SafeGuard Disk Encryption 4.x vers SafeGuard Enterprise 5.6x..... | 90 |
| 19 | À propos de la désinstallation..... | 97 |
| 20 | Support technique..... | 98 |
| 21 | Mentions légales..... | 99 |

1 Présentation 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 PC et les périphériques terminaux mobiles.

L'administration centralisée est effectuée avec le SafeGuard Management Center. Les stratégies de sécurité, les clés, les certificats, les cartes à puce et les clés cryptographiques 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 de SafeGuard appelé l'authentification au démarrage (POA, Power-On Authentication), assure la protection nécessaire des accès et offre une prise en charge conviviale lors de la récupération des codes d'accès.

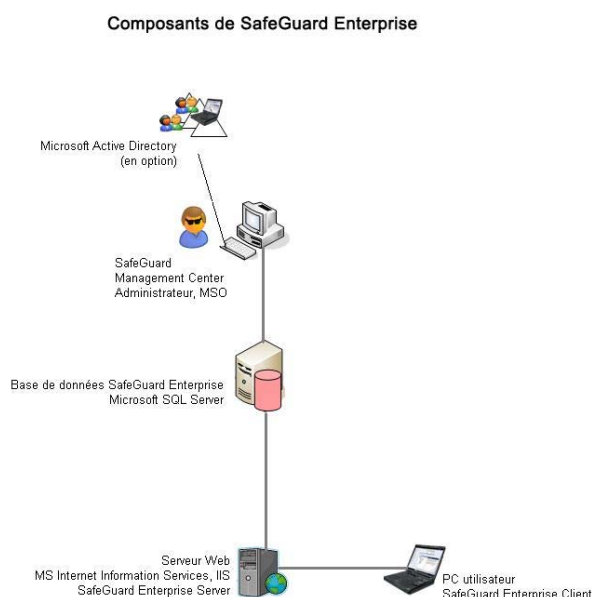
Remarque : nos didacticiels vidéo constituent le moyen idéal pour découvrir SafeGuard Enterprise. Ils figurent avec le produit livré dans la rubrique Didacticiels. Ils décrivent l'installation de SafeGuard Enterprise et l'utilisation du SafeGuard Management Center.

2 Composants de SafeGuard Enterprise

Dans ce chapitre, vous prendrez connaissance des composants de SafeGuard Enterprise et apprendrez comment les composants individuels fonctionnent les uns avec les autres.

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

Les ordinateurs de bureau/portables des utilisateurs 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. Ces bases de données sont accessibles via le serveur SafeGuard Enterprise et uniquement par un seul responsable de la sécurité du SafeGuard Management Center, habituellement le MSO. 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 | Microsoft Internet Information Services (ISS) avec .NET Framework 3.5 SP1 et ASP.NET 2.0. Le serveur Web utilisé pour SafeGuard Enterprise doit être basé sur IIS. Nous recommandons d'utiliser un serveur IIS dédié pour le serveur SafeGuard Enterprise. Le serveur IIS peut être mis en cluster. |
| | Le serveur SafeGuard Enterprise fait l'interface entre la base de données SafeGuard Enterprise et les ordinateurs 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. |
| SafeGuard Management Center avec .NET Framework 3.0 SP1 et ASP.Net 2.0 sur l'ordinateur d'administrateur | Outil de gestion centralisée pour les ordinateurs protégés par SafeGuard Enterprise, la gestion des clés et des certificats, les utilisateurs et les ordinateurs et la création des stratégies SafeGuard Enterprise. Le SafeGuard Management Center communique avec la base de données SafeGuard Enterprise. |

| Composant | Description |
|--|--|
| Services d'annuaire (facultatif) | Importation d'un annuaire actif, qui contient la structure organisationnelle de l'entreprise avec les utilisateurs et les ordinateurs. |
| Le client SafeGuard Enterprise sur les ordinateurs d'extrémité | Logiciel client pour l'authentification et le chiffrement des données sur les ordinateurs d'extrémité. Le client SafeGuard Enterprise (administré) communique avec le serveur SafeGuard Enterprise. En outre, les ordinateurs autonomes, c'est-à-dire les clients Sophos SafeGuard autonomes qui ne sont jamais connectés au serveur SafeGuard Enterprise peuvent être protégés avec SafeGuard Enterprise. |

3 Démarrage

Ce chapitre explique comment préparer l'installation de SafeGuard Enterprise.

- Première installation : un assistant d'installation simplifie la première configuration des composants d'administration, notamment les stratégies par défaut. Pour lancer cet assistant pour les nouvelles installations de SafeGuard Enterprise, démarrez **SGNInstallAdvisor.bat** à partir du répertoire racine du produit.
- Mise à jour de l'installation : suivez les étapes décrites dans cette aide.

3.1 Configuration système requise

Pour 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, consultez la page de configuration requise du site Web de Sophos

(<http://www.sophos.fr/products/enterprise/encryption/safeguard-enterprise/sysreqs.html>).

Concernant les configurations spécifiques requises sur les ordinateurs d'extrémité, reportez-vous à la section [Restrictions générales](#) à la page 52.

3.2 Paramètres de langue

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

3.2.1 Langue de l'assistant de configuration

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 l'anglais.

3.2.2 Langue du SafeGuard Management Center

Pour déterminer la langue du SafeGuard Management Center au sein même du SafeGuard Management Center :

1. Dans le menu **Outils**, cliquez sur **Options**, puis cliquez sur **Général**. Cliquez sur **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.
2. Redémarrez le SafeGuard Management Center après quoi il doit apparaître dans la langue sélectionnée.

3.2.3 Langue de SafeGuard Enterprise sur les ordinateurs d'extrémité

Pour paramétrer la langue de SafeGuard Enterprise sur l'ordinateur d'extrémité, créez une stratégie de type **Paramètres généraux** dans le SafeGuard Management Center et sélectionnez la langue dans le champ **Langue utilisée sur le client** sous **Personnalisation** :

- 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 une langue disponible dans SafeGuard Enterprise est sélectionnée, les fonctions de SafeGuard Enterprise apparaissent dans la langue sélectionnée sur l'ordinateur d'extrémité.

3.3 Interaction avec les autres produits SafeGuard

Notez les interactions suivantes :

3.3.1 Compatibilité avec SafeGuard LAN Crypt

- La version 3.7x de SafeGuard LAN Crypt et la version 5.6x de SafeGuard Enterprise peuvent coexister sur le même ordinateur et sont entièrement compatibles.

Remarque :

Si la version 5.6x de SafeGuard Enterprise est installée en plus de SafeGuard LAN Crypt, le programme d'installation vous avertit que le composant de chargement du profil SGLC est déjà en cours d'utilisation. Ce message est généré car SafeGuard LAN Crypt et SafeGuard Enterprise partagent des composants communs. Vous pouvez donc l'ignorer. Les composants affectés seront mis à jour au redémarrage.

- Les versions antérieures à la version 3.7 de SafeGuard LAN Crypt ne sont pas compatibles avec la version 5.6x de SafeGuard Enterprise et ne peuvent pas coexister sur le même ordinateur.

Si vous essayez d'installer la version 5.6x de SafeGuard Enterprise sur un ordinateur sur lequel la version 3.6x de SafeGuard LAN Crypt ou une version antérieure est déjà installée, l'installation est annulée et un message d'erreur apparaît.

- La version 3.7x de SafeGuard LAN Crypt et les versions de SafeGuard Enterprise antérieures à la version 5.40 ne sont pas compatibles et ne peuvent pas coexister sur un ordinateur.

Si vous essayez d'installer la version 3.7x de SafeGuard LAN Crypt sur un ordinateur sur lequel est déjà installée une version de SafeGuard Enterprise antérieure à la version 5.40, l'installation est annulée et un message d'erreur apparaît.

3.3.2 Compatibilité avec SafeGuard PrivateCrypto et SafeGuard PrivateDisk

La version 5.6x de SafeGuard Enterprise et les produits autonomes SafeGuard PrivateCrypto (à partir de la version 2.30) et SafeGuard PrivateDisk (à partir de la version 2.30) peuvent coexister sur le même ordinateur.

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

3.3.3 Compatibilité avec SafeGuard Removable Media

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

Les clés locales créées avec une version de SafeGuard Removable Media antérieure à la version 1.20 avant de passer à SafeGuard Data Exchange peuvent être utilisées sur le client SafeGuard Enterprise. En revanche, elles ne sont pas transférées automatiquement dans la base de données SafeGuard Enterprise.

3.3.4 Compatibilité avec SafeGuard Easy 4.x

La version 4.x de SafeGuard Easy et la version 5.6.x de SafeGuard Enterprise peuvent être installées sur le même ordinateur tant que le module SafeGuard Device Encryption de SafeGuard Enterprise n'est pas installé. Les deux produits installent leur propre processus d'identification et d'authentification graphique (GINA ou Graphical Identification and Authentication), SafeGuard Enterprise fonctionnera uniquement si le processus GINA lui correspondant est utilisé. Pour garantir une configuration correcte, la version 4.x de SafeGuard Easy doit être installée sans la prise en charge de GINA (utilisez l'option GINASY=0) avant d'installer le module SafeGuard Enterprise approprié. Si la version 4.x de SafeGuard Easy a été installée avec la prise en charge de GINA, elle doit être désinstallée avant de procéder à l'installation de la version 5.6.x de SafeGuard Enterprise.

Remarque :

Lorsque la version 4.x de SafeGuard Easy et le module SafeGuard Data Exchange sont installés sur un ordinateur, les mécanismes GINA de SafeGuard Easy (surtout l'ouverture de session automatique sécurisée de Windows) cessent de fonctionner. En guise de solution, la version 4.x de SafeGuard Easy doit d'abord être installée et les deux produits doivent impérativement être désinstallés ensemble (sans redémarrage) pour éviter les conflits GINA.

3.4 Mesures de sécurité générales

Les ordinateurs sur lesquels le serveur SafeGuard Enterprise, la base de données SafeGuard Enterprise et le SafeGuard Management Center sont exécutés, doivent être protégés contre les attaques locales non autorisées. Voici quelques mesures pratiques qui doivent être prises :

- Faites uniquement appel à des administrateurs de confiance ou appliquez la règle dite des deux personnes.
- Protégez-vous contre les attaques électroniques (pare-feu, configuration sécurisée, analyse de virus, mises à jour régulières, mots de passe renforcés, etc.).
- Protégez-vous contre les accès physiques (par exemple avec des salles sécurisées).

3.5 Sécurisation de la connexion 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 le SafeGuard Management Center peuvent être chiffrées avec SSL.
- La connexion entre le serveur SafeGuard Enterprise et le client SafeGuard Enterprise administré peut être protégée via SSL ou 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.

Remarque :

Nous vous conseillons fortement d'utiliser la communication chiffrée SSL entre le serveur SafeGuard Enterprise et le client SafeGuard Enterprise, sauf pour des configurations de démonstration ou de test. Si, pour une certaine raison, ce n'est pas possible et le chiffrement propriétaire doit être utilisé, il y a une limite supérieure de 1000 clients se connectant à une instance unique du serveur.

Le chiffrement SSL pour SafeGuard Enterprise peut être défini lors de la configuration des composants de SafeGuard Enterprise directement après l'installation. Il est également possible de l'activer ultérieurement à tout moment. Les composants ne doivent pas être réinstallés si SSL est activé ultérieurement. Un nouveau package de configuration peut tout au plus être créé et déployé sur le serveur ou le client concerné.

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

3.5.1 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 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. Sinon, le client et le serveur ne peuvent pas communiquer. 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.

Pour plus d'informations, contactez notre support technique ou consultez :

- <http://msdn2.microsoft.com/en-us/library/ms998300.aspx>
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;316898>
- https://blogs.msdn.com/sql_protocols/archive/2005/11/10/491563.aspx

3.5.2 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 du package de configuration du SafeGuard Management Center. Pour plus d'informations, reportez-vous à la section [Configuration de la connexion au serveur de base de données](#) à la page 33 ou consultez : <http://www.sophos.fr/support/knowledgebase/article/109012.html>.

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

Activez le chiffrement SSL dans l'assistant de configuration initiale du SafeGuard Management Center, reportez-vous à la section [Configuration de la connexion au serveur de base de données](#) à la page 33.

- 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 le client SafeGuard Enterprise (administré) dans l'outil du package de configuration du SafeGuard Management Center, reportez-vous à la section [Création d'un package de configuration de SafeGuard Enterprise \(administré\)](#) à la page 56.

3.6 Étapes d'installation pour SafeGuard Enterprise

Pour installer SafeGuard Enterprise, suivez ces étapes d'installation.

Tous les composants d'installation de SafeGuard Enterprise (packages .msi) sont disponibles dans le produit.

Remarque :

Pour la plupart des packages d'installation client, les versions 64 bits sont disponibles pour les systèmes d'exploitation Windows 7 64 bits et Windows Vista 64 bits (<nom package>_64

.msi). Lorsque le système d'exploitation de l'ordinateur d'extrémité est Windows 7 64 bits ou Windows Vista 64 bits, vous pouvez installer la variante 64 bits des packages "Client" .msi.

| Numéro | Étape | Installation/configuration |
|--------------------------------------|---|--|
| 1 | Préparation des installations. | |
| Serveur SafeGuard Enterprise | | |
| 2 | Configuration de Internet Information Services (IIS) pour SafeGuard Enterprise avec .NET Framework 3.5 et ASP.NET 2.0 | |
| 3 | Configuration supplémentaire pour SSL. | |
| 4 | Installation du serveur SafeGuard Enterprise sur le serveur Web IIS. | SGNServer.msi |
| Base de données SafeGuard Enterprise | | |
| 5 | Configuration de l'authentification du responsable principal de la sécurité de SafeGuard Enterprise. Le compte utilisateur est créé sur le serveur Microsoft SQL. | |
| 6 (facultatif) | Génération des bases de données SafeGuard Enterprise à l'aide d'un script. | Scripts SQL dans le répertoire Outils du produit livré |
| SafeGuard Management Center | | |
| 7 | Configuration du SafeGuard Management Center pour l'administration centralisée (domaines, utilisateurs, clés, stratégies, etc.). | SGNManagementCenter.msi |
| 8 | Configuration de base de l'administration : configuration des connexions à la base de données, génération des bases de données SafeGuard Enterprise et du responsable principal de la sécurité. | Assistant de configuration initiale du SafeGuard Management Center |
| 9 | Enregistrement et configuration du serveur SafeGuard Enterprise : création du package de configuration du serveur et déploiement sur le serveur Web. | Package de configuration du serveur : outil du package de configuration du SafeGuard Management Center |
| 10 | Création ou importation de la structure organisationnelle depuis Active Directory. | SafeGuard Management Center |
| Client SafeGuard Enterprise | | |
| 11 | Installation du package obligatoire d'avant installation pour préparer les ordinateurs d'extrémité à une installation réussie | SGxClientPreinstall.msi |
| 12 | Installation d'un des packages logiciels de chiffrement sur les ordinateurs d'extrémité : | |

| Numéro | Étape | Installation/configuration |
|--------------------|--|---|
| | SafeGuard Device Encryption <ul style="list-style-type: none"> ■ Chiffrement basé sur volume ■ Chiffrement basé sur fichier (SafeGuard Data Exchange) Valide à la fois pour les clients SafeGuard Enterprise administrés et les clients Sophos SafeGuard autonomes. | SGNClient.msi SGNClient_x64.msi |
| | SafeGuard Data Exchange : <ul style="list-style-type: none"> ■ Chiffrement basé sur fichier ■ Sans authentification au démarrage Valide à la fois pour les clients SafeGuard Enterprise administrés et les clients Sophos SafeGuard autonomes. Non disponible pour la prise en charge de BitLocker Device Encryption. | SGNClient_withoutDE.msi SGNClient_withoutDE_x64.msi |
| 13 (facultatif) | Installation de la protection de la configuration SafeGuard : protection des ports et gestion des périphériques sur les ordinateurs d'extrémité. Valable uniquement pour les clients SafeGuard Enterprise administrés, non disponible pour les clients Sophos SafeGuard autonomes. | SGN_CP_Client.msi |
| 14 | Configuration des ordinateurs d'extrémité : génération du package de configuration pour les ordinateurs d'extrémité administrés ou autonomes et installation sur ces derniers. | Package de configuration : outil du package de configuration du SafeGuard Management Center |

3.7 Étapes d'installation du client SafeGuard Enterprise sur plusieurs systèmes d'exploitation (runtime)

Le client d'exécution (Runtime Client) permet de démarrer l'ordinateur depuis un volume d'initialisation secondaire lorsque plusieurs systèmes d'exploitation sont installés et d'accéder à ces volumes lorsqu'ils sont chiffrés par une installation de SafeGuard Enterprise sur le volume principal.

La solution est disponible à la fois pour les clients SafeGuard Enterprise administrés et les clients Sophos SafeGuard autonomes.

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.

Seul le package d'installation de SafeGuard Device Encryption peut être utilisé. Runtime Client ne peut pas être utilisé avec SafeGuard Data Exchange seulement. Lorsque le système

d'exploitation de l'ordinateur d'extrémité est Windows 7 64 bits ou Windows Vista 64 bits, vous pouvez installer la variante 64 bits des packages "Client" .msi.

Pour installer le client SafeGuard Enterprise sur plusieurs systèmes d'exploitation, suivez ces étapes d'installation :

| N ^o | Étape | Description | Installation/configuration |
|----------------|--|---|---|
| 1 | Configurer le système d'exécution sur l'ordinateur d'extrémité. | Installez le package d'exécution du client SafeGuard sur le ou les volumes d'initialisation secondaires de l'ordinateur d'extrémité. | SGNClientRuntime.msi SGNClientRuntime_x64.msi |
| 2 | Configurer le logiciel de chiffrement SafeGuard sur les ordinateurs d'extrémité. | Appliquez la configuration nécessaire sur les ordinateurs d'extrémité pour une installation réussie du logiciel de chiffrement (obligatoire). | SGxClientPreinstall.msi |
| | | Installez le package d'installation de SafeGuard Device Encryption sur le volume d'initialisation principal de l'ordinateur d'extrémité. | SGNClient.msi SGNClient_x64.msi |
| 3 | Configurer les ordinateurs d'extrémité. | Générez le package de configuration pour les ordinateurs d'extrémité administrés ou autonomes et installez-le sur ces derniers. | SGNClientConfig.msi Package de configuration du client généré à l'aide de l'outil de package de configuration du SafeGuard Management Center |

3.8 Préparation à l'installation

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

- Assurez-vous de disposer des droits d'administrateur Windows.
- Fermez toutes les applications ouvertes.
- Consultez la liste des configurations requises sur <http://www.sophos.fr/products/enterprise/encryption/safeguard-enterprise/sysreqs.html>.
- Lisez attentivement les notes de publication.

Concernant les préparations sur l'ordinateur d'extrémité, reportez-vous à la section [Préparation au chiffrement](#) à la page 53.

3.8.1 Téléchargement des programmes d'installation

1. Rendez-vous sur <https://secure.sophos.fr/support/updates/>.
2. Saisissez vos nom utilisateur et mot de passe MySophos.
3. Sur la page Web des téléchargements **Data Protection**, cliquez sur **SafeGuard Enterprise** et téléchargez les programmes d'installation et la documentation de SafeGuard Enterprise.
4. Placez-les à un emplacement auquel vous pouvez accéder pour effectuer l'installation.

4 Configuration du serveur SafeGuard Enterprise

Le serveur SafeGuard Enterprise sert d'interface avec les clients SafeGuard Enterprise. Comme le 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 Microsoft Internet Information Services (IIS).

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 à propos, par exemple, de la version d'ASP.NET à utiliser.

Ce chapitre décrit l'installation du serveur SafeGuard Enterprise sur IIS. Commencez par installer et configurer Microsoft Internet Information Services (IIS).

4.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies :

- Vous devez disposer de droits d'administrateur Windows.
- Microsoft Internet Information Services (IIS) doit être disponible.
IIS est gratuit. Ce programme se trouve, par exemple, sur votre DVD de Windows ou sur le site Web Microsoft.
- Si vous utilisez le chiffrement de transport SSL entre le serveur SafeGuard Enterprise et le client SafeGuard Enterprise, vous devez configurer IIS à l'avance, reportez-vous à la section [Sécurisation de la connexion de transport avec SSL](#) à la page 8.

Un certificat doit être généré et le serveur 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. Sinon, le client et le serveur ne peuvent pas communiquer. 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.

- Le Service Pack 1 de .NET Framework 3.5 doit être disponible.
Ce programme est fourni avec le produit SafeGuard Enterprise.
- La version 2.0.50727 de ASP.NET doit être disponible.

Ce programme se trouve, par exemple, sur votre DVD de Windows. Selon la version Windows de votre ordinateur, il a peut-être déjà été installé par défaut. Vous pouvez aussi le télécharger sur : <http://www.asp.net/> . ASP.NET est gratuit.

4.2 Installation et configuration de Microsoft Internet Information Services (IIS)

Ce chapitre décrit la méthode de préparation de Microsoft Internet Information Services (IIS) devant être exécuté avec le serveur SafeGuard Enterprise.

Les paramètres varient selon la version d'IIS que vous utilisez et selon votre système d'exploitation. Une configuration spécifique est mentionnée pour les serveurs suivants :

- IIS 6 sur Microsoft Windows Server 2003
- IIS 7 sur Microsoft Windows Server 2008

4.2.1 Installation et configuration de IIS 6 sur Microsoft Windows Server 2003

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

1. Sur le menu **Démarrer**, cliquez sur **Panneau de configuration** et sélectionnez **Ajouter ou supprimer des composants Windows**.
2. Dans la liste des **Composants**, cliquez sur **Serveur d'applications**.
3. Dans **Serveur d'applications**, cliquez sur **Détails** et sélectionnez **Services Internet (IIS)**.
4. Sélectionnez également **ASP.NET**.
5. Cliquez sur **OK**.

IIS 6 est installé avec une configuration par défaut pour l'hébergement de ASP.NET.

6. Vérifiez que la page Web apparaît correctement à l'aide de `http://<nom serveur>`. Pour plus d'informations, rendez-vous sur : <http://support.microsoft.com>.

4.2.1.1 Vérification de l'installation et de l'enregistrement de .NET Framework

La version 3.5 SP1 de .NET Framework est requise. Ce programme est fourni avec le produit SafeGuard Enterprise.

Pour vérifiez 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 que la version 3.5 SP1 de .NET Framework apparaît dans la liste. 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 "v3.5".

4.2.1.2 Vérification de l'enregistrement d'ASP.NET sous IIS 6

La version 2.0.50727 de ASP.NET est requise.

Pour vérifier que la bonne version de ASP.NET est installée et enregistrée sur IIS 6 :

1. Ouvrez le **Gestionnaire des services IIS** sur le serveur IIS.
2. Dans la zone de navigation à droite, sous **Internet Information Services**, cliquez sur **SGNSRV (ordinateur local)**, puis sur **Sites Web**.
3. Sous **Sites Web**, cliquez avec le bouton droit de la souris sur **Sites Web par défaut**, et cliquez sur **Propriétés**. Sélectionnez l'onglet **ASP.NET**. La version 2.0.50727 doit apparaître sous **version ASP.NET**.
 - Si cette version apparaît, sélectionnez-la. Cliquez sur **Appliquer**, puis sur **OK**.
 - Si elle n'apparaît pas, saisissez la commande
`aspnet_regiis.exe -i` à l'invite de commande pour vous assurer de l'installation de la version 2.050727 des services ASP.
4. Pour vérifier que la bonne version est installée, saisissez `aspnet_regiis.exe -lv` à l'invite de commande.

La version 2.0.50727 d'ASP.NET doit apparaître.

4.2.1.3 Configuration de ASP.NET pour IIS 6 sous Windows Server 2003 64 bits

Lorsque vous exécutez IIS 6 et voulez installer le serveur SafeGuard Enterprise sous Windows Server 2003 64 bits, exécutez les étapes supplémentaires suivantes :

1. Saisissez la commande suivante : `cscript %SYSTEMDRIVE%\inetpub\adminscripts\adsutil.vbs SET W3SVC/AppPools/Enable32bitAppOnWin64 1`
2. Enregistrez la version requise d'ASP.NET avec la commande suivante : `%SYSTEMROOT%\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe -i`
3. Pour activer la version 32 bits d'ASP.Net 2.0.50727, ouvrez **Gestionnaire des services IIS** sur le serveur IIS.
4. Dans **Gestionnaire des services IIS**, cliquez sur **Serveur (ordinateur local)**, puis sur **Extensions du service Web**.
5. Cliquez avec le bouton droit de la souris sur **ASP.NET v2.0.50727 (32 bit)**, cliquez sur **Propriétés** et définissez l'état sur **Autorisé**.
6. Cliquez sur **Appliquer** et cliquez sur **OK**.

4.2.1.4 Compte d'utilisateur SafeGuard spécifique à IIS 6

Au cours de l'installation d'IIS 6, un utilisateur est créé pour une authentification anonyme à partir du client vers le site SGNSRV sur IIS.

Lorsque le serveur SafeGuard Enterprise est installé sur le serveur IIS, un utilisateur personnalisé **IUSR_SafeGuard** est créé. Grâce à **IUSR_SafeGuard**, vous pouvez toujours utiliser un accès anonyme au site SGNSRV en cas de modification du nom d'hôte IIS.

Sous IIS 6, le nom utilisateur standard est IUSR_MACHINENAME. Si le nom d'hôte IIS est renommé suite à l'installation, il ne correspondra plus au nom utilisateur standard et l'accès anonyme va échouer. Avec **IUSR_SafeGuard**, vous disposez toujours d'un nom de connexion valide même si le nom d'hôte IIS a été renommé.

4.2.2 Installation et configuration de IIS 7 sur Microsoft Windows Server 2008

IIS est gratuit. Ce programme se trouve sur le programme sur votre DVD de Windows ou sur le site Web 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. Sur le côté droit, sélectionnez aussi : **ASP.NET** qui va également sélectionner tous les services des sous-rôles. Puis, sélectionnez **Extensibilité .NET**, **Extensions ISAPI**, **Filtres ISAPI**.
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 7 est installé avec une configuration par défaut pour l'hébergement d'ASP.NET sous Windows Server 2008.

9. Vérifiez que la page Web apparaît correctement à l'aide de `http://<nom serveur>`. Pour plus d'informations, rendez-vous sur : <http://support.microsoft.com>.

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

La version 3.5 SP1 de .NET Framework est requise.

1. Pour vérifier que la bonne version de .NET Framework est installée et enregistrée, reportez-vous à la section [Vérification de l'installation et enregistrement de .NET Framework](#) à la page 14.

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

La version 2.0.50727 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 2.0.50727 d'ASP.NET doit apparaître.

4.2.3 Activation du recyclage de la mémoire

Nous vous conseillons d'activer **Recycler les processus de travail** sous IIS 6 et sous IIS 7.

1. Ouvrez le **Gestionnaire des services IIS** sur le serveur IIS.
2. Dans **Gestionnaire IIS**, cliquez sur **Serveur (ordinateur local)**.
3. Cliquez avec le bouton droit de la souris sur **Pools d'applications**, puis cliquez sur **Propriétés**.
4. Sous **Recyclage de la mémoire**, définissez les valeurs suivantes :
 - a) Mémoire virtuelle maximale = 500 Mo
 - b) Mémoire maximale utilisée = 192 Mo
5. Cliquez sur **Appliquer**, puis sur **OK**.

Le recyclage de la mémoire est désormais activé sous IIS 6 et sous IIS 7.

4.3 Renforcement du serveur IIS

Afin d'améliorer la sécurité de l'intranet de votre entreprise, il est recommandé de protéger tous les serveurs IIS et les applications qui y sont exécutées à l'aide des paramètres de sécurité, de manière à ce qu'ils soient «renforcés».

Ce chapitre décrit la méthode de configuration du serveur IIS de manière à ce qu'il utilise SafeGuard Enterprise Server conformément aux recommandations de sécurisation renforcée de Microsoft. Si d'autres paramètres sont activés et non recommandés par Microsoft ou non conformes aux explications de ce chapitre, les résultats obtenus risquent d'être incorrects.

Remarque :

Retrouvez des informations détaillées sur le renforcement du serveur Web dans les solutions Microsoft for Security and Compliance : le Guide de sécurité Windows Server 2003 disponible gratuitement au téléchargement depuis le site Web de Microsoft.

Les explications de ce chapitre sont basées sur l'exemple de configuration suivant :

■ Serveur1 :

- Microsoft Windows Server2003SP1
- Dernière version de SafeGuard Enterprise Server
- Dernière version du SafeGuard Enterprise Management Center
- Microsoft SQL Server 2005 Express

IIS doté des composants minimaux

■ Serveur 2 :

Microsoft Windows Server2003SP1
Dernière version de SafeGuard Enterprise Server
Microsoft SQL Server 2005 Express
IIS doté des composants minimaux

Seul le Serveur2 exécute SafeGuard Enterprise Server (serveur IIS). Si le Serveur 2 est en cours d'utilisation, les services activés pour le Serveur 1 seront automatiquement désactivés.

■ Client :

Client SafeGuard Enterprise
Dernière version du SafeGuard Enterprise Management Center

4.3.1 Installation des composants IIS requis

Assurez-vous que seuls les composants IIS essentiels et nécessaires sont installés afin de réduire les risques d'attaques du serveur IIS. Désactivez tous les paramètres non requis.

L'ensemble de composants minimal que le serveur IIS doit posséder pour être exécuté avec le serveur SafeGuard Enterprise est le suivant :

- Fichiers communs
- Gestionnaire Internet Information Services (IIS)
- Services World Wide Web

4.3.2 Activation des extensions de service Web importantes

Assurez-vous que seules les extensions de service Web importantes sont activées afin de réduire les risques d'attaques du serveur IIS. Désactivez tous les paramètres non requis.

Les paramètres nécessaires à l'exécution du serveur IIS avec le serveur SafeGuard Enterprise sont les suivants:

Extension de service Web :

- ASP.NET v.1.1.4322 **Interdit**
- ASP.NET v.2.50727 **Autorisé**

4.3.3 Mise en place du contenu d'un site Web sur un volume de disque dédié

IIS stocke les fichiers pour son site Web par défaut dans le dossier suivant :

`%systemroot%\inetpub\wwwroot`

`%systemroot%` est le lecteur sur lequel est installé le système d'exploitation Windows Server 2003.

Déplacez tous les fichiers et dossiers de génération des sites Web et applications sur des volumes de disque dédiés, indépendants du système d'exploitation. Cette opération permet d'éviter les attaques au cours desquelles l'attaquant envoie des requêtes pour un fichier externe à la structure des répertoires d'un serveur IIS.

Dans le cas de l'exemple de configuration, les éléments sont déplacés comme suit :

- Fichiers web IIS dans **E:\inetpub**
- Fichiers Web du serveur SafeGuard Enterprise dans **F:\mycompany.web**

Remarque :

Une fois les fichiers Web déplacés, vous devez mettre à jour en conséquence les informations du chemin d'accès, dans le gestionnaire IIS.

4.3.4 Définition des autorisations NTFS

Les ordinateurs qui exécutent Windows Server2003 SP1 étudient les autorisations du système de fichiers NTFS pour déterminer les types d'accès attribués à un utilisateur/processus concernant un fichier/dossier. Vous devez attribuer les autorisations NTFS de manière à autoriser ou à interdire l'accès au site Web à des utilisateurs spécifiques du serveur IIS.

Dans le cas de l'exemple de configuration, les autorisations NTFS minimales sont les suivantes :

| Utilisateur/Dossier | Autorisations NTFS pour E:\inetpub | Autorisations NTFS pour F:\mycompany.web |
|---------------------|------------------------------------|--|
| Administrateurs | contrôle total | contrôle total |
| Système | contrôle total | contrôle total |
| Utilisateurs | exécution | exécution |

Vous pouvez définir un autre compte ou groupe pour les utilisateurs, du moment qu'il est présent sur le serveur IIS. Dans ce cas, vous devez mettre à jour en conséquence le compte IUSR_SRVERNAME sur le serveur IIS.

Les autorisations NTFS concernant les types de fichier sont les suivantes:

| Type de fichier | Autorisations NTFS recommandées |
|--------------------------------------|---|
| Fichiers CGI (.exe, .dll, .cmd, .pl) | Administrateurs (contrôle total) Système (contrôle total) Tout le monde/Utilisateur (exécution) |
| Fichiers de script (.asp) | Administrateurs (contrôle total) Système (contrôle total) Tout le monde/Utilisateur (exécution) |

| Type de fichier | Autorisations NTFS recommandées |
|--|---|
| Fichiers d'inclusion (.inc, .shtm, .shtml) | Administrateurs (contrôle total) Système (contrôle total) Tout le monde/Utilisateur (exécution) |
| Contenu statique (.txt, .gif, .jpg, .htm, .html) | Administrateurs (contrôle total) Système (contrôle total) Tout le monde/Utilisateur (lecture seule) |

4.3.5 Désactivation de l'authentification Windows intégrée

Nous vous recommandons de désactiver l'authentification Windows intégrée dans IIS pour empêcher l'envoi d'informations d'authentification inutiles.

1. Dans le gestionnaire IIS, cliquez deux fois sur l'ordinateur local, cliquez avec le bouton droit de la souris sur le dossier **Sites Web**, puis cliquez sur **Propriétés**.
2. Cliquez sur l'onglet **Sécurité de répertoire** puis, dans la section **Authentification et contrôle d'accès**, cliquez sur **Edition**.
3. Dans la section **Accès authentifié**, désélectionnez la case **Authentification intégrée de Windows**.
4. Cliquez deux fois sur **OK**.

4.3.6 Paramètres du pool d'applications "DefaultAppPool"

Les paramètres dépendent de l'endroit où le serveur IIS réside :

- Si le serveur SQL réside sur le même ordinateur que le serveur IIS, définissez le compte utilisateur intégré Service local pour "DefaultAppPool". Dans le cas de l'exemple de configuration, il s'agit du Serveur 1.
- Si le serveur SQL réside sur un ordinateur autre que celui du serveur IIS, définissez le compte utilisateur intégré Service réseau pour "DefaultAppPool". Dans le cas de l'exemple de configuration, il s'agit du Serveur 2. Si vous n'effectuez pas cette opération, la synchronisation avec le client échoue.

4.4 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** se trouve dans le produit livré.

1. Démarrez **SGNServer.msi**.
2. Sur la page **Bienvenue**, cliquez sur **Suivant**.
3. Acceptez le contrat de licence.
4. Acceptez le chemin d'installation par défaut.
5. Cliquez sur **Terminer** pour terminer l'installation.

Le serveur SafeGuard Enterprise est installé.

Remarque :

Afin d'améliorer les performances, une fois le serveur SafeGuard Enterprise installé, la concaténation des événements consignés dans le journal est désactivée par défaut pour la base de données SafeGuard Enterprise. Toutefois, sans concaténation, aucune protection d'intégrité n'est appliquée aux événements consignés dans le journal. La concaténation rassemble sous forme de chaînes toutes les entrées du tableau des événements, de manière à ce que la suppression éventuelle d'une entrée soit clairement visible et puisse être contrôlée à l'aide d'une vérification de l'intégrité. Pour utiliser la protection d'intégrité, vous devez définir manuellement la concaténation. Pour plus d'informations, consultez le chapitre *Rapports de l'aide de l'administrateur*.

5 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 SQL Server actuellement pris en charge dans la liste des [configurations requises](#).

Vous pouvez configurer la base de données soit automatiquement à la première configuration dans le 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. Pour plus d'informations, reportez-vous à la section [Droits d'accès à la base de données](#) à la page 22.

Afin d'améliorer les performances, la base de données SafeGuard Enterprise peut être répliquée sur plusieurs serveurs SQL. Pour configurer une duplication de base de données, reportez-vous à la section [Réplication de la base de données SafeGuard Enterprise](#) à la page 77.

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). Pour configurer l'architecture mutualisée (multi-tenancy), reportez-vous à la section [Configurations d'une architecture mutualisée](#) à la page 32.

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-ordinateur. 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.

5.1 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. Pour plus d'informations, reportez-vous à la section [Configuration de SSL](#) à la page 8.

5.1.1 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 le SafeGuard Management Center et délivré uniquement au premier responsable de la sécurité du 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 du SafeGuard Management Center nécessite uniquement les droits en lecture/écriture sur la base de données du SafeGuard Management Center.

La base de données SafeGuard Enterprise peut soit être créée manuellement soit automatiquement lors de la configuration initiale dans le 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 du 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 droits pendant la configuration du 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.

| Droit d'accès | SQL Server 2005, SQL Server 2005 Express | SQL Server 2008, SQL Server 2008 Express |
|--------------------------------|--|--|
| Création de la base de données | | |

| Droit d'accès | SQL Server 2005, SQL Server 2005 Express | SQL Server 2008, SQL Server 2008 Express |
|--------------------------------------|--|---|
| Serveur | db_creator | db_creator |
| Base de données maître | Aucune | Aucune |
| Base de données SafeGuard Enterprise | db_ownerpublic (par défaut) | db_ownerpublic (par défaut) |
| Utilisation de la base de données | | |
| Serveur | Aucune | Aucune |
| Base de données maître | Aucune | Aucune |
| Base de données SafeGuard Enterprise | db_datareaderdd b_datawriter publique (par défaut) | db_datareader db_datawriter publique (par défaut) |

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

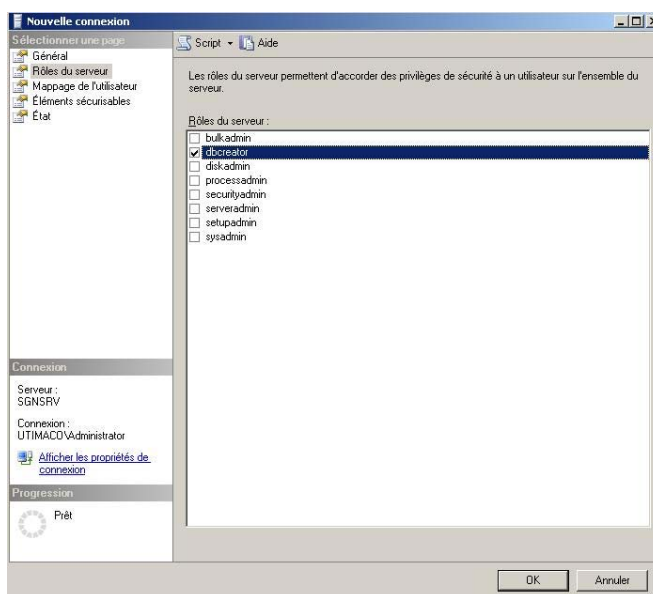
La description des étapes de configuration individuelle ci-dessous est destinée aux administrateurs SQL et concerne Microsoft Windows Server 2008 et Microsoft SQL Server 2008 Standard ou Express Edition. Pour plus d'informations sur l'authentification avec Windows Server 2003 et SQL Server 2005, consultez l'article :

<http://www.sophos.fr/support/knowledgebase/article/108339.html>

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 du SafeGuard Management Center, vous devez changer les droits d'accès. 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**.



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

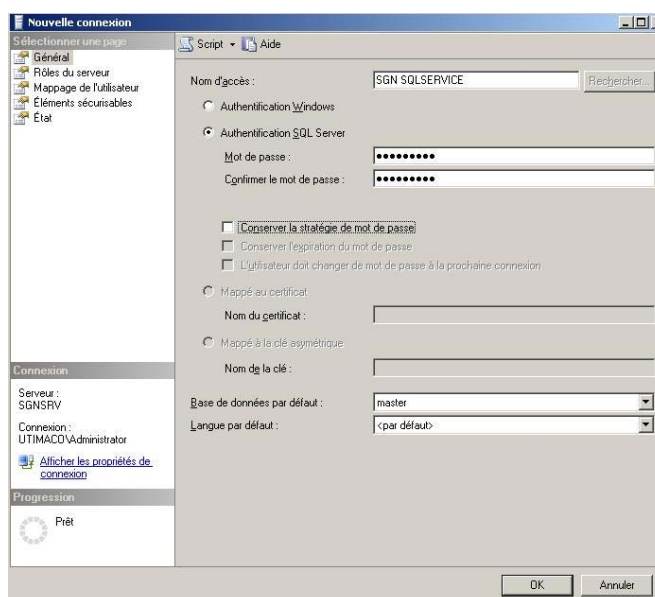
La description des étapes de configuration individuelle décrite ci-dessous s'adresse aux administrateurs SQL. Elle s'applique à Microsoft Windows Server 2003 avec Microsoft SQL Server 2005 et à toutes les éditions de Microsoft Windows Server 2008 avec Microsoft SQL Server 2008 Standard Edition.

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

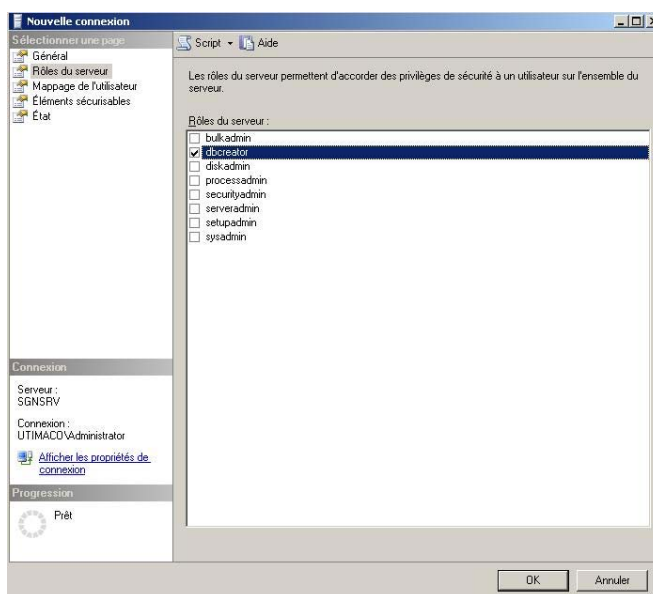
1. Ouvrez SQL Server Management Studio. Connectez-vous à SQL Server à l'aide de vos codes d'accès.
2. Ouvrez l'**Explorateur d'objets**, cliquez avec le bouton droit de la souris sur **Sécurité**, choisissez **Nouveau**, puis cliquez sur **Connexions**.
3. Dans **Connexion - Nouveau** sur la page **Général**, 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) Deselectionnez **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 du SafeGuard Management Center.



- Pour créer automatiquement la base de données lors de la première configuration du SafeGuard Management Center, vous devez changer les droits d'accès. Dans **Connexion - Nouveau** sur la page **Général**, attribuez les droits d'accès/rôles en cliquant sur **Rôles du serveur** sur la gauche puis en sélectionnant **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.

5.2 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 :

- Dans l'assistant de configuration du SafeGuard Management Center

Au titre de responsable de la sécurité, vous pouvez facilement créer la base de données SafeGuard Enterprise suite à l'installation du 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 poursuivre l'installation et la configuration du SafeGuard Management Center, reportez-vous à la section [Configuration du SafeGuard Management Center](#) à la page 30 et pour continuer à changer les droits d'accès adéquats, reportez-vous à la section [Configuration de droits d'accès restreints pour la base de données SafeGuard Enterprise](#) à la page 27.

- Avec des scripts SQL fournis avec le produit

Cette procédure est généralement favorisée si l'extension des autorisations SQL pendant la configuration du 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 clarifier ce point.

5.2.1 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 du SafeGuard Management Center, vous pouvez passer cette étape. Si les permissions SQL étendues ne sont pas souhaitables au cours de la configuration du SafeGuard Management Center, veuillez effectuer cette étape. Deux scripts sont fournis à cet effet dans le produit livré (dossier Outils) :

- 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 pour lancer 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 sur le produit livré 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 la table.

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

5.3 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 le 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 requis pour la connexion à la base de données SafeGuard Enterprise sont décrits.

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 sur **Connexions**.

3. Cliquez avec le bouton droit de la souris sur le nom d'utilisateur respectif et sélectionnez **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**.

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

La description concerne Microsoft Windows Server 2008 (R2) et Microsoft SQL Server 2008 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 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 sélectionnez **Activé**.
6. Cliquez avec le bouton droit de la souris sur le protocole **TCP/IP** et sélectionnez **Activé**.
7. Ensuite, cliquez avec le bouton droit de la souris sur le protocole **TCP/IP** et sélectionnez **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.

5.5 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 2008 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 le SafeGuard Management Center.

1. Sur l'ordinateur hébergeant l'instance SQL Server, cliquez sur **Démarrer**, sélectionnez **Outils d'administration** et 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** depuis la barre de menu, puis, cliquez 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**.

5.6 Exécution d'une configuration supplémentaire lors de l'utilisation d'un compte Windows pour la connexion au serveur SQL

La description concerne Microsoft Windows Server 2008 avec Microsoft SQL Server 2008 Standard Edition et IIS 7. Pour plus d'informations sur l'authentification avec Windows Server 2003 et SQL Server 2005, consultez l'article :

<http://www.sophos.fr/support/knowledgebase/article/108339.html>

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 **Sécurité**.
6. Dans **Sécurité**, cliquez sur **Ajouter**, et sous **Nom d'objet**, saisissez le nom d'utilisateur Windows respectif. Cliquez sur **OK**.
7. Dans **Sécurité**, sous **Autorisations**, sélectionnez **Autorisations spéciales**, puis paramétrez les autorisations spéciales dans la boîte de dialogue **Objet sur Autoriser : Création de fichier/écriture de données**, **Supprimer** et **Autorisations de lecture**.
8. Cliquez sur **OK** et quittez 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 informations d'identification**, 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. Dans le volet **Actions** à droite, sélectionnez **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.

6 Configuration du SafeGuard Management Center

Ce chapitre décrit l'installation et la configuration du SafeGuard Management Center.

Le 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 n'est pas nécessaire d'installer le SafeGuard Enterprise Management Center sur un seul ordinateur uniquement. Il peut être installé sur tout ordinateur du réseau à partir duquel il est possible d'accéder les bases de données SafeGuard Enterprise.

Le SafeGuard Management Center permet de prendre en charge plusieurs bases de données via les configurations mutualisées de base de données (architecture mutualisée). Vous pouvez configurer et conserver différentes bases de données SafeGuard Enterprise pour différents locataires, 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.

6.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies :

- Assurez-vous de disposer des droits d'administrateur Windows.
- .NET Framework 3.0 Service Pack 1 est installé.

.NET Framework est gratuit. Ce programme se trouve, par exemple, sur votre DVD de Windows. Selon la version Windows de votre ordinateur, il a peut-être déjà été installé par défaut. Vous pouvez aussi le télécharger : <http://microsoft.com/downloads>.

- Pour créer une nouvelle base de données SafeGuard Enterprise pendant la configuration du SafeGuard Management Center, vous devez disposer des droits d'accès SQL nécessaires, reportez-vous à la section [Droits d'accès à la base de données](#) à la page 22.

6.2 Installation du 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. Dans la fenêtre de bienvenue, cliquez sur **Suivant**.
3. Acceptez le contrat de licence.
4. Acceptez le chemin d'installation par défaut.
5. Sélectionnez le type d'installation :
 - Pour que le SafeGuard Management Center prenne en charge une seule base de données, sélectionnez **Classique**.
 - Pour que le SafeGuard Management Center prenne en charge plusieurs bases de données (**Architecture mutualisée**), sélectionnez **Complète**. Pour plus d'informations, reportez-vous à la section [Configurations mutualisées](#) à la page 32.
6. Cliquez sur **Terminer** pour terminer l'installation.

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

6.3 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 XP/Windows Vista/Windows 7 - Internet Explorer 6/7/8 - 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.
- Windows 2003 Server Enterprise Edition - Internet Explorer 6 - Configuration de sécurité renforcée (configuration de l'installation par défaut) :

Une boîte de dialogue s'affiche vous informant que la Configuration de sécurité renforcée est activée et que la page exécute les scripts. Vous pouvez désactiver ce message.
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 ne pourront pas être utilisées comme par exemple la fonctionnalité de Recherche.

6.4 Configuration du SafeGuard Management Center

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

Vous pouvez configurer le 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).

6.4.1 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.

Les 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.

6.4.2 Configurations mutualisées

Vous pouvez configurer différentes bases de données SafeGuard Enterprise et les maintenir à jour pour une instance du 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 Server 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 du SafeGuard Management Center, effectuez d'abord la configuration initiale, puis procédez aux étapes plus spécifiques de la configuration partagée.

6.4.3 Démarrage de la configuration initiale du SafeGuard Management Center

Après l'installation du SafeGuard Management Center, vous devez effectuer la configuration initiale. Vous devez exécuter cette opération en mode Single Tenancy et en mode Multi Tenancy.

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

1. Sélectionnez le **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**.

6.4.4 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 le 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 informations d'identification 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 **Authentification au serveur SQL** car ce paramètre chiffrera le transport des informations d'identification SQL. Le chiffrement SSL requiert un environnement SSL actif sur le serveur de base de données SQL que vous avez préalablement configuré, reportez-vous à la section [Sécurisation de la connexion de transport avec SSL](#) à la page 8.

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 le SafeGuard Management Center puisse communiquer avec la base de données :

- Sélectionnez **Utiliser l'authentification Windows NT** pour utiliser vos informations d'identification Windows.

Remarque :

Utilisez ce type d'authentification si votre ordinateur appartient à un domaine. Une configuration supplémentaire est obligatoire car l'utilisateur a besoin d'être autorisé pour se connecter à la base de données, reportez-vous aux sections [Configuration d'un compte Windows pour la connexion au serveur SQL](#) à la page 23 et [Exécution d'une configuration supplémentaire lors de l'utilisation d'un compte Windows pour la connexion au serveur SQL](#) à la page 29.

- Sélectionnez **Utiliser l'authentification SQL Server** pour accéder à la base de données avec vos informations d'identification SQL respectives. 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.

6.4.5 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 appropriés, [voir Droits d'accès à la base de données](#) à la page 22. 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 le 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**.

6.4.6 Création du responsable principal de la sécurité (MSO)

En tant que responsable de la sécurité, vous pouvez accéder au 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 **ID du responsable principal de la sécurité**, saisissez un nom de responsable principal de la sécurité.
2. Sous **Connexion avec la clé cryptographique**, spécifiez si vous voulez utiliser ou non une clé cryptographique/carte à puce pour la connexion.

Au départ, nous vous conseillons de ne pas activer la connexion avec la clé cryptographique comme **Obligatoire**. La connexion avec une clé cryptographique ou une carte à puce nécessite une configuration distincte qui doit être effectuée dans le SafeGuard Management Center.

3. Dans **Certificat pour MSO**, exécutez l'une des actions suivantes :
 - Cliquez sur **Créer** pour créer un nouveau certificat pour MSO. 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 pour MSO**.
 - Cliquez sur **Importer** pour utiliser un certificat pour MSO déjà disponible sur le réseau. Dans **Importer le certificat d'authentification**, recherchez le fichier de clés sauvegardé. Sous **Mot de passe du fichier de clés**, saisissez et confirmez le mot de passe spécifié pour ce fichier. Sélectionnez **Stocker le fichier de clés dans le magasin de certificats** et saisissez le mot de passe pour le magasin. Cliquez sur **OK**. Le certificat est importé et apparaît sous **Certificat pour MSO**.

Le MSO a besoin du magasin de certificats pour se connecter au SafeGuard Management Center. Prenez note de ce mot de passe et conservez-le en lieu sûr ! Si vous le perdez, le MSO ne pourra pas se connecter au SafeGuard Management Center.

Le MSO a besoin du fichier de clés privées pour restaurer une installation interrompue du SafeGuard Management Center.

4. Cliquez sur **Suivant**.

Le responsable principal de la sécurité (MSO) est créé.

6.4.6.1 Création du certificat MSO

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

1. Sous **ID 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 au SafeGuard Management Center.

6.4.6.2 Exportation du certificat MSO

Le certificat MSO est exporté dans un fichier, communément appelé le fichier de clés 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 du 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 clés privées.

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. Pour plus d'informations, consultez le chapitre *Exportation du certificat d'entreprise et du responsable principal de la sécurité* de l'aide de l'administrateur.

6.4.6.3 Importation du certificat 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 **Importer le certificat d'authentification**, cliquez sur [...] et sélectionnez le fichier de clés. Saisissez maintenant le **mot de passe du fichier de clés**. Saisissez le mot de passe du magasin de certificats défini précédemment dans **Mot de passe du magasin de certificat ou code PIN de la carte**. Sélectionnez **Importer dans le magasin de certificats** ou sélectionnez **Copier sur la carte à puce** pour stocker le certificat sur une carte à puce.
2. 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.

6.4.7 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. Donnez un nom de votre choix.
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.

Pour restaurer une configuration de base de données endommagée, reportez-vous à la section [Restauration d'une configuration de base de données corrompue](#) à la page 42.

6.4.8 Configuration initiale complète du SafeGuard Management Center

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

Le SafeGuard Management Center est lancé une fois que l'assistant de configuration s'est fermé.

6.5 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 exécutée, reportez-vous à la section [Démarrage de la configuration initiale du SafeGuard Management Center](#) à la page 33.

Remarque :

Configurez une instance distincte par base de données du serveur SafeGuard Enterprise.

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

1. Démarrez le SafeGuard Management Center. La boîte de dialogue **Sélectionner une configuration** s'affiche.
2. Cliquez sur **Nouveau**. L'assistant de configuration du 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 le 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**.

Le SafeGuard Management Center est lancé et relié à la nouvelle configuration de base de données. Au prochain lancement du SafeGuard Management Center, la nouvelle configuration de base de données peut être sélectionnée dans la liste.

Remarque :

Pour d'autres tâches concernant la configuration mutualisée, reportez-vous à la section *Fonctionnement avec plusieurs configurations de base de données* de l'aide de l'administrateur.

6.6 Configuration des instances supplémentaires du SafeGuard Management Center

Vous pouvez configurer des instances supplémentaires du SafeGuard Management Center pour donner l'accès aux responsables de la sécurité pour l'exécution des tâches administratives sur différents ordinateurs. Le SafeGuard Management Center peut être installé sur n'importe quel ordinateur du réseau permettant d'accéder aux 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 le 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 Server**, 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 Mutualisé 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 **Importer le certificat d'authentification**, cliquez sur [...] et sélectionnez le fichier de clés. Saisissez maintenant le **mot de passe du fichier de clés**. Saisissez le mot de passe du magasin de certificats défini précédemment dans **Mot de passe du magasin de certificats ou code PIN de la carte**. Sélectionnez **Importer dans le magasin de certificats** ou sélectionnez **Copier sur la carte à puce** pour stocker le certificat sur une carte à puce.
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.

6.7 Connexion au SafeGuard Management Center

La connexion au SafeGuard Management Center dépend du mode d'exécution : Indépendant ou Mutualisé.

Pour en savoir plus sur les premières étapes dans le SafeGuard Management Center, reportez-vous à l'aide de l'administrateur de SafeGuard Enterprise.

6.7.1 Connexion en mode Indépendant

1. Démarrez le 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**.

Le 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 le journal.

6.7.2 Connexion en mode Mutualisé

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

1. Démarrez le SafeGuard Management Center à partir du dossier des produits dans le menu **Démarrer**. La boîte de dialogue **Sélection de configurations** apparaît.
2. Sélectionnez la configuration de base de données que vous souhaitez utiliser dans la liste et cliquez sur **OK**. La configuration de base de données sélectionnée est connectée au SafeGuard Management Center et s'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**.

Le 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 le journal.

6.8 Installation de la structure organisationnelle dans le SafeGuard Management Center

Deux méthodes vous permettent de mapper 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 méthodes ou combiner les deux. Par exemple, vous pouvez importer un service Active Directory (AD) partiellement ou intégralement, et créer manuellement d'autres unités organisationnelles. Si la structure organisationnelle est importée ou créée manuellement, l'attribution des stratégies est assurée de toutes manières.

Remarque :

Sachez qu'en combinant les deux méthodes, les unités organisationnelles créées manuellement ne sont pas mappées dans le service AD. Si les unités organisationnelles créées dans SafeGuard Enterprise doivent être mappées dans AD, vous devez les ajouter séparément à AD.

Remarque :

Pour plus d'informations sur l'importation ou la création d'une structure organisationnelle, reportez-vous au chapitre *Configuration de la structure organisationnelle* de l'Aide de l'administrateur.

6.9 Importation du fichier de licence

SafeGuard Enterprise dispose d'un compteur de licences intégré. Par défaut, un nombre fixe de 5 licences pour chaque module SafeGuard Enterprise disponible fait partie de l'installation. Ceci doit permettre une évaluation facile d'autres modules SafeGuard Enterprise sans aucun effet secondaire. En revanche, lors de l'achat de SafeGuard Enterprise, chaque client reçoit un fichier de licence personnalisé pour son entreprise qui doit être importé dans le SafeGuard Management Center.

Pour plus d'informations, consultez le chapitre *Licences* de l'aide de l'administrateur.

6.10 Restauration de l'installation corrompue du SafeGuard Management Center

Si l'installation du SafeGuard Management Center est corrompue mais la base de données est toujours intacte, l'installation peut être restaurée en réinstallant le 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 également connaître les mots de passe de ce fichier .p12, ainsi que du magasin de certificats.

Pour restaurer l'installation corrompue du SafeGuard Management Center :

1. Réinstallez le package d'installation du SafeGuard Management Center. Ouvrez le SafeGuard Management Center. L'assistant de configuration démarre automatiquement.
2. Dans **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. Dans **Paramètres de base de données**, cliquez sur **Sélectionner une base de données disponible** et sélectionnez dans la liste la base de données correspondante.
4. Dans **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 le 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 le SafeGuard Management Center.

5. Cliquez sur **Suivant**, puis sur **Terminer** pour achever la configuration du SafeGuard Management Center.

L'installation corrompue du SafeGuard Management Center est restaurée.

6.11 Restauration d'une configuration de base de données corrompue

La configuration corrompue d'une base de données peut être restaurée en réinstallant le 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. Cette procédure évite de devoir configurer et restaurer de zéro l'intégralité de la base de données.

- 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 le SafeGuard Management Center. Pour plus d'informations, consultez l'aide de l'administrateur.
- Vous devez également connaître les mots de passe de ces deux fichiers .p12, ainsi que du magasin de certificats.

Pour restaurer une base de données corrompue :

1. Réinstallez le package d'installation du SafeGuard Management Center. Ouvrez le SafeGuard Management Center. L'assistant de configuration démarre automatiquement.
2. Dans **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. Dans **Données du responsable de la sécurité**, sélectionnez le responsable principal de la sécurité correspondant, puis cliquez sur **Importer**.
4. Dans **Importer le certificat d'authentification**, recherchez le fichier de clés sauvegardé. Sous **Mot de passe du fichier de clés**, saisissez et confirmez le mot de passe spécifié pour ce fichier. Sélectionnez **Stocker le fichier de clés 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. Dans **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.

7 Test de la communication

Une fois que le serveur SafeGuard Enterprise, la base de données et le SafeGuard Management Center ont été configurés, vous devez exécuter un test de connexion. Ce chapitre décrit les étapes requises.

7.1 Conditions préalables

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

7.1.1 Ports/connexions

Les ordinateurs d'extrémité doivent créer les connexions suivantes :

| Connexion du client SafeGuard à | Port |
|---------------------------------|--|
| Serveur SafeGuard Enterprise | Port 80/TCP Port 443 lors de l'utilisation de la connexion de transport SSL |

Le SafeGuard Management Center doit créer les connexions suivantes :

| Connexion du SafeGuard Management Center à | Port |
|--|---|
| Base de données SQL | Port dynamique SQL Server 2005/SQL Server 2008 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 2005 (Express) |
| Active Directory | Port 389/TCP |

7.1.2 Méthode d'authentification

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

2. Dans l'arborescence, cliquez sur **Internet Information Services**. 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 accès anonyme**. Sous **Accès authentifié**, dessélectionnez la case **Authentification intégrée de Windows**.

7.1.3 Paramètres du serveur proxy pour le serveur Web et l'ordinateur d'extrémité

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**.

7.1.4 Paramètres de Microsoft SQL Server 2005

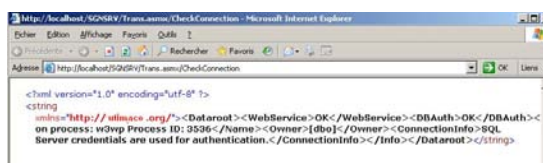
Lors de l'utilisation de Microsoft SQL Server 2005, procédez de la manière suivante :

1. Ouvrez Microsoft SQL Server Management Studio.
2. Dans le volet gauche de l'**Explorateur d'objets**, naviguez vers **Sécurité**.
3. Cliquez avec le bouton droit de la souris sur **Connexions** et cliquez sur **Nouvelle connexion**. Ajoutez l'utilisateur suivant dans Microsoft SQL Server Management Studio (rôle "sysadmin") : NT AUTHORITY\NETWORK SERVICE.

7.2 Test de connexion (IIS 6 sous Windows Server 2003)

1. Sur l'ordinateur sur lequel est installé le serveur SafeGuard Enterprise, ouvrez le **Gestionnaire des services IIS**.
2. Dans l'arborescence, cliquez sur **Internet Information Services**. Cliquez sur **"Nomserveur", Sites Web, Site Web par défaut**. Assurez-vous 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**, puis cliquez sur **Parcourir**. Une liste d'actions possibles apparaît à droite de la fenêtre.
4. Dans cette liste, sélectionnez **Vérifier la connexion**. L'action possible apparaît à droite de la fenêtre.
5. Pour tester la connexion, cliquez sur **Appeler**.

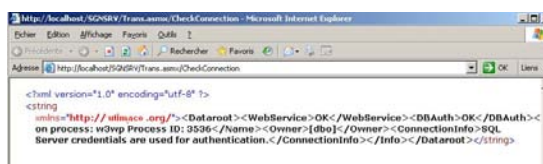
Le test de connexion est un succès lorsque les résultats suivants apparaissent :



7.3 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 IIS**.
2. Dans l'arborescence, cliquez sur "**Nomserveur**", **Sites**, **Site Web par défaut**. Assurez-vous 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 **Application** et cliquez sur **Parcourir** pour ouvrir la page d'**Accueil de SGNSRV Sophos SafeGuard Web Service**.
4. Sur la page **Sophos SafeGuard Web Service**, une liste d'actions possibles apparaît.
5. Dans cette liste, cliquez sur **Check Connection**.
6. Sur la page **Check Connection**, cliquez sur **Invoke**.

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



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 le client SafeGuard. Les informations sont stockées dans un package de configuration de serveur (MSI).

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

Après l'installation du 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 la fonctionnalité mutualisée est installée.

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

La configuration du serveur SafeGuard Enterprise démarre automatiquement.

5. 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 **Enregistrer le serveur**. 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 le package de configuration du serveur obsolète. 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 une utilisation sur un ordinateur différent

Après l'installation du serveur SafeGuard Enterprise sur un ordinateur différent de celui sur lequel se trouve le SafeGuard Management Center, enregistrez et configurez le serveur SafeGuard Enterprise :

1. Démarrez le SafeGuard Management Center.
2. Dans le menu **Outils**, cliquez sur **Outil du package de configuration**.
3. Sélectionnez l'onglet **Enregistrer le serveur**, 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 est situé 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 le SafeGuard Management Center, ce fichier .cer doit être accessible sous la forme d'une copie ou d'une autorisation réseau.

Ne sélectionnez pas le certificat MSO.

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

Remarque :

Si vous utilisez le chiffrement de transport SSL entre le client et le serveur, le nom du serveur spécifié ici doit être identique à celui qui est spécifié dans le certificat SSL, faute de quoi le client et le serveur ne peuvent pas communiquer.

5. Cliquez sur **OK**.

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

6. Cliquez sur l'onglet **Créer un package de configuration de serveur**. Les serveurs disponibles sont affichés. Sélectionnez le serveur requis. Spécifiez 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 **Enregistrer le serveur**, 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. A tout moment, vous pouvez changer la configuration du serveur dans l'onglet **Enregistrer le serveur**.

Remarque :

Si vous voulez installer un nouveau package de configuration du serveur (MSI) sur le serveur SafeGuard Enterprise, veillez à désinstaller le package de configuration du serveur obsolète. 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 Changement des paramètres de configuration 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 SafeGuard Management Center **Outil de package de configuration**, sélectionnez le serveur requis dans l'onglet **Enregistrer le serveur**.

2. 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. |
| Rôles du serveur | Cliquez pour sélectionner/désélectionner 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 | <p>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. Pour plus d'informations, reportez-vous à la section Configuration de la connexion au serveur de base de données à la page 33. 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.</p> <p>Remarque :</p> <p>Il n'est pas nécessaire de relancer l'assistant de configuration du 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 une fois le package du serveur à jour installé sur le serveur.</p> |

3. Créez un nouveau package de configuration du serveur dans l'onglet **Créer un package de configuration de serveur**.
4. Désinstallez le package de configuration du serveur obsolète, 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 client 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 nécessaires 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. Pour plus d'informations, reportez-vous à la section [Enregistrement et configuration du serveur SafeGuard Enterprise pour une utilisation sur un ordinateur différent](#) à la page 46.

9 Configuration de SafeGuard Enterprise sur les ordinateurs d'extrémité

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.

9.1 Configurations SafeGuard pour les ordinateurs d'extrémité

Vous pouvez configurer les ordinateurs d'extrémité comme suit :

■ Clients SafeGuard Enterprise administrés

Administration centralisée basée sur serveur dans le SafeGuard Management Center.

Pour les clients SafeGuard Enterprise administrés, il existe une connexion au serveur SafeGuard Enterprise. 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.

■ Clients Sophos SafeGuard autonomes

Administration locale dans le SafeGuard Management Center.

Les clients Sophos SafeGuard autonomes 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.

La différence majeure entre un client SafeGuard Enterprise administré et un client Sophos SafeGuard autonome est que ce dernier reçoit les stratégies SafeGuard Enterprise uniquement via un package de configuration. Ils ne reçoivent jamais de stratégies via une connexion établie avec le serveur SafeGuard Enterprise.

Les stratégies SafeGuard Enterprise sont créées dans le 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.

9.1.1 Packages d'installation pour clients SafeGuard Enterprise administrés

Remarque :

Lorsque le système d'exploitation de l'ordinateur d'extrémité est Windows 7 64 bits ou Windows Vista 64 bits, vous pouvez installer la variante 64 bits des packages d'installation "Client" (<nom du package>_x64.msi). Le package 64 bits du client de protection de la configuration est disponible pour Windows 7 64 bits.

Le tableau suivant affiche les packages d'installation disponibles pour les clients SafeGuard Enterprise (administrés).

| Package | Description |
|--|--|
| SGxClientPreinstall.msi | Doit être installé sur les ordinateurs d'extrémité avant le logiciel de chiffrement (obligatoire). Fournit aux ordinateurs d'extrémité tous les éléments nécessaires à la configuration requise afin de garantir la réussite de l'installation du logiciel de chiffrement. |
| SGNClient.msi SGNClient_x64.msi | Destiné aux clients SafeGuard Enterprise natifs et aux clients SafeGuard Enterprise prenant en charge BitLocker. SafeGuard Enterprise Device Encryption Chiffrement basé sur volume avec authentification au démarrage SafeGuard Data Exchange Facilité d'échange de données avec des supports amovibles sur toutes les plates-formes sans rechiffrement Chiffrement basé sur fichier |
| SGNClient_withoutDE.msi SGNClient_withoutDE_x64.msi | Ce package n'est pas disponible pour les clients SafeGuard Enterprise prenant en charge BitLocker. SafeGuard Data Exchange Facilité d'échange de données avec des supports amovibles sur toutes les plates-formes sans rechiffrement Chiffrement basé sur fichier Sans authentification au démarrage |
| SGN_CP_Client.msi SGN_CP_Client_x64.msi | Destiné aux clients SafeGuard Enterprise natifs et aux clients SafeGuard Enterprise prenant en charge BitLocker. La variante 64 bits de ce package est disponible pour les systèmes d'exploitation Windows 7 64 bits. Protection de la configuration Protection des ports et gestion des périphériques |
| SGNClientRuntime.msi SGNClientRuntime_x64.msi | Client runtime permettant le démarrage de l'ordinateur depuis un volume d'initialisation secondaire lorsque plusieurs systèmes d'exploitation sont installés. L'accès à ces volumes lorsqu'ils |

| Package | Description |
|---------|--|
| | sont chiffrés par une installation SafeGuard Enterprise sur le volume principal. |

9.1.2 Packages d'installation pour les clients Sophos SafeGuard autonomes

Remarque :

Lorsque le système d'exploitation de l'ordinateur d'extrémité est Windows 7 64 bits ou Windows Vista 64 bits, vous pouvez installer la variante 64 bits des packages d'installation "Client" (<nom du package>_x64.msi).

Le tableau suivant affiche les packages d'installation disponibles pour les clients Sophos SafeGuard (autonomes).

| Package | Description |
|--|--|
| SGxClientPreinstall.msi | Doit être installé sur les ordinateurs d'extrémité avant le logiciel de chiffrement (obligatoire). Afin de garantir la réussite de l'installation du logiciel de chiffrement, vous devez fournir aux ordinateurs d'extrémité la configuration requise. |
| SGNClient.msi SGNClient_x64.msi | SafeGuard Enterprise Device Encryption Chiffrement basé sur volume avec authentification au démarrage SafeGuard Data Exchange Facilité d'échange de données avec des supports amovibles sur toutes les plates-formes sans rechiffrement Chiffrement basé sur fichier |
| SGNClient_withoutDE.msi SGNClient_withoutDE_x64.msi | SafeGuard Data Exchange Facilité d'échange de données avec des supports amovibles sur toutes les plates-formes sans rechiffrement Chiffrement basé sur fichier Sans authentification au démarrage |
| SGNClientRuntime.msi SGNClientRuntime_x64.msi | Client runtime permettant le démarrage de l'ordinateur depuis un volume d'initialisation secondaire lorsque plusieurs systèmes d'exploitation sont installés. L'accès à ces volumes lorsqu'ils sont chiffrés par une installation SafeGuard Enterprise sur le volume principal. |

9.2 Restrictions

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

9.2.1 Restrictions générales

Notez les restrictions générales suivantes pour les clients SafeGuard Enterprise :

- SafeGuard Enterprise pour Windows ne prend pas en charge le matériel d'Apple et ne peut pas être installé dans un environnement Bootcamp.
- Si vous utilisez le mécanisme Intel Advanced Host Controller Interface (AHCI) sur l'ordinateur, 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 à base de volume pour les volumes ne se trouvant pas sur les disques dynamiques et sur les disques de table de partition GUID (GPT) ne sont pas pris en charge. Dans ces cas-là, l'installation est interrompue. Si de tels disques sont trouvés sur l'ordinateur ultérieurement, ils ne sont pas pris en charge.
- Le module SafeGuard Enterprise Device Encryption ne prend pas en charge les systèmes équipés de disques durs reliés par un bus SCSI.

9.2.2 Restrictions pour les clients SafeGuard Enterprise administrés

Notez les restrictions suivantes pour le chiffrement initial des clients administrés.

- Restrictions pour le chiffrement initial :

La configuration initiale des clients SafeGuard Enterprise (administrés) peut impliquer la création de stratégies de chiffrement pouvant être distribuées aux clients SafeGuard Enterprise sous forme de package de configuration.

Toutefois, lorsque le client 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 sur le client SafeGuard Enterprise :

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 le client SafeGuard Enterprise, les packages de configuration correspondants doivent également être réaffectés à l'unité organisationnelle du client. Les clés définies par l'utilisateur sont créées uniquement lorsque la connexion entre le client SafeGuard Enterprise et le serveur SafeGuard Enterprise est rétablie.

Cela est dû au fait que la clé machine définie est directement créée sur le client SafeGuard Enterprise lors du premier redémarrage après installation, alors que les clés définies par l'utilisateur ne peuvent être créées sur le client SafeGuard Enterprise qu'une fois que ce dernier a été enregistré sur le serveur SafeGuard Enterprise.

- Restrictions pour la prise en charge de BitLocker Device Encryption :

Les packages d'installation SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi ne sont pas disponibles pour l'utilisation avec BitLocker Device Encryption.

Remarque :

Le chiffrement basé sur volume SafeGuard Enterprise ou BitLocker Device Encryption peuvent être utilisés sous Windows Vista ou Windows 7, mais pas les deux méthodes de chiffrement simultanément. Pour changer de type de chiffrement, déchiffrez d'abord toutes les partitions, désinstallez le package d'installation du client SafeGuard Enterprise, puis réinstallez-le avec les fonctions souhaitées. L'installation est interrompue si vous essayez d'installer les deux fonctions en même temps.

9.2.3 Restrictions pour les clients Sophos SafeGuard autonomes

Les fonctions suivantes ne sont pas prises en charge avec les clients Sophos SafeGuard autonomes :

- BitLocker Device Encryption, BitLocker To Go
- Protection de la configuration

9.3 Préparation au chiffrement

Avant de déployer SafeGuard Enterprise, nous vous recommandons de vous préparer comme suit.

- Pour effectuer les opérations de préparation générale, reportez-vous à la section [Préparation à l'installation](#) à la page 12.
- Un compte utilisateur doit être configuré et actif sur les ordinateurs d'extrémité.
- Créez une sauvegarde complète des données sur l'ordinateur d'extrémité.
- Sophos fournit une liste des configurations matérielles afin de réduire le risque de conflits entre l'authentification au démarrage et le matériel de votre ordinateur. La liste est fournie avec le package d'installation du logiciel de chiffrement.

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 : <ftp://POACFG:POACFG@ftp.ou.utimaco.de>

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.

Pour plus d'informations, voir

<http://www.sophos.fr/support/knowledgebase/article/110285.html> et
<http://www.sophos.fr/support/knowledgebase/article/65700.html>.

- Recherchez les erreurs sur le ou les disques durs à l'aide de la commande suivante :

chkdsk %lecteur% /F /V /X

Dans certains cas, vous pouvez être invité à redémarrer votre ordinateur et à exécuter de nouveau la commande **chkdsk**. Pour plus d'informations, consultez :

<http://www.sophos.fr/support/knowledgebase/article/107799.html>

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

Windows XP : Sélectionnez **Application, Winlogon**.

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

- Utilisez la fonction de défragmentation de Windows pour localiser et consolider les éléments fragmentés, notamment les fichiers d'initialisation, les fichiers de données et les dossiers sur les volumes locaux. Pour plus d'informations, rendez-vous sur : <http://www.sophos.fr/support/knowledgebase/article/109226.html>.
- Désinstallez les gestionnaires d'initialisation tiers, tels que PROnetworks Boot Pro et Boot-US.
- Si vous avez utilisé un outil d'imagerie/clonage, nous vous recommandons de remplacer le MBR. Pour installer Sophos SafeGuard, votre MBR (Master Boot Record) doit être unique et sain. Il se peut que, suite à l'utilisation d'outils d'imagerie/clonage, le MBR ne soit plus sain.

Vous pouvez nettoyer le MBR (Master Boot Record) en démarrant à partir d'un DVD Windows et en exécutant la commande **FIXMBR** dans la Console de récupération Windows. Pour plus d'informations, rendez-vous sur :

<http://www.sophos.fr/support/knowledgebase/article/108088.html>

- Si la partition d'initialisation a été convertie du format FAT au format NTFS et si le système n'a pas encore été redémarré, n'installez pas SafeGuard Enterprise. Il se peut que l'installation ne soit pas terminée car le système de fichiers était encore au format FAT lors de l'installation mais que c'est le format NTFS qui a été détecté au moment de l'activation. Le cas échéant, vous devez redémarrer l'ordinateur une fois avant l'installation de SafeGuard Enterprise.
- Pour les clients SafeGuard Enterprise (administrés) seulement : vérifiez s'il existe une connexion avec le 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 est établie avec succès. Pour plus d'informations, reportez-vous à la section [Test de la connexion \(IIS 6 sur Windows Server 2003\)](#) à la page 44.

9.3.1 Préparations spécifiques pour la prise en charge de BitLocker Drive Encryption

Remarque :

Avant l'installation, décidez si vous souhaitez utiliser SafeGuard Enterprise en association avec BitLocker Drive Encryption ou uniquement le chiffrement basé sur volume 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 Vista Enterprise ou Ultimate ou Windows 7 doit être installé sur l'ordinateur d'extrémité.

- Une seconde partition doit exister pour le volume système de BitLocker, la partition en texte au format NTFS contenant au moins 1,5 Go. Microsoft fournit un outil de partitionnement BitLocker.
- BitLocker Device Encryption doit être installé et activé.
- Si TPM doit être utilisé pour l'authentification, TPM doit être initialisé 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 BitLocker Drive Encryption. Dans le cas contraire, le système risque d'être endommagé.
- Pour installer la prise en charge de BitLocker Drive Encryption, désactivez le contrôle d'accès d'utilisateur ou ouvrez une session à l'aide du compte administrateur intégré.

Pour plus d'informations, contactez le support technique Microsoft ou consultez les sites Web suivants :

- Préparation de BitLocker :

<http://technet2.microsoft.com/WindowsVista/en/library/c61f2a12-8ac6-4957-b031-97b4d762c311033.mspx?mf=true>

- FAQ sur BitLocker :

<http://technet2.microsoft.com/WindowsVista/en/library/58358421-a7f5-4c97-ab41-2bcc61a58a701033.mspx?mf=true>

9.3.2 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 un 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. Ce message peut être ignoré 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 À propos de la création de packages de configuration

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

- Pour les clients SafeGuard Enterprise administrés
- Pour les clients Sophos SafeGuard autonomes
- Lors de l'utilisation de comptes de service pour la tâche d'après installation

9.4.1 Création d'un package de configuration SafeGuard Enterprise (administré)

1. Dans le SafeGuard Management Center, dans le menu **Outils**, cliquez sur **Outil du package de configuration**.

2. Sélectionnez **Créer un package de configuration (administré)**.
3. Cliquez sur **Ajouter un package de configuration**.
4. Donnez un nom au package de configuration.
5. Attribuez un serveur principal SafeGuard Enterprise (le serveur secondaire n'est pas indispensable).
6. Si besoin est, spécifiez un groupe de stratégies qui doit avoir été créé auparavant dans le SafeGuard Management Center qui sera appliqué aux ordinateurs. Si vous voulez utiliser des comptes de service utilisateur pour les tâches d'après installation sur l'ordinateur, assurez-vous d'inclure le paramètre de stratégie respectif dans ce premier groupe de stratégie, [voir Comptes de service pour les tâches d'après installation](#) à la page 57.
7. Sélectionnez le mode **Chiffrement du transport** définissant comment chiffrer la connexion entre le client SafeGuard Enterprise et le serveur SafeGuard Enterprise : chiffrement Sophos ou SSL.

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. Pour plus d'informations, [voir Configuration de SSL](#) à la page 8.

8. Spécifiez 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 ce package sur le client SafeGuard Enterprise (administré) et le déployer sur celui-ci.

9.4.2 Création d'un package de configuration Sophos SafeGuard (autonome)

1. Dans le SafeGuard Management Center, dans le menu **Outils**, cliquez sur **Outil du package de configuration**.
2. Sélectionnez **Créer un package de configuration (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 le SafeGuard Management Center et que vous souhaitez appliquer aux ordinateurs.

6. Sous **Emplacement de la sauvegarde de la clé**, spécifiez ou sélectionnez un chemin réseau partagé pour le stockage du fichier de récupération de clé. Saisissez le chemin de partage sous la forme suivante : `\\ordinateurréseau\`, par exemple `\\monentreprise.edu\`. Si vous ne spécifiez 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 Sophos SafeGuard. Il est généré sur chaque ordinateur protégé par Sophos SafeGuard.

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 à des fins de récupération. Il peut également être envoyé par courriel.

7. Sous **Groupe d'authentification au démarrage**, vous pouvez sélectionner le groupe de comptes d'accès d'authentification au démarrage que vous souhaitez affecter à l'ordinateur d'extrémité. Une fois l'authentification au démarrage activée, les comptes d'accès d'authentification au démarrage fournissent un accès à l'ordinateur d'extrémité pour effectuer des tâches administratives. Pour attribuer des comptes d'accès POA, le groupe d'authentification au démarrage doit avoir été préalablement créé dans la zone **Utilisateurs et ordinateurs** du SafeGuard Management Center.
8. Spécifiez 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 ce package aux ordinateurs d'extrémité et le déployer sur ceux-ci.

9.4.3 Comptes de service pour les tâches d'après 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 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 l'ordinateur d'extrémité après l'installation est considéré, dans l'authentification au démarrage, comme étant le compte principal. Les utilisateurs inclus dans ces listes sont, en revanche, traités comme des utilisateurs invités SafeGuard Enterprise.

Avec les comptes de service, le flux de travail est le suivant :

- SafeGuard Enterprise est installé sur un ordinateur d'extrémité.
- Après le redémarrage de l'ordinateur, 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 à l'ordinateur, l'utilisateur est identifié comme un compte de service et traité comme utilisateur invité.

- L'opérateur en charge du déploiement n'est pas ajouté à la POA et l'authentification au démarrage ne sera pas active. L'utilisateur final peut se connecter et activer la POA.

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. Pour plus d'informations, consultez l'aide de l'administrateur.

10 Configuration centralisée des ordinateurs d'extrémité

La configuration centralisée des ordinateurs d'extrémité permet de garantir une installation standardisée sur plusieurs ordinateurs.

L'installation et la configuration sont décrites pour les clients SafeGuard Enterprise administrés et les clients Sophos SafeGuard autonomes. La procédure d'installation est identique sauf que vous attribuez un package de configuration différent pour chacun.

Les tâches requises pour l'installation des ordinateurs d'extrémité avec Windows BitLocker Device Encryption sont également décrites. Pour plus de détails sur la préparation de la prise en charge BitLocker, voir [Préparations spécifiques pour la prise en charge de BitLocker Drive Encryption](#) à la page 54.

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 l'aide utilisateur.

Remarque :

Dans le cadre de la distribution centralisée des logiciels, les packages d'installation et de configuration doivent uniquement être attribués à un ordinateur et pas à un utilisateur.

10.1 Installation centralisée du logiciel de chiffrement

1. Préparez les ordinateurs d'extrémité à l'installation en vous reportant à la section [Préparation au chiffrement](#) à la page 53.

- 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 :

| Élément | Description |
|--|--|
| Package d'installation de préparation SGxClientPreinstall.msi | Le package fournit aux ordinateurs d'extrémité la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement, notamment le fichier DLL MSVCR80.dll , version 8.0.50727.4053. Remarque : Si ce package n'est pas installé, l'installation du logiciel de chiffrement échoue. |
| Package d'installation du logiciel de chiffrement | Concernant les packages disponibles pour les clients administrés, voir Packages d'installation pour les clients SafeGuard Enterprise (administrés) à la page 50. Concernant les packages disponibles pour les clients autonomes, reportez-vous à la section Packages d'installation pour les clients Sophos SafeGuard (autonomes) à la page 51. |
| Package de configuration pour ordinateurs d'extrémité | Utilisez les packages de configuration créés auparavant dans le SafeGuard Management Center. Des packages de configuration différents doivent être installés pour les ordinateurs d'extrémité administrés et autonomes, reportez-vous à la section À propos de la création de packages de configuration à la page 55. Avant d'installer un nouveau package de configuration, assurez-vous de désinstaller tous ceux obsolètes. |
| Script avec les commandes de l'installation préconfigurée | Nous recommandons l'utilisation de l'outil de ligne de commande de Windows Installer msiexec pour créer le script. Pour plus d'informations, reportez-vous à la section Commande pour l'installation centralisée à la page 60 ou consultez http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx . |

- Créez un dossier appelé **Logiciels** à utiliser pour centraliser toutes les applications.
- Pour créer le script, ouvrez une invite de commande et saisissez les commandes de script.
- Distribuez ce package sur les ordinateurs d'extrémité à l'aide des mécanismes de distribution de logiciels de l'entreprise.

Le package est exécuté sur les ordinateurs d'extrémité. Les ordinateurs d'extrémité sont ensuite prêts à utiliser SafeGuard Enterprise.

- Après l'installation, redémarrez les ordinateurs d'extrémité deux fois pour activer l'authentification au démarrage. Redémarrez l'ordinateur une troisième fois pour effectuer une sauvegarde des données de noyau à chaque initialisation Windows. Cette sauvegarde ne se produira pas si l'ordinateur d'extrémité est seulement en hibernation ou transféré en mode attente. Assurez-vous que l'ordinateur ne passe pas en mode hibernation ou attente mais qu'il soit redémarré une troisième fois pour sauvegarder le 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 après l'installation, depuis l'authentification au démarrage, ou via un paramètre de configuration supplémentaire passé à la commande `msiexec` de Windows Installer. Pour plus d'informations, rendez-vous sur :

<http://www.sophos.fr/support/knowledgebase/article/107781.html>

<http://www.sophos.fr/support/knowledgebase/article/107785.html>

10.2 Commande pour l'installation centralisée

Lorsque vous installez SafeGuard Enterprise de manière centralisée sur les ordinateurs d'extrémité, utilisez le composant Windows Installer **msiexec**. Inclus dans Windows XP, Vista et Windows 7, **Msiexec** exécute automatiquement une installation préconfigurée de SafeGuard Enterprise. Comme la source et la destination du programme d'installation peuvent également être spécifiées, une installation standard sur plusieurs ordinateurs d'extrémité existe.

Pour plus d'informations, rendez-vous sur :

[http://msdn.microsoft.com/en-us/library/aa367988\(VS.85\).aspx](http://msdn.microsoft.com/en-us/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 Sophos SafeGuard à installer, par exemple, le chiffrement basé sur volume.
- Les paramètres de Sophos SafeGuard, pour spécifier le répertoire d'installation, par exemple.

Options de commande

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

| Option | Description |
|------------------|--|
| <code>/i</code> | Spécifie qu'il s'agit d'une installation. |
| <code>/qn</code> | Exécute une installation sans interaction de l'utilisateur et n'affiche pas d'interface utilisateur. |

| Option | Description |
|--------------------------------------|--|
| ADDLOCAL= | Répertorie les fonctions à installer. Si l'option n'est pas spécifiée, toutes les fonctions d'une installation standard sont installées. Notez les éléments suivants : Séparez les fonctions à l'aide d'une virgule et non d'un espace. Respectez la casse. Ajoutez toutes les fonctions parentes de la fonction sélectionnée à la ligne de commande. |
| ADDLOCAL=ALL | Installe toutes les fonctions disponibles |
| REBOOT=Force ReallySuppress | 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 /L <chemin + nom de fichier> consigne uniquement les messages d'erreur |
| InstallDir= <répertoire> | Spécifie le répertoire dans lequel installer le client SafeGuard Enterprise. Si aucune valeur n'est spécifiée, le répertoire d'installation par défaut est <SYSTEM>:\PROGRAM FILES\SOPHOS. |

10.3 Fonctions de SafeGuard Enterprise (ADDLOCAL)

Pour procéder à une installation centralisée, définissez en amont quelles fonctions de Sophos SafeGuard doivent être installées sur les ordinateurs d'extrémité. Une liste des fonctions s'affiche après avoir saisi l'option **ADDLOCAL** dans la commande.

Remarque :

Même s'il est possible d'installer uniquement une sous-catégorie de fonctions lors d'une première installation, nous vous conseillons d'installer la fonction de chiffrement des périphériques (chiffrement du volume) dès le démarrage.

Avant l'installation, décidez si vous souhaitez utiliser SafeGuard Enterprise en association avec BitLocker Device Encryption ou le chiffrement de SafeGuard Enterprise natif uniquement.

Les tableaux ci-dessous dressent la liste des fonctions SafeGuard Enterprise qui peuvent être installées sur les ordinateurs d'extrémité. Pour plus d'informations, rendez-vous sur : <http://www.sophos.fr/support/knowledgebase/article/108426.html>.

10.3.1 Fonctions de SafeGuard Device Encryption

Remarque :

Enumérez les fonctions **Client** et **Authentification** par défaut. Si vous sélectionnez une fonction, vous devez également ajouter les fonctions parentes à la ligne de commande !

| Fonctions parentes | Fonction |
|-------------------------------|---|
| Client | <p>Authentication</p> <p>Indiquez la fonction Authentication et sa fonction parente Client par défaut.</p> |
| Client, Authentication | <p>CredentialProvider</p> <p>Vous devez sélectionner cette fonction pour les ordinateurs dotés de Windows Vista et Windows 7. Elle permet d'activer la connexion avec le fournisseur d'informations d'identification.</p> |
| Client, BaseEncryption | <p>SectorBasedEncryption</p> <p>Installe le chiffrement basé sur volume de SafeGuard Enterprise avec les fonctions suivantes :</p> <p>Tous les volumes, supports amovibles inclus, peuvent être chiffrés avec le chiffrement basé sur volume de SafeGuard Enterprise.</p> <p>Authentification au démarrage (POA) de SafeGuard Enterprise.</p> <p>Récupération de SafeGuard Enterprise avec Challenge/Réponse.</p> <p>Remarque :</p> <p>Vous pouvez spécifier SectorBasedEncryption OU BitLockerSupport.</p> |
| Client | <p>SecureDataExchange</p> <p>SafeGuard Data Exchange avec chiffrement basé sur fichier est toujours installé localement et pour les supports amovibles. SafeGuard Data Exchange fournit le chiffrement sécurisé pour les supports amovibles. Les données peuvent être partagées avec d'autres utilisateurs en toute sécurité et facilement. Tous les processus de chiffrement et de déchiffrement sont exécutés de manière transparente et impliquent une interaction utilisateur minimale. Si vous avez installé SafeGuard Data Exchange sur votre ordinateur, SafeGuard Portable l'est également. SafeGuard Portable permet aux données d'être partagées en toute sécurité avec les ordinateurs sur lesquels SafeGuard Data Exchange n'est pas installé.</p> <p>Remarque :</p> <p>SafeGuard Data Exchange peut être installé parallèlement au client BitLocker.</p> |
| Client | <p>BitLockerSupport</p> <p>Installe la prise en charge de BitLocker pour SafeGuard Enterprise avec les fonctions suivantes:</p> <p>Chiffrement basé sur volume d'initialisation avec BitLocker.</p> <p>Chiffrement d'autres volumes avec BitLocker.</p> <p>Authentification de préinitialisation de BitLocker.</p> |

| Fonctions parentes | Fonction |
|--------------------|--|
| | <p>Récupération BitLocker</p> <p>Vous pouvez spécifier SectorBasedEncryption OU BitLockerSupport.</p> <p>Remarque :</p> <p>Non disponible pour les clients Sophos SafeGuard (autonomes)</p> |
| Client | <p>ConfigurationProtection</p> <p>Protection des ports et gestion des périphériques : pour installer la protection de la configuration SafeGuard, ajoutez cette fonction à la commande msiexec pour le package d'installation du client ET exécutez les étapes d'installation supplémentaires, reportez-vous à la section Configuration de la protection de la configuration SafeGuard à la page 71.</p> <p>Remarque :</p> <p>Non disponible pour les clients Sophos SafeGuard (autonomes).</p> |

10.3.2 Fonctions pour SafeGuard Data Exchange

Remarque :

Enumérez les fonctions **Client** et **Authentification** par défaut. Si vous sélectionnez une fonction, ajoutez également les fonctions parentes à la ligne de commande !

| Fonctions parentes | Fonction |
|--------------------|---|
| Client | <p>Authentification</p> <p>Indiquez la fonction Authentification et sa fonction parente Client par défaut.</p> |
| Client | <p>SecureDataExchange</p> <p>SafeGuard Data Exchange avec chiffrement basé sur fichier est toujours installé localement et pour les supports amovibles. SafeGuard Data Exchange fournit le chiffrement sécurisé pour les supports amovibles. Les données peuvent être partagées avec d'autres utilisateurs en toute sécurité et facilement. Tous les processus de chiffrement et de déchiffrement sont exécutés de manière transparente et impliquent une intervention minimale de l'utilisateur. Si vous avez installé SafeGuard Data Exchange sur votre ordinateur, SafeGuard Portable l'est également. SafeGuard Portable permet aux données d'être partagées en toute sécurité avec les clients sur lesquels SafeGuard Data Exchange n'est pas installé.</p> |

| Fonctions parentes | Fonction |
|--------------------|--|
| Client | <p>ConfigurationProtection</p> <p>Protection des ports et gestion des périphériques : pour installer la protection de la configuration SafeGuard, ajoutez cette fonction à la commande msiexec pour le package d'installation du client ET effectuez les étapes d'installation supplémentaires, reportez-vous à la section Configuration de la protection de la configuration de SafeGuard à la page 71.</p> <p>Remarque :</p> <p>Non disponible pour les clients Sophos SafeGuard autonomes.</p> |

10.3.3 Exemple de commande pour le chiffrement basé sur fichier et sur volume

La commande indiquée ci-dessous a l'effet suivant :

- Les ordinateurs d'extrémité sont fournis avec la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement.
- L'authentification au démarrage (POA) de SafeGuard Enterprise est installée.
- Le chiffrement basé sur volume de SafeGuard Enterprise est installé.
- L'installation du chiffrement basé sur fichier de SafeGuard Data Exchange en spécifiant **SecureDataExchange**.
- La création d'un fichier journal.
- Le package de configuration du client SafeGuard Enterprise (administré) est exécuté.

Exemple :

```
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,Authentication,BaseEncryption,SectorBasedEncryption,
SecureDataExchange
```

```
InstallDir=C:\Program Files\Sophos\SafeGuard Enterprise
```

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

10.3.4 Exemple de commande pour la prise en charge de BitLocker sous Windows Vista

Une fois la commande indiquée ci-dessous exécutée :

- Les ordinateurs d'extrémité sont fournis avec la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement.
- Les utilisateurs se connectent à leurs PC à l'aide du fournisseur d'informations d'identification Windows Vista.
- L'installation de SafeGuard Enterprise prenant en charge BitLocker avec chiffrement basé sur volume de BitLocker.
- L'installation du chiffrement basé sur fichier de SafeGuard Data Exchange en spécifiant **SecureDataExchange**.
- La création d'un fichier journal.
- Enfin, l'exécution du package de configuration du client SafeGuard Enterprise.

Remarque :

Lors de l'installation de SafeGuard Enterprise avec BitLocker, vérifiez que seul **BitLockerSupport** est exécuté. N'ajoutez pas SafeGuard Enterprise **BaseEncryption** à la ligne de commande.

Exemple :

```
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,Authentication,CredentialProvider,  
BaseEncryption,BitLockerSupport,SecureDataExchange
```

```
InstallDir=C:\Program Files\Sophos\SafeGuard Enterprise
```

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

10.4 Installation conforme à 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. Par défaut, une nouvelle mise en place plus rapide des algorithmes AES est installée mais n'est pas encore certifiée FIPS.

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

Cela peut être effectuée de deux manières :

- Ajoutez la propriété au script par lignes de commande suivant :
`msiexec /i F:\Software\SGNClient.msi FIPS_AES=1`
- Utilisez une transformation.

10.5 Installation sur des ordinateurs d'extrémité avec disques durs à auto-chiffrement et conformes à Opal

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

Pour vous assurer que la prise en charge des disques durs à auto-chiffrement 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 si le lecteur s'identifie en tant que lecteur de disque dur "OPAL", si les propriétés de communications sont correctes et si 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 en dehors de SafeGuard Enterprise. Dans ce cas, SafeGuard Enterprise refuse l'accès au lecteur et un message d'information apparaît.

En cas d'échec irrémédiable d'une de ces vérifications, l'installation ne restaure pas le chiffrement logiciel utilisé pour les lecteurs de disque dur non Opal. Tous les volumes sur le disque Opal demeurent non chiffrés.

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 de 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. Pour voir une liste des lecteurs de disque dur nécessitant l'utilisation d'un commutateur d'installation et pour obtenir plus d'informations sur les lecteurs de disque dur pris en charge, reportez-vous aux 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>  
IGNORE_OPAL_AUTHORITYCHECK_RESULTS=1
```

Si vous choisissez de procéder à l'installation avec les fichiers .mst files ou d'utiliser, par exemple, ORCA pour modifier votre fichier .msi, sachez que la propriété interne de MSI porte le même nom.

Pour plus d'informations sur l'utilisation de SafeGuard Enterprise avec des lecteurs de disque dur conformes à la norme Opal, reportez-vous à l'aide administrateur et à l'aide utilisateur de SafeGuard Enterprise.

11 Configuration locale des ordinateurs d'extrémité

Si vous souhaitez exécuter une version d'évaluation sur un ordinateur d'extrémité, il peut être utile d'installer d'abord SafeGuard Enterprise en local.

L'installation et la configuration sont décrites pour les clients SafeGuard Enterprise administrés et les clients Sophos SafeGuard autonomes. La procédure d'installation est identique sauf que vous attribuez un package de configuration différent pour chacun.

Les tâches requises pour l'installation des ordinateurs d'extrémité avec Windows BitLocker Device Encryption sont également décrites. Pour plus de détails sur la préparation de la prise en charge BitLocker, voir [Préparations spécifiques pour la prise en charge de BitLocker Drive Encryption](#) à la page 54.

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 l'aide utilisateur.

11.1 Installation locale du logiciel de chiffrement

Pour installer localement le logiciel de chiffrement :

1. Préparez les ordinateurs d'extrémité à l'installation, reportez-vous à la section [Préparation au chiffrement](#) à la page 53.
2. Ouvrez une session sur l'ordinateur en tant qu'administrateur.
3. Installez le package de préinstallation **SGxClientPreinstall.msi**, qui fournit à l'ordinateur d'extrémité la configuration requise pour une installation réussie du logiciel de chiffrement.

Remarque : vous pouvez également installer **vcredist_x86.exe**, téléchargeable sur le site suivant :

<http://www.microsoft.com/downloads/details.aspx?FamilyID=766a6af7-ec73-40ff-b072-9112bab119c2>
ou vérifiez que le fichier **MSVCR80.dll**, version 8.0.50727.4053 se trouve sur l'ordinateur, dans le dossier Windows\WinSxS.

4. Cliquez deux fois sur le package d'installation (MSI) <client> correspondant pour démarrer l'assistant d'installation du logiciel de chiffrement. Il vous guidera tout au long des étapes nécessaires.
5. Acceptez les valeurs par défaut dans les boîtes de dialogue suivantes.

6. Si vous y êtes invité, sélectionnez le type d'installation et les fonctions d'après vos besoins. Les clients installant SGNClient.msi ou SGNClient_x64.msi doivent exécuter l'une des actions suivantes :

- Sélectionnez **Complète** pour installer SafeGuard Enterprise Device Protection et Data Exchange.
- Sélectionnez **Classique** pour installer SafeGuard Enterprise Device Encryption seulement.
- Sélectionnez **Personnalisé** pour installer BitLocker Device Encryption. Sous **Fonctions**, sélectionnez **Chiffrement de périphérique**, activez **Prise en charge de BitLocker** et désélectionnez **Chiffrement de base**.

Remarque :

Même s'il est possible d'installer seulement un sous-ensemble de fonctions lors d'une première installation, nous vous conseillons d'installer la fonction Device Encryption (chiffrement basé sur volume) dès le départ.

7. Acceptez les valeurs par défaut dans toutes les boîtes de dialogue suivantes pour terminer l'assistant d'installation.

SafeGuard Enterprise est installé sur l'ordinateur d'extrémité.

8. Accédez à l'emplacement d'enregistrement du package de configuration par défaut (MSI) créé auparavant dans le SafeGuard Management Center. Des packages de configuration différents doivent être installés pour les ordinateurs d'extrémité administrés et autonomes, voir [À propos de la création de packages de configuration](#) à la page 55.

9. Installez le package de configuration (MSI) correspondant sur l'ordinateur.

SafeGuard Enterprise est installé sur l'ordinateur d'extrémité. Effectuez ensuite votre première connexion à l'ordinateur après l'installation. Consultez l'aide de l'utilisateur pour le comportement de l'ordinateur après l'installation de SafeGuard Enterprise.

12 Installation de SafeGuard Enterprise sur les ordinateurs disposant de plusieurs systèmes d'exploitation

Le logiciel de chiffrement SafeGuard Enterprise peut être installé sur un ordinateur afin d'en protéger les données si plusieurs systèmes d'exploitation sont installés sur différents volumes du disque dur. SafeGuard Enterprise propose un système d'exécution. SafeGuard Enterprise Runtime permet les opérations suivantes lorsqu'il est installé sur des volumes disposant d'une installation supplémentaire de Windows :

- L'installation Windows résidant sur ces volumes peut être démarrée avec succès via un gestionnaire de démarrage.
- Vous pouvez accéder aux partitions des volumes chiffrés avec une clé machine définie lors d'une installation complète du client SafeGuard Enterprise.

12.1 Conditions requises et restrictions

Notez les éléments suivants :

- SafeGuard Enterprise Runtime ne fournit aucune fonction ou fonctionnalité spécifique au client SafeGuard Enterprise.

- SafeGuard Enterprise Runtime prend seulement en charge les systèmes d'exploitation qui sont aussi pris en charge par le logiciel de chiffrement de SafeGuard Enterprise.
- Le fonctionnement des claviers USB peut être limité.
- Seuls les gestionnaires d'initialisation activés à la suite d'une authentification au démarrage sont pris en charge.
- La prise en charge des gestionnaires d'initialisation tiers n'est pas garantie. Nous recommandons d'utiliser les gestionnaires d'initialisation Windows.
- SafeGuard Enterprise Runtime ne peut pas être mis à jour à une installation complète du client SafeGuard Enterprise.
- Le package d'installation Runtime doit être installé avant la version complète du package d'installation du client SafeGuard Enterprise.
- Seuls les volumes chiffrés avec la clé machine définie de SafeGuard Enterprise sont accessibles.

12.2 Préparations

Pour configurer le client d'exécution SafeGuard Enterprise, effectuez les préparatifs suivants dans l'ordre indiqué :

1. Assurez-vous que les volumes sur lesquels le client d'exécution SafeGuard Enterprise est exécuté sont visibles au moment de l'installation et peuvent porter leur nom Windows (par exemple C:).
2. Choisissez le ou les volumes du disque dur sur lesquels installer le client d'exécution SafeGuard Enterprise. Dans SafeGuard Enterprise, ces volumes sont définis en tant qu'installations secondaires de Windows. Il peut exister plusieurs installations secondaires de Windows. Utilisez le package suivant : SGNClientRuntime.msi ou SGNClientRuntime_x64.msi (sous Windows Vista 64 bits, Windows 7 64 bits).
3. Choisissez le volume du disque dur sur lequel installer la version complète du client SafeGuard Enterprise. Dans SafeGuard Enterprise, ce volume est défini en tant qu'installation principale de Windows. Il ne peut y avoir qu'une installation principale de Windows. Utilisez le package suivant : SGNClient.msi ou SGNClient_x64.msi (sous Windows Vista 64 bits, Windows 7 64 bits). Si nécessaire, vous pouvez en plus installer la protection de la configuration (SGN_CP_Client.msi / SGN_CP_Client_x64.msi disponibles pour les systèmes d'exploitation Windows 7 64 bits).

12.3 Installation de SafeGuard Enterprise Runtime

1. Sélectionnez le ou les volumes secondaires requis du disque dur sur lesquels installer le client runtime SafeGuard Enterprise.
2. Démarrez l'installation secondaire de Windows sur le volume sélectionné.
3. Installez le package d'installation runtime sur le volume sélectionné.
4. Acceptez les valeurs par défaut de la boîte de dialogue suivante du programme d'installation. Il n'est pas nécessaire de sélectionner les fonctions spéciales.
5. Sélectionnez un dossier d'installation runtime.

6. Cliquez sur **Terminer** pour finir l'installation runtime.
7. Sélectionnez le volume principal du disque dur sur lequel installer le client SafeGuard Enterprise.
8. Démarrez l'installation principal de Windows sur le volume sélectionné.
9. Démarrez le package d'installation SGxClientPreinstall.msi, qui fournit aux ordinateurs d'extrémité la configuration requise pour une installation réussie du logiciel de chiffrement.
10. Installez le package d'installation du client SafeGuard Enterprise sur le volume sélectionné.
11. Créez un package de configuration pour un client SafeGuard Enterprise (administré) ou Sophos SafeGuard (autonome) selon vos besoins et déployez-le sur l'ordinateur d'extrémité.
12. Chiffrez les deux volumes à l'aide de la clé machine définie.

12.4 Démarrage à partir d'un volume secondaire via un gestionnaire d'initialisation

1. Démarrez l'ordinateur.
2. Connectez-vous à l'authentification au démarrage avec vos codes d'accès.
3. Démarrez le gestionnaire d'initialisation et sélectionnez le volume secondaire requis en tant que volume d'initialisation.
4. Redémarrez l'ordinateur à partir de ce volume.

Vous pouvez accéder à chacun des volumes chiffrés avec la clé machine définie.

13 Configuration de la protection de la configuration SafeGuard

La protection de la configuration SafeGuard permet de définir les interfaces et les périphériques à autoriser sur les ordinateurs d'extrémité. Ceci pour empêcher l'introduction de malwares ou de données exportées par l'intermédiaire de voies indésirables comme le réseau local sans fil (WLAN). La protection de la configuration SafeGuard détecte et bloque également les matériels nuisibles tels que les enregistreurs de frappe (keyloggers).

13.1 Conditions préalables et restrictions

Notez les éléments suivants :

- Pour paramétrer la protection de la configuration SafeGuard sur des systèmes d'exploitation Windows 7 en 64 bits, vous pouvez utiliser les variantes 64 bits des packages d'installation "Client".
- La protection de la configuration SafeGuard est uniquement disponible pour les clients SafeGuard Enterprise administrés. Elle n'est pas prise en charge pour les clients Sophos SafeGuard autonomes.
- .NET Version 2.0 doit être installé.

13.2 Installation centralisée de la protection de la configuration SafeGuard

Lorsque vous effectuez une installation centralisée de la protection de la configuration SafeGuard sur les ordinateurs d'extrémité, utilisez le composant msiexec de Windows Installer.

La ligne de commande est la suivante :

```
msiexec /i SGN_CP_Client.msi /quiet /norestart
```

Pour installer avec succès la protection de la configuration SafeGuard, exécutez les tâches en respectant l'ordre indiqué :

1. Préparez les ordinateurs d'extrémité à l'installation en vous reportant à la section, [Préparation au chiffrement](#) à la page 53.

- 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 :

| | |
|---|--|
| <p>Package d'installation de préparation SGxClientPreinstall.msi</p> | <p>Le package fournit aux ordinateurs d'extrémité la configuration requise pour une installation réussie du logiciel de chiffrement, notamment le fichier DLL MSVCR80.dll, version 8.0.50727.4053.</p> <p>Remarque :</p> <p>Si ce package n'est pas installé, l'installation du logiciel de chiffrement échoue.</p> |
| <p>Package d'installation du client SafeGuard Enterprise</p> | <p>Utilisez soit SafeGuard Device Encryption (SGNClient.msi), soit SafeGuard Data Exchange (SGN_withoutDe.msi). Pour paramétrer la protection de la configuration SafeGuard sur des systèmes d'exploitation Windows 7 en 64 bits, vous pouvez utiliser les variantes 64 bits des packages d'installation "Client".</p> <p>Ajoutez ConfigurationProtection comme fonction vers l'option ADDLOCAL.</p> |
| <p>Package d'installation de la protection de la configuration SafeGuard</p> | <p>Utilisez SGN_CP_Client.msi. Pour paramétrer la protection de la configuration SafeGuard sur des systèmes d'exploitation Windows 7 en 64 bits, vous pouvez utiliser la variante 64 bits des packages d'installation "Client".</p> <p>Assurez-vous que l'ordinateur n'a pas redémarré en utilisant le paramètre /norestart : msiexec /i SGN_CP_Client.msi /quiet /norestart</p> |
| <p>Package de configuration pour le client SafeGuard Enterprise (administré)</p> | <p>Utilisez un package de configuration créé auparavant dans le SafeGuard Management Center. Avant d'installer un nouveau package de configuration, assurez-vous de désinstaller tous ceux obsolètes.</p> |
| <p>Script avec les commandes de l'installation préconfigurée</p> | <p>Nous recommandons d'utiliser l'outil de ligne de commande de Windows Installer msiexec pour créer le script.</p> |

- Créez un dossier **Logiciels** à utiliser pour centraliser toutes les applications.
- Pour créer le script, ouvrez une invite de commande et saisissez les commandes de script.
- À l'aide des mécanismes de distribution de logiciels de l'entreprise, distribuez ce package sur les ordinateurs d'extrémité.

13.2.1 Exemple de commande pour la protection de la configuration SafeGuard avec SafeGuard Device Encryption

La commande msiexec doit être exécutée dans l'ordre spécifié dans l'exemple. Dans cet exemple, les événements suivants ont lieu :

- Les ordinateurs d'extrémité sont fournis avec la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement.
- Le chiffrement basé sur fichier de SafeGuard Device Encryption est installé.
- La protection de la configuration SafeGuard doit être répertoriée comme fonction pour le package d'installation du client SafeGuard Device Encryption.
- Pour commencer l'installation du module de la protection de la configuration SafeGuard, ajoutez un package d'installation distinct en spécifiant une autre commande msiexec.
- Un fichier journal est créé.
- Le package de configuration pour le client SafeGuard Enterprise administré est exécuté.

Exemple :

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

```
msiexec /i F:\Software\SGNClient.msi /qn /log  
I:\Temp\SGNClient.log  
ADLOCAL=Client,Authentication,BaseEncryption,SectorBasedEncryption,ConfigurationProtection
```

```
InstallDir=C:\Program Files\Sophos\SafeGuard Enterprise
```

```
msiexec /i F:\Software\SGN_CP_Client.msi /quiet /norestart
```

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

13.2.2 Exemple de commande pour la protection de la configuration SafeGuard avec SafeGuard Data Exchange

La commande msiexec doit être exécutée dans l'ordre spécifié dans l'exemple. Dans cet exemple, les événements suivants ont lieu :

- Les ordinateurs d'extrémité sont fournis avec la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement.
- Le chiffrement basé sur fichier de SafeGuard Data Exchange est installé.
- La protection de la configuration SafeGuard doit être répertoriée comme fonction pour le package d'installation du client SafeGuard Data Exchange.
- Pour initier l'installation du module de la protection de la configuration SafeGuard, ajoutez un package d'installation distinct en spécifiant une autre commande msiexec.
- Un fichier journal est créé.
- Le package de configuration pour le client SafeGuard Enterprise (administré) est exécuté.

Exemple :

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

```
msiexec /i F:\Software\SGNClient.msi /qn /log  
I:\Temp\SGNClient.log  
ADDLOCAL=Client,Authentication,SecureDataExchange,ConfigurationProtection
```

```
InstallDir=C:\Program Files\Sophos\SafeGuard Enterprise
```

```
msiexec /i F:\Software\SGN_CP_Client.msi /quiet /norestart
```

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

13.3 Installation locale de la protection de la configuration SafeGuard

Pour effectuer une installation locale de la protection de la configuration SafeGuard, exécutez les étapes suivantes dans l'ordre indiqué :

1. Préparez les ordinateurs d'extrémité à l'installation, reportez-vous à la section [Préparation au chiffrement](#) à la page 53.
2. Ouvrez une session sur l'ordinateur en tant qu'administrateur.
3. Installez le package d'installation **SGxClientPreinstall.msi**, qui fournit à l'ordinateur d'extrémité la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement, et notamment les fichiers DLL appropriés.
4. Sélectionnez l'un des packages d'installation suivants du client SafeGuard Enterprise à installer sur l'ordinateur d'extrémité. Pour paramétrer la protection de la configuration SafeGuard sur des systèmes d'exploitation Windows 7 en 64 bits, utilisez les variantes 64 bits des packages d'installation "Client" :
 - SafeGuard Device Encryption (SGNClient.msi/SGNClient_x64.msi)
 - SafeGuard Data Exchange (SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi).
5. Dans l'assistant d'installation, sélectionnez une installation du type **Personnalisé**. Sous **Fonctions**, assurez-vous de sélectionner en plus **Protection de la configuration**.
6. Installez le package d'installation de la protection de la configuration SafeGuard SGN_CP_Client.msi/SGN_CP_Client_x64.msi (disponible pour les systèmes d'exploitation Windows 7 en 64 bits).

Changez le répertoire d'installation pour C:\Program Files\Sophos\SafeGuard Enterprise\ pour vous assurer que le module de protection de la configuration est installé dans le répertoire SafeGuard Enterprise.
7. Ne redémarrez pas l'ordinateur.
8. Générez un package de configuration pour le client SafeGuard Enterprise (administré) et installez-le sur l'ordinateur d'extrémité immédiatement après l'installation du logiciel de chiffrement.
9. Redémarrez l'ordinateur d'extrémité.

La protection de la configuration SafeGuard est installée sur l'ordinateur d'extrémité.

13.4 Désinstallation de la protection de la configuration SafeGuard

Pour désinstaller SafeGuard Configuration Protection, exécutez les tâches en respectant l'ordre indiqué :

1. Désinstallez le package de configuration du client SafeGuard Enterprise (administré).
2. Démarrez le package d'installation du client SafeGuard Enterprise sur l'ordinateur, SGNClient.msi ou SGNClient_withoutDE.msi ou la variante 64 bits correspondante.
3. Dans l'assistant d'installation, sélectionnez une installation du type **Modifier**.
4. Sous **Fonctions**, désélectionnez la fonction **Protection de configuration**.
5. Lorsque la désinstallation est terminée, ne redémarrez pas l'ordinateur.
6. Désinstallez le package d'installation de la protection de la configuration SafeGuard SGN_CP_Client.msi/SGN_CP_Client_x64.msi.
7. Redémarrez l'ordinateur.

SafeGuard Configuration Protection est supprimé de l'ordinateur d'extrémité.

13.5 Mise à jour de la protection de la configuration SafeGuard

Pour mettre à jour la protection de la configuration SafeGuard, exécutez les tâches en respectant l'ordre indiqué :

1. Démarrez le package d'installation SGxClientPreinstall.msi, qui fournit aux ordinateurs d'extrémité la configuration requise pour une installation réussie du logiciel de chiffrement.
2. Démarrez le dernier package d'installation du client SafeGuard Enterprise sur l'ordinateur, SGNClient.msi ou SGNClient_withoutDE.msi ou la variante 64 bits correspondante pour le mettre à jour. Pour paramétrer la protection de la configuration SafeGuard sur des systèmes d'exploitation Windows 7 en 64 bits, vous pouvez utiliser les variantes 64 bits des packages d'installation Client.

Ne redémarrez pas l'ordinateur lorsque la mise à jour est terminée.

3. Dans **Ajout/Suppression de programmes**, supprimez le client SGN_CP_Client.msi de la protection de la configuration SafeGuard.
4. Redémarrez l'ordinateur d'extrémité.
5. Installez le package d'installation du client SGN_CP_Client.msi/SGN_CP_Client_x64.msi de la protection de la configuration SafeGuard.
6. Redémarrez l'ordinateur d'extrémité.
7. Dans le SafeGuard Management Center, réattribuez la stratégie de protection de la configuration correspondante pour la réactiver.

La protection de la configuration SafeGuard est mise à jour sur l'ordinateur d'extrémité.

14 Réplication de la base de données SafeGuard Enterprise

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

Ce chapitre décrit la méthode de configuration de 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.

14.1 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

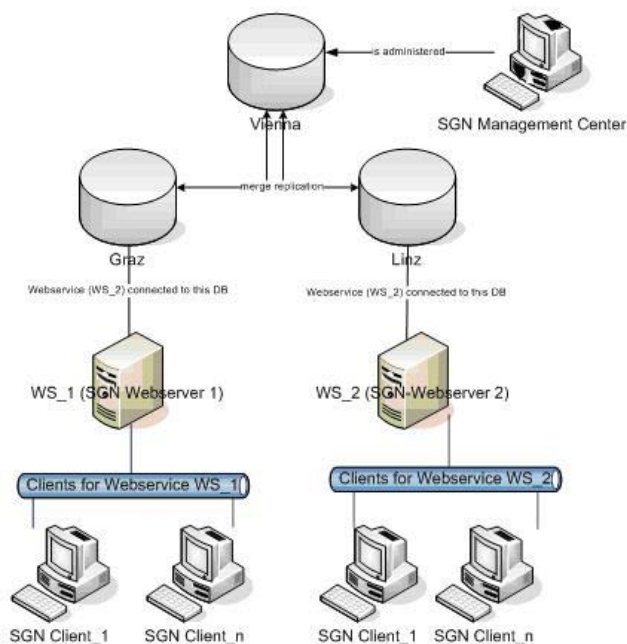
synchronisées continuellement entre les serveurs, à intervalles réguliers ou sur demande. Puisque les mises à jour sont effectuées sur plusieurs serveurs, les mêmes données peuvent avoir été mises à jour par l'éditeur ou par plusieurs abonnés. Des conflits peuvent donc apparaître lors de la fusion.

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.

14.2 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 Server2005.

Dans l'exemple, SafeGuard Enterprise est administré de manière exclusive depuis la base de données à **Vienne**. Toute modification est transmise par le SafeGuard Management Center aux bases de données de **Graz** et **Linz** par réplication dans Microsoft SQL Server 2005. Les modifications signalées par les ordinateurs client par l'intermédiaire des serveurs Web sont également transmises à Microsoft SQL Server2005 par réplication.



14.2.1 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 VIENNE.

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 du SafeGuard Management Center.

Cette procédure requiert que le SafeGuard Management Center soit déjà installé. Pour plus d'informations, reportez-vous à la section [Démarrage de la configuration initiale du SafeGuard Management Center](#) à la page 33.

- Générez la base de données principale avec un script SQL disponible dans le répertoire du produit.

Cette procédure est généralement préférée si l'extension des autorisations SQL lors de la configuration de SafeGuard Management Center n'est pas souhaitée. Pour plus d'informations, reportez-vous à la section [Génération de la base de données SafeGuard Enterprise à l'aide d'un script](#) à la page 27.

14.2.2 Génération des bases de données de réplication Graz et Linz

Une fois la base de données principale configurée, vous pouvez générer les bases de données dupliquées. Dans notre exemple, les bases de données de réplication se nomment 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 concaténées, 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 concaténés, 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.

14.3 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 le SafeGuard Management Center : dans le menu **Outils**, cliquez sur **Outil de package de configuration**, puis cliquez sur **Enregistrer le serveur**. Dans l'onglet **Enregistrer le serveur**, cliquez sur **Ajouter**.
4. Vous êtes invité à ajouter les certificats de serveur **ws_1.cer** et **ws_2.cer**. Vous les trouvez dans le dossier **\Program Files\Sophos\SafeGuard Enterprise\MachCert**. Ces certificats sont nécessaires à la création des packages de configuration appropriés.

Les serveurs SafeGuard Enterprise sont installés et enregistrés.

14.4 Création des packages de configuration de la base de données GRAZ

Vous devez 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 SafeGuard Management Center, dans le menu **Outils**, cliquez sur **Options**, puis sur **Connexion à la base de données**.
2. Dans **Connexion à la base de données**, sélectionnez **WS_1** comme **Serveur de base de données** et **GRAZ** comme **Base de données**. Cliquez sur **OK**.
3. Dans le menu **Outils**, cliquez sur **Outil de package de configuration**, puis cliquez sur **Créer un package de configuration de serveur**. Sélectionnez le serveur **WS_1**, sélectionnez le chemin de sortie et cliquez sur **Créer un package de configuration**.
4. Ouvrez l'onglet **Créer un package de configuration (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 sont 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.

14.5 Création des packages de configuration de la base de données LINZ

Vous devez 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 SafeGuard Management Center, dans le menu **Outils**, cliquez sur **Options**, puis sur **Connexion à la base de données**.

2. Dans **Connexion à la base de données**, sélectionnez **WS_2** comme **Serveur de base de données** et **LINZ** comme **Base de données**. Cliquez sur **OK**.
3. Dans le menu **Outils**, cliquez sur **Outils de package de configuration**, puis cliquez sur **Créer un package de configuration de serveur**. Sélectionnez le serveur **WS_2**, sélectionnez le chemin de sortie et cliquez sur **Créer un package de configuration**.
4. Ouvrez l'onglet **Créer un package de configuration (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 sont connectés : **WS_2**. Sélectionnez le chemin de sortie et cliquez sur **Créer un package de configuration**. Cliquez sur **Fermer**.
5. Connectez de nouveau le SafeGuard Management Center à la base de données VIENNA : dans le menu **Outils**, cliquez sur **Options**, puis cliquez sur **Connexion à la 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.

14.6 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, reportez-vous à la section [Exécution du test de connexion](#) à la page 44.

14.7 Installation du logiciel client SafeGuard Enterprise et configuration sur les ordinateurs d'extrémité

Installez le logiciel client SafeGuard Enterprise de la même façon que pour les clients SafeGuard Enterprise sans réplication. Pour plus d'informations, reportez-vous à la section [Commande pour l'installation centralisée](#) à la page 60.

Remarque :

Pour obtenir la configuration appropriée, veillez à installer le package de configuration du client approprié une fois que vous avez installé chacun des clients SafeGuard Enterprise :

1. Installez le package de configuration du client **GRAZ** sur les clients à connecter au serveur **GRAZ WS_1**.
2. Installez le package de configuration du client **LINZ** sur les clients à connecter au serveur **LINZ WS_2**.

Pour plus d'informations sur la mise à jour des bases de données SafeGuard Enterprise répliquées, reportez-vous à la section [Mise à jour des bases de données SafeGuard Enterprise répliquées](#) à la page 83.

15 Mise à jour de SafeGuard Enterprise

Si vous avez déjà installé une version précédente de SafeGuard Enterprise, vous pouvez mettre à jour ce logiciel en installant la toute dernière version. La mise à jour directe vers SafeGuard Enterprise version 5.6x est prise en charge pour SafeGuard Enterprise version 5.40 et supérieures. Lors de la mise à jour depuis les versions antérieures, vous devez d'abord mettre à jour vers SafeGuard Enterprise 5.40.

À l'exception de la base de données SafeGuard Enterprise, les mises à jour du serveur SafeGuard Enterprise, du SafeGuard Management Center et des ordinateurs d'extrémité protégés par SafeGuard Enterprise sont les mêmes qu'une nouvelle installation.

Depuis SafeGuard Enterprise 5.30 et versions supérieures, l'importation d'un fichier de licence valide est requise pour couvrir tous les clients déployés. Si le nombre de licences est dépassé, le transport de stratégies est bloqué après la mise à jour du client. Contactez au préalable votre partenaire commercial pour lui demander un fichier de licence.

Remarque :

Il est essentiel de mettre à jour les composants dans l'ordre indiqué ci-dessous. Toute mise à jour d'une version précédente vers la version actuelle de SafeGuard Enterprise n'aboutissent que si vous respectez cet ordre :

1. Base de données SafeGuard Enterprise
2. Serveur SafeGuard Enterprise
3. SafeGuard Management Center
4. Ordinateurs d'extrémité protégés par SafeGuard Enterprise

15.1 Mise à jour de la base de données SafeGuard Enterprise

Conditions préalables

- SafeGuard Enterprise Database 5.20 ou une version ultérieure doit être installée.
- Les scripts SQL à exécuter doivent être présents sur l'ordinateur hébergeant la base de données.
- NET Framework 3.0 Service Pack 1 doit être installé pour la mise à jour vers la dernière version.
- Assurez-vous de disposer des droits d'administrateur Windows.
- Sauvegardez la base de données avant de procéder à la mise à jour.

Dans le répertoire Outils du produit livré, vous trouverez plusieurs scripts SQL pour la mise à jour de la base de données.

Pour mettre à jour la base de données :

1. Déconnectez tous les serveurs SafeGuard Enterprise (serveurs IIS) reliés à la base de données SafeGuard Enterprise correspondante.
2. Fermez le SafeGuard Management Center.
3. Définissez la base de données correspondante en mode SINGLE_USER pour exécuter les scripts SQL afin d'avoir un accès exclusif à la base de données.

4. La base de données doit être convertie version par version jusqu'à la version actuelle. En fonction de la version installée, démarrez les scripts SQL suivants dans cet ordre :
 - a) 5.20 > 5.3x : exécutez **MigrateSGN520_SGN530.sql** ou **MigrateSGN520_SGN535.sql**.
Les stratégies SafeGuard Enterprise existantes seront modifiées car la structure de stratégie a changé de la version 5.20 à la version 5.3x.
 - b) 5.3x > 5.35 : exécutez **MigrateSGN530_SGN535.sql**.
 - c) 5.3x > 5.4x : exécutez **MigrateSGN530_SGN535.sql**.
 - d) 5.35 > 5.4x : exécutez **MigrateSGN530_SGN535.sql**.
 - e) 5.4x > 5.5x : exécutez **MigrateSGN540_SGN550.sql**.
 - f) 5.5x > 5.6x : exécutez **MigrateSGN550_SGN560.sql**
5. Redéfinissez la base de données correspondante en mode MULTI_USER.

Les sommes de contrôle cryptographiques de certains tableaux peuvent ne plus être correctes après la mise à jour de la base de données. Lorsque vous démarrez le SafeGuard Management Center, des messages d'avertissement apparaissent. Vous pouvez réparer les tableaux dans la boîte de dialogue correspondante.

La dernière version de la base de données SafeGuard Enterprise est prête à l'utilisation.

Remarque :

A l'étape suivante, mettez à jour le Safeguard Management Center vers la dernière version. Sinon, un message d'erreur apparaîtra.

15.2 Mise à jour des bases de données répliquées SafeGuard Enterprise

Lorsque la base de données SafeGuard Enterprise est à mettre à jour vers une version ultérieure et que les bases de données sont en cours d'utilisation, il est recommandé de désinstaller les bases de données dupliquées avant de démarrer la mise à jour sur la base de données principale.

La mise à jour de la base de données SafeGuard Enterprise nécessite l'exécution de scripts de migration SQL spécifiques qui risquent sinon d'entrer en conflit avec les bases de données répliquées.

Pour mettre à jour la base de données répliquée :

1. Désinstallez les bases de données dupliquées.
2. Exécutez les scripts de migration SQL sur la base de données principale. Elle est disponible dans le dossier Outils de votre produit livré, [voir Mise à jour de la base de données SafeGuard Enterprise](#) à la page 82.
3. Configurez depuis le début les bases de données de réplication, [voir Réplication de la base de données SafeGuard Enterprise](#) à la page 77.

15.3 Mise à jour du serveur SafeGuard Enterprise

Conditions préalables

- SafeGuard Enterprise Server 5.35 ou une version ultérieure doit être installée. Les versions antérieures à la version 5.35 doivent d'abord être mises à jour vers SafeGuard Enterprise Server 5.40.
- .NET Framework 3.0 Service Pack 1 doit être installé. ASP.NET doit être mis à jour vers la version 2.0.
- Assurez-vous de disposer des droits d'administrateur Windows.

Pour mettre à jour le serveur SafeGuard Enterprise :

1. Installez la dernière version du package d'installation du serveur SafeGuard Enterprise.

Le serveur SafeGuard Enterprise est mis à jour. Il est automatiquement redémarré et prêt à l'utilisation.

15.4 Mise à jour du SafeGuard Management Center

Conditions préalables

- SafeGuard Management Center 5.40 ou une version ultérieure doit être installé. Les versions antérieures à la version 5.40 doivent d'abord être mises à jour vers SafeGuard Management Center 5.40.
- La base de données SafeGuard Enterprise et le serveur SafeGuard Enterprise doivent avoir été mis à jour vers la dernière version.
- La base de données SafeGuard Enterprise a déjà été mise à jour vers la dernière version. Pour que l'opération réussisse, les numéros de versions de la base de données SafeGuard Enterprise et du SafeGuard Management Center doivent correspondre.
- .NET Framework 3.0 Service Pack 1 doit être installé. ASP.NET doit être mis à jour vers la version 2.0.
- Assurez-vous de disposer des droits d'administrateur Windows.
- Vous devez disposer d'un fichier de licence valide. Contactez au préalable votre partenaire commercial pour lui en demander un.

Remarque :

Si le SafeGuard Management Center est installé sur un ordinateur sur lequel le client SafeGuard Enterprise est installé, procédez d'abord à la mise à jour du logiciel du client SafeGuard Enterprise à la version 5.6x. Procédez ensuite à la mise à jour du SafeGuard Management Center à la version 5.6x. La mise à jour du SafeGuard Management Center seule peut conduire à des échecs de connexion au niveau de Windows.

Suite à la mise à jour de SafeGuard Management Center à la version 5.6x, les utilisateurs de l'authentification au démarrage ne doivent pas être transférés vers les versions 5.4x ou 5.5x des clients SafeGuard Enterprise. Ce cas de figure n'est pas pris en charge sinon l'utilisateur de l'authentification au démarrage deviendrait propriétaire de l'ordinateur.

Pour mettre à jour le SafeGuard Management Center :

1. Installez la dernière version du package d'installation du SafeGuard Management Center avec les fonctions requises, reportez-vous à la section [Configuration du SafeGuard Management Center](#) à la page 30.
2. Importez le fichier de licence.
3. Démarrez le SafeGuard Management Center. Le comportement du SafeGuard Management Center au premier démarrage après la mise à jour dépend de l'installation ou non des fonctionnalités :

| Option | Description |
|--|--|
| La fonctionnalité d'architecture mutualisée n'est pas installée. | Vous êtes invité à saisir les informations d'identification du responsable de la sécurité du SafeGuard Management Center. |
| La fonctionnalité d'architecture mutualisée est nouvellement installée. | L'assistant de configuration du SafeGuard Management Center démarre et vous invite à sélectionner la base de données à utiliser. L'assistant présélectionne déjà une base de données utilisée précédemment. Sélectionnez la base de données requise et terminez la configuration avec l'assistant. |
| La fonctionnalité d'architecture mutualisée n'est pas installée. | La configuration de la base de données utilisée en dernier sera utilisée dans le SafeGuard Management Center. |

Le SafeGuard Management Center est mis à niveau vers la dernière version.

Remarque :

- API de script : le fichier de configuration par défaut a été renommé et stocké dans un emplacement différent. Assurez-vous que le chemin et le nom de fichier sont changés pour le nouvel emplacement lors de l'utilisation de la méthode suivante avec le paramètre **confFilePathName : AuthenticateOfficer (chaîne OfficerName, chaîne PinOrPassword, stringconfFilePathName)**.
- Les stratégies SafeGuard Enterprise existantes peuvent avoir été modifiées en raison du changement de structure des stratégies effectué à partir de la version 5.30 et supérieure de SafeGuard Enterprise.

15.5 Mise à jour des ordinateurs protégés par SafeGuard Enterprise

Conditions préalables

- SafeGuard Enterprise Client 5.40 ou une version ultérieure doit être installée. Les versions antérieures doivent d'abord être mises à jour vers SafeGuard Enterprise Client 5.40.

SafeGuard Management Center 5.6x et SafeGuard Enterprise Server 5.6x peuvent gérer les clients SafeGuard Enterprise (administrés et autonomes) version 5.40 ou ultérieure. Un mélange de versions clientes doit seulement être présente lors de la mise à jour, mais doit être évité pour l'utilisation générale.

Remarque :

Suite à la mise à jour de SafeGuard Management Center à la version 5.6x, les utilisateurs de l'authentification au démarrage ne doivent pas être transférés vers les versions 5.4x ou 5.5x des clients SafeGuard Enterprise. Ce cas de figure n'est pas pris en charge sinon l'utilisateur de l'authentification au démarrage deviendrait propriétaire de l'ordinateur.

- La base de données SafeGuard Enterprise, le serveur SafeGuard Enterprise et le SafeGuard Management Center doivent avoir été mis à jour vers la dernière version.
- SafeGuard Enterprise Client 5.6x ne peut pas être connecté à un serveur SafeGuard Enterprise au-dessous de la version 5.6x.
- Assurez-vous de disposer des droits d'administrateur Windows.

Cette section est valide pour les ordinateurs d'extrémité administrés et autonomes.

Pour mettre à jour les ordinateurs protégés par SafeGuard Enterprise :

1. Installez le package d'installation MSI **SGxClientPreinstall.msi**, qui fournit à l'ordinateur d'extrémité la configuration requise pour une installation réussie du logiciel de chiffrement courant.
2. Installez la version du package d'installation du logiciel de chiffrement respectif (*Client*.msi) par version jusqu'à ce que la toute dernière version soit atteinte, [voir Installation centralisée du logiciel de chiffrement](#) à la page 58 ou [voir Installation locale du logiciel de chiffrement](#) à la page 68.

Windows Installer reconnaît les fonctions déjà installées et ne réinstalle que celles-ci. Si l'authentification au démarrage est installée, un noyau POA à jour est également disponible après une mise à jour réussie (stratégies, clés, etc.).

Pour installer les nouvelles fonctionnalités avec la mise à jour, sélectionnez un type d'installation **Personnalisée**. Puis sélectionnez les nouvelles fonctionnalités et celles à mettre à jour. Avec une installation sans surveillance, utilisez la propriété ADDLOCAL= pour sélectionner les fonctionnalités désirées (existantes et nouvelles).

3. Si la configuration de l'ordinateur d'extrémité a changé, par exemple lorsque les paramètres de stratégie ont changé, créez un nouveau package de configuration.
4. Pour des raisons de sécurité, supprimez tous les packages de configuration obsolètes ou non utilisés sur les ordinateurs d'extrémité.
5. Déployez le nouveau package de configuration sur les ordinateurs d'extrémité correspondants.

Si vous tentez de remplacer un package de configuration récent par un plus ancien, l'installation est interrompue.

L'ordinateur d'extrémité est mis à jour avec la toute dernière version du logiciel de chiffrement avec les fonctionnalités sélectionnées.

Remarque :

Les utilisateurs importés lors de l'installation de SafeGuard Data Exchange ne sont pas automatiquement importés dans l'authentification au démarrage lorsque SafeGuard Device Encryption est installé ultérieurement. Vous devez déclencher une mise à jour utilisateur, par exemple en attribuant provisoirement une clé au répertoire racine.

15.6 Mise à jour des clients Sophos SafeGuard (autonomes) avec le chiffrement basé sur volume

Si vous voulez ajouter le chiffrement basé sur volume sur un client Sophos SafeGuard (autonome) sur lequel seulement le module SafeGuard Data Exchange avec chiffrement basé sur fichier est installé, exécutez les étapes suivantes : ces étapes sont nécessaires pour garantir une authentification au démarrage sécurisée et correcte.

1. Désinstallez le package d'installation de SafeGuard Data Exchange (SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi).
2. Désinstallez le package de configuration.
3. Installez le package d'installation de SafeGuard Enterprise Device Encryption avec chiffrement basé sur volume et sur fichier (SGNClient.msi/SGNClient_x64.msi). Sélectionnez les fonctions **Chiffrement de périphérique** et **Echange de données** lorsque vous y êtes invité et terminez l'assistant d'installation.
4. Créez un nouveau package de configuration et déployez-le sur l'ordinateur.

Le chiffrement basé sur volume a été ajouté sur le client Sophos SafeGuard (autonome).

Remarque :

Le fichier de récupération de clé ainsi que les clés locales créées lors de l'installation du package d'installation Data Exchange restent disponibles.

15.7 Mise à niveau du client Sophos SafeGuard (autonome) vers un client SafeGuard Enterprise (administré)

Vous pouvez mettre à niveau les ordinateurs d'extrémité avec une configuration de client SafeGuard (autonome) vers une configuration de client SafeGuard Enterprise (administré). Les ordinateurs d'extrémité sont ainsi définis dans le SafeGuard Management Center en tant qu'objets pouvant être gérés et disposant d'une connexion au serveur SafeGuard Enterprise.

Conditions préalables

- Sauvegardez l'ordinateur d'extrémité avant de démarrer la mise à niveau.
- Assurez-vous de disposer des droits d'administrateur Windows.

Pour mettre à niveau le client Sophos SafeGuard (autonome) vers un client SafeGuard Enterprise (administré) :

1. Dans le SafeGuard Management Center, dans le menu **Outils**, cliquez sur **Outil du package de configuration**. Pour créer le package de configuration pour le client SafeGuard Enterprise (administré), cliquez sur **Créer un package de configuration (administré)**.
2. Attribuez ce package à l'ordinateur d'extrémité à l'aide d'une stratégie de groupe.

L'authentification est désactivée car l'attribution utilisateur-ordinateur n'est pas mise à niveau. Après la mise à niveau, les ordinateurs d'extrémité ne sont donc plus protégés !

3. Redémarrez l'ordinateur d'extrémité. La première connexion est toujours effectuée avec l'ouverture de session automatique. De nouvelles clés et de nouveaux certificats sont attribués à l'utilisateur.
4. Redémarrez l'ordinateur d'extrémité une deuxième fois. Connectez-vous à l'authentification au démarrage. Les ordinateurs sont de nouveau protégés seulement après le second redémarrage.
5. Supprimez tous les packages de configuration obsolètes ou non utilisés.

Le client Sophos SafeGuard (autonome) est maintenant un client SafeGuard Enterprise (administré).

15.8 Mise à jour du client SafeGuard Configuration Protection

Pour mettre à jour le module du client SafeGuard Configuration Protection, [voir Mise à jour de SafeGuard Configuration Protection](#) à la page 77.

16 Mise à jour du système d'exploitation

Une fois SafeGuard Enterprise installé, il est uniquement possible de mettre à jour la version du Service Pack du système d'exploitation installé.

Par exemple, vous pouvez installer une mise à jour du Service Pack Windows XP. Vous ne pouvez cependant pas migrer d'un système d'exploitation à un autre lorsque SafeGuard Enterprise est installé. Par exemple, vous ne pouvez pas migrer de Windows Vista vers Windows 7 sur lequel SafeGuard Enterprise est installé.

17 Mise à niveau de Sophos SafeGuard vers SafeGuard Enterprise

Vous pouvez facilement effectuer la mise à niveau de Sophos SafeGuard vers la suite SafeGuard Enterprise avec gestion centralisée, afin d'utiliser l'ensemble des fonctions de SafeGuard Enterprise, par exemple, la gestion des utilisateurs et des ordinateurs ou les fonctions étendues de journalisation.

Sophos SafeGuard inclut les produits suivants :

- Sophos SafeGuard Disk Encryption disponible avec ESDP (Endpoint Security and Data Protection)
- SafeGuard Easy : à partir de la version 5.50, SafeGuard Easy est le nouveau nom de produit de la solution autonome SafeGuard Enterprise.

La mise à niveau comporte les étapes suivantes :

- Procédez à la mise à niveau du SafeGuard Policy Editor vers le SafeGuard Management Center.
- Les ordinateurs d'extrémité protégés par Sophos SafeGuard (autonome) doivent être dotés d'une configuration SafeGuard Enterprise (administré).

17.1 Migration du SafeGuard Policy Editor vers le SafeGuard Management Center

Conditions préalables

- Vous n'avez pas besoin de désinstaller le SafeGuard Policy Editor.
- SafeGuard Enterprise Server doit être installé et mis à niveau vers la dernière version.
- Assurez-vous de disposer des droits d'administrateur Windows.

Pour la mise à niveau, installez simplement le SafeGuard Management Center sur l'ordinateur sur lequel le SafeGuard Policy Editor a été configuré.

1. Démarrez SGNManagementCenter.msi à partir du dossier d'installation du produit livré. Un assistant vous guide tout au long des étapes nécessaires.
2. Sur la page **Bienvenue**, cliquez sur **Suivant**.
3. Acceptez le contrat de licence.
4. Acceptez le chemin d'installation par défaut.
5. Sélectionnez le type d'installation :
 - Pour que le SafeGuard Management Center prenne en charge une seule base de données, sélectionnez **Classique**.
 - Pour que le SafeGuard Management Center prenne en charge plusieurs bases de données (**architecture mutualisée**), sélectionnez **Complète**. Pour plus d'informations, reportez-vous à la section [Configurations d'une architecture mutualisée](#) à la page 32.
6. Cliquez sur **Terminer** pour terminer l'installation.
7. Si nécessaire, redémarrez votre ordinateur.
8. Démarrez le SafeGuard Management Center pour exécuter la configuration initiale, reportez-vous à la section [Configuration du SafeGuard Management Center](#) à la page 32.

Le SafeGuard Policy Editor a été mis à niveau vers le SafeGuard Management Center.

17.2 Mise à niveau du client Sophos SafeGuard (autonome) vers un client SafeGuard Enterprise (administré)

Vous pouvez mettre à niveau les ordinateurs d'extrémité avec une configuration de client SafeGuard (autonome) vers une configuration de client SafeGuard Enterprise (administré). Les ordinateurs d'extrémité sont ainsi définis dans le SafeGuard Management Center en tant qu'objets pouvant être gérés et disposant d'une connexion au serveur SafeGuard Enterprise.

Conditions préalables

- Sauvegardez l'ordinateur d'extrémité avant de démarrer la mise à niveau.
- Assurez-vous de disposer des droits d'administrateur Windows.

Pour mettre à niveau le client Sophos SafeGuard (autonome) vers un client SafeGuard Enterprise (administré) :

1. Dans le SafeGuard Management Center, dans le menu **Outils**, cliquez sur **Outil du package de configuration**. Pour créer le package de configuration pour le client SafeGuard Enterprise (administré), cliquez sur **Créer un package de configuration (administré)**.
2. Attribuez ce package à l'ordinateur d'extrémité à l'aide d'une stratégie de groupe.
L'authentification est désactivée car l'attribution utilisateur-ordinateur n'est pas mise à niveau. Après la mise à niveau, les ordinateurs d'extrémité ne sont donc plus protégés !
3. Redémarrez l'ordinateur d'extrémité. La première connexion est toujours effectuée avec l'ouverture de session automatique. De nouvelles clés et de nouveaux certificats sont attribués à l'utilisateur.
4. Redémarrez l'ordinateur d'extrémité une deuxième fois. Connectez-vous à l'authentification au démarrage. Les ordinateurs sont de nouveau protégés seulement après le second redémarrage.
5. Supprimez tous les packages de configuration obsolètes ou non utilisés.

Le client Sophos SafeGuard (autonome) est maintenant un client SafeGuard Enterprise (administré).

18 Mise à niveau de SafeGuard Easy 4.x et de Sophos SafeGuard Disk Encryption 4.x vers SafeGuard Enterprise 5.6x

SafeGuard Easy (SGE) 4.5x et Sophos SafeGuard Disk Encryption 4.6x peuvent être directement mis à niveau vers SafeGuard Enterprise 5.6x en installant le package d'installation du client SafeGuard Device Encryption sur l'ordinateur.

Le chiffrement du disque dur est conservé et vous évite ainsi d'avoir à déchiffrer et chiffrer à nouveau le disque dur. Il n'est pas non plus nécessaire de désinstaller SafeGuard Easy ou Sophos SafeGuard Disk Encryption.

Ce chapitre décrit la mise à niveau vers Sophos SafeGuard, explique quelles fonctions peuvent être migrées et aborde en détail les restrictions.

18.1 Conditions préalables

- La mise à niveau directe a été testée. Elle est prise en charge pour SafeGuard Easy 4.5x. La mise à niveau directe doit également fonctionner pour les versions qui se trouvent entre la version 4.3x et la version 4.4x.

La mise à niveau directe n'est pas prise en charge pour les versions antérieures à la version 4.3x. Ces versions doivent d'abord être mises à niveau vers SafeGuard Easy 4.50.

- La mise à niveau est, par contre, prise en charge pour Sophos SafeGuard Disk Encryption version 4.6x.
- SafeGuard Easy/Sophos SafeGuard Disk Encryption doivent être exécutés sur le système d'exploitation suivant :

Windows XP Professionnel Service Pack 2 et 3

- La version 3.01 ou ultérieure de Windows Installer doit être installée.

- Le matériel doit respecter la configuration requise pour SafeGuard Enterprise 5.6x.
- Si vous utilisez un logiciel spécifique, par exemple un middleware Lenovo, celui-ci doit respecter la configuration système requise pour SafeGuard Enterprise 5.6x.
- La mise à niveau peut être effectuée uniquement si les disques durs sont chiffrés à l'aide des algorithmes suivants : AES128, AES256, 3DES et IDEA.
- Les utilisateurs doivent disposer d'un compte et d'un mot de passe Windows valides. S'ils ne connaissent pas leur mot de passe Windows parce qu'ils s'étaient auparavant connectés à Windows via la connexion automatique sécurisée, le mot de passe utilisateur Windows doit être réinitialisé avant la mise à niveau et le nouveau mot de passe doit être communiqué aux utilisateurs. Pour plus d'informations, voir [Préparation à la mise à niveau](#) à la page 94.

18.2 Restrictions

- Seul le package d'installation de SafeGuard Device Encryption, avec les fonctions standard, peut être installé (SGNClient.msi). Si le module SafeGuard Data Exchange doit également être installé (SGNClient_withoutDE.msi), cette installation doit s'effectuer dans une étape séparée car une mise à niveau directe n'est pas prise en charge pour ce package.
- Les installations suivantes ne peuvent pas être mises à niveau vers SafeGuard Enterprise et l'installation de ce dernier ne doit pas être tentée.

Remarque :

Si vous démarrez une mise à niveau dans les cas énoncés ci-dessous, un message d'erreur s'affiche (numéro d'erreur 5006).

Installations à double initialisation

Installations avec commutateur Compaq actif

Installations Lenovo Computrace

Disques durs partiellement chiffrés, par exemple avec le chiffrement du secteur de démarrage uniquement

Disques durs avec des partitions masquées

Disques durs chiffrés avec l'un des algorithmes suivants: XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16

Scénarios à plusieurs initialisations avec une seconde partition Windows ou Linux

- Les supports amovibles qui ont été chiffrés avec les algorithmes suivants ne peuvent pas être mis à niveau : XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16.

Remarque :

Des données risquent d'être perdues si un périphérique amovible a été chiffré avec les algorithmes XOR, STEALTH, DES, RIJNDAEL, Blowfish-8 ou Blowfish-16. Il est impossible d'accéder aux données du support amovible avec Sophos SafeGuard après la migration !

- Les supports amovibles avec des volumes Super Floppy ne peuvent pas être transformés après la mise à niveau.

- Les supports amovibles peuvent être convertis dans un format compatible avec SafeGuard Enterprise. Après la conversion, un support de données chiffrées ne peut être lu que par SafeGuard Enterprise et uniquement sur l'ordinateur d'extrémité sur lequel il a été converti.

18.3 Fonctionnalités mises à niveau

Le tableau ci-dessous indique quelles fonctionnalités sont mises à niveau et leur correspondance dans SafeGuard Enterprise.

| SafeGuard Easy/Sophos SafeGuard Disk Encryption | Mise à niveau | SafeGuard Enterprise |
|---|--------------------------|--|
| Disques durs chiffrés | Oui | Les clés des disques durs sont protégées par l'authentification au démarrage (POA) de SafeGuard Enterprise. Elles ne sont donc jamais exposées. Si le mode de protection à l'initialisation a été sélectionné dans SafeGuard Easy, désinstallez la version actuelle. L'algorithme de chiffrement du disque dur n'est pas modifié par la mise à niveau. En conséquence, l'algorithme réel de ce type de disque dur mis à niveau peut différer de la stratégie générale de SafeGuard Enterprise. |
| Supports amovibles chiffrés (seulement applicable lors de la migration depuis SafeGuard Easy) | Oui | Les supports de données chiffrées, par exemple les cartes mémoire USB, peuvent être convertis au format SafeGuard Enterprise. Remarque : après la conversion, un support de données chiffrées ne peut être lu que par SafeGuard Enterprise et uniquement sur l'ordinateur d'extrémité sur lequel il a été converti. La conversion doit être confirmée cas par cas. |
| Algorithmes de chiffrement | Dans une certaine mesure | Les algorithmes AES128, AES256, 3DES et IDEA peuvent être migrés. AES-128 et 3-DES ne peuvent néanmoins pas être sélectionnés dans le SafeGuard Management Center pour les supports à chiffrer. |
| Challenge/Réponse | Dans une certaine mesure | La procédure challenge/réponse est conservée. |
| Noms d'utilisateur | Non | Étant donné que les noms d'utilisateur Windows sont utilisés dans SafeGuard Enterprise, vous n'avez pas besoin de réutiliser les noms d'utilisateur SafeGuard Easy/Sophos SafeGuard Disk Encryption spécifiques. L'enregistrement des ordinateurs mis à niveau s'effectue donc de la même manière que pour une nouvelle installation de SafeGuard Enterprise, c'est-à-dire en attribuant de manière centralisée les utilisateurs de l'ordinateur ou en les enregistrant localement. Remarque : |

| SafeGuard Easy/Sophos SafeGuard Disk Encryption | Mise à niveau | SafeGuard Enterprise |
|--|--------------------------|--|
| | | Après la mise à niveau, le premier utilisateur qui se connecte à Windows est défini comme utilisateur principal au sein de l'authentification au démarrage (sauf s'il est indiqué sur la liste de comptes de service). |
| Mots de passe utilisateur | Non | Étant donné que les mots de passe utilisateur Windows sont utilisés dans SafeGuard Enterprise, vous n'avez pas besoin de réutiliser les mots de passe SafeGuard Easy/Sophos SafeGuard Disk Encryption spécifiques. Les mots de passe SafeGuard Easy/Sophos SafeGuard Disk Encryption ne sont donc pas mis à niveau. |
| Stratégies, paramètres (par exemple, longueur minimum de mot de passe) | Non | Pour garantir la cohérence de tous les paramètres, aucune mise à niveau automatique n'est exécutée. Les paramètres doivent être réinitialisés dans le SafeGuard Management Center. |
| Authentification de préinitialisation | Non | L'authentification de préinitialisation (PBA) est remplacée par l'authentification au démarrage (POA) de Sophos SafeGuard. |
| Installations sans GINA | Oui | Les installations sans GINA sont mises à niveau vers SafeGuard Enterprise avec installation de SGNGINA. |
| Clés cryptographiques/cartes à puces (s'applique uniquement lors de la migration à partir de SafeGuard Easy) | Dans une certaine mesure | Vous pouvez continuer à utiliser les clés cryptographiques/cartes à puce dans SafeGuard Enterprise. Néanmoins, les codes d'accès ne sont pas mis à niveau. Les clés cryptographiques utilisées dans SafeGuard Easy doivent donc être de nouveau générées dans SafeGuard Enterprise, et comme pour tout autre ordinateur d'extrémité SafeGuard Enterprise, configurées à l'aide de stratégies. Les codes d'accès SafeGuard Easy, regroupés sous forme de fichier sur les clés cryptographiques/cartes à puce, restent tels quels, et peuvent uniquement être utilisés pour la connexion aux ordinateurs prenant en charge SafeGuard Easy. Si besoin est, le middleware de la clé cryptographique/carte à puce doit être mis à jour vers une version prise en charge par SafeGuard Enterprise. |
| Connexion avec le lecteur d'empreintes digitales Lenovo | Dans une certaine mesure | Vous pouvez continuer à utiliser la connexion par empreinte digitale dans SafeGuard Enterprise. Le matériel et le logiciel du lecteur d'empreintes digitales doivent être pris en charge par SafeGuard Enterprise et les données d'empreintes digitales de l'utilisateur doivent être redéployées. Pour plus |

| SafeGuard Easy/Sophos SafeGuard Disk Encryption | Mise à niveau | SafeGuard Enterprise |
|--|------------------|--|
| | | d'informations sur la connexion par empreinte digitale, reportez-vous à l'Aide de l'utilisateur. |

18.4 Préparation à la mise à niveau

- Pour réduire le risque de perte de données, nous vous recommandons de créer une sauvegarde complète des ordinateurs que vous souhaitez mettre à niveau.

Avant d'installer le logiciel de chiffrement, exécutez les étapes conseillées comme l'utilisation de **chkdsk** et **defrag**. Pour plus d'informations, voir [Préparation au chiffrement](#) à la page 53. Voir aussi :

chkdsk : <http://www.sophos.fr/support/knowledgebase/article/107799.html>.

defrag : <http://www.sophos.fr/support/knowledgebase/article/109226.html>.

- Nous vous recommandons de créer une sauvegarde valide du noyau et de l'enregistrer dans un emplacement toujours accessible (par exemple, un chemin d'accès au réseau). Pour plus d'informations, reportez-vous aux manuels ou aux aides de SafeGuard Easy 4.5x/Sophos SafeGuard Disk Encryption 4.6x, chapitre *Enregistrement du noyau système et création d'un support d'urgence*.
- Pour réduire le risque de perte de données, nous vous recommandons de créer un environnement de test pour la première mise à niveau.
- Si vous effectuez une mise à niveau de versions antérieures de SafeGuard Easy, vous devez d'abord mettre à niveau vers la version 4.50.
- Laissez les ordinateurs allumés tout au long du processus de mise à niveau.
- Le responsable de la sécurité doit conserver les informations d'identification Windows des utilisateurs au cas où les utilisateurs perdraient leur mot de passe Windows après la mise à niveau. Cela peut se produire si les utilisateurs se sont connectés auparavant via l'authentification de préinitialisation et se connectent ensuite via la connexion sécurisée Windows (SAL, Secure Autologon). Ainsi, ils n'ont jamais utilisé leurs codes d'accès Windows.

Remarque :

Les utilisateurs doivent connaître leur mot de passe de connexion à Windows avant de procéder à la mise à niveau. Cette étape est essentielle car il est impossible de définir un mot de passe Windows après la mise à niveau et l'installation de SafeGuard Enterprise. Si les utilisateurs ne le connaissent pas car ils ont utilisé la connexion automatique sécurisée de SafeGuard Easy/Sophos SafeGuard Disk Encryption, ils ne pourront pas se connecter à SafeGuard Enterprise. Dans ce cas, la connexion automatique vers Windows est refusée et les utilisateurs ne peuvent pas se connecter à SafeGuard Enterprise. Il existe donc un risque de perte de données car les utilisateurs ne peuvent plus accéder à leurs ordinateurs.

18.5 Démarrage de la mise à niveau

Remarque :

L'installation peut être effectuée sur un système exécutant SafeGuard Easy/Sophos SafeGuard Disk Encryption. Aucun déchiffrement de disques durs ou de volumes chiffrés n'est nécessaire.

Utilisez le package d'installation du client SafeGuard Device Encryption (SGNClient.msi) depuis le dossier d'installation, avec la fonction standard définie. Vous ne pouvez pas utiliser le package client SGNClient_withoutDE.msi pour effectuer la mise à niveau. Il est préférable d'effectuer l'installation de manière centralisée en mode sans surveillance. L'installation via le dossier de configuration n'est pas recommandée !

Pour mettre à niveau :

1. Cliquez deux fois sur le fichier WIZLDR.exe dans le dossier de programme de SafeGuard Easy/Sophos SafeGuard Disk Encryption de l'ordinateur d'extrémité que vous souhaitez mettre à niveau. Cette opération démarre l'assistant de migration.
2. Dans l'assistant de migration, saisissez le mot de passe SYSTEM et cliquez sur **Suivant**. Dans **Dossier de destination**, cliquez sur **Suivant**, puis sur **Terminer**. Un fichier de configuration de migration **SGEMIG.cfg** est créé.
3. Dans l'Explorateur Windows, renommez le fichier **SGEMIG.cfg** en **SGE2SGN.cfg**.

Remarque : les droits du propriétaire/de l'auteur doivent être définis pour ce fichier et pour le chemin d'accès au dossier dans lequel il est stocké pendant la mise à niveau. Autrement, la mise à niveau risque d'échouer et un message indiquant que le fichier **SGE2SGN.cfg** est introuvable s'affiche.

4. Saisissez la commande **msiexec** à l'invite de commande pour installer le package de préinstallation SafeGuard Enterprise ainsi que le package d'installation du client SafeGuard Enterprise Device Encryption sur l'ordinateur d'extrémité SafeGuard Easy/Sophos SafeGuard Disk Encryption. Ajoutez le paramètre MIGFILE qui indique le chemin d'accès au fichier de configuration de migration **SGE2SGN.cfg**.

Exemple :

```
msiexec /i \\Distributionserver\Software\Sophos\SafeGuard\SGxClientPreinstall.msi
msiexec /i \\Distributionserver\Software\Sophos\SafeGuard\SGNClient.msi
/L*VX“\\Distributionserver\Software\Sophos\SafeGuard\%Computername%.log“
MIGFILE=\\Distributionserver\Software\Sophos\SafeGuard\SGE2SGN.cfg
```

- Une fois la mise à niveau correctement effectuée, SafeGuard Enterprise est prêt sur l'ordinateur.
- Si la mise à niveau échoue, SafeGuard Easy/Sophos SafeGuard Disk Encryption restent disponibles sur l'ordinateur. Le cas échéant, SafeGuard Enterprise est automatiquement supprimé.

18.6 Connexion à l'ordinateur d'extrémité après la mise à niveau

Pour se connecter à l'ordinateur qui a été mis à niveau à partir de SafeGuard Easy 4.5x/Sophos SafeGuard Disk Encryption 4.6x vers SafeGuard Enterprise 5.6x :

1. Redémarrez l'ordinateur d'extrémité mis à niveau. La première connexion est toujours effectuée avec l'ouverture de session automatique. De nouvelles clés et de nouveaux certificats sont attribués à l'utilisateur.
2. Redémarrez l'ordinateur d'extrémité une deuxième fois. Connectez-vous à l'authentification au démarrage. Les ordinateurs sont de nouveau protégés seulement après le second redémarrage.
3. Pour déchiffrer le disque dur ou ajouter et supprimer des clés de chiffrement du disque dur, redémarrez de nouveau l'ordinateur.

Après une mise à niveau réussie, les éléments suivants sont disponibles dans SafeGuard Enterprise après la connexion à l'authentification au démarrage:

- les clés et algorithmes des volumes chiffrés ;
Les volumes chiffrés restent inchangés et les clés de chiffrement sont automatiquement converties dans un format compatible avec SafeGuard Enterprise.
- les clés et algorithmes des supports amovibles chiffrés (uniquement applicable lors d'une mise à niveau à partir de SafeGuard Easy).
Ils doivent être convertis dans un format compatible avec SafeGuard Enterprise.

18.7 Configuration des ordinateurs d'extrémité mis à niveau

Les ordinateurs d'extrémité sont initialement configurés par des packages de configuration qui permettent, entre autres, d'activer l'authentification au démarrage.

Conditions préalables :

La configuration des ordinateurs d'extrémité doit avoir lieu seulement après la mise à niveau et seulement après que la POA a été activée et que l'utilisateur s'est connecté avec succès à Windows sur l'ordinateur mis à niveau.

1. Dans le SafeGuard Management Center, dans le menu **Outils**, cliquez sur **Outil du package de configuration** et créez le package de configuration initiale avec les paramètres de stratégie requis.
Les stratégies transférées avec le premier package de configuration doivent correspondre à la configuration précédente de l'ordinateur doté de SafeGuard Easy/Sophos SafeGuard Disk Encryption.
Si aucun package de configuration n'est installé après la mise à niveau, tous les lecteurs qui ont été chiffrés par SafeGuard Easy/Sophos SafeGuard Disk Encryption restent chiffrés.
2. Installez le package de configuration sur les ordinateurs d'extrémité.

18.8 Conversion des clés des supports amovibles chiffrés

La stratégie appropriée de chiffrement basé sur volume doit être présente sur l'ordinateur avant la conversion. Faute de quoi les clés ne sont pas converties.

Le support amovible chiffré reste inchangé également, mais les clés doivent être converties dans un format compatible avec SafeGuard Enterprise.

Remarque :

Par conséquent, après la conversion, un support de données chiffrées ne peut être lu que par SafeGuard Enterprise et uniquement sur l'ordinateur final sur lequel il a été converti pendant la migration.

1. Déconnectez les supports de l'ordinateur et réinsérez-les de nouveau. Ceci pour s'assurer que vous pouvez déchiffrer les supports amovibles ou ajouter et supprimer les clés pour le chiffrement des supports amovibles.
2. Dans l'Explorateur Windows, cliquez deux fois sur les supports auxquels vous voulez accéder.
3. Vous êtes invité à confirmer la transformation des clés de chiffrement dans un format compatible avec SafeGuard Enterprise.
 - Si vous confirmez la conversion, un accès complet aux données migrées est assuré.
 - Si vous refusez la conversion, les données migrées peuvent tout de même être lues et modifiées.

Les supports amovibles nouvellement ajoutés sont chiffrés, comme avec tout ordinateur SafeGuard Enterprise, si la configuration de stratégie appropriée est présente sur l'ordinateur d'extrémité.

19 À propos de la désinstallation

- Lorsque le logiciel de chiffrement du client de SafeGuard Enterprise est installé sur le même ordinateur que le SafeGuard Management Center, que le serveur SafeGuard Enterprise ou que SafeGuard Web Help Desk, assurez-vous de bien suivre la procédure de désinstallation afin de pouvoir continuer à les utiliser :
 1. Désinstallez le SafeGuard Management Center, le serveur SafeGuard Enterprise ou SafeGuard Web Help Desk.
 2. Désinstallez le package de configuration du client SafeGuard Enterprise.
 3. Désinstallez le logiciel de chiffrement du client SafeGuard Enterprise.
 4. Installez à nouveau le package que vous souhaitez continuer à utiliser. Pour utiliser le SafeGuard Management Center, assurez-vous d'importer l'ancien certificat de la machine suite à l'installation. Pour utiliser le logiciel de chiffrement du client SafeGuard Enterprise, assurez-vous installer le package de configuration du client suite à l'installation du logiciel de chiffrement.
- Avant de désinstaller le logiciel de chiffrement, désinstallez d'abord le package de configuration.

- Vous ne pouvez pas désinstaller le logiciel de chiffrement pour les volumes chiffrés avec une clé spécifique à l'utilisateur qui ne vous a pas été attribuée.
- Ils seront déchiffrés lors de la désinstallation des volumes du client de SafeGuard Device Encryption qui ont été chiffrés à l'aide d'une clé machine par défaut. Pour déchiffrer les volumes chiffrés à l'aide d'autres clés, créez et attribuez une stratégie appropriée avant de désinstaller SafeGuard Device Encryption.
- Au cours de la désinstallation du logiciel de chiffrement qui inclut le déchiffrement des volumes chiffrés, n'arrêtez, ni ne redémarrez l'ordinateur d'extrémité. En effet, ceci entraîne la création d'un message d'erreur de la part du programme de désinstallation.
- Si la désinstallation est déclenchée via Active Directory, assurez-vous que tous les volumes chiffrés ont été déchiffrés correctement auparavant.
- Il est possible qu'après une désinstallation, certains fichiers et certaines entrées de registre ne puissent pas être supprimés. Veuillez consulter la base de connaissances Sophos (mots-clés "SGN & désinstaller") pour savoir comment nettoyer l'installation manuellement. Un nettoyage manuel est nécessaire pour réinstaller avec succès le logiciel de chiffrement sur le même ordinateur.
- Si vous avez installé SafeGuard Device Encryption et SafeGuard Data Exchange sur un ordinateur, vous ne pouvez pas désinstaller SafeGuard Device Encryption seul. Vous devez désinstaller le package complet.
- Déchiffrez tous les supports amovibles chiffrés avant de désinstaller le dernier client SafeGuard Enterprise accessible. Sinon, il se peut que vous ne puissiez plus accéder à vos données. Tant que vous conservez votre base de données SafeGuard Enterprise, les données sur les supports amovibles peuvent être récupérées.

19.1 Interdiction de désinstallation sur les ordinateurs d'extrémité

Pour renforcer la protection de vos ordinateurs d'extrémité, vous pouvez interdire la désinstallation locale de Sophos SafeGuard. Définissez l'option **Désinstallation autorisée** de la stratégie **Paramètres spécifiques à la machine** sur **Non** et déployez cette stratégie sur les ordinateurs d'extrémité. Une fois ce type de stratégie appliqué à l'ordinateur d'extrémité, les tentatives de désinstallation sont annulées et les tentatives non autorisées sont consignées dans le journal.

Remarque :

Si vous utilisez une version de démonstration, n'activez pas ce paramètre de stratégie ou ne le désactivez pas avant l'expiration de cette version afin de garantir une désinstallation facile.

20 Support technique

Vous pouvez obtenir du support technique pour les produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur <http://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 <http://www.sophos.fr/support/>
- Téléchargez la documentation des produits sur <http://www.sophos.fr/support/docs/>
- Envoyez un courriel à support@sophos.fr, y compris le ou les numéros de version du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte du ou des messages d'erreur.

21 Mentions légales

Copyright © 1996 - 2011 Sophos Group. Tous droits réservés. SafeGuard est une marque déposée de Sophos Group.

Sophos est une marque déposée de Sophos Limited, Sophos Group et Utimaco Safeware AG, selon le cas. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées de leurs propriétaires respectifs.

Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Les informations de copyright des fournisseurs tiers sont disponibles dans le fichier appelé Disclaimer and Copyright for 3rd Party Software.rtf dans votre répertoire des produits.